# PrintCounts Technical Overview

## Contents


Abbreviations ..... 3
Overview ..... 4
Discovery Phase ..... 5
Staging Phase ..... 5
Reporting Phase ..... 5
Network & Security ..... 6
Secure External Communication ..... 6
Types of Data Collected ..... 6
HIPAA Compliancy ..... 6
Firewall ..... 6
Supported Protocols ..... 7
DCA Appliances and Software ..... 7
Patrol Appliance DCA ..... 7
Overview ..... 7
System Requirements ..... 8
Dimensions & Specifications ..... 8
Patrol Wi-Fi ..... 9
Overview ..... 9
System Requirements ..... 9
DEXMPS DCA Software ..... 10
Overview ..... 10
System Requirements ..... 10
Installation ..... 11
FAQ's ..... 12
How do the DCAs collect & process data? ..... 12
What type of data is collected by the DCA? ..... 12
Is the collection and transmission of printer information secure? ..... 12
What is the data format of printer information collected by the DCA? ..... 12

Is the data collected by the DCA HIPAA-compliant? 13
Will there be an impact on my network traffic during a printing device scan? 13
How does the DCA know which devices to scan? 13
Can I have multiple PrintCounts appliances on my network? 13
How do a DCA and a Patrol Wi-Fi communicate? 14
What is the process for installation of the DCA? 14
What is the reporting process of the DCA? 14
What is the Configuration Phase of a PrintCounts appliance? 14
What are the imaging device hostname considerations? 15
Which Versions of SNMP (Simple Network Management Protocol) are supported? 15
What is SNMPv3 and what are the usage considerations? 15
Is there any network firewall considerations? 16
What is a MIB file? 16
Why do I see communications on ports other than 443 & 161? 16

# Abbreviations

MIB: Management Information Base

HTTP: Hypertext Transfer Protocol

HIPAA: Health Insurance Portability and Accountability Act

TLS: Transport Layer Security

SNMP: Simple Network Management Protocol

DCA: Data Collection Agent

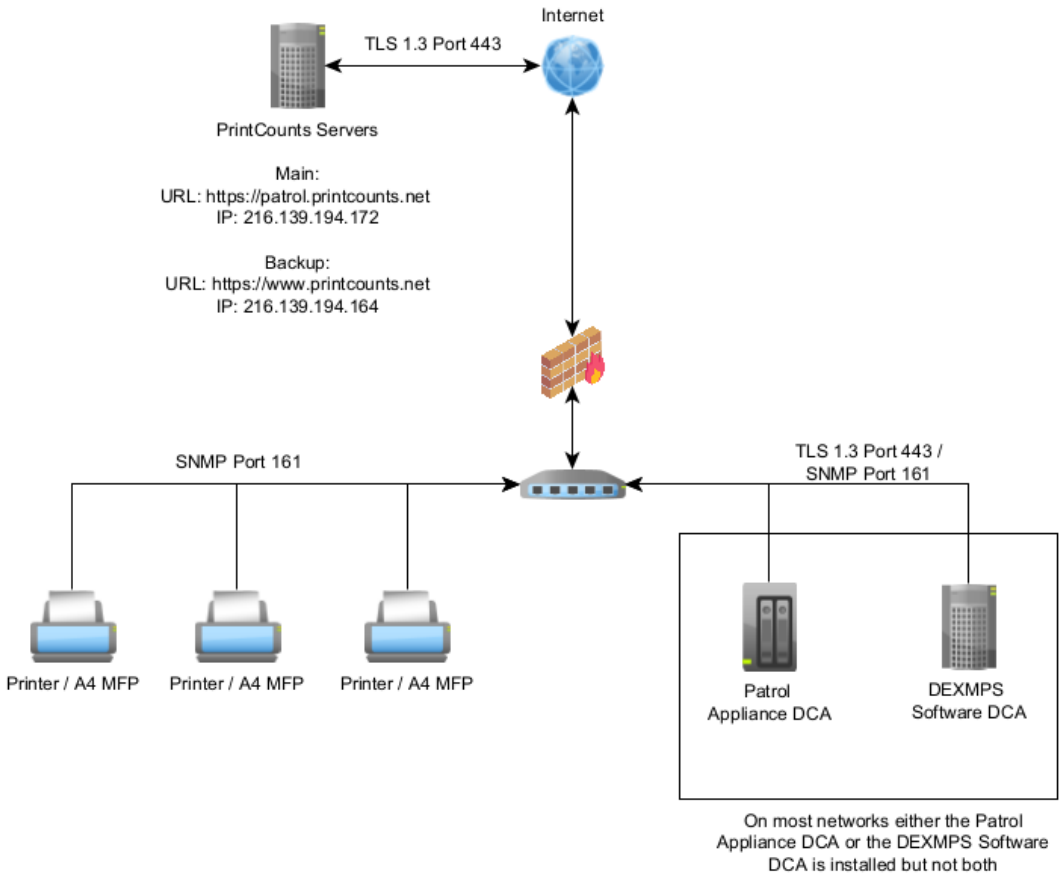
# Overview

PrintCounts is a managed print service that offers automated monitoring and reporting of networked and locally attached printers through a dedicated Patrol DCA appliance or DEXMPS DCA Software. The installation is performed in 3 phases which are described in the Installation Phases section:

1. Discovery
2. Staging
3. Reporting

As shown in the diagram below:

1. The DCA connects to PrintCounts servers using TLS 1.3 and retrieves a configuration file that tells the device which IP addresses to scan.
2. It then traverses the specified IP ranges, performing SNMP queries to get information about the equipment at that IP address.
3. Metadata is gathered on imaging equipment. The metadata is aggregated into an XML format and uploads to PrintCounts servers via TLS 1.3.




4.

# Discovery Phase

The first phase involves PrintCounts technician(s) configuring the DCA through the PrintCounts server web application and installing the Patrol Device on the client network or DEXMPS Software on a server on the client network.

Here are the client requirements for this phase:

1. The Patrol Appliance must be plugged into a **reliable source of AC power.** Additionally, a **surge protector** is highly recommended.
2. The Patrol Appliance requires a **network jack** to enable the device to connect to any network segment containing imaging equipment to be monitored.

Or

1. The DEXMPS Software DCA requires a **client server or PC** with 100MB of free disk space and 100MB of RAM.
2. The server or PC the DEXMPS Software DCA is installed on **must always be on** and connected to the client network.

Upon starting, the DCA connects to the PrintCounts server, obtains a configuration, and iterates through IP ranges specified in that configuration. This gathers metadata on printing equipment as they are discovered.

If the Patrol Device encounters a Patrol Wi-Fi during the scan of the network:

- The Patrol Wi-Fi device relays the SNMP traffic to the printer/copier it is attached to
- The Patrol Wi-Fi device then returns the results as if the printing equipment was network attached.

*It's important to note* that only SNMP traffic originating from a Patrol Device will be relayed by the Patrol Wi-Fi Device, preventing the sharing and remote administration of the printing equipment being monitored. The resultant data is aggregated on the Patrol Device then uploaded to PrintCounts servers, where the data is processed and recorded into a database.

# Staging Phase

In the Staging phase, the information from the printing equipment that was uploaded to PrintCounts servers is correlated with make/model information and assigned a unique asset number for interfacing with PrintCounts billing system.

Once the printing equipment is staged, the Reporting phase begins.

# Reporting Phase

The DCA repeats the scan on either a specified interval or at a specific time each day. Like the Discovery phase, the DCA iterates through the specified IP ranges, gathers the required information about the imaging equipment, and updates the database.

# Network & Security

## Secure External Communication

All external communications between client networks and PrintCounts servers are done securely using TLS 1.3 encryption. The data is stored in a safe, secure, offsite datacenter with failover and redundancy capability.

## Types of Data Collected

The data collected includes page counts, toner levels, serial numbers, device description, etc. and does not include any personal information or content from the imaging device.  Data collected by the DCA is limited to an SNMP Get.

## HIPAA Compliancy

According to the regulations as published by the Department of Health and Human Services (HHS), the HIPAA regulations do not provide for a central resting or certification of any procedure, device, or system. The PrintCounts solution does not compromise any areas of security or confidentiality as it relates to HIPAA.

## Firewall

The below firewall requirements apply specifically to the PrintCounts DCA. For installations with the Patrol Managed Print system in place, no additional firewall exceptions are required as the Patrol Wi-Fi Device does not communicate outside the local network.

| Component | Minimum Requirement |
|---|---|
| White-list items | • **Server IPs**: Main-**216.139.194.172**<br>Backup-**216.139.194.164**<br>• **URLs**: Main reporting **https://patrol.printcounts.net**<br>Backup Reporting – **https://www.printcounts.net**<br>Update server: **https://dexmpsupdateservice-qa.azurewebsites.net** |
| Needed Ports and Protocols | • Outbound TCP/IP allow to the **external** PrintCounts servers on port 443 using HTTPS protocol<br>• Outbound UDP exception to **internal** printers on port 161 using SNMP protocol<br>*-Note: Certificate substitution interferes with device authentication and cannot be enabled, this is known by varying names, Decrypt and Resign (Cisco), DPI (SonicWall), SSL Forward Proxy (Palo Alto)* |

## Supported Protocols

PrintCounts supports SNMP v1, v2 and v3.

SNMP v3 is the latest version of the SNMP (Simple Network Management Protocol). The primary feature of SNMP version 3 is its enhanced security in communications between the SNMP agent (the print device) and the SNMP information collection system, PrintCounts. If the client location has Patrol Wi-Fi and the DCA, an additional handshake between the PrintCounts Wi-Fi appliance and the DCA happens in the form of an HTTP GET with a response.

SNMP version 3 provides security enhancements over previous SNMP versions to provide an increased level of protection against possible attacks or intrusions, primarily:

- Users: when trying to access data stored in a printer's MIB, a username is required providing a higher level of security than simply providing a Community Name.
- Authentication: additional security is provided by using either a SHA or MD5 hash algorithm applied to the passwords.
- Encryption: DES/AES level security can be added to the data being transferred. Note that PrintCounts recommends using DES as described below.

The additional security provided by SNMPv3 comes with some considerations however and an understanding of your network topology is required to obtain and/or configure the following from SNMP3-enabled printing devices. Community strings in versions 1 and 2 are relatively easy to administer particularly if they all default to "public". In addition:

- Implementing SNMPv3 requires additional effort from the PrintCounts client's IT department to ensure that the deployment is successful and maintainable.
- Improper implementation can result in print devices not scanning.
- Troubleshooting mixed SNMP environments can be difficult and time consuming.

If you are using SNMP3, there are some additional authentication and encryption considerations during appliance installation, including:

- The user name associated with the printing device
- The passphrases associated with the printing device and avoiding certain special characters in passphrase generation, such as +:=[];#\~
- As a best security practice, avoid using terms associated with your company in your community strings

# DCA Appliances and Software

## Patrol Appliance DCA

### Overview

The Patrol Device is completely self-contained and embedded. It is designed to monitor networked imaging devices, allowing management of print volume and toner information locally or globally. The patrol device does not require or reside on a server. It is configured to communicate with the assigned imaging device(s), scan the device(s) on a periodic

basis, and report the results to the PrintCounts servers and therefore PrintCounts billing system.

Upon power up, the Patrol Device obtains an IP address from a DHCP server or from its internal non-volatile memory depending on if the device has been configured to use DHCP or a static IP. Once an IP address is obtained, the device connects to the PrintCounts server to determine if the firmware version installed on the patrol device is current. If not, a new firmware package is downloaded and installed on the patrol device and the power is cycled internally, thus restarting process.

After the firmware is verified up to date, the device downloads two configuration files via a secure TLS 1.3 connection to the PrintCounts servers by making an HTTP request for the files. One of the files contains a list of OID's the device uses to query printing equipment to obtain relevant information about the device being monitored. The other file that is downloaded contains the information about the customer's locations and what IP ranges to scan per location.

Once all downloads are complete, the device walks through each IP specified in the downloaded configuration file and issues queries to printers using SNMP to obtain the information required to monitor print volume, toner levels and optionally service states. The SNMP queries are issued over port 161 (UDP) and only internal firewalls needs to have this port exception created. For locally attached (NSDP) printers, an agent is installed on the workstation attached to the printer that poses as an SNMP server and reports black and white meter values for the printer attached. The results of the scans are aggregated into an XML and securely uploaded to our servers using TLS 1.3 on port 443.

Additionally, the customer account is created in the PrintCounts system where the patrol device links the account in our PrintCounts system to the device's unique MAC address during the process above. The customer patrol device is configured to scan periodically and monitor the IP address or range from within our PrintCounts system.

Upon initial setup, the imaging devices reporting from the monitored IP address(es) are then staged in the PrintCounts system, linking the IP address to an Equipment ID number and the device's physical location.

## System Requirements

| Component | Minimum Requirement |
|---|---|
| Power | • NEMA 1-15 or NEMA 5-15 electrical outlet (15A / 125 V)<br>• A surge protector is highly recommended |
| Network | • Ethernet connection via wall or router<br>• Static IP or DHCP |
| Proxy Server | • If a proxy server is in use, the server address and port must be provided |

## Dimensions & Specifications

Patrol2 Box

- The Patrol2 box is 3" x 5" x 1"
- Typical draw 0.3A to 0.4A from the 5V DC power supply.
- 5V DC power supply is rated for 1A.
- 2-port 100Base-T switch
- Typical network bandwidth is 5kb / second during scan.

# Patrol Wi-Fi

## Overview

The Patrol Wi-Fi is a bridge between standalone copiers or USB attached printers and the Patrol Managed Print system. Only SNMP traffic originating from approved managed print system such as a patrol device is allowed to communicate with the Patrol Wi-Fi device. This enables the reporting of managed print data from locally attached, USB printers or standalone copiers while preventing the equipment from being remotely accessed or shared over the network.

Initially, the Patrol Wi-Fi Device is configured to connect to a wireless network. After the wireless configuration is completed, the device is attached to an un-used network interface card on a printer and powered by the USB line that connects the printer to a user's PC. The Patrol Wi-Fi device may optionally be powered by an external AC power supply or a USB port on a copier.

## System Requirements

Equipment to be monitored must have an available network interface card and have DHCP enabled. The location where the Patrol Wi-Fi device is installed must have wireless coverage. If the wireless network uses Enterprise class authentication, a certificate must be provided.

| Component | Minimum Requirement |
|---|---|
| Power | • Powered by USB cable<br>• The device may optionally be powered by an external DC power supply using the provided USB cable. (300mA nominal, 480mA peak at 5V) |
| Network | • Wi-Fi connection to corporate Wi-Fi network<br>• Network topology must support the issuance and receipt of TCP/IP and SNMP commands between the Patrol Device the Patrol Wi-Fi Device<br>• Device (printer/copier) being monitored must have DHCP enabled<br>• Ethernet connection to device (printer/copier) to be monitored<br>• DHCP (DNS Reservation preferred if DHCP is in use)<br><br>Wireless Networks Supported:<br>• Open<br>• WEP<br>• WAP/WAP2 Personal<br>• WAP/WAP Enterprise |

# DEXMPS DCA Software

## Overview

DEXMPS DCA Software is a Windows service that functions as an alternative software solution to a physical Patrol device. Like the Patrol device, it is designed to monitor networked imaging devices, and allow management of print volume and toner information locally or globally. DEXMPS DCA Software must be installed on a server with an internet connection. It is configured to communicate with the assigned imaging device(s), scan the device(s) on a periodic basis, and report the results to the PrintCounts servers and therefore PrintCounts billing system.

After installation, (detailed below) DEXMPS DCA Software will establish a secure TLS connection to the PrintCounts servers via an HTTPS request. Once the connection is established the server will send a configuration file that contains the information about the customer's locations and what IP ranges to scan per location. After the initial configuration is completed, the service will poll the server to determine if any software updates are required and perform updates or restarts as necessary. If the user has opted to disable automatic updates via the PrintCounts website, a new installer must be acquired from the website to update the service, after uninstalling the previous version.

After the software is verified up to date, the service will restart and repeat the authentication and configuration process. Once connection has been reestablished, the service will download a file which contains a list of OID's the device uses to query printing equipment to obtain relevant information about the device being monitored.

Once all downloads are complete, the device walks through each IP specified in the downloaded configuration file and issues queries to printers using SNMP to obtain the information required to monitor print volume, toner levels and optionally service states. The SNMP queries are issued over port 161 (UDP) and only internal firewalls needs to have this port exception created. For locally attached (NSDP) printers, an agent is installed on the workstation attached to the printer that poses as an SNMP server and reports black and white meter values for the printer attached. The results of the scans are aggregated into an XML document and securely uploaded to our servers. The frequency at which the printers are scanned can be configured on the PrintCounts website.

## System Requirements

| Component | Minimum Requirement |
|---|---|
| CPUs | • Minimum: 2 cores<br>• Recommended: 6 Cores |
| RAM | • 8 GB of RAM. |
| Disk Space | • 100MB of free disk space. |
| Permissions | • The service requires elevated permissions. |
| Network | • Ethernet connection to the network containing printers to be monitored. |

## Installation

To receive a DEXMPS DCA Software installer, the user will need to create an account on the PrintCounts website. Once the account has been created, the user can login and request a DEXMPS DCA Software installer, at which point they will receive a secure download link to our file storage system. Once the installer has been downloaded from the storage system, please run the .msi installer and verify that your organization's name is listed on the Welcome screen. If you do not see the name of your organization, please contact PrintCounts support.

The DEXMPS DCA Software installer is self-contained, and no other files or frameworks need to be downloaded. After running the installer, select the appropriate DCA name for the location at which you wish to install this instance. After clicking finish, the service will install and start itself automatically as it runs with the "Local System" user account permissions. To verify that the service is running, navigate to services.msc and search for DEXMPS DCA Software.

# FAQ's

## How do the DCAs collect & process data?

In a nutshell, the DCA connects to PrintCounts servers using TLS 1.3 and retrieves a configuration file that tells the device which IP addresses to scan. It then traverses the specified IP ranges, performing SNMP queries to get information about the equipment at that IP address. As a last step, it aggregates this data in an XML file and uploads to PrintCounts servers via TLS 1.3.

## What type of data is collected by the DCA?

DCAs only collect information from network printers, copiers and multifunction devices. The information collected from the SE network devices is formatted in an XML document. The device only collects information from devices that return the Printer MIB v2 as defined by the IETF: http://tools.ietf.org/html/rfc3805.

More specifically, data collected by a PrintCounts appliance is limited to imaging metadata from the SNMP MIB data. This data typically includes page counts, serial numbers, device description, etc. and does not include personal information or content from the imaging device.

## Is the collection and transmission of printer information secure?

All external communications between client networks and PrintCounts servers are done securely using TLS 1.3 encryption. The data is stored in a safe, secure, offsite datacenter with failover and redundancy capability.

Patrol Device supports both static and dynamic IP address assignments via DHCP. It will also operate in customer environments where a proxy server is in place. The hardware is based on an ARM core embedded microcontroller.

The firmware contained on the device was designed and developed internally by PrintCounts. It uses the SNMP protocol to collect information from networked printers or copiers and communicates this information as an XML file to a secure data center over the HTTP/S protocol.

## What is the data format of printer information collected by the DCA?

Data of imaging devices are transmitted in an XML format. See Example below.




## Is the data collected by the DCA HIPAA-compliant?

According to the regulations as published by the Department of Health and Human Services (HHS), the HIPAA regulations do not provide for a central resting or certification of any procedure, device, or system. The PrintCounts web application solution and patrol appliances do not compromise any areas of security or confidentiality as it relates to HIPAA.

## Will there be an impact on my network traffic during a printing device scan?

There is minimum impact on network at time of scan, which typically occurs every 4 hours—but in some rarer cases, may occur at a specific time during the day. On average, the process takes 15 minutes, or 2.5 seconds per IP scanned.

## How does the DCA know which devices to scan?

Patrol appliances use TLS 1.3 to connect to a PrintCounts server and retrieve a client configuration file that informs the device of what IP addresses to scan.

## Can I have multiple PrintCounts appliances on my network?

Yes - you can have more than one Patrol appliance, DEXMPS Software & Patrol Wi-Fi appliance on your network. The Patrol Devices are configured in a way to handle multiple physical locations connected to 1 WAN. Within each physical location, an IP address or a range of IP addresses are configured for the patrol device to scan. This can include imaging devices reporting via Patrol Wi-Fis. However, if the customer network is configured with imaging devices that span across multiple LANs, a Patrol Device will

need to be configured for each LAN.

## How do a DCA and a Patrol Wi-Fi communicate?

If the DCA encounters a Patrol Wi-Fi during a scan of the network:

- The Patrol Wi-Fi device relays the SNMP traffic to the printer/copier it is attached to
- The Patrol Wi-Fi device then returns the results as if the printing equipment was network attached.

*It's important to note* that only SNMP traffic originating from a PrintCounts DCA will be relayed by the Patrol Wi-Fi Device, preventing the sharing and remote administration of the printing equipment being monitored. The resultant data is aggregated on the DCA then uploaded to PrintCounts servers, where the data is processed and inserted into a database.

## What is the process for installation of the DCA?

The installation includes two phases, 1) Discovery and 2) Staging.

The Discovery phase involves PrintCounts technician(s) initially configuring the DCA through a PrintCounts server web application (e.g. PrintCounts) and installing the device on the client network. Upon power up, the DCA connects to the PrintCounts server and retrieves a configuration file which is used to iterate through the specified IP ranges. This step essentially dynamically gathers metadata on printing equipment as they are discovered.

See additional info on the configuration phase.

The Staging phase correlates the information from the printing equipment (that was uploaded to the PrintCounts server, e.g. PrintCounts) with the make/model information and assigns a unique asset number for future interfacing with the PrintCounts billing system.

Once these two steps are completed, e.g. the client printing equipment is staged, the Reporting phase can begin. Note that during the installation phase, a Reporting process may be initiated.

## What is the reporting process of the DCA?

During a *Reporting* process, the DCA typically scans printing equipment at a specified interval, e.g. every 4 hours—but in some rarer cases, may scan the equipment at a specific time during the day.

During this process, the PrintCounts appliance iterates through the specified IP ranges, gathers the required information about the imaging equipment, transmits the data to the PrintCounts server which subsequently updates the database.

## What is the Configuration Phase of a PrintCounts appliance?

Upon power up, the DCA connects to a PrintCounts server, obtains a configuration, and iterates through IP ranges specified in that configuration. This gathers metadata on imaging devices as they are discovered.

If the DCA encounters a Patrol Wi-Fi during the scan of the network:

- The Patrol Wi-Fi device relays the SNMP traffic to the printer/copier it is attached to
- The Patrol Wi-Fi device then returns the results as if the printing equipment was network attached.

It's important to note that only SNMP traffic originating from a DCA will be relayed by the Patrol Wi-Fi Device, preventing the sharing and remote administration of the printing equipment being monitored. The resultant data is aggregated on the DCA and then uploaded to PrintCounts servers, where the data is processed and inserted into a database.

## What are the imaging device hostname considerations?

The imaging device must be DHCP-enabled and registered with the DNS server. The PrintCounts system will need to know the hostname for each printing device, which is typically a combination of client domain name and the printer hostname. The hostname is typically assigned at the factory level and can typically be found by printing status pages from the imaging device.

## Which Versions of SNMP (Simple Network Management Protocol) are supported?

SNMP 1/2 and 3 are supported. If the client location has Patrol Wi-Fi and a DCA, an additional handshake between the Patrol Wi-Fi and the Patrol Device happens in the form of an HTTP GET with a response.

## What is SNMPv3 and what are the usage considerations?

SNMP v3 is the latest version of the SNMP protocol. The primary feature of SNMP version 3 is its enhanced security in communications between the SNMP agent (the print device) and the SNMP information collection system, PrintCounts. SNMP version 3 provides security enhancements over previous SNMP versions to provide an increased level of protection against possible attacks or intrusions, primarily:

- Users: when trying to access data stored in a printer's MIB, a username is required providing a higher level of security than simply providing a Community Name.
- Authentication: additional security is provided by using either a SHA or MD5 hash algorithm applied to the passwords.
- Encryption: DES/AES level security can be added to the data being transferred. Note that PrintCounts recommends using DES as described below.

The additional security provided by SNMPv3 comes with some considerations however and an understanding of your network topology is required to obtain and/or configure the following from SNMP3-enabled printing devices. Community strings in versions 1 and 2 are relatively easy to administer particularly if they all default to "public". In addition:

- Implementing SNMPv3 requires additional effort from the PrintCounts client's IT department to ensure that the deployment is successful and maintainable.
- Improper implementation can result in print devices not scanning.
- Troubleshooting mixed SNMP environments can be difficult and time consuming.

If you are using SNMP3, there are some additional authentication and encryption considerations during appliance installation, including:

- The user name associated with the printing device
- The passphrases associated with the printing device and avoiding certain special characters in passphrase generation, such as +:=[];#\~
- As a best security practice, avoid using terms associated with your company in your community strings

## Is there any network firewall considerations?

The printing device must be DHCP-enabled and registered with the DNS server. The PrintCounts system will need to know the hostname for each printing device, which is typically a combination of client domain name and the printer hostname. The hostname is typically assigned at the factory level and can typically be found by printing status pages from the printing device.

## What is a MIB file?

The MIB, or Management Information Base, is an ASCII text file that describes SNMP network elements as a list of data objects. Think of it as a dictionary of the SNMP language as every object referred to in an SNMP message must be listed in the MIB.

The fundamental purpose of the MIB is to translate numerical strings into human-readable text. When an SNMP device sends a Trap or other message, it identifies each data object in the message with a number string called an object identifier, or OID.

OIDs or Object Identifiers uniquely identify managed objects in the MIB. For example, the typical objects to monitor on a printer are the different cartridge states and may be the number of printed files. Every single object has its own object ID. Generally, an OID is a long sequence of numbers, coding the nodes, separated by dots, such as:
*1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3*

## Why do I see communications on ports other than 443 & 161?

Patrol appliances send initial request to equipment via 161 port. The equipment then responds back to patrol appliances on an ephemeral port that was created by the patrol appliance.

**Note:** This section should only be reviewed & handled by persons with network experience & knowledge.

Additional Information regarding an ephemeral port:
An ephemeral port is a short-lived transport protocol port for Internet Protocol (IP) communications. Ephemeral ports are allocated automatically from a predefined range by the IP stack software. An ephemeral port is typically used by the Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or the Stream Control Transmission Protocol (SCTP) as the port assignment for the client end of a client–server communication to a particular port (usually a well-known port) on a server.

On servers, ephemeral ports may also be used as the port assignment on the server end of a communication. This is done to continue communications with a client that initially connected to one of the server's well-known service listening ports. File Transfer Protocol (FTP) and Remote Procedure Call (RPC) applications are two protocols that can behave in this manner. Note that the term "server" here includes workstations running network services that receive connections initiated from other clients (e.g. Remote Desktop Protocol).

The allocations are temporary and only valid for the duration of the communication session. After completion (or timeout) of the communication session, the ports become available for reuse. Since the ports are used on a per request basis they are also called dynamic ports.