Printanista Hub Technical Whitepaper

Version 1.8

Table of Contents

ECI will provide support services exclusively for the latest commercially available release of the Software, as well as the immediately preceding version of the Software. This policy applies to all ECI Device Management products.

Microsoft®, .NET Framework®, Windows® and Windows Server® are either registered trademarks or trademarks of Microsoft Corporation

Overview

The Printanista suite of products delivers an enterprise class managed print solution that is quite easy to use and deploy. It is architected and designed to take advantage of the advanced features and benefits of the Microsoft .NET platform. Thus, it no longer requires skilled technicians to install software, configure and maintain the system. The Printanista products cannot in any way be configured to perform a task beyond the ones for which it was designed. The transmission of data from the products to outside sources is tightly restricted. The products do not report any other details except for information on the equipment being monitored (i.e., type of equipment). No confidential information is ever transmitted out of the network via Printanista products. The suite consists of the following components:

Printanista Hub: A website and backend system housing all the data received from the Printanista data collection tools. It is a repository that allows you to view data using a browser, generate reports, configure alert workflows and notifications, and synchronize data with your ERP systems for billing or supply fulfillment.

ECI DCA: This newest Data Collection Agent-DCA brings about major advantages over Onsite Data Collection Agent-DCA without losing any features, including full native cross-platform support of Windows, macOS, Linux, and Raspberry Pi, each with unique installation steps, support documentation, and trained support staff on these platforms. ECI DCA also brings ongoing discovery and scanning of devices, improved MIBWalk and Log collection capability, and many more meter types are collected now.

Onsite DCA: A legacy data collection agent tool automatically performs print assessments and monitors consumable levels, printer status, and error logs. This application is installed at the customer site and can perform print assessments automatically on a scheduled basis without human intervention. The data captured is sent to the Printanista Hub website using HTTPS, HTTP, or if the customer prefers a propriety encrypted file.

The purpose of this document is to provide a product line overview of the Printanista Suite of Products from a technical perspective to help facilitate answers to the most frequent questions Information Technology teams will receive.

How Printanista Works

Printanista Hub Designed as a Hosted Application

Printanista Hub is hosted by ECI Software Solutions within secure and protected datacenters in different regions of the world. ECI Software Solutions understands the confidentiality, integrity, and availability of our customers' information is vital to their business operations and to our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes, to meet the growing demands and challenges of security.

ECI Secure Data Centers

Our service is collocated in dedicated spaces at top-tier data centers. These facilities provide carrier-level support. This link is to the ECI detailed document related to Data Centers Security.
ECI Cloud Security Overview 2021 (ecisolutions.com)

Data Collection Agent (DCA)

The data collection agent's core engine, which is the heart of every Printanista product, correctly identifies and extracts data from networked printers, copiers and MFPs utilizing the protocols the devices support.

Printanista currently supports (Simple Network Management Protocol) SNMP v1, v2c and v3 protocol. SNMP v3 provides increased packet protection to ensure information and communication is transmitted via reliable sources. Unlike SNMPv1 or v2, SNMP v3 is encrypted for increased security and requires both a username and a password. A benefit to using SNMP v3 is network administrators can determine the encryption method as well as a strong username and password.

SNMP is a network protocol facilitating the exchange of information between network devices extracting data from the Management Information Base (MIB) and other locations within the print device. The Management Information Base (MIB) is an internal database most network-connected devices have as part of their anatomy. The Management Information Base (MIB) holds data such as model name, toner levels and current status of the printer.

Printanista Requirements

Printanista Hub Backend Application

All collected data is sent to the Printanista Hub server where it is made available for reporting and alerting.
ECI DCA connects to your Printanista Hub server using HTTPS (port **443/TCP**). Please contact your ECI Solutions administrator for information on domain names and IP address(es) used by your server.

This connection is protected by industry standard **TLS** (Transport Layer Security).
Minimum version TLS 1.2 is required.

This connection stays open the entire time ECI DCA is running. Normally a **WebSocket** connection is used, but in some situations ECI DCA may fall back to using either **server-sent events** or **HTTP long polling**.

IMPORTANT NOTE: Several Secure HTTPS outbound connections are required from the server where Printanista Hub is installed:

- https://www.gttechonline.com
- https://modelmatch.printanista.net
- https://models.printanista.net
- https://updates.printanista.net
- https://api.printanista.net
- https://dcaregistry.printanista.net
- https://remotedevicelink.printanista.net
- https://install.printanista.net

Printanista Application Requirements

Data Collection Agent (ECI DCA)

Printers, copiers, and MFPs must have the SNMP protocol (Port 161) enabled for discovery and extraction of information. The SNMP protocol is a standard part of the Application Layer of the TCP/IP suite.

PC/Server requirements for ECI DCA:

Microsoft Windows (x86/64)
Requirements:

- Microsoft .NET Framework 4.7.2. or newer (recommended: latest version)
- Fully-released, Microsoft-supported versions of Windows Server (excluding Datacenter and Core editions) and Windows
  - *Microsoft versions no longer supported by Microsoft are not supported by ECI DCA.*
- Local network and/or firewall settings allow connection to ECI Updates Server services and the Printanista Hub server.

Linux (x86/64 or ARM)
Requirements:

- Mono Framework 5.4 or higher (recommended: latest version)
- Local network and/or firewall settings allow connection to ECI Updates Server services and the Printanista Hub server.
- Only Ubuntu LTS 20.04 and above are officially supported.

macOS (x64)
Requirements:

- Mono Framework 5.4 or higher (recommended: latest version)
- macOS® Sierra (10.12) through Sequoia (15.4). Newer versions are not supported.
- Local network and/or firewall settings allow connection to ECI Updates Server services and the Printanista Hub server.

Raspberry Pi
Requirements:

- Raspberry Pi 3 Model B or Pi 4 Rev 1.5. Newer versions not supported.
- Blank 8GB or larger microSD card
- PC capable of writing to microSD card
- Local network and/or firewall settings allow connection to ECI Updates Server services and the Printanista Hub server.

Firewall Considerations for ECI DCA:

Inbound Connections - There are no inbound connections from the internet to ECI DCA.
Outbound Connections

Service	Port	Connection To
Data Upload	**443/TCP** (HTTPS)	Your Printanista Hub Server
Software Updates	**443/TCP** (HTTPS)	ECI Updates Server
Registration (fallback)	**53/UDP** (DNS)	Local Network DNS server (primary) ECI Updates Server (fallback)

ECI Updates Server

ECI Updates Server is a service run by ECI Device Management to facilitate DCA registration, automatic software updates, and DCA installations (this site), and is required for ECI DCA operation. Note: ECI DCA does not send any collected device or configuration data to ECI Updates Server.

Software Updates

ECI DCA auto-updates itself by downloading updates published on https://updates.printanista.net/ . Connections are always made on the standard HTTPS port **443/tcp**.

Registration

ECI DCA uses DNS requests to `*.reg.pf-d.ca` to register. It will first try to do this using the local network DNS servers, and then fall back to talking directly to ECI Updates Server IP addresses (using port **53/udp**). The firewall only needs to allow this connection to ECI Updates Server if local DNS server(s) do not resolve the registration requests.

Service Region

ECI DCA is routed to the region to which it has the lowest network latency and based on service availability. In certain locations, the region being used may change over time as activity on the global internet infrastructure can affect latency.

Data Collected and Encryption

Data Encryption

All data packages from ECI DCA and legacy Onsite DCA are encoded and obfuscated. Printanista requires using HTTPS for communication between the DCA's and Printanista Hub. ECI DCA requires HTTPS to function. Additionally, all sensitive settings and jobs between ECI DCA and Printanista are encrypted using AES256 standard symmetric encryption algorithm, using a protected shared key. This ensures end-to-end encryption, so data is protected from being read if intercepted by a third party, a competitive or otherwise non-authorized Printanista instance.

Security Matters

ECI DCA and legacy Onsite DCA communicate with Printanista Hub over HTTPS protocol, using industry standard **TLS 1.2** (Transport Layer Security). Confidential data is not collected, viewed, or saved by any Printanista application. Only printer-related data is collected and viewed. No other network data can be identified or collected by ECI DCA or legacy Onsite DCA, except for IP Address, MAC Address, and Hostname.

ECI DCA and legacy Onsite DCA do not collect or process any personal data. The only way the system will collect this type of information is if you or your customer(s) input the data into Printanista within a field or label such as location or customer name. ECI DCA and legacy Onsite DCA enable you to monitor network devices using Simple Network Management Protocol (SNMP). The application is deployed inside the customer's network and from there, it communicates with devices to gather operational information about the device that is made available via the device firmware and an SNMP Management Information Base (MIB). The data exposed by the device varies by manufacturer and model. It is always technical or operational in nature and specific to the device itself. At the most basic level the data exposed by a printer MIB is documented in the IETF RFC 3805 (https://tools.ietf.org/html/rfc3805). Additional device information may be exposed by the manufacturer through extensions and private MIBs (Management Information Base), but the information is fundamentally technical and device specific.

Printanista Hub only stores:

- Hostname
- Operating System
- Remote IP Address
- System Architecture

Other network/environment information is collected and displayed while connected for troubleshooting purposes, but never stored in Printanista.

Types of Information Collected

ECI DCA and legacy Onsite DCA attempts to collect the following information from networked printing devices during a network scan:

Device Attributes

- IP address (can be masked)
- Manufacturer
- Serial number
- Asset number
- MAC address
- Device description
- Location
- Miscellaneous (machine specific)

Service

- LCD reading
- Device status
- Error codes
- Firmware

Supplies

- Toner cartridge serial number
- Toner cartridge supply level
- Drum levels
- Maintenance kit levels
- Non-toner supply levels
- Miscellaneous levels
- Label-based printers supply details

Coverage and Meters

- Meter reads
- Meter type
- Coverage level
- Monochrome or color identification

Network Discovery and Data Collection

To add to the efficiency of the DCA, only when there is new or changed data from the devices will this information be sent into the Printanista Hub Server. This will ensure minimal network load and remove the frequency of any backlogs of device data submissions. Also, discovery and scanning of devices are now independent to ensure only the IP address (or hostname) of devices previously discovered are being scanned on the periodically set basis versus a full network scan (this is completed initially, periodically, or when determined by an admin user).

This will ensure the speed of device data submissions is as up to date as possible. This allows users to be notified of troublesome devices within minutes or even seconds in many situations. ECI DCA separates device discovery from other scan types, enabling you to set custom scan intervals for retrieving meters, supplies attributes and errors. The default, minimum and maximum values for the scan intervals are:

Scan Function	Default	Minimum	Maximum
Discovery	60 minutes	10 minutes	7 days
Meters	24 hours	30 minutes	14 days
Supplies	4 hours	30 minutes	7 days
Errors	60 minutes	30 minutes	7 days
Attributes	24 hours	1 hour	14 days

Please note the scan intervals (meters, supplies, errors, and attributes) are only available if a device has a Model Definition File (MDF). If this is not present, a full scan will be done on the device in question using a predefined interval.

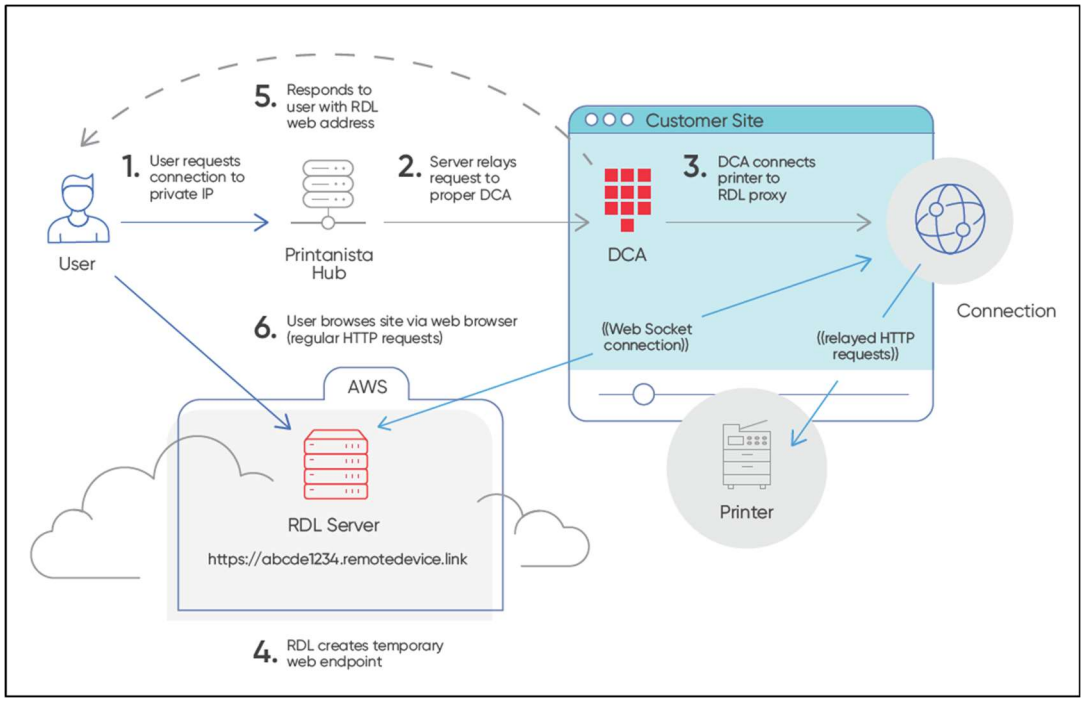
Printanista Hub administrators can remotely manage ECI DCA that have been activated on the server. Can remotely trigger the ECI DCA to execute predefined commands such as data collection tasks, providing ECI DCA logs, running remote MIB Walks, or updating ECI DCA settings.

Note: ECI DCA always initiates the communication to the Printanista server, and not the other way around.

Note: Only when meter, supply or errors information has updated or changed does communication occur, reducing bandwidth usage.

Note: HP JAMC is only functional with legacy Onsite DCA at present time.

Remote Device Link (RDL)



System Overview – Remote Device Link (RDL)

Remote Device Link (RDL) is a service allowing a remote **end-user** to access an HTTP endpoint on a private LAN.
There are 4 major components to it:

1. The **end-user** accessing the device
2. The **Remote Device Link server**, on public internet (via https://*.remotedevice.link URL)
3. The **RDL client** (embedded in the DCA), running on the private LAN
4. The **HTTP endpoint** (printer) being accessed (running on the private LAN)

Security: Ports and SSL (Secure Sockets Layer)

The public-facing path for RDL is always an https:// URL on port 443, regardless of the endpoint port and/or SSL status.

Enablement and Permissions

1. Global enablement option per dealer instance
2. Local enablement for each end-customer account
3. Permissions are required for a user to be able to access the feature

Auditing Capabilities

1. Printanista Hub local auditing of each session details
    a. Printanista Hub Administration reports for Remote Device Link (RDL) Auditing
2. Remote Device Link (RDL) AWS (Amazon Web Services) cloud logging of all session details

Remote Device Link (RDL) Security

Security of Remote Device Link (RDL) was a key concern when developing this tool.

Authorization:

- User must have permission from within Printanista Hub to access Remote Device Link (RDL) feature on the specific account
- The Data Collection Agent (DCA) will only accept Remote Device Link (RDL) requests from the Printanista Hub server which is mutually authenticated
- The Data Collection Agent (DCA) only establishes Remote Device Link (RDL) connection to known and currently monitored print devices within the Data Collection Agents (DCA) discovery IP range(s).
- Each individual web request must be to the same IP – The Data Collection Agent (DCA) will not follow redirects

Connection Security:

- All connections to and from the Remote Device Link (RDL) and Printanista Hub servers are encrypted using standard minimum version TLS 1.2 (Transport Layer Security)
- Each connection is given a unique domain name which uses a 19-character (96-bit) random alpha/numeric combination
- Each request requires a 160-bit security token, stored as a browser cookie, and only set at the very start of the session secured by TLS encryption
- The Data Collection Agent (DCA) may establish a non-encrypted HTTP connection to the print device across the local network, but supports minimum version TLS 1.2 if the device does

Session Time Limits:

- Each individual Remote Device Link (RDL) session times out after 20 minutes of inactivity by default with an absolute maximum of 2 hours.

Implications

The connection between ECI DCA and Printanista Hub is protected by authentication keys that are DCA installation specific, and the connection requires a valid trusted SSL certificate to use over a TLS connection.

All traffic transiting from the DCA to the internet is encrypted. However, the ECI DCA can talk to the device in the local network over plain HTTP connections if the device does not support secure connections.

Printanista Hub Application

Printanista Hub functionality is accessible via a web-based user interface.

Permissions based User Management

Access to the Printanista Hub web front-end is controlled with permissions-based user management. Users must log in to Printanista using a designated username and password. Users are assigned one or more roles which specify permissions and are granted access to one or more groups of devices. Administrators with full permission can specify exactly which screens each user can view and/or interact with.

HTTPS access

Printanista requires all sites to use HTTPS with a valid SSL security certificate. This ensures encryption of data being transferred over the Internet.

Printanista Side-By-Side

Printanista Hub utilizes a Model metadata Database known as Side-by-Side (SBS), which has various model attributes such as: printing speeds, when was introduced on the market or OEM Part Numbers compatibilities, which is periodically updated as future models and versions are released by OEMs. Printanista Hub will communicate with Side-by-Side to check for new updates as well as retrieve device metadata to cache them locally on each Printanista Hub system.

Printanista Hub Application Hosting

Printanista Hub is hosted by ECI Software Solutions within secure and protected datacenters in different regions of the world. ECI Software Solutions understands the confidentiality, integrity, and availability of our customers' information is vital to their business operations and to our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes, to meet the growing demands and challenges of security.

ECI Secure Data Centers

Our service is collocated in dedicated spaces at top-tier data centers. These facilities provide carrier-level support.

Click on the following link to get the ECI detailed document related to the Data Centers Security

ECI Cloud Security Overview 2021 (ecisolutions.com)

Version Management

Testing and Release Process

Each major and minor release of the software goes through a quality control process, in which multiple Printanista personnel will regression test altered portions of the system to ensure there has not been a downgrade in security or functionality of the system, as well as validate the new functional aspects. Major releases go through a beta release process where select clients run the new and old systems in parallel.

Source Code Security

Printanista source code is kept in a secured revision control system, accessible only to authorized persons. Every change to the source code requires two authorized developers to approve the changes before being accepted in the production code repository where every change is tracked, which includes which developer made the change and why. Products are encrypted and digitally signed with a trusted code-signing certificate before shipping. An escrow deposit can be made available based on request.

ECI engages an industry leading CREST, SOC 2, NSA-CIRA, CSA-STAR certified independent third-party to conduct application-level penetration tests and remediates findings based on its business requirements and internal risk management framework. Penetration tests are conducted at least annually or when major changes are made to the system. ECI's policy is to use commercially reasonable efforts to remediate all critical findings within 30 days or within a reasonable timeframe with a provided business case. ECI does not disclose details regarding our security controls or results of penetration testing as that information is proprietary and confidential and in the wrong hands can lead to increased risk.

Data Privacy and Legislation

General Data Protection Regulations (GDPR)

As of May 2018, the European Union's General Data Protection Regulations (GDPR) came into full effect. The GDPR replaces the Data Protection Directive 95/46/EC and is designed to strengthen and unify data privacy laws across Europe.

ECI has implemented a structured and comprehensive GDPR compliance program. The program consists of, among other things, training of staff, audit and risk assessment across the business, policies and procedures, governance, and ongoing compliance efforts. We encourage our customers to take similar steps to ensure their own businesses comply with GDPR and for the years to come.

The Printanista products do not process, monitor, or manage any personal records or any records or information specific to any one person or group of persons.

Printanista software applications do not collect, house, or transmit any information regarding the content of print jobs.

Printanista has no way of accessing, housing, or transmitting high risk information, even if this information is printed or otherwise sent to print devices monitored by Printanista software applications.

Printanista software applications do not store, process, or transmit cardholder data or personal information.

The product engine communications are controlled, using limited access to contact specific IP address and/or range.

All communications must originate from the Printanista products, and there is no way to contact and access the products from outside the network.

Communication outside of the network uses a proprietary, compressed data stream that is sent using industry-standard SSL over HTTPS.

For information related to compliance of specific laws and/or regulations, please contact your ECI Account Manager.

The following is a link to the ECI Cloud Security: [ECI Cloud Security Overview 2021 (ecisolutions.com)]

Frequently Asked Questions (FAQs)

Do Printanista products work with Internet proxies?
Yes, ECI DCA can work with most proxies. Configuration of the Proxy settings is required on the system where the ECI DCA is installed and operates.
What are the Printanista Hub, ECI DCA, Onsite minimum requirements?
Please refer to the Printanista Application Requirements section in this document.

Is Printanista Products compatible with Mac, Linux, or Raspberry Pi environments?
This ECI DCA brings about major advantages over Onsite DCA without losing any features, including full native cross-platform support of Windows, macOS, Linux, and Raspberry Pi. Each with unique installation steps, support documentation, and trained support staff on these platforms. The installation process has also greatly improved and is much more intuitive for all types of users.

Does ECI DCA require Microsoft Internet Information Services (IIS)?
No. ECI DCA and Onsite DCA includes its own server to host the web-based User Interface (UI) and is set up automatically during the installation.

Can you install ECI DCA on a computer which already hosts another IIS website?
Yes. However, the below listed ports must be whitelisted to ensure connectivity of ECI DCA.

Service	Port	Connection To
Data Upload	**443/TCP** (HTTPS)	Your Printanista Hub Server
Software Updates	**443/TCP** (HTTPS)	ECI Updates Server
Registration (fallback)	**53/UDP** (DNS)	Local Network DNS server (primary) ECI Updates Server (fallback)

ECI DCA uses port 31816 by default for the local DCA Web-based User Interface.

How much ongoing maintenance does ECI DCA require?
ECI DCA and Onsite DCA is a service which runs in the background and performs audits and exports to configured destinations on predefined schedules. It is recommended to use subnets (IP ranges) instead of fixed IPs. When adding new devices to the network they will be discovered and included in the audit results, limiting manual intervention.

Which brands of equipment will Remote Device Link (RDL) monitoring work with?
What are the requirements for it to work?
All brands with an embedded webpage are discovered by ECI DCA. The information on the embedded webpages will vary by manufacturer and model. Local devices will not show the embedded webpage.

Are there added security concerns with Remote Device Link (RDL)?
A secure channel is opened between the device on the local customer network and an operator located outside of that network. RDL will only report back devices discovered and actively monitored through ECI DCA. A message appears indicating device connection is not supported through the DCA

Remote Device Link (RDL) seems a bit slow, why is this?
This can be expected as the connection needs to be tunneled through our cloud services. However, the main influencing factor is how quickly the devices respond to Web User Interface (UI) requests.
We have seen devices responding in tenths of seconds to the first connection attempts, to being influenced by current usage or resources available for the User Interface (UI).

What features are available with Remote Device Link (RDL)?
Any options the OEM provides access to through the embedded webpage are accessible through Remote Device Link (RDL).

Can the Remote Device Link (RDL) feature be turned off?
Yes, there is the ability to switch this feature off per account.
It is also possible to turn this feature off per user, allowing you to block a user's access to Remote Device Link (RDL).

Where do I get additional information for Printanista Hub, ECI DCA, legacy Onsite DCA, etc.?
Additional information can be found on the ECI's Printanista website:
https://www.ecisolutions.com/products/printanista-hub/

Legacy Onsite DCA Information

ECI DCA is recommended to be used with Printanista. However, legacy Onsite DCA currently functions with Printanista.
PC/Server requirements for Onsite DCA:

- 1GB RAM
- 400 MB Disk Space
- Microsoft .NET Framework 4.7.2 or newer
- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- Onsite Version 4.1.3 and newer supports Windows Server 2022
- Internet Explorer 11.0 or newer, Chrome, Firefox
- MDAC 2.8 or higher (normally included when Windows is installed)
- JET 4.0 or higher (normally included when Windows is installed)
- Loaded on a machine that is up 24/7 or at least the entire business day
- Must be logged on as a Local Administrator (or equivalent) during the installation

Outbound Firewall considerations (Port 80 or 443):

Data transmission:

- https://(company_Printanista_FQDN)/WebServices/Onsite2Service.asmx
- Application: fmaonsite.exe
- SOAP over HTTP(s) must be allowed past firewall

Network Requirements:

SNMP (Port 161) traffic must be routable across the LAN or WAN (Wide Area Networks)

Please use ECI DCA if macOS, Linux or Raspberry Pi operating systems are necessary
The legacy Java Onsite on Linux and macOS Systems is non-functional.

PC/Printer requirements for using the Local Agent (Optional installation):

- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- Microsoft .NET Framework 4.7.2 or newer
- Current driver for the local printer (UPD is recommended for HP devices)
- Printer must support Printer Job Language (PJL) or Printer Management Language (PML)
- Remove any unused print drivers
- Driver's bi-directional support is enabled
- Windows Firewall modifications — Port 161/33333 inbound/outbound for both TCP and UDP

Microsoft-supported versions of Windows and Windows Server. Versions no longer supported by Microsoft are not supported by ECI.

Note: For recent Operating System versions using driver model 4 (e.g., Windows 10), only Kyocera and Ricoh OEMs, and their variations, are supported currently.

Network Discovery and Meter and Supply Collection (Onsite DCA)

The Printanista patented Automatic Network Discovery Settings use a mixture of algorithms to identify the network ranges where print devices may be located and then discover and communicate with the devices that are online, routing through multiple network elements such as active workstations or servers, routers, hubs, switches, and additional network hardware.

Printanista Hub administrators can remotely manage activated Onsite DCAs (Data Collection Agent) on the server as well as remotely trigger the Onsite to execute predefined commands such as data collection tasks, providing Onsite logs, running remote MIBWalks, installing HP JAMC, or updating Onsite settings. These are explained in further detail below:

Function	Location	Description
Tasks	Onsite Settings	Can remotely configure tasks to run on a preset schedule but can select tasks (Cache, Meters, Supplies, Service) to run immediately and collect device data on command.
MIB Walks	Onsite Settings	Can indicate certain IPv4/IPv6/Hostnames of devices and trigger the Onsite to Start the Collection of the MIB Walks immediately.
Logs (Detailed)	Onsite Settings	Can instruct the Onsite to collect the Logs (Critical, Error, Warning, Details, Debug) from a certain date.

None of these commands lead to data collection beyond the types of information collected as described above. Data exchanged between Onsite DCA and Printanista Hub is encrypted using strong encryption protocols that are FIPS compliant. Onsite receives secure software updates from the Printanista Updates servers.

The legacy Onsite DCA communicates with Printanista at a predefined interval to determine if there are any queued actions not already executed. This ensures actions are executed in a timely manner.

Note: Onsite DCA always initiates this communication to the Printanista server, and not the other way around.

Note: HP JAMC is only supported while used in conjunction with the legacy Onsite DCA at the initial launch of Printanista.

Network Traffic

Audits conducted by the software use an intelligent system to extract minimal information for each printer, copier, or MFP. Unlike similar products that send a fixed set of queries (a superset of all possible queries) to every networked device, Onsite DCA only sends the relevant queries according to the fields the target device supports, with each device query being no more than a few kilobytes of data. To further reduce the amount of network bandwidth used, Onsite DCA communicates with no more than 20 devices at a single time. Each IP within the configured ranges will be queried and if no response is received within the configured timeout period it will move onto the next IP address. A rule-of-thumb is Printanista will gather information on approximately 65,000 devices in just under one hour.

Manufacturer Support

Printanista products are manufacturer neutral. They support all major manufacturers and model families. Some devices have limitations preventing extraction of certain information.

Virus Concerns

The Printanista application files have been digitally signed to prevent execution if the file integrity is compromised. This ensures if any virus may be present is not activated and prevents spreading the virus from one network to another. For added assurance, we recommend using antivirus software on your network.

ECI will provide support services exclusively for the latest commercially available release of the Software, as well as the immediately preceding version of the Software. This policy applies to all ECI Device Management products.

