marco

Managed Services

Copiers & Printers

Audio Visual

Business IT Services

800.847.3098
MARCONET.COM

Simple.
Secure.
Better.

PRINT AWARE SECURITY TECHNICAL WHITEPAPER

TABLE OF CONTENTS

I. Introduction

The purpose of this White Paper is to provide a high-level technical overview of the InSight Solution.

Insight is a multi-tier application designed to support the delivery of Managed Office Print Services. It supports service delivery processes that enable End User customers or outsource Service Providers to deliver highly automated Asset management, Consumables supply chain management, Incident service chain management, billing reconciliation, active service delivery, as well as management information reporting.

Insight comprises three components as illustrated below.

- Insight Portal Server- For centralized remote service delivery across multiple customers. Installed as a private or multi-tenanted Cloud service for processing all information received from the Data Collection Applications (Monitoring application)
- Data Collection Application- Small footprint service installed on the customer network to collect information and report the information back to a Portal server.
- Messaging Server- Delivered as part of the Portal infrastructure and used to pass encrypted XML data securely from the Insight Monitoring application to the Insight Portal Server and authorized service administrators. This is a 'hidden' component and seamlessly integrated onto the Portal structure.

In addition, a natural language command system is available to allow remote management, diagnostics, and support for all Insight monitoring systems. This language is called IMIL. This enables remote configuration of the DCA without VPN access.

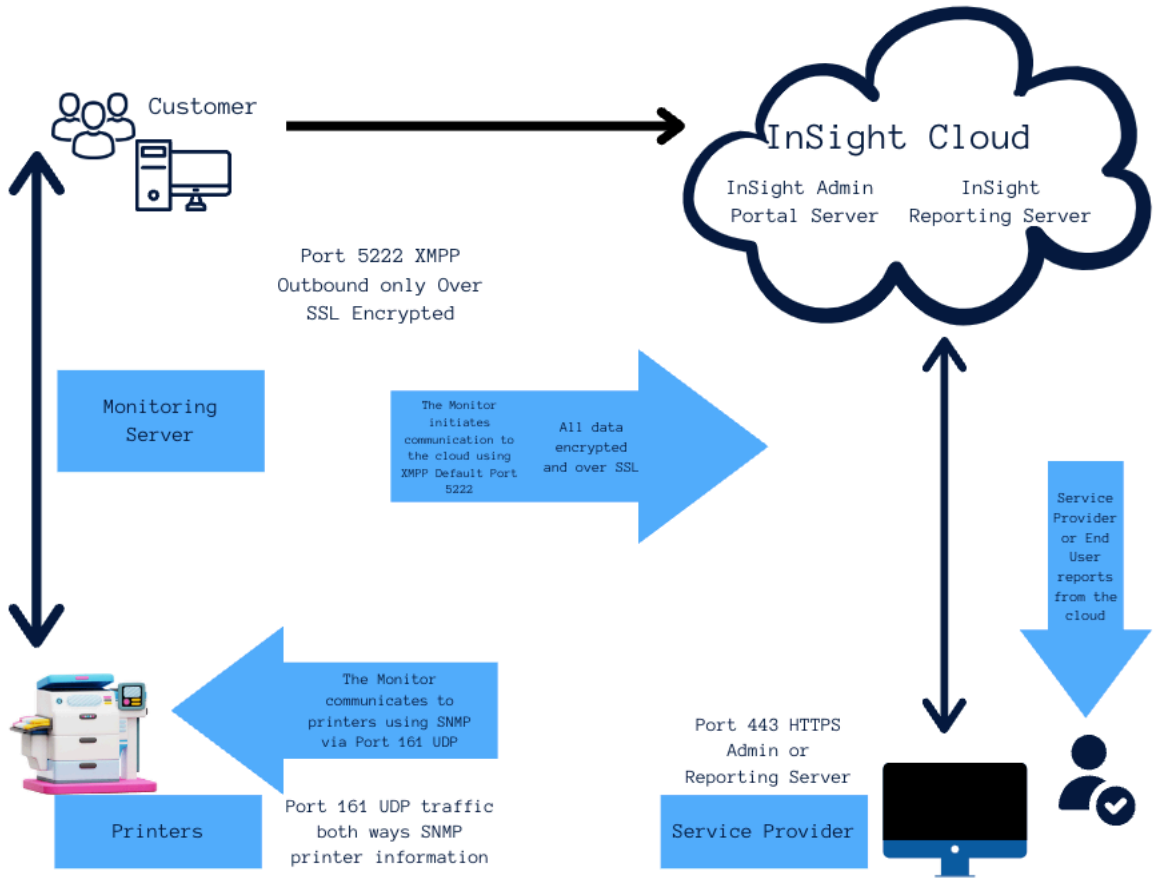
Insight monitoring applications discover and monitor network devices using SNMP UDP over port 161, they do not Ping, multicast, or broadcast.

Working data is stored in an internal administration database for local processing before transmission to the Insight portal.

Management of the Insight Portal is provided through a web interface running over HTTPS. See figure 1.

The Management requirement of the monitoring server is minimal and can be achieved remotely via the Portal Server should this be required. Service Management is delivered from the Insight Portal. Further Monitoring or device diagnostic information can be captured via the IMIL™ interface.

Fig. 1 Typical remote service system diagram.



The Management requirement of the monitoring server is minimal and can be achieved remotely via the Portal Server should this be required. Service Management is delivered from the Insight Portal. Further Monitoring or device diagnostic information can be captured via the IMIL™ interface.

Data is transmitted to the Insight Portal via the internet using XMPP, by default over port 5222 TCP. Alternative ports can be used such as port 443 and the Monitoring Application (DCA) will automatically select the port which is available. All data is encrypted and sent via SSL. All communication is initiated by the customer monitoring application.
All communication is outbound only.

The Insight Portal processes this information and enables print service delivery managing the core functions of Asset Management, Consumable supply chain management and Service chain management. Where required, integration with the Service Provider's Service Management or ERP Systems can be implemented. Service Management systems typically provide help desk, engineer scheduling, further asset management, stock control, procurement and invoicing systems to which Insight can feed highly qualified structured data for further processing.

Local support and notifications to end user contacts or to contacts in the service or supply chains can be provided via email to defined multiple destinations.

Please note access to IMIL allows a remote user to restart the DCA service or initiate the auto-update to perform a version upgrade. The endpoint **updates.ekmglobal.com** may need to be whitelisted in your Web Proxy/Firewall to allow this. It is possible to block access to **updates.ekmglobal.com** within the firewall to prevent the auto-update process from working. The user account associated with the Windows service can also be changed to a lower, or a non-system privileges account to effectively limit any risk of the DCA affecting the host computer.

II. Device Import and Discovery

Discovery of network print devices is done using defined IP address ranges or via point discoveries for devices at known locations.

Lists can be created offline or exported from other systems imported into Insight Portal which will be read by the monitoring application the next time it communicates to the portal.

If an HP JAMC is installed, then the device IP will be transmitted to the JAMC automatically for inclusion into the JAMC monitoring.

Once a device has been discovered for the first time, added to the Asset List and registered for management InSight monitoring application will begin to monitor the device.

III. Moves and Changes

The discovery process is designed to support the critical function of active moves and change management providing notifications of change events if required. It is also designed to create minimal network traffic through targeting specific device information only.

Discoveries run at regular intervals to identify changes to the fleet e.g., new, moved or changed devices.

In addition, the monitoring loops will also track any IP address changes, Serial and MAC address changes and change of monitoring application name.

IV. Network Print and Device Monitoring

Network device monitoring uses the SNMP protocol on port 161 using UDP for most printing equipment. The Insight application supports SNMP V1, V2 & V3. SNMP V2 provides the best performance together with minimal network traffic. The extra security requirement of SNMP V3 creates extra performance and administration overheads so should be avoided unless the additional security is necessary.

The monitoring process comprises five independent sub-processes that scan devices to confirm they are available, collect alerts, record consumable levels, record media status and record page counts. Device Monitoring is self- optimizing with each sub-process only reading the specific information it needs to perform its specific task thereby minimizing network traffic and maximizing the number of actively monitored devices per server. For very large fleets multiple monitoring applications can be deployed or the network segmented with the data consolidated at a Portal Server.

All data items are checked for validity before being stored in the database. Data that is inconsistent with previous readings and usage trends is rejected then collected during the next monitoring cycle.

The timing of the sub-processes is optimized such that information that is less time critical e.g., page counts is retrieved less frequently than time critical information e.g., device alert status.

Most of the information used by Insight is retrieved from the standard Printer MIB (RFC 1759). In addition, information is also retrieved from the Manufacturer's Private MIB or other sources where required for effective service management.

V. Information Collection

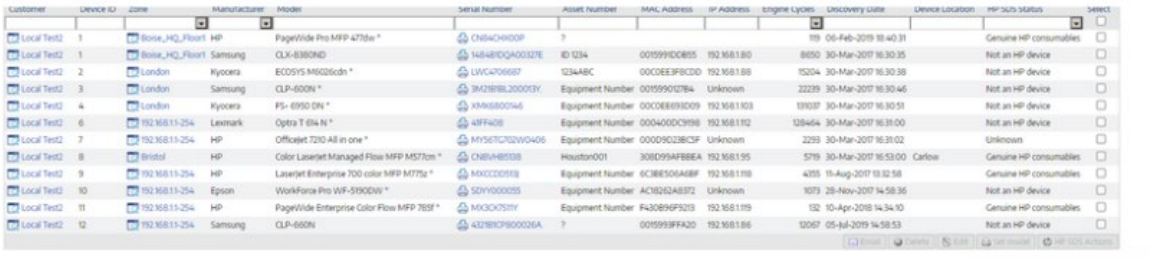
The information collected during active service management falls into three main categories:

- Asset information, including meter usage information
- Consumables Supply chain information
- Incident Service Chain information

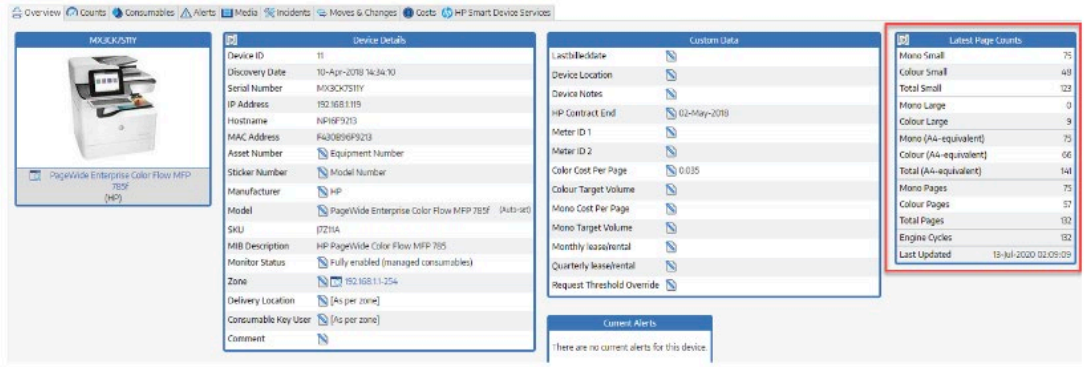
The Insight Monitoring applications do not collect any user identifiable information from the network print devices. Although many print devices do record job information, Insight does not retrieve this information.

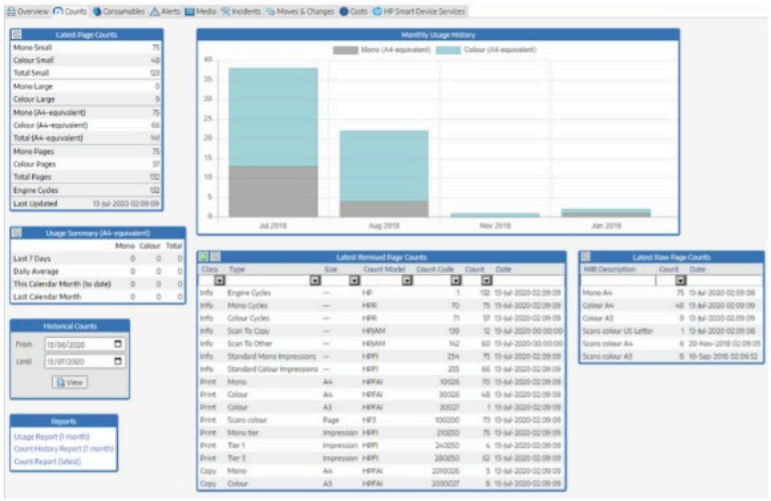
The Insight monitoring server sends four key types of information back to the Insight Portal Server:

- Asset information - manufacturer, model, location, device identification

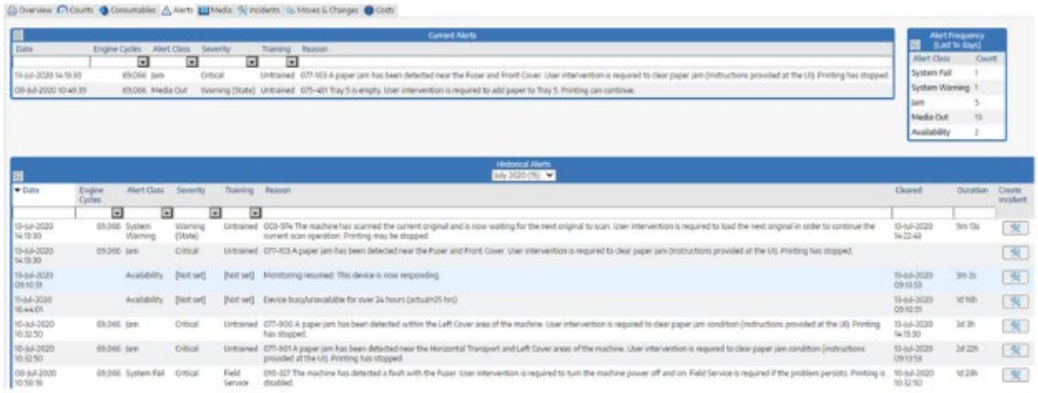


- Usage Information - page counts recorded by the print device both in summary and in detail





- Incident Service chain Management and alert information – alerts reported by the print device



- Consumable supply chain information - consumable levels reported by the print device.

This information is carefully analyzed in real-time to generate service management messages and route them to the appropriate destination for action enabling very large fleets to be managed highly effectively by exception.

VI. Number of Devices Supported

The number of devices that can be monitored by a single Insight monitoring Server depends on a variety of factors including network speed, age and complexity of the printer fleet, DNS efficiency, the longest allowable alert response time, the processor speed, and memory capacity of the actual Insight Enterprise or Monitoring Servers. It is therefore not possible to provide a definitive answer. As a guide, typically one Monitoring Server can handle between 1 and 5,000 physical devices. If there are more devices to be monitored multiple Insight monitoring applications can be deployed.

There is no limit on the number of devices supported at the Portal server.

VII. Insight Monitor (DCA) / Server Hardware and Operating System Specifications

The Insight Monitoring Server can be installed on most typical Windows PC/Server/VM platforms.

However, for live service operation with more than 250 devices we would recommend a server operating system as this will provide a more reliable service. As the system does continuous quality of service monitoring, we further recommend that the server is operating continuously and is not switched off.

It is not recommended to use laptops if possible due to the transient nature of these devices.

VIII. Virtual Machines

Deploying on virtual machines is fully supported. Insight is a real-time monitoring application however and this must be considered.

The Insight Monitoring Server use very little system resources but do require constant access to the LAN card to perform monitoring of the fleet, VMs needs to be configured to support this method of operation to optimize performance.

IX. Data and Traffic Network

The SNMP network traffic generated by the Insight application is generally less than 10Kbits per second.

For device management devices generate approximately 1 Kbyte per device per day. Alternatively, this can be viewed as 25 devices creating the same data as a single A4 text only page sent to print. It is not recommended to use laptops if possible due to the transient nature of these devices.

X. Network Ports

InSight uses the following TCP/IP ports:

Customer Network:

PROTOCOL	PORT (DEFAULT)	FUNCTION
SNMP	Port 161 UDP	Device Monitoring
HTTPs (SSL/TLS)	Port 443 TCP	Access to Insight web interface and device web pages/ Product updates https://updates.ekmglobal.com
HTTP	Port 80	Device monitoring where done via device web services
SMTP	Port 25 TCP	Internal Customer email communications e.g., email alerts to Customer Helpdesk
HP JAMC	443/Various	Please see detailed HP JAMC specification for detailed information

Communication to Service Provider:

PROTOCOL	PORT (DEFAULT)	FUNCTION
XMPP	Port 5222 TCP (others can be used if they allow encrypted XML traffic e.g., 443)	Operational Data communication to Service Provider
HTTPS	443	License verification-**DCA V28 ONWARDS**
HTTP	Port 80	Licence verification- **LEGACY DCA"S ONLY**.
VPN	Customer Specific	Remote access to InSight server where needed
HP JAMC	Port 25 TCP	Please see detailed HP JAMC specification for detailed information

XI. External Firewall Rules

Outbound Management Data

For outbound traffic to the Portal Server the monitoring application must be able to initiate a session with the InSight portal via XMPP IANA defined port for this encrypted XML traffic. This is Port 5222.

Once initiated the session must allow two-way communications.

Please contact or your Service Provider should you wish to use an alternative port, however Port 5222 is the most secure and highly recommended port to use. Please contact your Service Provider for the URL of the Portal server for "whitelisting" should this be required.

License Verification

Periodically the monitoring server contacts the or service provider license server via port 80. Please contact your Service Provider for the URL of the Portal server for "whitelisting" should this be required.

If port 80 is unavailable, please contact support and a license file (.lic) can be provided.

Version: 4.9