Technisches Whitepaper zum Printanista Hub

Version 1.5

Inhaltsübersicht

eci Printanista

Übersicht

Die Printanista Hub Familie von Produkten liefert eine Firmen-entsprechende Managed Print Lösung, die einfach zu installieren und benutzen ist. Sie ist entworfen und entwickelt unter Nutzung der Vorteile der modernen Features der Microsoft .NET Plattform. Das bedeutet, dass keine hochqualifizierten Techniker für die Installation, der Konfiguration und der Wartung der Software nötig sind. Printanista kann nicht in der Weise umkonfiguriert werden, um andere Aufgaben zu erfüllen als diejenigen, für die sie gedacht ist. Die Übertragung von Daten von der eigentlichen lokalen Software an außen betriebenen Quellen wird maximal kontrolliert und ist streng begrenzt. Die Software liefert keine anderen Details als die technischen Druckerdaten, die erfasst werden sollen. Es werden niemals vertrauliche Informationen aus dem Netzwerk des Kunden über Printanista übertragen. Die Software Suite besteht aus den folgenden Komponenten:

Printanista Hub: Eine Website, also ein Backendsystem, das alle Daten erfasst und speichert, die es vom Printanista Data Collection Agend (DCA) erhält. Es ist ein Datendepot um die Daten unter Nutzung eines Browsers zu sehen, Berichte zu generieren, Alarm Workflows und Mitteilungen zu konfigurieren und Daten zur Rechnungserstellung und automatischen Supply Lieferung mit eine ERP System zu synchronisieren.

ECI DCA: Der neueste Data Collection Agent-DCA liefert die Hauptvorteile über die onsite Daten Erfassung einschließlich einer der Unterstützung durch Plattformen wie Windows, macOS, Linux, and Raspberry Pi. Jede erfordert spezifische Installationsschritte, spezielle Dokumentation und Trainings für die Plattformen. ECI DCA liefert ebenfalls laufende Entdeckung und Scannen von Geräten, verbesserte MIB Walk- und Log-Erfassungsmöglichkeiten sowie mehr Zählerstände, die jetzt erfasst werden können.

Onsite DCA: Ein Data Collection Agent führt automatische Druckererfassung aus und überwacht Verbrauchsmaterial Levels, den Druckerstatus, und die Fehler Logs. Diese Software ist auf der Kundenseite installiert und kann die Printerüberwachung automatisch nach einem Zeitprogramm ohne menschliche Intervention durchführen. Die erfassten Daten werden zum Printanister Hub Server unter Benutzung von HTTPS, HTTP oder mit kundeneigener Verschlüsselung geschickt.

WebAudit Assessment Tool: A Ein Druckerdaten-Erfassungs Tool, das Teil des Printanista Hub Servers ist. So können Flotten Audits direkt vom Browser aus ausgeführt werden, ohne das seine Software beim Kunden installiert wird. Die erfassten Daten werden direct an den Printanista Hub Server geschickt.

Der Zweck dieses Dokumentes ist es, eine Übersicht über die Printanista Suite aus technischer Sicht zu geben, um Antworten auf die meist gestellten Fragen, die das technische Team erhielt, zu geben.

eci Printanista

Wie funktioniert Printanista Hub?

Der Data Collection Agent (DCA) ist das Herzstück der Software, das korrekt Daten von Network Printern, Kopierern und MFP´s identifiziert und herausfiltert, dessen Protokoll dem Erfassungstool entspricht.

Printanista unterstützt (Simple Network Management Protocol) SNMP v1, v2c und v3 Protokolle. SNMP v3 liefert eine erhöhte Paketsicherheit, um Informationen und Kommunikation über zuverlässige Quellen zu lenken. Im Gegensatz zu SNMPv1 oder v2 ist SNMP v3 zur Erhöhung der Sicherheit verschlüsselt und benötigt einen Usernamen und ein Passwort. Ein Vorteil von SNMP v3 ist, dass der Administrator eine Verschlüsselungsmethode sowie einen Usernamen und ein starkes Passwort festlegen kann.

SNMP ist ein Network Protokoll, das Informationen zwischen Netzwerkgeräten transportiert, die aus der MIB (Management Information Base) der Geräte oder anderer Quellen in den Geräten gewonnen gesammelt werden. The Management Information Base (MIB) ist eine geräteinterne Database, welche die meisten Netzwerkgeräte als Teil Ihre IT Architektur besitzen. Die MIB liefert z.B. Aussagen über Modellnamen, Tonerlevels und Status der Drucker.

Printanista System-Anforderungen

Printanista Hub Backend Server

Printanista Hub Product Specifications

	Printanista Hub 5.0	ECI DCA 1.5	Onsite 4.1	Viewer 3	WebAudit on v4	Agent 4	Microsoft Support	Notes
Supported OSes[1]								
Windows 7 SP1 (32/64)	No	Yes	Yes	Yes	Yes	Yes	~~April 2015~~ January 2020	
Windows 8 (32/64)	No	Yes	No	No	No	Partial[3]	~~April 2018~~ ~~January 2023~~	
Windows 8.1 (32/64)	No	Yes	Yes	Yes	No	Partial[3]	~~April 2018~~ ~~January 2023~~	
Windows 10 (32/64)	No	Yes	Yes	Yes	No	Partial[3]	~~October 2020~~ October 2025	
Windows Server 2003 (32/64) Internet Information Services 6[2]	No	No	No	Yes	Yes	Yes	~~April 2010~~ ~~April 2015~~	
Windows Server 2008 (32/64) Internet Information Services 7.0	No	No	No	Yes	Yes	Yes	~~April 2015~~ ~~January 2020~~	
Windows Server 2008 R2 (32/64) Internet Information Services 7.5	No	Yes	Yes	Yes	Yes	Yes	~~April 2015~~ ~~January 2020~~	
Windows Server 2012 Internet Information Services 8.0	No	Yes	Yes	Yes	Yes	Yes	~~October 2018~~ ~~January 2023~~	
Windows Server 2012 R2 Internet Information Services 8.5	No	Yes	Yes	Yes	Yes	Yes	~~October 2018~~ October 2023	
Windows Server 2016 Internet Information Services 10	Yes	Yes	Yes	Yes	Yes	Yes	January 2022 January 2027	Recommended by ECI
Windows Server 2019 Internet Information Services 10	Yes	Yes	Yes	Yes	Yes	Yes	January 2024 January 2029	Recommended by ECI
Linux (x86/64 or ARM) Debian, Ubuntu and similar distributions	N/A	Yes	No	No	No	No	---	Mono 5.4 or higher required
macOS (x64) Sierra (10.12 or higher)	N/A	Yes	No	No	No	No	---	Mono 5.4 or higher required
Raspberry Pi 4B, 3B+, 3B, 2B	N/A	Yes	No	No	No	No	---	8GB or larger SD card required

Benutze den folgenden Link, um auf die komplette Printanista Produktspezifikation zu kommen: SysReq v3.0.html

Alle gesammelten Daten werden zum Printanista Hub Server gesendet, wo sie für Reports und Alarme zur Verfügung stehen. ECI DCA verbindet sich mit dem Printanista Hub Server über HTTPS (port **443/TCP**). Bitte fragen Sie Ihre Support nach Informationen über Domain Namen und IP Adressen, die Ihr Server hat. Diese Verbindung ist geschützt durch den Indutriestandard **TLS** (Transport Layer Security). **TLS 1.2 ist empfohlen. (**TLS 1.0 and TLS 1.1 are currently supported but not recommended for security purposes. Support for TLS 1.0 and TLS 1.1 will be discontinued in the future).

This Diese Verbindung ist offen über die gesamte Zeit, in der die DCA arbeitet. Normalerweise wird eine **WebSocket** Verbindung benutzt, aber in einigen Fällen gibt es ein fall back der ECI DCA und sie benutzt entweder **server-sent events** oder **HTTP long polling**.

IMPORTANT NOTE: Mehrere Secure HTTPS outbound Verbindungen werden von dem Server gefordert, auf dem Printanista Hub installiert ist:

- 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

Printanista Anwendungsanforderungen

Data Collection Agent (ECI DCA)

Drucker, Kopierer und MFPs müssen das SNMP Protokoll (Port 161) unterstützen, was zur Gewinnung der Daten benötigt wird. Das SNMP Protokoll ist ein Standard der Application Layer von TCP/IP.

PC/Server Anforderungen für ECI DCA:

Microsoft Windows (x86/64)

Anforderungen:

- Windows 10 oder höher
- Windows Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, Server 2019, and Server 2022
- Microsoft .NET Framework 4.7.2. oder neue

Linux (x86/64 or ARM)

Anforderungen:

- Ubuntu 14.04, 16.04 or 18.04, Debian 9.5+, Raspbian Jessie or Stretch, RedHat Enterprise 7.5+, CentOS 7.5+, Fedora 28+
- Mono 5.4 oder höher

macOS (x64)

Anforderungen:

- Sierra (10.12) oder höher
- Mono 5.4 oder höher

Raspberry Pi 2 Model B, Raspberry P 3 Model B, Raspberry Pi 3 Model B+, and Raspberry Pi 4 Model

Anforderungen:

- Blank 8GB or larger microSD card
- PC capable of writing to microSD card

Firewall Beachtungen für ECI DCA:

Inbound Connections

Es gibt keine inbound connections vom Internet zur ECI DCA.

Outbound Connections

Service	Port	Connection To
Data Upload	**443/TCP** (HTTPS)	Ihrem 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 ist ein Server, der vom ECI Device Management der betrieben wird, um die DCA Registrierung, automatische Software updates und DCA Installationen (this site) auszuführen und wird für den Betrieb der ECI DCA benötigt. Note: ECI DCA sendet keine gesammelten Geräte Daten oder Konfigurationsdaten an den ECI Update Server.

Software Updates

ECI DCA auto-updates selbst erforgen durch Downloads von: https://updates.printanista.net/ . Die Verbindung ist immer nach dem Standard HTTPS Protokoll port **443/tcp** geschützt.

Registration

ECI DCA benutzt einen DNS requests an `*.reg.pf-d.ca` um sich zu registrieren. Es versucht zunächst dies über den lokalen DNS Server und geht dann in den Fall back , um direkt mit dem ECI Updates Server IP Adresses (using port **53/udp**) zu kommunizieren. Die Firewall muss nur diese Verbindung zum ECI Update Server, wenn der lokale DNS Server die Registration nicht ausführt.

Service Region

ECI DCA wird zu dem Server geroutet, der die geringste Latenzzeit basierend auf der Service Verfügbarkeit hat. In bestimmten Orten kann die Server Region gelegentlich wechseln je nach Auslastung des Internets.

Gesammelte Daten und Verschlüsselung

Data Encryption

Alle Daten Pakete der ECI DCA sind verschlüsselt und verschleiert. Printanista erfordert HTTPS zur Kommunikation zwischen DCA's und Printanista Hub. ECI DCA erfordert HTTPS, um zu funktionieren. Zusätzlich sind alle sensitive Dateneinstellungen und Routinen zwischen ECI DCA und Printanista unter Gebrauch des „AES256 Standard symmetric encryption algorithm", verschlüsselt durch Gebrauch eines gemeinsamen geschützten Schlüssels. Die sichert eine end2end Verschlüsselung, was bedeutet, dass die Daten vor dem Lesen durch Dritte nicht autorisierte Personen geschützt sind.

Sicherheitsaspekte

ECI DCA und die Historie auf der DCA Seite ckommuniziert mit dem Printanista Hub über das HTTPS Protokoll unter Benutzung des Industrie Standards **TLS 1.2** (Transport Layer Security). Vertrauliche Daten werden nicht erfasst oder gesammelt, gezeigt oder gar gespeichert durch die Printanista Anwendung. Nur Drucker bezogene Daten warden erfasst und angezeigt. Andere Netzwerkdaten können weder identifiziert noch von der ECI DCA gesammelt warden, mit Ausnahme der IP Adressen, MAC Adressen und des Hostnamen.

ECI DCA erfasst und sammelt keine Personendaten. Die einzige Möglichkeit, dass Printanista diesen Typ von Informationen sommelt, ist, wenn der Kunde Daten in die Felder "Ort" oder "Kundenname" einträgt. ECI DCA befähigt sie, Netzwerk Geräte unter Nutzung des SNMP Protokolls zu überwachen. Die Anwendung wird innerhalb des Kundennetzwerkes installeir, um Geräteinformationen zu gewinnen, die Netzwerkgereäte aus der Firmware und aus der Management Information Base (MIB)zur Verfügung stellen. Die Daten, die gewonnen werden können, hängen in starkem Maße vom Hersteller und vom Gerätemodell ab. Die am meisten verwendeten MIB Daten sind im Dokument IETF RFC 3805 (https://tools.ietf.org/html/rfc3805) zu finden. Manche Hersteller haben zusätzlich eine Privat MIB, aber deise Daten sind sehr technisch und spezifisch.

Printanista Hub speichert nur:

- 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.

Informationsdaten, die erfasst werden

ECI DCA versucht, die folgenden Infromationen von Netzwerkdruckern zu durch einen Netzwerkscan zu gewinnen:

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

Netzwerk Neu-Erfassung und Data Collection

Um die Effizienz der DCA zu erhöhen, werden nur neue oder geänderte Daten der Netzwerkgeräte zum Printanista Hub Server gesendet. Das sichert eine minimale Netzwerkauslastung und reduziert die Häufigkeit von Backlogs. Ausserdem sind Neuerfassung und normales Scannen der Geräte voneinander unabhängig und sichert, dass nur die IP Adresse (hostname) der zuvor entdeckten Geräte und nicht alle Geräte im gesamten netzwerk immer wieder zeitaufwändig gescannt werden.
(das wird am Anfang ausgeführt, periodisch oder wenn der Admin es anders festlegt).

Das sichert, dass die Geschwindigkeit der Datenübertragung so aktuell wie möglich ist. Dies ermöglicht dem Benutzer über Fehler innerhalb von Minuten oder Sekunden informiert zu werden. ECI DCA separiert ausserdem Erfsassungsscans von Scan Typen für Zähler, Supplies, Fehler und andere Parameter, um die Möglichkeit zu geben, kundenspezifische Scanfrequenzen einzustellen. Die Standard Einstellungen für max. und min. Werte sind in der Tabelle zusammmengefaßt:

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

Es ist zu beachten, dass die Scan-Intervalls (meters, supplies, errors, and attributes) nur zur Verfügung stehen, wenn die Geräte ein Model Definition File (MDF) haben. Wenn dieser nicht zur Verfügung steht, wird in voller Scan auf den in Frage kommenden Geräten gemacht unter Nutzung des vorbestimmten Scan Intervalls.

Der Printanista Hub Administrator kann die ECI DCA, die auf dem Server aktiviert ist, aus der Ferme managen. Er kann remote die ECI DCA triggern, bestimmte Kommandos auszuführen, z.B. Daten Erfassung, Bereitstellung von DCA logs, ausführen von remote MIB walks oder Updates der DCA Einstellungen.

Note: ECI DCA initiiert immer die Kommunikation zum Printanista Server und nicht umgekehrt.

Note: Nur wenn Zähler-, Supply- oder Fehlerinformationen upgedatet oder gewechselt haben, werden Informationen gesendet, um die Bandbreite zu reduzieren.

Note: HP JAMC funktioniert zur Zeit nur mit legacy Onsite.

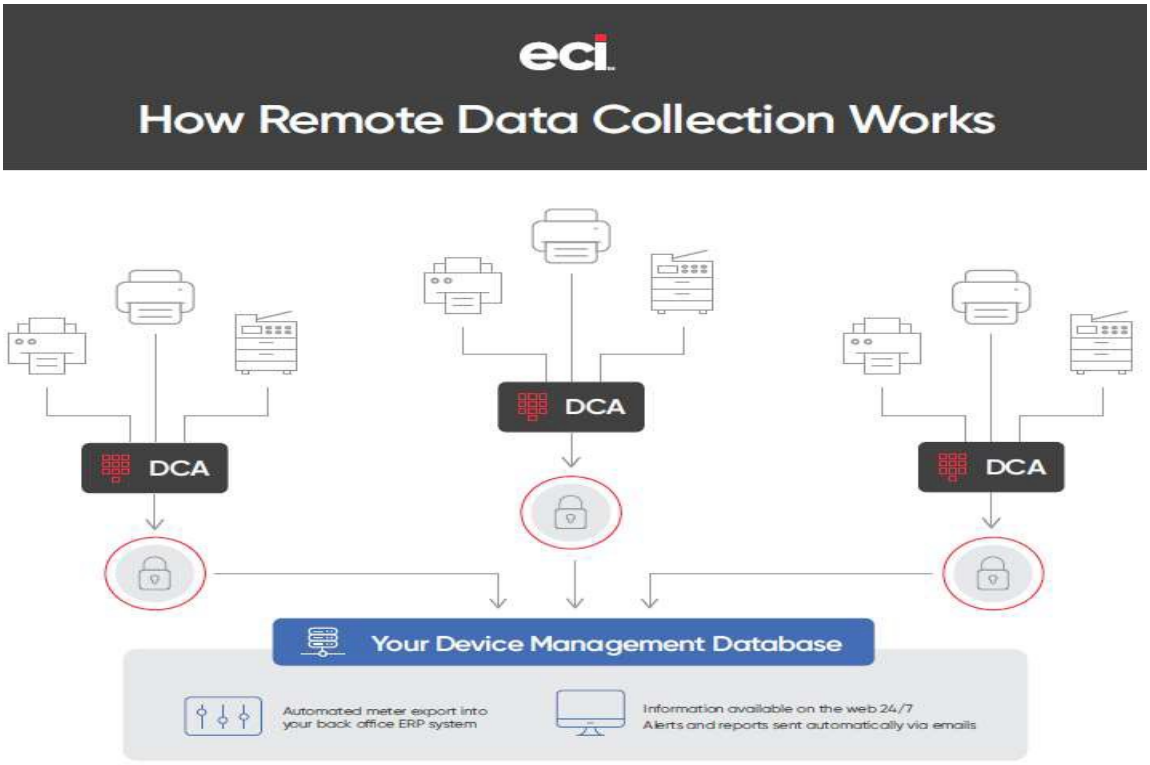
Lokale Drucker

Printanista Workflow

Printanista Workflow ist ein zuverlässiges Druck Management Werkzeug. Printanista Workflow kann dabei helfen, die Kosten beim Dukumenten Output zu reduzieren, die Dukumentensicherheit zu erhöhen und flexible Kostenzuordnung zu Kunden zu realisieren. Unter Benutzung eines vereinfachten Installationsprozesses können ihre Kunden alle Druckinformationen an einem Punkt zusammengefasst überblicken. Befähigen sie Ihre Kunden, kosten zu reduzieren durch Verstehen jedes gedruckten Dokuments, das die produzieren.

Was ist Printanista Workflow?

Printanista Workflow ist die neueste Generation unserer User-Management Software, die weltweit Managed Printservice für Hunderte von Organisationen und Geschäftsfelder gewährleistet. Wenn sie das ältere User Management System (PA 6) kennen, werden Sie über erfreut sein über die Installation und Konfiguration der Anwendung. Die Menüs, Werkzeuge und die gesamte Administration des System wurde beibehalten. Wenn sie ein Upgrade von PA6 auf diese neue Version vornehmen, wird für sie alles vertraut erscheinen.



Wie arbeitet Printanista Workflow (through the ECI DCA data is collected from Workflow)

Printanista Workflow ist die nächste Generation unseres Device Managements , die nur mit der ECI DCA arbeitet.
Printanista Workflow arbeitet nicht mit einem Onsite DCA.

-Workflow Client kann auf einem MAC und einem Windows Operating System desktops installiert werden, der local über eine USB Verbindung die Zählerstände erfasst.
-die Zähler werden aus dem Spooler, der Anwendung oder dem Treiber gewonnen.
-die Zähler werden in der Workflow Database gespeichert.
-ECI DCA fragt die Zähler Information vom Workflow via API Call (Application Programming Interface) an einen Webservice
-ECI DCA liefert Data an Printanista Hub
-Workflow zur ECI DCA ist verschlüsselt (https)

Printanista Workflow System Requirements

Server und Admin Tools

Printanista Workflow Server Komponenten können installiert werden auf:

- Microsoft Windows Server 2012 R2 oder neuer
- Windows 8 Professional oder neuer

(64bit) Eine vollständige Server Installation
erfordert:

- mindestens 5 Gigabytes freien Speicher, um die Workflow Software zu unterstützen.
- SQL Database und SQL Express 2012 sind erforderlich. SQL Express 2012 wird installiert, wenn nicht vorhanden.
- Internet Information Service (IIS) ist notwendig und wird installiert, falls nicht vorhanden
- Microsoft .NET Framework 4.7.2 ist nötig und wird installiert, falls nicht vorhanden.
- In der Standardausführung werden alle Druckjobs und Logs auf diesem Server gespeichert.

Important: Microsoft Home und Microsoft Small Business Server werden nicht unterstützt.

Windows Client Requirements und Memory Usage:

Printanista Workflow Client Popup Software kann auf allen Computern mit Microsoft Windows 8 oder neuer installiert werden.

- Eine volle Installation erfordert etwa 10-20 MB Speicher. Der Client ist

ausgeführt als: Desktop Client und als Client Service

- Der Desktop Client benötigt zwischen 5 – 20 Megabytes, abhängig vom Jobumfang.
- Keine weitere Software wird benötigt.

System Requirements für den Workflow Client für Mac®

- Workflow Client for Mac® wird von Mac® OS gemäß Apple's Support.
- Mac® Client unterstützt nur die neuste und 2 frühere OS Versionen
- Workflow Client for Mac® benötigt auch 1 Windows-based PC zum Hosting des Workflow Servers und der Database.

Important: Printanista Workflow muss in einem Netzwerk mit mindestens einem Windows Computer.

IIS Web Server Support

Workflow benutzt Internet Information Services (IIS), um mit den Geräten und intern zwischen den Workflow Komponenten zu kommunizieren. Die Installation erfordert die vollständige Version von IIS. Der Installer stellt fest, ob eine IIS Version schon existiert. Wenn nicht, erzeugt der Installer einen neuen Standort und Anwendungspool unter Benutzung von IIS.

Netzwerk Anforderungen

Printanista Workflow benutzt Standard HTTP/SSL Kommunikation über die Ports 80/443 für Web Services. Falls dies Port nicht zur Verfügung stehen, wird der Workflow 6320/6321 benutzen. Wie auch immer, die Kommunikation Ports können geändert werden, falls es Konflikte im Kundennetzwerk gibt.

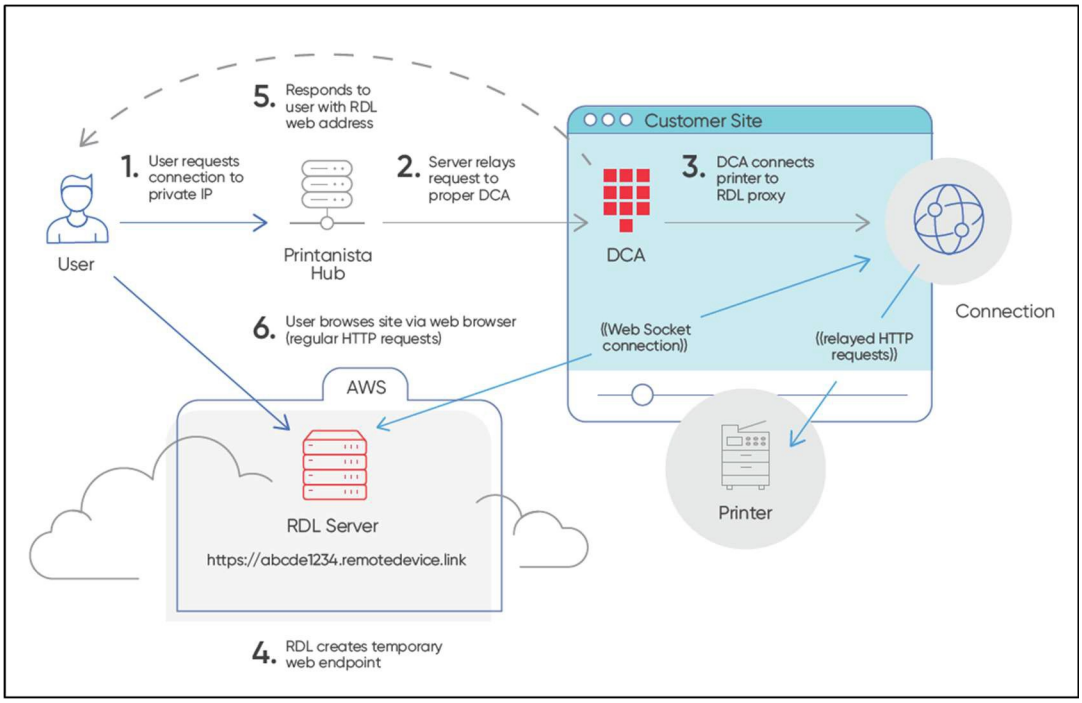
Daten, die die ECI DCA an den Workflow Server liefert:

Beispiele einiger Geräte Indentifikationsdaten wie: Hersteller, Model, IP Adresse, Serial/Asset Nummer, Standort, Color/Monochrome Seiten, Color/Monochrome Drucke, etc.

Printanista Workflow Help Dokumentation kann hier eingesehen werden:

Printanista Workflow Help

Remote Device Link (RDL)



System Überblick – Remote Device Link (RDL)

Remote Device Link (RDL) ist ein Service, der es entfernten Benutzern erlaubt, einen HTTP Endpunkt in einem privaten LAN zu erreichen. Dazu gehören 4 Hauptkomponenten:

1. Ein **Benutzer,** der auf das Gerät aus der Ferne zugreift
2. Der **Remote Device Link Server**, im Public Internet (via https://*.remotedevice.link URL)
3. Der **RDL client** (embedded in the DCA), der im privaten LAN arbeitet
4. Der **HTTP Endpunkt** (Drucker, auf den zugegriffen wird

Sicherheit: Ports and SSL (Secure Sockets Layer)

Der public Path für RDL ist immer https:// URL auf Port 443, unabhängig vom Endpunkt Port und/oder SSL Status.

Befähigung des Systems und Erlaubnisse

1. Allgemeine Befähigung der Option für einen Händler
2. Lokale Befähigung je Endkunden Account
3. Erlaubnis für die Person, um diese Option zu nutzen

Prüfungsmöglichkeiten

1. Printanista Hub lokale Prüfungsmöglichkeit jeder Aktion
    a. Printanista Hub Administration Berichte für jede RDL Aktion
2. Remote Device Link (RDL) AWS (Amazon Web Services) Cloud logging aller Session Details

Remote Device Link (RDL) Sicherheit

Bei der Entwicklung des Remote Device Link (RDL) stand die Sicherheit im Mittelpunkt

Notwendige Berechtigungen:

- Der Nutzer muss eine Berechtigung zur Nutzung des RDL für den speziellen Account haben.
- Der Data Collection Agent (DCA) akzeptiert nur eine Remote Device Link (RDL) Anforderung vom Printanista Hub Server, die gegenseitig authentifiziert ist
- Der Data Collection Agent (DCA) baut nur eine Remote Device Link (RDL) Verbindung zu bekannten und als "Monitored" eingestuften Geräten und innerhalb des eingestellten IP Bereiches der DCA auf.
- Jeder individuelle Web Request muss an dieselbe IP Adresse gerichtet sein.– Der Data Collection Agent (DCA) befolgt keine Redirect Umwege.

Verbindungssicherheit:

- Alle Verbindungen zum/vom Remote Device Link (RDL) zum/vom Printanista Hub sind verschlüsselt nach dem Standard TLS 1.2 (Transport Layer Security)
- Jede Verbindung hat einen einzigartigen Domain Namen mit einer 19-stelligen (96-bit) zufälligen erzeugten Buchstaben/Zahlenkombination
- Jeder Request erfordert einen 160-bit security token, der als Browser Cookie gespeichert ist und zu Beginn der Session mit einer TSL Verschlüsselung gesetzt wird.
- Die Data Collection Agent (DCA) kann may establish eine nicht-verschlüsselte HTTP Verbindung zum Gerät über das locale Netzwerk herstellen, aber unterstützt auch TLS 1.2, wenn das Gerät dies kann.

Session Time Limits:

- Jede individuelle Remote Device Link (RDL) Session läuft standardmäßig nach 20 minutes Inaktivität aus und läßt sich auf maximal 2 Stunden erweitern

Schlussfolgerungen:

Die Verbindung zwischen ECI DCA und Printanista Hub sind mit einem Authentication Keys , der installationsspezifisch ist, geschützt und die Verbindung verlangt nach einem gültigen SSL Zertifikat für die Verbindung über TLS.

Alle Kommunikation von der DCA über das Internet ist verschlüsselt. Trotzdem kann die ECI DCA im lokalen Netzwerk über das einfache HTTP Protokoll mit den Geräten kommunizieren, falls das Gerät keine Secure Connection unterstützt.

Printanista Hub Application

Die Printanista Hub Funktionalität ist über ein Web-based Userinterface zu bedienen. Die Zugrifferlaubnis basiert auf einem User Management

Zugang zum Printanista Hub Web-Frontend wird durch eine benutzerbasierte Berechtigungsverwaltung kontrolliert. Benutzer müssen sich bei Printanista mit einem festgelegten Benutzernamen und Passwort anmelden. Benutzern werden eine oder mehrere Rollen zugewiesen, die Berechtigungen festlegen, und sie erhalten Zugriff auf eine oder mehrere Gruppen von Geräten. Administratoren mit vollen Berechtigungen können genau festlegen, welche Bildschirme jeder Benutzer anzeigen und/oder mit ihnen interagieren kann.

HTTPS-Zugang Printanista erfordert, dass alle Websites HTTPS mit einem gültigen SSL-Sicherheitszertifikat verwenden. Dies gewährleistet die Verschlüsselung von Daten, die über das Internet übertragen werden.

Printanista Side-By-Side Printanista Hub verwendet eine Modell-Metadatenbank namens Side-by-Side (SBS), die verschiedene Modellattribute wie Druckgeschwindigkeiten, Markteinführungszeitpunkte oder Kompatibilität mit OEM-Teilenummern enthält, die regelmäßig aktualisiert werden, wenn zukünftige Modelle und Versionen von OEMs veröffentlicht werden. Printanista Hub wird mit Side-by-Side kommunizieren, um nach neuen Updates zu suchen und Gerätemetadaten abzurufen, um sie lokal auf jedem Printanista-Hub-System zu zwischenspeichern.

Printanista Hub Anwendungs-Hosting Printanista Hub wird von ECI Software Solutions in sicheren und geschützten Rechenzentren in verschiedenen Regionen der Welt gehostet. ECI Software Solutions versteht, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen unserer Kunden für ihren Geschäftsbetrieb und unseren eigenen Erfolg entscheidend ist. Wir verwenden einen mehrschichtigen Ansatz, um diese wichtigen Informationen zu schützen, überwachen und verbessern ständig unsere Anwendung, Systeme und Prozesse, um den wachsenden Anforderungen und Herausforderungen der Sicherheit gerecht zu werden. ECI-Sichere Rechenzentren Unsere Dienste sind in dedizierten Bereichen in Rechenzentren der Spitzenklasse untergebracht. Diese Einrichtungen bieten Trägerunterstützung. Klicken Sie auf den folgenden Link, um das detaillierte Dokument von ECI zum Thema Datensicherheit der Rechenzentren zu erhalten.

ECI Cloud Security Overview 2021 (ecisolutions.com)

Versionsmanagement-Test- und Freigabeprozess

Jede Haupt- und Nebenversion der Software durchläuft einen Qualitätskontrollprozess, bei dem mehrere Mitarbeiter von Printanista geänderte Teile des Systems einer Regressionstest unterziehen, um sicherzustellen, dass es keine Verschlechterung der Sicherheit oder Funktionalität des Systems gegeben hat, sowie die neuen funktionalen Aspekte validieren. Hauptversionen durchlaufen einen Beta-Freigabeprozess, bei dem ausgewählte Kunden die neuen und alten Systeme parallel ausführen.

Quellcode-Sicherheit

Der Quellcode von Printanista wird in einem gesicherten Revisionskontrollsystem aufbewahrt, das nur autorisierten Personen zugänglich ist. Jede Änderung am Quellcode erfordert die Zustimmung von zwei autorisierten Entwicklern, bevor sie im Produktionscode-Repository akzeptiert wird, wo jede Änderung nachverfolgt wird, einschließlich des Entwicklers, der die Änderung vorgenommen hat und warum.

Produkte werden vor dem Versand verschlüsselt und digital signiert mit einem vertrauenswürdigen Code-Signaturzertifikat. Ein Treuhandkonto kann auf Anfrage zur Verfügung gestellt werden.

ECI beauftragt eine der führenden CREST, SOC 2, NSA-CIRA, CSA-STAR zertifizierten unabhängigen 3rd Party Firmen, um einen anwendungsbezogenen Test durchzuführen, der die Geschäftsanforderungen des Risikomanagement nachweist.

Penetrationstests werden mindestens einmal jährlich durchgeführt oder wenn wesentliche Änderungen am System vorgenommen werden. Die Politik von ECI besteht darin, kommerziell angemessene Anstrengungen zu unternehmen, um alle kritischen Ergebnisse innerhalb von 30 Tagen oder innerhalb eines angemessenen Zeitrahmens mit einem bereitgestellten Geschäftsfall zu beheben. ECI gibt keine Details zu unseren Sicherheitskontrollen oder Ergebnissen von Penetrationstests preis, da diese Informationen proprietär und vertraulich sind und in falsche Hände geraten könnten, was zu erhöhtem Risiko führen kann.

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.

How does the WebAudit Assessment Tool process work?
From Printanista Hub, the dealer specifies the end-user's (your clients/customers) applicable billing cycle. At this time, an email is automatically generated and sent to the proper contact informing them it is time to collect their meters. The instructions include a URL whereby when the end-user clicks the link, it automatically launches their web browser, ready to perform the action. The end-user then clicks "'start" and "'save"'. Done. No software is installed at any time. A link to the WebAudit page may also be posted on the dealers' existing website, i.e., Enter Meter Readings web page. This allows the user to automate the collection, rather than manually walking from device to device, print the configuration page and transcribe the meters.

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, Printanista Workflow, 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

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.

Local USB Agent (ONLY functional with Onsite DCA)

The Local USB Agent is the solution used to extract information from one or more local printers attached to any Windows port type, such as USB and parallel. The Local USB Agent does not interrupt the printing job flow, it only activates when called upon by one of Printanista's collection application tools—Onsite DCA or WebAudit— and then closes. The Local USB Agent collects specific information dependent upon the intelligence levels of the device from the engine and not the print spooler. Most common attributes reported are model, serial number, life-time meters, consumable coverage, consumable level, and service. Printanista Local USB Agent may be deployed to the workstations using a solution such as Microsoft SMS. Reconfiguration of antivirus or software firewalls may be required if blocking the SNMP port 161 or the alternative Agent fallback port 33333.

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.

