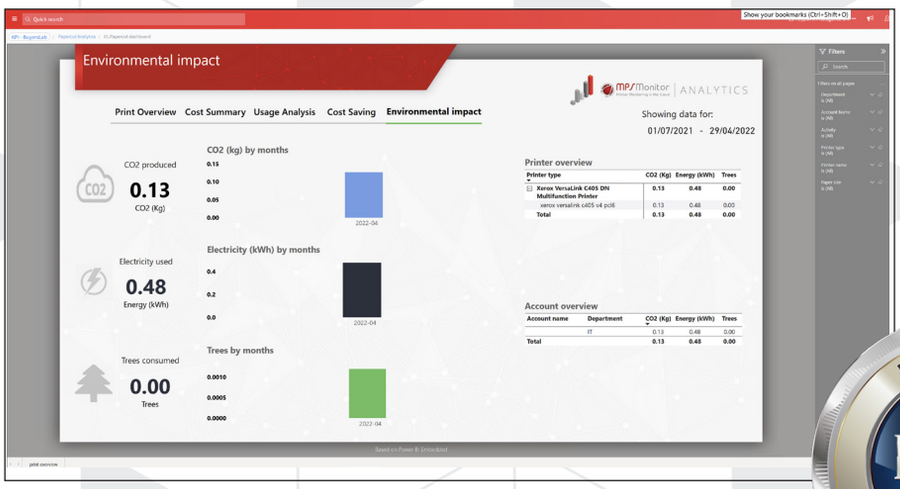
KEYPOINT INTELLIGENCE

MPS Monitor
Printer Monitoring in the Cloud

WHITE PAPER

Keypoint Intelligence Report

MPS Monitor DCA4: Ground-breaking Features and Security



BUYERS LAB 2022 BLI OUTSTANDING ACHIEVEMENT

Test Objective

MPS Monitor commissioned Keypoint Intelligence to conduct testing and research on its new DCA4 data collection agent, and to review the testing conducted by independent third-party security testing firms to appraise the quality of DCA4's security. Areas to consider included DCA4's multi-platform support, remote access of devices' internal web servers, PaperCut integration, granular data collection, improved security, and other features and attributes.

JUNE 2022

Introduction

Data collection agents (DCAs) are essential for effective managed print services (MPS) solutions as a key way to gather status and information from printers and MFPs at the customer site and relay it to the MPS provider for action and analysis. A well-crafted DCA collects data efficiently, has minimal impact on network bandwidth, and reports actionable and granular data. More importantly, given its access to the customer's network and the world outside the confines of the firewall, a DCA must have the utmost security. A good independent software vendor (ISV) will also improve DCAs as new technologies emerge and as print environments and business requirements change.

When Keypoint Intelligence technicians tested the previous iteration of the MPS Monitor DCA agent, called eXplorer 3, we found it worked well in testing and delivered convenient features such as clustering, HP SDS integration, and the ability to auto update among other things. With DCA4, MPS Monitor undertook a "clean sheet" design to deliver the standout eXplorer 3 features along with improvements such as multi-platform code (so that the same code could be run on different operating systems and platforms), increased security to combat modern threats, better data collection and processing, and remote connection to devices' internal web servers. The company's goal was to deliver true IoT (Internet of Things) technology that allows continuous, real-time monitoring of devices. (Note that MPS Monitor will not phase out eXplorer 3 or render it end-of-life, as eXplorer 3 is still necessary for older Windows operating systems and some proxy servers that don't support the new technologies and code libraries used in DCA4.)

DCA4 can be downloaded via the MPS Monitor portal, and the wizard-driven DCA4 installer for Windows detects and installs any missing packages, which means the user doesn't have to look for them elsewhere. It took Keypoint Intelligence's software analyst only five minutes and 12 clicks to install DCA4. Keypoint Intelligence tested DCA4 features such as Device Web Access, discovering devices and installing and configuring DCA4, but performed desk research and reporting where it wasn't possible to test or benchmark features.

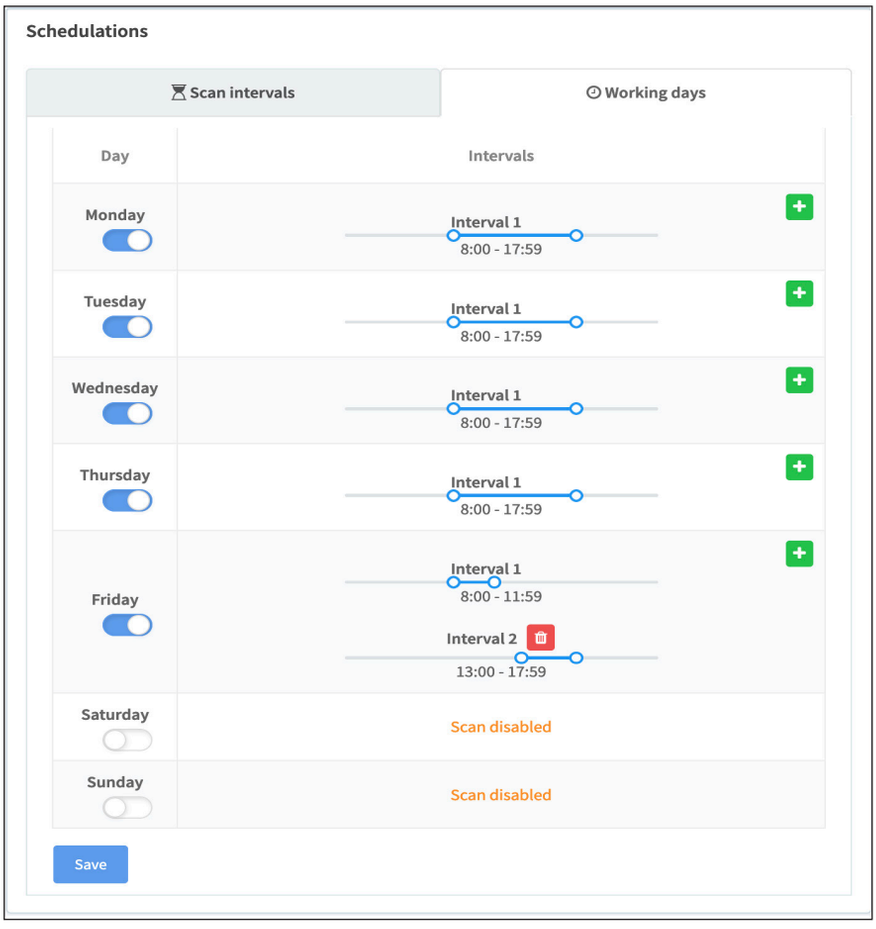
Real-Time Communication

DCA4 uses the MQTT (MQ Telemetry Transport) messaging protocol to allow real-time connection between dealers using the MPS Monitor portal, the DCA, and managed devices. MQTT is designed to be lightweight and efficient so that there's minimal effect on network bandwidth, and solutions using it consume minimal computing resources. The MQTT protocol also allows bi-directional communication, which makes it easy to broadcast messages to groups of devices, while support for persistent connections means quicker reconnections between a client and broker when they are connected over unreliable networks. MQTT also allows for message encryption via TLS and the use of modern authentication methods such as the OAuth standard. Dealers will be pleased to note that MQTT can scale to over 1,000,000 devices, so one instance of DCA4 will have no problem handling a device fleet in a customer's building. In addition, DCA4 uses the HTTP/2 protocol for communication, unlike DCA3 which uses the slower HTTP/1 protocol. More specifically, DCA4 uses HTTP/2 in conjunction with gRPC (Google Remote Procedure Call), which augments HTTP/2 and benefits DCA4 with resiliency, performance, long- or short-lived communication and customization. HTTP/2 with gRPC can scale to huge amounts of traffic and remain efficient.

Optimized Device Discovery

Fast, efficient device discovery is an obvious need and desire for MPS dealers, and DCA4 has some features that help speed up device discovery. The discovery process is now asynchronous, so data about a new printer is sent directly to MPS Monitor from DCA4, and DCA4 retrieves meter readings and consumable data from a device soon after it has been discovered. Data is kept on DCA4 and is held there until the next reading at which point it is updated, which keeps data fresh for the MPS Monitor web portal.

Dealers can set device discovery to occur once a day or every few hours, whichever is most convenient for them and the customer. It's also possible to provide hostnames for device detection instead of IP addresses, which means there's no need to scan the entire network or a wide IP range. Dealers can schedule printer discovery to occur every two, four or six hours, and can spit data detection intervals at certain times and on certain days to tune more finely the data collection process. Dealers can set data collection intervals for between 07:00 and 09:00 on Friday morning, for example, and then have another one between 18:00 and 20:00. Moreover, there's no longer a need to provide a MIB walk and screenshots to support devices because SNMP MIBs are sent directly to the server.



Dealers can easily adjust scan intervals using sliders to fine-tune data collection events.

Improved Security

Security was a key driver for MPS Monitor in the development of DCA4, and the applet contains a host of improvements. MQTT in DCA4 uses the WebSocket Secure (WSS) protocol, which helps prevent man-in-the-middle attacks. In addition, the combination of HTTP/2 and gRPC means that DCA4 can use TLS 1.3 on supported devices, which is not possible with just HTTP/2 alone. This bolsters DCA4's security credentials, as does the use of the secure shell (SSH) protocol.

A one-time password is required to configure DCA4 and the Device Web Access feature, SNMP v3 is used (including its credentials management), and two services are now used instead of one. A service is used to monitor and manage DCA4's status, and the other service scans the network and monitors devices. The latter service runs with fewer privileges, so MPS Monitor says it is less susceptible to attack. DCA4 was coded using Microsoft .NET 6 Core which is more secure than .NET FW which was used to create DCA3.

To put these security measures to the test, ECSC Group plc accomplished a complete code review of DCA4 in March 2022. The review was performed to identify security weaknesses and deviations from the OWASP (Open Web Application Security Project) code review guidelines and consisted of both automated and manual analysis of the code. ECSC analysts employed a collection of tools to aid in automatically reviewing the target source code of the three components that comprise DCA4: DCA, DCARemote, and DCAServer. The tools helped the testers gain initial coverage across the entire code base. Automated findings were followed up by manual analysis to help rule out any initial findings as false positives.

From there, the analysts developed an overall threat model designed to be an accurate representation of credible threats against the organization and infrastructure; their subsequent testing exercise attempted to simulate threats using this model. Where appropriate, the testers attempted to exploit vulnerabilities and play out various attack vectors. In its final report, ESCS analysts stated "…the level of risk associated with the tested scope was low…". There were no critical- or high-risk issues identified, and MPS Monitor remediated the one medium-risk issue.

In addition to the code review, ECSC Group performed a dynamic penetration test on the DCA4 service itself. Conducted from the dealer's perspective, the test was designed to determine the presence of any vulnerabilities that could compromise data, affect integrity, or undermine confidentiality. An overall risk-rating was determined based on the findings identified by ECSC during the testing, given the context of the environment, the likelihood, impact, and ease of exploitation. This penetration test revealed no critical or high-risk security vulnerabilities, and ECSC analysts also noted that it was not possible to compromise the underlying hosts during the assessment.

Multi-Platform Support

DCA4 is available for the Windows (Server 2016 or later and Windows or later), Linux (Debian and Ubuntu) and Raspberry Pi 3 (Raspbian) platforms, with a Mac OS version of DCA4 to be released in the third quarter of 2022 according to MPS Monitor. This provides dealers with greater flexibility when deploying DCA4 at customers' sites and means that they can collect data from locally connected devices no matter what operating system is running on the computer to which the device is connected.

For Dealers using HP Smart Device Services (SDS), the Windows version of DCA4 may contain HP JetAdvantage Management Connector (JAMC) which it also installs on the Windows PC. HP JAMC integrates MPS Monitor with the HP SDS remote-management platform for in-depth management and configuration of compatible HP devices.

Device Web Access (DWA)

DCA4 lets dealers and fleet managers access remotely the internal web server of devices that they manage, so that a fleet manager can access the internal web server of a printer to configure it or view the device's settings, for example. MPS Monitor says this is a rare feature for MPS software, and Keypoint Intelligence must admit that is something it rarely sees. However, what differentiates MPS Monitor is the level of security applied to the process of connecting MPS Monitor and a device's internal web server.

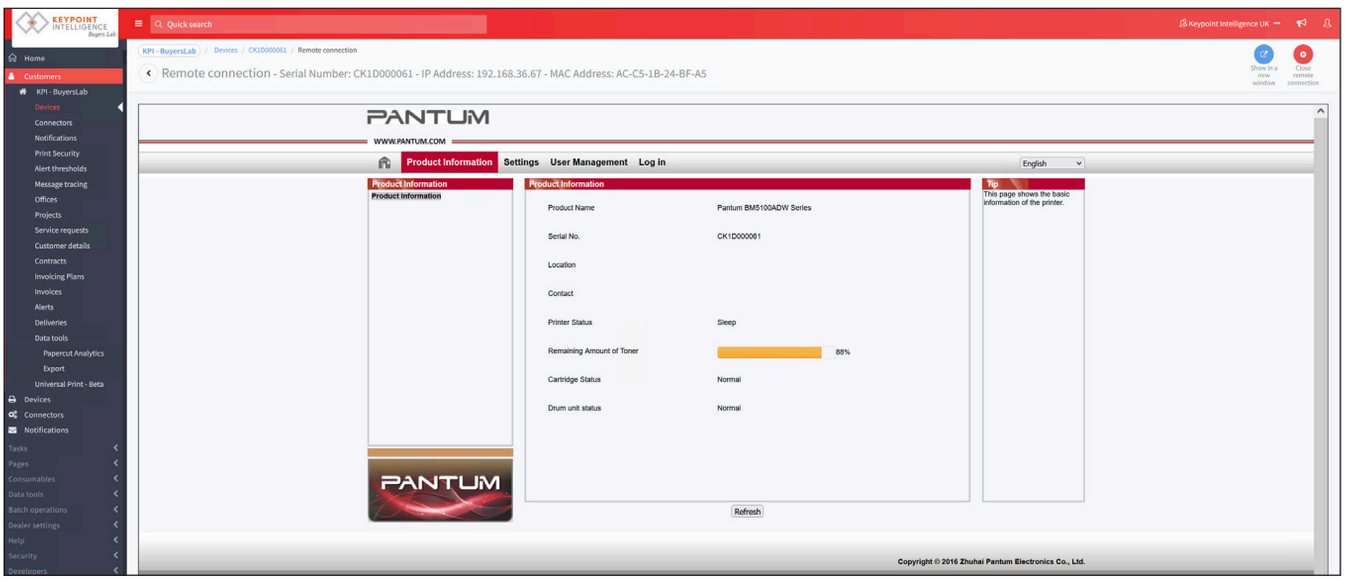
Two-factor authentication or Active Directory integration must be enabled for Device Web Access to work to ensure that the user who gains access is a legitimate user and is not using stolen credentials. Meanwhile, complex cross-checks between DCA4 and the Azure and MPS Monitor datacentres are in place to prevent man-in-the-middle attacks. The Device Web Access connection is only opened when a device's IP, SN, MAC, brand and model match the data within MPS Monitor, and the Azure server's firewall rules are created and cancelled each time so that the same data is not reused. Files can't be uploaded to prevent malicious code or firmware being uploaded, and DWA sessions are limited to 10 minutes, so users won't be logged in permanently and run the risk of others accessing a device's internal web server via their unattended PC.

Device Web Access uses Microsoft Azure's SSH gateway and reverse proxy to work, and port 22 must be open on a user's network to allow a DWA connection. DWA uses Windows' own OpenSSH component, which means that no third-party SSH code libraries are used.

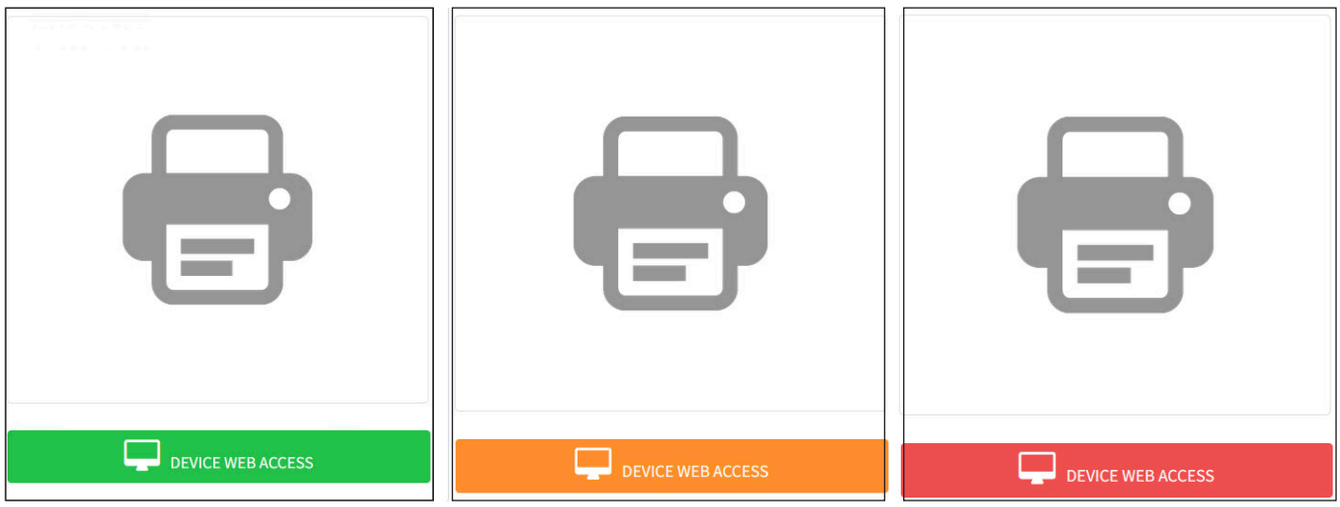
Users can get a full audit of DWA session history within the MPS Monitor portal's device page. Both dealers and end users can disable the Device Web Access feature entirely if they feel it is unnecessary. If the feature is disabled on the DCA local host configuration page, the dealer cannot re-enable it remotely, which means customers can keep full control over who accesses their printers remotely.

Colour coding in the printer's page in the MPS Monitor Portal denotes the availability of Device Web Access, with green indicating that all requirements are met and connection is possible, orange indicating that not all requirements are met so connection may or may not be possible, and red which indicates that connection is not at all possible.

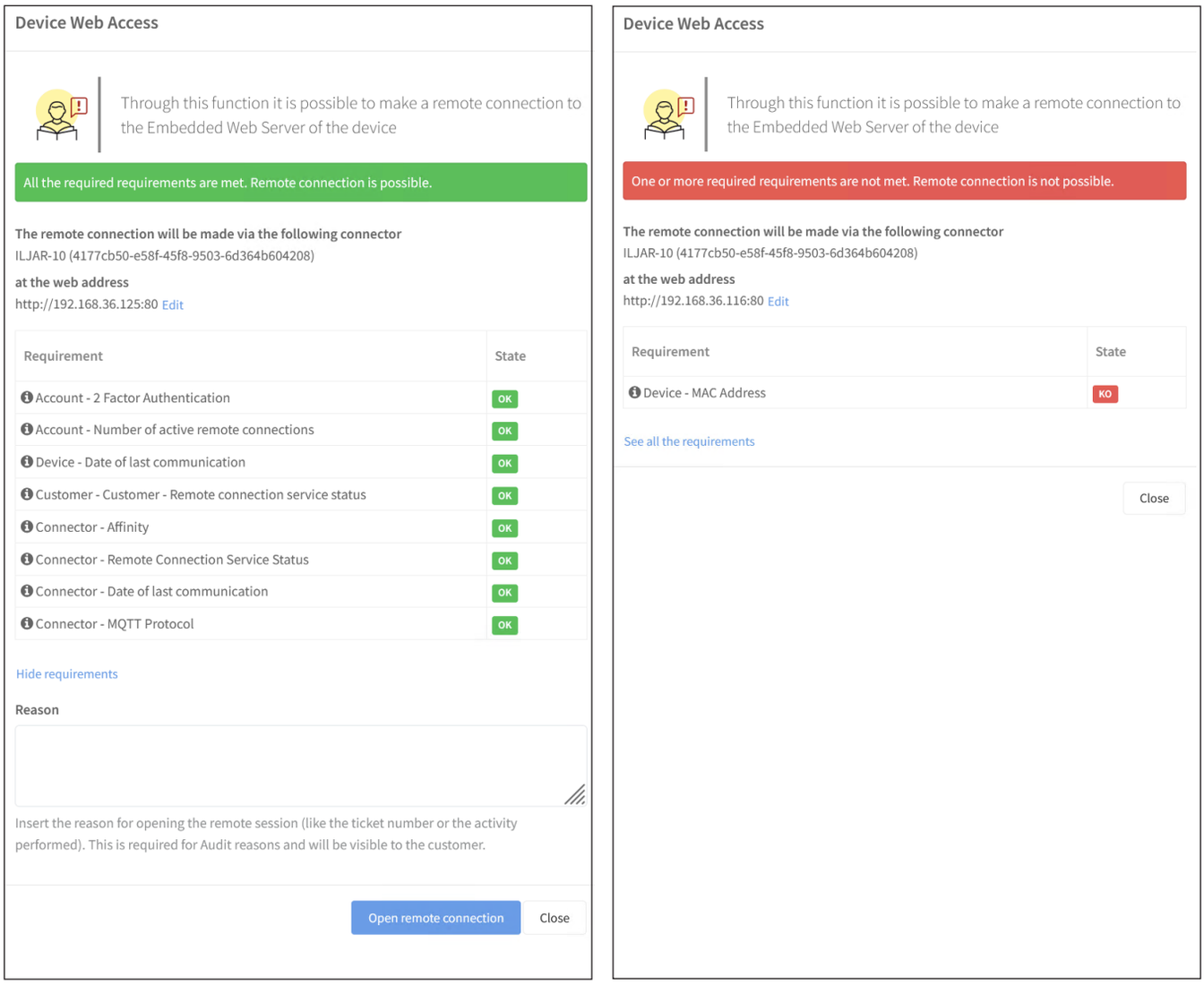
DWA worked well in use, and was much faster than expected despite the security involved. It's a powerful and convenient feature that will help dealers and fleet managers provide even greater degrees of service to their customers.



Device Web access lets dealers and fleet managers access devices remotely so that they don't have to make site visits or ask customers to get data or change settings on their behalf.



Colour coding denotes the viability of remote connection to a device's internal web server.

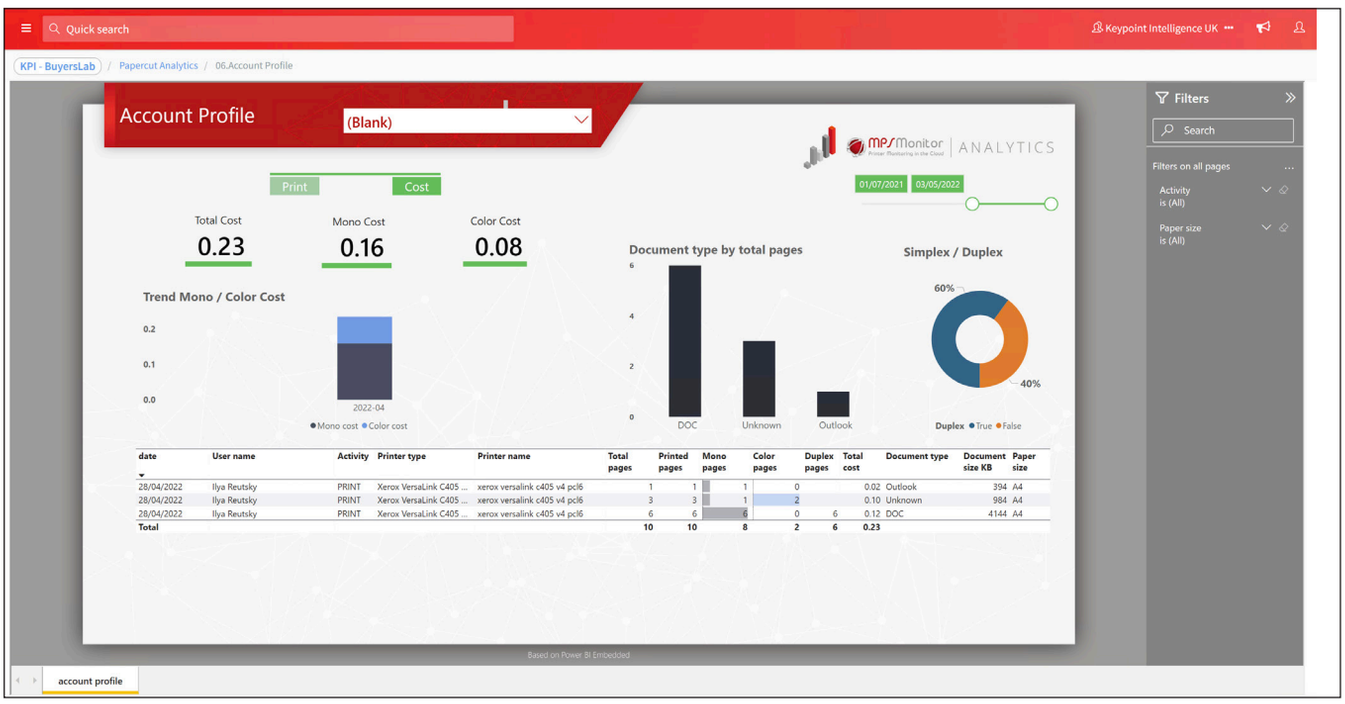


MPS Monitor tells the user which requirements have been met and which haven't.

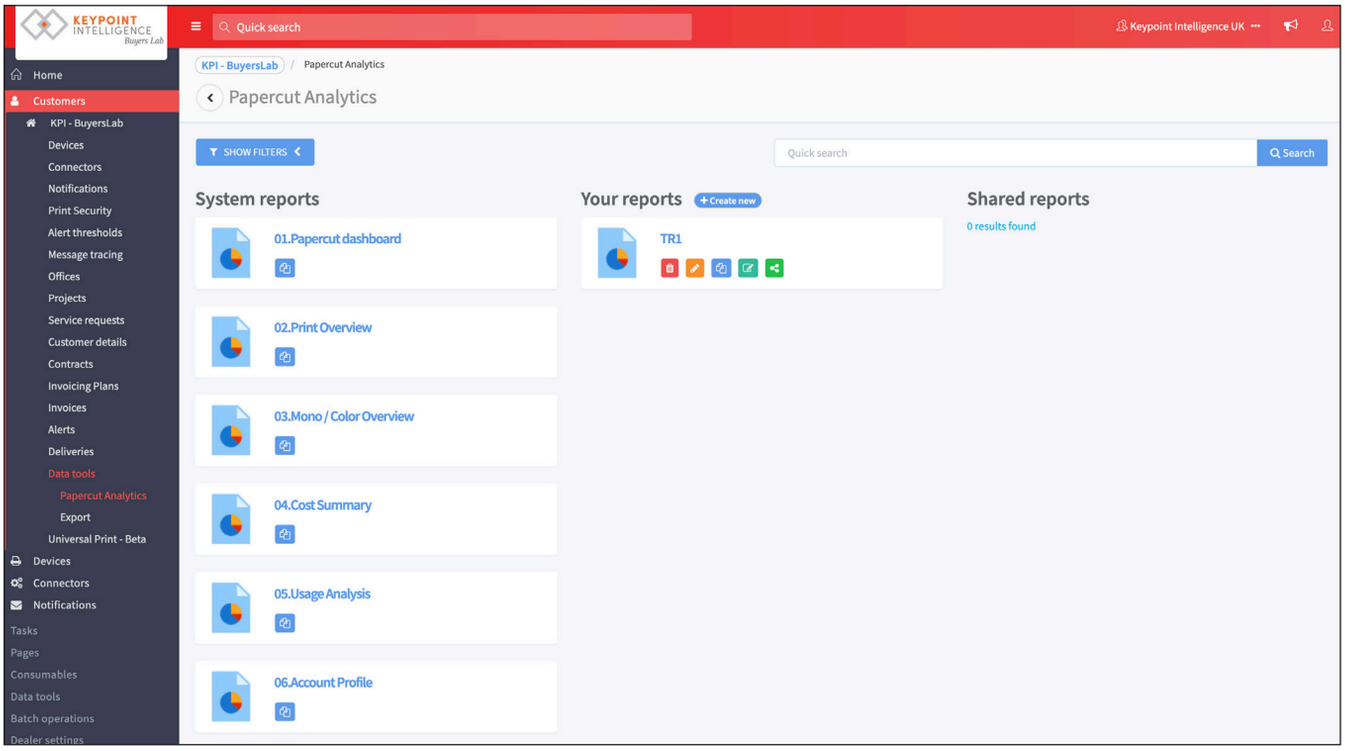
PaperCut Integration

PaperCut is one of the most popular print management solutions available and a bliQ Pick Award winner, so some dealers will be delighted that DCA4 allows them to import data from PaperCut MF and NG in to MPS Monitor. Once the PaperCut data has been imported dealers can visualise and analyse that data in MPS Monitor's Power BI Analytics environment. MPS Monitor says this integration lets dealers manage printing patterns, uncover hidden costs, identify areas of improvement, track print volumes, reduce their dealerships environmental impact and analyze trends to discover inefficiencies. Power BI is interactive, and visualisations can be altered on screen. Dealers have access to a number of pre-made PaperCut Analytics reports, and they can create their own.

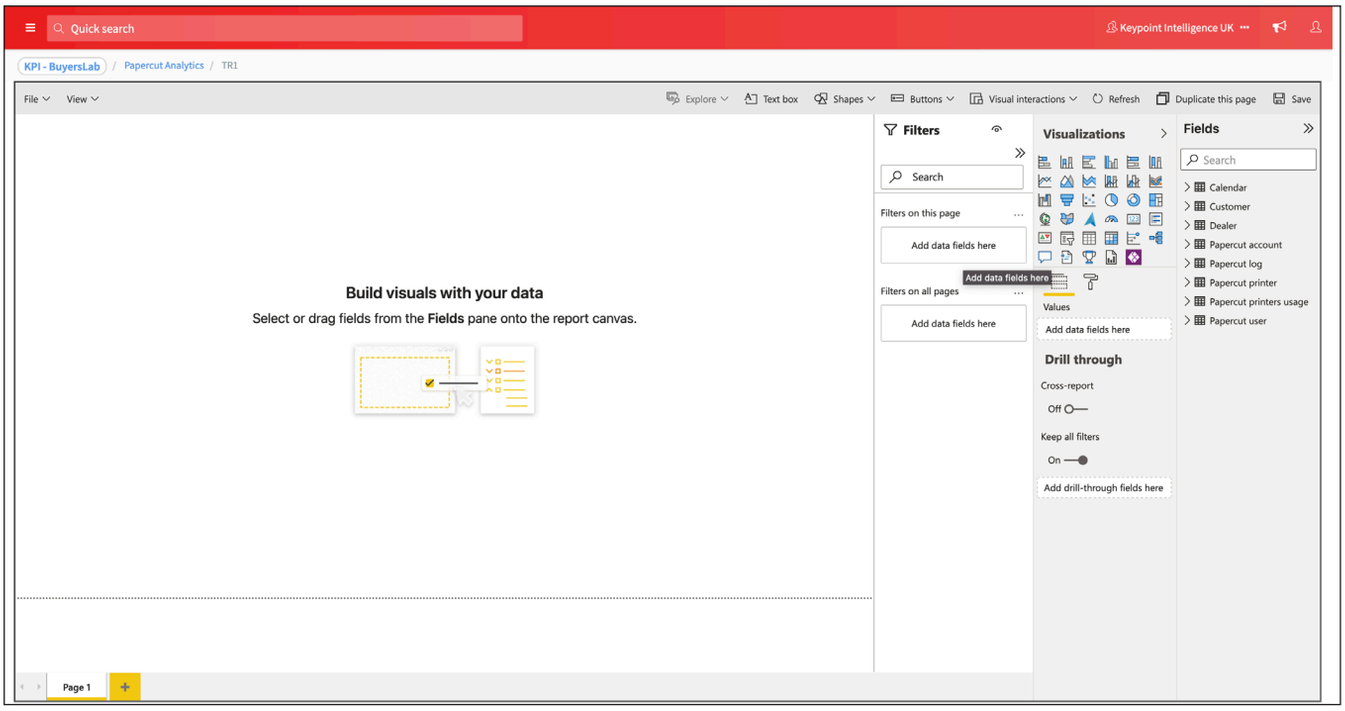
There's a minimal bit of configuration needed to integrate PaperCut, such as modifying the data integration template in PaperCut then verifying that data's been exported, specifying the location of the exported CSV file within MPS Monitor, and making a couple of other tweaks within MPS Monitor. Data doesn't appear immediately, and Keypoint Intelligence's analyst reported that it took around one hour for the first set of PaperCut data to appear in MPS Monitor, and historical data can take a little longer to appear.



MPS Monitor's Power BI-based PaperCut reports are graphical, informative and interactive.



There are a number of pre-made PaperCut analysis reports for dealers to use in MPS Monitor.



Dealers can create their own reports, too.

Opinion

MPS Monitor's improvements have produced a leading-edge data collection agent that is equipped to deal with the worst security threats and to provide efficient, simple and versatile data collection. DCA4 strengthens MPS Monitor's market appeal and is yet another reason to take on or continue an MPS Monitor subscription.

About Keypoint Intelligence

For 60 years, clients in the digital imaging industry have relied on Keypoint Intelligence for independent hands-on testing, lab data, and extensive market research to drive their product and sales success. Keypoint Intelligence has been recognized as the industry's most trusted resource for unbiased information, analysis, and awards due to decades of analyst experience. Customers have harnessed this mission-critical knowledge for strategic decision-making, daily sales enablement, and operational excellence to improve business goals and increase bottom lines. With a central focus on clients, Keypoint Intelligence continues to evolve as the industry changes by expanding offerings and updating methods, while intimately understanding and serving manufacturers', channels', and their customers' transformation in the digital printing and imaging sector.

For more information on Keypoint Intelligence, please call David Sweetnam at +44 (0) 118 977 2000 or email him at david.sweetnam@keypointintelligence.com