Technisches Whitepaper zum Printanista Hub

Version 1.7

©2025 ECI and the ECI logo are registered trademarks of ECI Software Solutions, Inc. All rights reserved.

Inhaltsübersicht

Übersicht 4

Wie Printanista funktioniert 5

Printanista Anforderungen 6

Printanista Hub Backend-Anwendung 6

Printanista Bewerbungsanforderungen 7

Datenerhebungsstelle (ECI DCA) 7

PC/Server-Anforderungen für ECI DCA 7

ECI aktualisiert Server 8

Software-Aktualisierungen 8

Anmeldung 8

Service Region 8

Erfasste Daten und Verschlüsselung 9

Datenverschlüsselung 9

Fragen der Sicherheit 9

Arten von gesammelten Informationen 9

Lokale Druckereien 11

Printanista Arbeitsablauf 11

Remote Device Link (RDL) 13

Systemübersicht - Remote Device Link (RDL) 13

Sicherheit: Ports und SSL (Secure Sockets Layer) 13

Freischaltung und Berechtigungen 13

Prüfungskapazitäten 13

Remote Device Link (RDL) Sicherheit 14

Die Sicherheit von Remote Device Link (RDL) war ein Hauptanliegen bei der Entwicklung dieses Tools 14

Printanista Hub Anwendung 15

Berechtigungsbasierte Benutzerverwaltung 15

HTTPS-Zugang 15

Printanista Seite-an-Seite 15

Printanista Hub Anwendungshosting 15

ECI Secure Data Centers 15

Versionsverwaltung 16

Test- und Freigabeprozess 16

Sicherheit des Quellcodes 16

Datenschutz und Gesetzgebung 17

Allgemeine Datenschutzbestimmungen (GDPR) 17

Häufig gestellte Fragen (FAQs) 18

Legacy Onsite DCA Informationen 20

PC/Server Anforderungen für Onsite DCA 20

Überlegungen zur ausgehenden Firewall (Port 80 oder 443) 20

©2025 ECI und das ECI-Logo sind eingetragene Warenzeichen von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Netzanforderungen 20
Das alte Java Onsite auf Linux- und macOS-Systemen ist nicht funktionsfähig 20
PC-/Druckeranforderungen für die Verwendung des lokalen Agenten (optionale Installation) 20
Netzerkundung und Erfassung von Zählern und Lieferungen (Onsite DCA) 21
Netzverkehr 21
Lokaler USB-Agent (NUR funktionsfähig mit DCA vor Ort) 22
Hersteller-Support 22
Virus-Bedenken 22

ECI erbringt Supportleistungen ausschließlich für die letzte im Handel erhältliche Version der Software für die unmittelbar vorangegangene Version der Software. Diese Richtlinie gilt für alle ECI Device Management-Produkte.

©2025 ECI und das ECI-Logo sind eingetragene Warenzeichen von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Printanista

Übersicht

Die Printanista-Produktsuite bietet eine verwaltete Drucklösung der Unternehmensklasse, die sehr einfach zu verwenden und einzusetzen ist. Sie ist so konzipiert, dass die fortschrittlichen Funktionen und Vorteile der Microsoft .NET-Plattform genutzt werden können. Daher sind keine qualifizierten Techniker mehr erforderlich, um Software zu installieren, zu konfigurieren und das System zu warten. Die Printanista-Produkte können in keiner Weise so konfiguriert werden, dass sie eine andere Aufgabe erfüllen als die, für die sie entwickelt wurden. Die Übermittlung von Daten von den Produkten an externe Quellen ist strengstens eingeschränkt. Die Produkte melden keine weiteren Details außer Informationen über das überwachte Gerät (z. B. den Gerätetyp). Über die Printanista-Produkte werden niemals vertrauliche Informationen aus dem Netzwerk heraus übertragen. Die Suite besteht aus den folgenden Komponenten:

Printanista-Hub: Eine Website und ein Backend-System, das alle von den Printanista-Datenerfassungstools erhaltenen Daten enthält. Es handelt sich um ein Repository, das es Ihnen ermöglicht, Daten über einen Browser anzuzeigen, Berichte zu generieren, Alarm-Workflows und Benachrichtigungen zu konfigurieren und Daten mit Ihren ERP-Systemen für die Rechnungsstellung oder Liefererfüllung zu synchronisieren.

ECI DCA: Dieser neueste Datenerfassungsagent-DCA bietet wesentliche Vorteile gegenüber dem Onsite-Datenerfassungsagenten-DCA, ohne dass Funktionen verloren gehen, einschließlich der vollständigen nativen, plattformübergreifenden Unterstützung von Windows, macOS, Linux und Raspberry Pi, jeweils mit eigenen Installationsschritten, Supportdokumentation und geschultem Supportpersonal für diese Plattformen. ECI DCA bietet außerdem eine fortlaufende Erkennung und Überprüfung von Geräten, verbesserte MIBWalk- und Log-Sammelfunktionen, und es werden jetzt viel mehr Zählertypen erfasst.

DCA vor Ort: Ein Legacy Data Collection Agent-Tool führt automatisch Druckbeurteilungen durch und überwacht Verbrauchsmaterialstände, Druckerstatus und Fehlerprotokolle. Diese Anwendung wird beim Kunden vor Ort installiert und kann Druckbewertungen automatisch auf einer geplanten Basis ohne menschliches Eingreifen durchführen. Die erfassten Daten werden über HTTPS, HTTP oder, falls der Kunde eine eigene verschlüsselte Datei bevorzugt, an die Printanista Hub-Website gesendet.

WebAudit-Bewertungstool: Ein Datenerfassungstool, das Teil der Printanista Hub-Anwendung ist. Flottenbewertungen werden direkt von einem Browser aus durchgeführt, ohne dass eine Software installiert werden muss. Die erfassten Daten werden direkt an Printanista Hub gesendet.

Der Zweck dieses Dokuments ist es, einen Überblick über die Printanista-Produktlinie aus technischer Sicht zu geben, um Antworten auf die häufigsten Fragen zu geben, die Informationstechnologie-Teams erhalten.

 ©2025 ECI und das ECI-Logo sind eingetragene Warenzeichen von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Printanista

So funktioniert Printanista

Die Kern-Engine des Datenerfassungsagenten, das Herzstück jedes Printanista-Produkts, identifiziert und extrahiert Daten von vernetzten Druckern, Kopierern und Multifunktionsgeräten unter Verwendung der von den Geräten unterstützten Protokolle korrekt.

Printanista unterstützt derzeit die Protokolle SNMP v1, v2c und v3 (Simple Network Management Protocol). SNMP v3 bietet einen erhöhten Paketschutz, um sicherzustellen, dass Informationen und Kommunikation über zuverlässige Quellen übertragen werden. Im Gegensatz zu SNMPv1 oder v2 ist SNMP v3 zur Erhöhung der Sicherheit verschlüsselt und erfordert sowohl einen Benutzernamen als auch ein Passwort. Ein Vorteil von SNMP v3 ist, dass Netzwerkadministratoren die Verschlüsselungsmethode sowie einen starken Benutzernamen und ein starkes Passwort festlegen können.

SNMP ist ein Netzwerkprotokoll, das den Informationsaustausch zwischen Netzwerkgeräten erleichtert, indem es Daten aus der Management Information Base (MIB) und anderen Stellen im Druckgerät extrahiert. Bei der Management Information Base (MIB) handelt es sich um eine interne Datenbank, die bei den meisten netzwerkverbundenen Geräten Teil ihrer Anatomie ist. Die Management Information Base (MIB) enthält Daten wie den Modellnamen, den Tonerstand und den aktuellen Status des Druckers.

 ©2025 ECI und das ECI-Logo sind eingetragene Warenzeichen von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Printanista Anforderungen

Printanista Hub Backend Anwendung

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

Unter dem folgenden Link finden Sie die aktuellen vollständigen Printanista-Produktspezifikationen: SysReq v3.0.html

Alle gesammelten Daten werden an den Printanista-Hub-Server gesendet, wo sie für Berichte und Warnmeldungen zur Verfügung stehen. ECI DCA verbindet sich mit Ihrem Printanista Hub Server über HTTPS (Port **443/TCP**). Bitte wenden Sie sich an Ihren ECI-Lösungsadministrator, um Informationen zu den von Ihrem Server verwendeten Domänennamen und IP-Adressen zu erhalten. Diese Verbindung ist durch den Industriestandard **TLS** (Transport Layer Security) geschützt. **Empfohlen wird TLS 1.2.** TLS 1.0 und TLS 1.1 werden derzeit unterstützt, aber aus Sicherheitsgründen nicht empfohlen. Die Unterstützung für TLS 1.0 und TLS 1.1 wird in Zukunft eingestellt werden.

Diese Verbindung bleibt während der gesamten Zeit, in der ECI DCA läuft, geöffnet. Normalerweise wird eine WebSocket-Verbindung verwendet, aber in manchen Situationen kann ECI DCA entweder auf **vom Server gesendete Ereignisse** oder auf **HTTP-Long-Polling** zurückgreifen.

WICHTIGER HINWEIS: Von dem Server, auf dem Printanista Hub installiert ist, sind mehrere sichere HTTPS-Ausgangsverbindungen erforderlich:

- 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

 ©2025 ECI und das ECI-Logo sind eingetragene Warenzeichen von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Printanista-Anwendung Anforderungen

Datenerhebungsstelle (ECI DCA)

Bei Druckern, Kopierern und Multifunktionsgeräten muss das SNMP-Protokoll (Port 161) aktiviert sein, damit sie erkannt und Informationen abgerufen können. Das SNMP-Protokoll ist ein Standardbestandteil der Anwendungsschicht der TCP/IP-Suite.

PC/Server-Anforderungen für ECI DCA:

Microsoft Windows (x86/64)
Anforderungen:

- Microsoft .NET Framework 4.7.2. oder neuer (empfohlen: neueste Version)
- Vollständig freigegebene, von Microsoft unterstützte Versionen von Windows Server (außer Datacenter und Core Editionen) und Windows
  - ➢ *Microsoft-Versionen, die von Microsoft nicht mehr unterstützt werden, werden von ECI DCA nicht unterstützt.*
- Die Einstellungen des lokalen Netzwerks und/oder der Firewall erlauben die Verbindung zu den ECI Updates Server Diensten und dem Printanista Hub Server.

Linux (x86/64 oder ARM) Anforderungen:

- Mono Framework 5.4 oder höher (empfohlen: neueste Version)
- Die Einstellungen des lokalen Netzwerks und/oder der Firewall erlauben die Verbindung zu den ECI Updates Server Diensten und dem Printanista Hub Server.
- Nur Ubuntu LTS 20.04 und höher werden offiziell unterstützt.

macOS (x64) Anforderungen:

- Mono Framework 5.4 oder höher (empfohlen: neueste Version)
- macOS® Sierra (10.12) bis Sequoia (15.4). Neuere Versionen werden nicht unterstützt.
- Die Einstellungen des lokalen Netzwerks und/oder der Firewall erlauben die Verbindung zu den ECI Updates Server Diensten und dem Printanista Hub Server.

Raspberry Pi Anforderungen:

- Raspberry Pi 3 Model B oder Pi 4 Rev 1.5. Neuere Versionen werden nicht unterstützt.
- Leere microSD-Karte mit 8 GB oder mehr
- PC, der eine microSD-Karte beschreiben kann
- Die Einstellungen des lokalen Netzwerks und/oder der Firewall erlauben die Verbindung zu den ECI Updates Server Diensten und dem Printanista Hub Server.

Firewall-Erwägungen für ECI DCA:

Eingehende Verbindungen - Es gibt keine eingehenden Verbindungen vom Internet zu ECI DCA.
Ausgehende Verbindungen

Dienst	Hafen	Verbindung zu
Hochladen von Daten	**443/TCP** (HTTPS)	Ihr Printanista Hub Server
Software-Aktualisierungen	**443/TCP** (HTTPS)	ECI aktualisiert Server
Registrierung (Fallback)	**53/UDP** (DNS)	Lokales Netzwerk DNS-Server (primär) ECI-Updates-Server (Fallback)

 ©2025 ECI und das ECI-Logo sind eingetragene Warenzeichen von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

ECI aktualisiert Server

ECI Updates Server ist ein Dienst, der von ECI Device Management betrieben wird, um die DCA-Registrierung, automatische Software-Updates und DCA-Installationen (diese Seite) zu erleichtern, und ist für den Betrieb von ECI DCA erforderlich. Hinweis: ECI DCA sendet keine gesammelten Geräte- oder Konfigurationsdaten an ECI Updates Server.

Software-Aktualisierungen

ECI DCA aktualisiert sich automatisch, indem es die auf https://updates.printanista.net/ veröffentlichten Updates herunterlädt. Die Verbindungen werden immer über den Standard-HTTPS-Port **443/tcp** hergestellt.

Anmeldung

ECI DCA verwendet DNS-Anfragen an *.reg.pf-d.ca zur Registrierung. Es wird zunächst versuchen, dies über die DNS-Server des lokalen Netzwerks zu tun, und dann auf eine direkte Verbindung zu den IP-Adressen des ECI-Updates-Servers (über Port **53/udp**) zurückgreifen. Die Firewall muss diese Verbindung zum ECI-Updates-Server nur dann zulassen, wenn der/die lokale(n) DNS-Server die Registrierungsanfragen nicht auflösen können.

Service Region

ECI DCA wird je nach Verfügbarkeit des Dienstes in die Region mit der geringsten Netzwerklatenz weitergeleitet. An bestimmten Standorten kann sich die verwendete Region im Laufe der Zeit ändern, da Aktivitäten in der globalen Internet-Infrastruktur die Latenzzeit beeinflussen können.

 ©2025 ECI und das ECI-Logo sind eingetragene Warenzeichen von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Erfasste Daten und Verschlüsselung

Datenverschlüsselung

Alle Datenpakete von ECI DCA und älteren Onsite DCA sind verschlüsselt und verschleiert. Printanista erfordert die Verwendung von HTTPS für die Kommunikation zwischen den DCAs und dem Printanista Hub. ECI DCA benötigt HTTPS, um zu funktionieren. Zusätzlich werden alle sensiblen Einstellungen und Aufträge zwischen ECI DCA und Printanista mit dem symmetrischen Verschlüsselungsalgorithmus AES256 verschlüsselt, der einen geschützten gemeinsamen Schlüssel verwendet. Dies gewährleistet eine Ende-zu-Ende-Verschlüsselung, so dass die Daten davor geschützt sind, von einem Dritten, einer konkurrierenden oder anderweitig nicht autorisierten Printanista-Instanz abgefangen zu werden.

Sicherheit Angelegenheiten

ECI DCA und herkömmliche Onsite DCA kommunizieren mit Printanista Hub über das HTTPS-Protokoll, das den Industriestandard **TLS 1.2** (Transport Layer Security) verwendet. Vertrauliche Daten werden von keiner Printanista-Anwendung erfasst, angezeigt oder gespeichert. Es werden nur druckerbezogene Daten erfasst und angezeigt. Mit Ausnahme von IP-Adresse, MAC-Adresse und Hostname können keine anderen Netzwerkdaten von ECI DCA oder dem alten Onsite DCA identifiziert oder erfasst werden.

ECI DCA und Legacy Onsite DCA sammeln und verarbeiten keine personenbezogenen Daten. Das System sammelt diese Art von Informationen nur, wenn Sie oder Ihr(e) Kunde(n) die Daten in Printanista in Feld oder ein Etikett eingeben, z. B. den Standort oder den Kundennamen. ECI DCA und das alte Onsite DCA ermöglichen Ihnen die Überwachung von Netzwerkgeräten mit Hilfe des Simple Network Management Protocol (SNMP). Die Anwendung wird im Netzwerk des Kunden installiert und kommuniziert von dort aus mit den Geräten, um Betriebsinformationen über das Gerät zu sammeln, die über die Gerätefirmware und eine SNMP Management Information Base (MIB) zur Verfügung gestellt werden. Die vom Gerät bereitgestellten Daten variieren je nach Hersteller und Modell. Sie sind immer technischer oder betrieblicher Natur und spezifisch für das Gerät selbst. Die grundlegendsten Daten, die von einer Drucker-MIB bereitgestellt werden, sind im IETF RFC 3805 (https://tools.ietf.org/html/rfc3805) dokumentiert. Zusätzliche Geräteinformationen können vom Hersteller durch Erweiterungen und private MIBs (Management Information Base) zur Verfügung gestellt werden, aber die Informationen sind grundsätzlich technisch und gerätespezifisch.

Printanista Hub speichert nur:

- Hostname
- Betriebssystem
- Entfernte IP-Adresse
- Systemarchitektur

Andere Netzwerk- und Umgebungsinformationen werden während der Verbindung Fehlerbehebung erfasst und angezeigt, aber niemals in Printanista gespeichert.

Arten von gesammelten Informationen

ECI DCA und Legacy Onsite DCA versuchen, die folgenden Informationen von vernetzten Druckgeräten während eines Netzwerkscans zu sammeln:

Geräte-Attribute

- IP-Adresse (kann maskiert werden)
- Hersteller
- Seriennummer
- Anlagennummer
- MAC-Adresse
- Beschreibung des Geräts
- Standort
- Sonstiges (maschinenspezifisch)

Dienst

- LCD-Anzeige
- Gerätestatus
- Fehlercodes
- Firmware

Lieferungen

- Seriennummer der Tonerkartusche
- Füllstand der Tonerkartusche
- Trommelebenen
- Füllstände der Wartungskits
- Liefermengen für Nicht-Toner
- Verschiedene Ebenen
- Etikettenbasierte Drucker liefern Details

Erfassungsbereich und Zähler

- Zählerstände
- Zählertyp
- Abdeckungsgrad
- Monochrome oder farbige Identifizierung

©2025 ECI und das ECI-Logo sind eingetragene Warenzeichen von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Netzwerkermittlung und Datenerfassung

Um die Effizienz des DCA zu erhöhen, werden nur dann Informationen an den Printanista Hub Server gesendet, wenn neue oder geänderte Daten von den Geräten vorliegen. Dies sorgt für eine minimale Netzwerkbelastung und verhindert, dass es zu einem Rückstau bei der Übermittlung von Gerätedaten kommt. Außerdem sind die Erkennung und das Scannen von Geräten jetzt unabhängig, um sicherzustellen, dass nur die IP-Adresse
(oder Hostname) der zuvor entdeckten Geräte auf der regelmäßig eingestellten Basis im Gegensatz zu einem vollständigen Netzwerk-Scan gescannt werden (dieser wird anfänglich, regelmäßig oder nach Festlegung durch einen Admin-Benutzer durchgeführt).

Dadurch wird sichergestellt, dass die Geschwindigkeit der Übermittlung von Gerätedaten so aktuell wie möglich ist. So können Benutzer in vielen innerhalb von Minuten oder sogar Sekunden über problematische Geräte informiert werden. ECI DCA trennt die Geräteerkennung von anderen Scan-Typen und ermöglicht es Ihnen, benutzerdefinierte Scan-Intervalle für das Abrufen von Zählern, Versorgungsattributen und Fehlern festzulegen. Die Standard-, Mindest- und Höchstwerte für die Scan-Intervalle sind:

Scan-Funktion	Standard	Minimum	Maximum
Entdeckung	60 Minuten	10 Minuten	7 Tage
Zähler	24 Stunden	30 Minuten	14 Tage
Lieferungen	4 Stunden	30 Minuten	7 Tage
Fehler	60 Minuten	30 Minuten	7 Tage
Attribute	24 Stunden	1 Stunde	14 Tage

Bitte beachten Sie, dass die Abfrageintervalle (Zähler, Verbrauchsmaterial, Fehler und Attribute) nur verfügbar sind, wenn ein Gerät über eine Modelldefinitionsdatei (MDF) verfügt. Ist diese nicht vorhanden, wird ein vollständiger Scan mit einem vordefinierten Intervall für das betreffende Gerät durchgeführt.

Printanista Hub-Administratoren können ECI DCA, die auf dem aktiviert wurden, aus der Ferne verwalten. Sie können ECI DCA aus der Ferne dazu veranlassen, vordefinierte Befehle auszuführen, wie z. B. Datenerfassungsaufgaben, die Bereitstellung von ECI DCA-Protokollen, die Durchführung von Remote MIB Walks oder die Aktualisierung von ECI DCA-Einstellungen.

Hinweis: ECI DCA initiiert immer die Kommunikation mit dem Printanista-Server und nicht .

Hinweis: Die Kommunikation erfolgt nur dann, wenn Zähler-, Versorgungs- oder Fehlerinformationen aktualisiert oder geändert wurden, wodurch die Bandbreitennutzung reduziert wird.

Hinweis: HP JAMC ist derzeit nur mit dem alten Onsite-DCA funktionsfähig.

 ©2025 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Lokale Druckereien

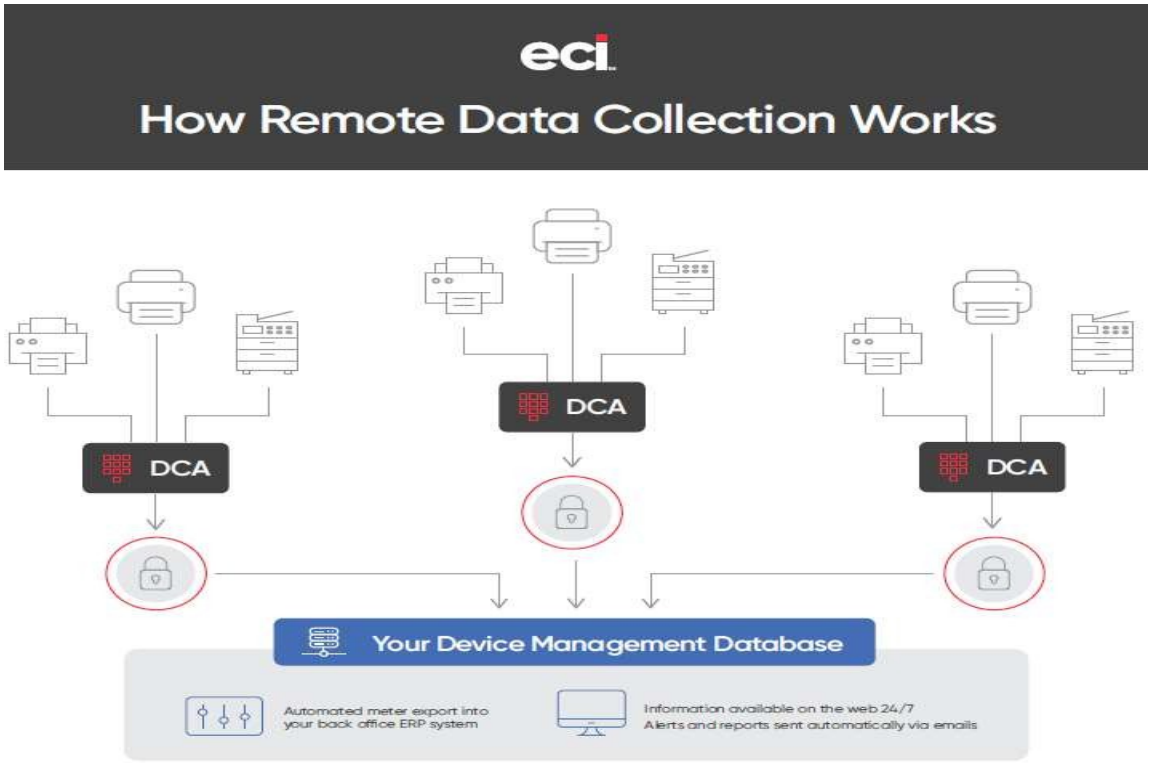
Printanista

Arbeitsablauf

Printanista Workflow ist ein robustes Druckmanagement-Tool. Printanista Workflow kann Ihren Kunden helfen, Kosten für die Dokumentenausgabe zu senken, die Dokumentensicherheit zu erhöhen und flexible Methoden zur Kostendeckung bereitzustellen. Durch einen vereinfachten Installationsprozess können Ihre Kunden schnell alle Druckinformationen an einem Ort einsehen. Sie geben Kunden die Möglichkeit, Kosten zu senken, indem sie jedes von ihnen produzierte Dokument verstehen.

Was ist der Printanista-Workflow?

Printanista Workflow ist die nächste Generation von Benutzerverwaltungsprodukten, die zur Verfolgung und Verwaltung von Druckvorgängen bei Hunderten von Organisationen und Unternehmen auf der ganzen Welt eingesetzt werden. Wenn Sie mit der Benutzerverwaltungsanwendung in der Vergangenheit vertraut waren, werden Sie sich freuen zu sehen, dass die Installation und Konfiguration der Anwendung immer noch so intuitiv ist wie in den Vorgängerversionen. Die Menüs, Werkzeuge und die allgemeine Verwaltung des Systems wurden beibehalten. Wenn Sie von einer früheren Version aufrüsten, wird Ihnen alles vertraut sein und Sie



werden sich problemlos zurechtfinden.

Wie Printanista Workflow funktioniert (durch die ECI werden DCA-Daten vom Workflow gesammelt)

Da Printanista Workflow die nächste Generation des Gerätemanagements ist, funktioniert diese Funktion nur mit dem ECI DCA. Printanista Workflow funktioniert nicht mit Onsite DCA.

Der Workflow-Client kann auf MAC- und Windows-Desktops installiert werden und ermöglicht die Erfassung von Zählern auf einem lokal angeschlossenen USB-Gerät.

-Zähler werden anhand von Daten aus Spooler, Anwendung und Druckertreiber ermittelt

-in der Workflow-Datenbank gespeichert

-ECI DCA fordert die Zählerinformationen vom Workflow über einen API-Aufruf (Application Programming Interface) an den Webservice an

-ECI DCA liefert Daten an Printanista Hub für ….

-Workflow zu ECI DCA Verbindung ist verschlüsselt (https)

 ©2025 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Printanista Workflow Systemanforderungen

Server und Verwaltungswerkzeuge

Sie können die Printanista Workflow Server-Komponenten auf Computern installieren, auf denen sie laufen:

- Microsoft Windows Server 2012 R2 oder höher
- Windows 8 Professional oder neuer (64bit)

Eine vollständige Serverinstallation erfordert:

- Mindestens 5 Gigabyte freier Speicherplatz zur Unterstützung der Workflow-Software
- SQL Database und SQL Express 2012 sind erforderlich. SQL Express 2012 wird installiert, wenn nicht vorhanden
- Internet Information Service (IIS) ist erforderlich und wird installiert, falls nicht vorhanden
- Microsoft .NET Framework 4.7.2 ist erforderlich und wird installiert, wenn es nicht vorhanden ist.
- Standardmäßig werden alle Druckdatenaufträge und Protokolle auf diesem Server gespeichert.

Wichtig: Die Betriebssysteme Microsoft Home und Microsoft Small Business Server werden nicht für alle Komponenten unterstützt.

Windows-Client-Anforderungen und Speichernutzung

Sie können die Printanista Workflow Client Popup Software auf Computern mit Microsoft Windows 8 oder höher installieren.

- Eine vollständige Client-Installation benötigt etwa 10-20 MB Speicherplatz. Der Client

besteht aus zwei Komponenten: dem Desktop Client und dem Client Service.

- Der Desktop Client benötigt je nach Aktivität zwischen 5 und 20 Megabyte.
- Es wird keine zusätzliche Software benötigt.

Systemanforderungen für Workflow Client für Mac®

- Workflow Client für Mac® wird auf Mac®-Betriebssystemen gemäß Apples Support-Modell unterstützt.
- Der Mac®-Client unterstützt nur die neueste und zwei frühere Mac® OS-Versionen.
- Klicken Sie in Ihrem Apple-Menü auf "Über diesen Mac® ", um herauszufinden, welche Version von Mac® OS auf Ihrem Arbeitsplatzrechner läuft.
- Workflow Client for Mac® benötigt außerdem einen (1) Windows-basierten PC als Host für den Workflow Server und die Datenbank.

Wichtig: Printanista Workflow muss in einem Netzwerk mit mindestens einem Windows-Computer installiert werden.

IIS-Webserver-Unterstützung

Workflow verwendet Internet Information Services (IIS) für die Kommunikation mit Geräten und intern zwischen Workflow-Komponenten. Die Installation erfordert die Vollversion von IIS. Das Installationsprogramm stellt fest, ob Sie eine bestehende IIS-Installation haben. Ist dies nicht der Fall, erstellt das Installationsprogramm eine neue Site und einen Anwendungspool unter Verwendung von IIS.

Anforderungen an die Vernetzung

Printanista Workflow verwendet HTTP/SSL-Kommunikation über die Ports 80/443 für Webdienste. Wenn diese Ports nicht verfügbar sind, verwendet Workflow 6320/6321. Sie können jedoch die Kommunikationsports ändern, wenn es in Ihrer Organisation einen Konflikt gibt.

Vom Workflow Server an ECI DCA gelieferte Daten:

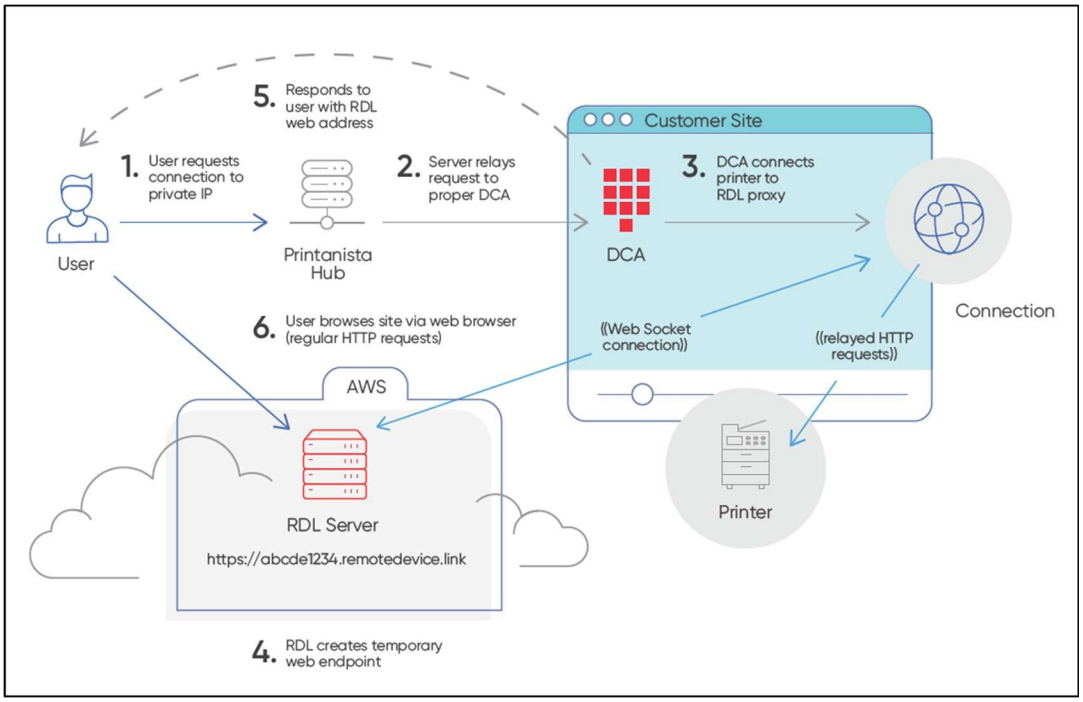
Beispiele für einige der Geräteidentifizierungsinformationen: Hersteller, Modell, IP-Adresse, Serien-/Assetnummer, Standort, Farb-/Monochromseiten, Farb-/Monochromdrucke usw.

Die Dokumentation der Printanista Workflow-Hilfe finden Sie hier:

Printanista Workflow Hilfe

 ©2025 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Remote Device Link (RDL)



Systemübersicht - Remote Device Link (RDL)

Remote Device Link (RDL) ist ein Dienst, der es einem entfernten **Endbenutzer** ermöglicht, auf einen HTTP-Endpunkt in einem privaten LAN zuzugreifen. Er besteht aus 4 Hauptkomponenten:

1. Der **Endbenutzer**, der auf das Gerät zugreift
2. Der **Remote Device Link-Server** im öffentlichen Internet (über https://*.remotedevice.link URL)
3. Der **RDL-Client** (eingebettet in den DCA), der im privaten LAN läuft
4. Der **HTTP-Endpunkt** (Drucker), auf den zugegriffen wird (läuft im privaten LAN)

Sicherheit: Ports und SSL (Secure Sockets Layer)

Der öffentlich zugängliche Pfad für RDL ist immer eine https:// URL auf Port 443, unabhängig vom Endpunkt-Port und/oder SSL-Status.

Freischaltung und Berechtigungen

1. Globale Aktivierungsoption pro Händlerinstanz
2. Lokales Enablement für jedes Endkundenkonto
3. Damit ein Benutzer auf die Funktion zugreifen kann, sind Berechtigungen erforderlich

Rechnungsprüfung Fähigkeiten

1. Printanista Hub überwacht lokal die Details jeder Sitzung
    a. Printanista Hub Administrationsberichte für Remote Device Link (RDL) Auditing
2. Remote Device Link (RDL) AWS (Amazon Web Services) Cloud-Protokollierung aller Sitzungsdetails

 ©2025 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Remote Device Link (RDL) Sicherheit

Die Sicherheit von Remote Device Link (RDL) war ein Hauptanliegen bei der Entwicklung dieses

Tools. Autorisierung:

- Der Benutzer muss vom Printanista Hub aus die Erlaubnis haben, auf die Remote Device Link (RDL)-Funktion für jeweilige Konto zuzugreifen.
- Der Data Collection Agent (DCA) akzeptiert nur RDL-Anfragen (Remote Device Link) vom Printanista Hub-Server, der gegenseitig authentifiziert ist.
- Der Datensammlungsagent (DCA) stellt nur eine Remote Device Link (RDL)-Verbindung zu bekannten und aktuell überwachten Druckgeräten innerhalb des IP-Ermittlungsbereichs des Datensammlungsagenten (DCA) her.
- Jede einzelne Webanforderung muss an dieselbe IP-Adresse gerichtet sein - Der Datenerfassungsagent (DCA) folgt keinen Weiterleitungen

Sicherheit der Verbindung:

- Alle Verbindungen zu und von den Servern Remote Device Link (RDL) und Printanista Hub werden mit dem Standard TLS 1.2 (Transport Layer Security) verschlüsselt.
- Jede Verbindung erhält einen eindeutigen Domänennamen, der eine 19-stellige (96-Bit) zufällige Kombination aus Buchstaben und Zahlen verwendet.
- Jede Anfrage erfordert ein 160-Bit-Sicherheitstoken, das als Browser-Cookie gespeichert wird und nur zu Beginn durch TLS-Verschlüsselung gesicherten Sitzung gesetzt wird.
- Der Data Collection Agent (DCA) kann eine nicht verschlüsselte HTTP-Verbindung zum Druckgerät über lokale Netzwerk herstellen, unterstützt aber TLS 1.2, wenn das Gerät

Zeitliche Begrenzung der Sitzung:

- Jede einzelne Remote Device Link (RDL)-Sitzung wird standardmäßig nach 20 Minuten Inaktivität beendet, absolute Maximum liegt bei 2 Stunden.

Auswirkungen

Die Verbindung zwischen ECI DCA und Printanista Hub ist durch DCA-spezifische Authentifizierungsschlüssel geschützt, und die Verbindung erfordert ein gültiges vertrauenswürdiges SSL-Zertifikat für die Verwendung über eine TLS-Verbindung.

Der gesamte Datenverkehr zwischen dem DCA und dem Internet ist verschlüsselt. Das ECI DCA kann jedoch mit dem Gerät im lokalen Netz über einfache HTTP-Verbindungen kommunizieren, wenn das Gerät keine sicheren Verbindungen unterstützt.

 ©2025 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Printanista Hub Anwendung

Die Funktionen von Printanista Hub sind über eine webbasierte Benutzeroberfläche zugänglich.

Berechtigungsbasierte Benutzerverwaltung

Der Zugriff auf das Printanista Hub-Webfrontend wird über eine auf Berechtigungen basierende Benutzerverwaltung gesteuert. Benutzer müssen mit einem bestimmten Benutzernamen und Passwort bei Printanista anmelden. Den Benutzern werden eine oder mehrere Rollen zugewiesen, in denen die Berechtigungen festgelegt sind, und ihnen wird der Zugriff auf eine oder mehrere Gerätegruppen gewährt. Administratoren mit voller Berechtigung können genau festlegen, welche Bildschirme jeder Benutzer sehen und/oder mit ihnen interagieren kann.

HTTPS-Zugang

Printanista verlangt, dass alle Websites HTTPS mit einem gültigen SSL-Sicherheitszertifikat verwenden. Dies gewährleistet die Verschlüsselung der über das Internet übertragenen Daten.

Printanista Seite-an-Seite

Printanista Hub verwendet eine Modell-Metadaten-Datenbank, die als Side-by-Side (SBS) bekannt ist und verschiedene Modellattribute enthält, z. B. Druckgeschwindigkeiten, das Datum der Markteinführung oder Kompatibilitäten mit OEM-Teilenummern, die regelmäßig aktualisiert werden, wenn neue Modelle und Versionen von OEMs veröffentlicht werden. Printanista Hub kommuniziert mit Side-by-Side, um nach neuen Updates zu suchen und die Metadaten der Geräte abzurufen, um sie lokal auf jedem Printanista Hub-System zwischenzuspeichern.

Printanista Hub Anwendungshosting

Printanista Hub wird von ECI Software Solutions in sicheren und geschützten Rechenzentren in verschiedenen Regionen der Welt gehostet. ECI Software Solutions ist sich bewusst, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen unserer Kunden für deren Geschäftsbetrieb und unseren eigenen Erfolg von entscheidender Bedeutung sind. Wir verwenden einen mehrschichtigen Ansatz, um diese wichtigen Informationen zu schützen, indem wir unsere Anwendungen, Systeme und Prozesse ständig überwachen und verbessern, um den wachsenden Anforderungen und Herausforderungen der Sicherheit gerecht zu werden.

ECI Secure Data Centers

Unser Service wird in speziellen Räumen in erstklassigen Rechenzentren untergebracht. Diese Einrichtungen bieten Support auf Carrier-Niveau. Klicken Sie auf den folgenden Link, um das ausführliche Dokument der ECI über die Sicherheit der Rechenzentren zu erhalten

ECI-Cloud-Sicherheitsübersicht 2021 (ecisolutions.com)

 ©2025 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Versionsmanagement Test- und

Freigabeprozess

Jede Haupt- und Nebenversion der Software durchläuft einen Qualitätskontrollprozess, bei dem mehrere Printanista-Mitarbeiter geänderte Teile des Systems einem Regressionstest unterziehen, um sicherzustellen, dass es keine Verschlechterung der Sicherheit oder der Funktionalität des Systems gegeben hat, und um die neuen funktionalen Aspekte zu validieren. Größere Releases durchlaufen einen Beta-Release-Prozess, bei dem ausgewählte Kunden das neue und das alte System parallel betreiben.

Sicherheit des Quellcodes

Der Quellcode von Printanista wird in einem gesicherten Revisionskontrollsystem aufbewahrt, das nur autorisierten Personen zugänglich ist. Jede Änderung Quellcode muss von zwei autorisierten Entwicklern genehmigt werden, bevor sie in Produktionscode-Repository aufgenommen wird, wo jede Änderung nachverfolgt wird, einschließlich der Angabe, welcher Entwickler die Änderung vorgenommen hat und warum. Die Produkte werden verschlüsselt und vor dem Versand mit einem vertrauenswürdigen Code-Signatur-Zertifikat digital signiert. Auf Wunsch kann ein Treuhanddepot zur Verfügung gestellt werden.

ECI beauftragt einen branchenführenden CREST-, SOC 2-, NSA-CIRA- und CSA-STAR-zertifizierten unabhängigen Dritten mit der Durchführung von Penetrationstests auf Anwendungsebene und der Behebung von Mängeln auf der Grundlage der Geschäftsanforderungen und des internen Risikomanagementrahmens. Penetrationstests werden mindestens einmal jährlich oder bei größeren Änderungen am System durchgeführt. ECI unternimmt alle wirtschaftlich vertretbaren Anstrengungen, um alle kritischen Feststellungen innerhalb von 30 Tagen oder innerhalb eines angemessenen Zeitrahmens zu beheben, wenn ein entsprechender Geschäftsfall vorliegt. Die ECI gibt keine Einzelheiten über ihre Sicherheitskontrollen oder Ergebnisse von Penetrationstests bekannt, da diese Informationen urheberrechtlich geschützt und vertraulich sind und in den falschen Händen zu einem erhöhten Risiko führen können.

 ©2025 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Datenschutz und Gesetzgebung

Allgemeine Datenschutzbestimmungen (GDPR)

Im Mai 2018 traten die allgemeinen Datenschutzbestimmungen der Europäischen (GDPR) vollständig in Kraft. Die DSGVO ersetzt die Datenschutzrichtlinie 95/46/EG und soll die Datenschutzgesetze in ganz Europa stärken und vereinheitlichen.

ECI hat ein strukturiertes und umfassendes Programm zur Einhaltung der GDPR eingeführt. Das Programm umfasst unter anderem Mitarbeiterschulungen, Audits und Risikobewertungen im gesamten Unternehmen, Richtlinien und Verfahren, Governance und laufende Compliance-Maßnahmen. Wir ermutigen unsere Kunden, ähnliche Schritte zu unternehmen, um sicherzustellen, dass ihre eigenen Unternehmen die GDPR einhalten, auch in den kommenden Jahren.

Die Printanista-Produkte verarbeiten, überwachen oder verwalten keine personenbezogenen Daten oder Daten oder Informationen, die sich auf eine bestimmte Person oder Personengruppe beziehen.

Die Printanista-Softwareanwendungen sammeln, speichern oder übertragen keine Informationen über den Inhalt von Druckaufträgen.

Printanista hat keine Möglichkeit, auf risikoreiche Informationen zuzugreifen, sie unterzubringen oder zu übertragen, selbst wenn diese Informationen gedruckt oder auf andere Weise an Druckgeräte gesendet werden, die von Printanista-Softwareanwendungen überwacht werden.

Die Printanista-Softwareanwendungen speichern, verarbeiten oder übermitteln keine Karteninhaberdaten oder persönlichen Informationen.

Die Kommunikation der Produkt-Engine wird kontrolliert, indem der Zugriff auf bestimmte IP-Adressen und/oder Bereiche eingeschränkt wird.

Die gesamte Kommunikation muss von den Printanista-Produkten ausgehen, und es gibt keine Möglichkeit, Produkte von außerhalb des Netzes zu kontaktieren oder auf sie zuzugreifen.

Für die Kommunikation außerhalb des Netzes wird ein proprietärer, komprimierter Datenstrom verwendet, der mit dem Industriestandard SSL über HTTPS übertragen wird.

Für Informationen über die Einhaltung bestimmter Gesetze und/oder Vorschriften wenden Sie sich bitte an Ihren ECI-Kundenbetreuer.

Im Folgenden finden Sie einen Link zur ECI Cloud Security: [ECI-Cloud-Sicherheitsübersicht 2021 (ecisolutions.com)]

 ©2025 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Häufig gestellte Fragen (FAQs)

Funktionieren Printanista-Produkte mit Internet-Proxys?
Ja, ECI DCA kann mit den meisten Proxys arbeiten. Die Konfiguration der Proxy-Einstellungen ist auf dem System erforderlich, auf dem ECI DCA installiert ist und arbeitet.
Was sind die Mindestanforderungen für Printanista Hub, ECI DCA, Onsite?
Bitte beachten Sie den Abschnitt Printanista Bewerbungsanforderungen in diesem Dokument.

Sind die Printanista-Produkte mit Mac-, Linux- oder Raspberry Pi-Umgebungen kompatibel?
Dieses ECI DCA bietet wesentliche Vorteile gegenüber dem Onsite DCA, ohne dass dabei irgendwelche Funktionen verloren gehen, einschließlich der vollständigen nativen plattformübergreifenden Unterstützung von Windows, macOS, Linux und Raspberry Pi. Für jede dieser Plattformen gibt es eigene Installationsschritte, Support-Dokumentation und geschulte Support-Mitarbeiter. Der Installationsprozess wurde ebenfalls stark verbessert und ist für alle Arten von Benutzern viel intuitiver.

Benötigt ECI DCA Microsoft Internet Information Services (IIS)?
Nein. ECI DCA und Onsite DCA verfügen über einen eigenen Server, auf dem die webbasierte Benutzeroberfläche (UI) gehostet wird und der während der Installation automatisch eingerichtet wird.

Können Sie ECI DCA auf einem Computer installieren, auf dem bereits eine andere IIS-Website läuft?
Ja, allerdings müssen die unten aufgeführten Ports in die Whitelist aufgenommen werden, um die Konnektivität von ECI DCA zu gewährleisten.

Dienst	Hafen	Verbindung zu
Hochladen von Daten	**443/TCP** (HTTPS)	Ihr Printanista Hub Server
Software-Aktualisierungen	**443/TCP** (HTTPS)	ECI aktualisiert Server
Registrierung (Fallback)	**53/UDP** (DNS)	Lokales Netzwerk DNS-Server (primär) ECI-Updates-Server (Fallback)

ECI DCA verwendet standardmäßig Port 31816 für die lokale webbasierte DCA-Benutzeroberfläche.

Wie hoch ist der laufende für ECI DCA?
ECI DCA und Onsite DCA ist ein Dienst, der im Hintergrund läuft und nach vordefinierten Zeitplänen Prüfungen und Exporte an konfigurierte Ziele durchführt. Es wird empfohlen, Subnetze (IP-Bereiche) anstelle von festen IPs zu verwenden. Wenn Sie dem Netzwerk neue Geräte hinzufügen, werden diese erkannt und in die Prüfergebnisse aufgenommen, so dass manuelle Eingriffe vermieden werden.

Wie das Verfahren des WebAudit Assessment Tools?
Über Printanista Hub gibt der Händler den für den Endnutzer (Ihre Kunden) geltenden Abrechnungszyklus an. Zu diesem Zeitpunkt wird automatisch eine E-Mail generiert und an die richtige Kontaktperson gesendet, um sie darüber zu informieren, dass es Zeit ist, ihre Zähler abzuholen. Die Anweisungen enthalten eine URL, die, wenn der Endnutzer auf den Link klickt, automatisch seinen Webbrowser startet, der dann bereit ist, die Aktion durchzuführen. Der Endnutzer klickt dann auf "Start" und "Speichern". Erledigt. Es wird keinem Zeitpunkt eine Software installiert. Ein Link zur WebAudit-Seite kann auch auf der bestehenden Website des Händlers platziert werden, z. B. auf der Seite "Zählerstände eingeben". So kann der Benutzer die Erfassung automatisieren, anstatt manuell von Gerät zu Gerät zu gehen, die Konfigurationsseite auszudrucken und die Zählerstände abzuschreiben.

 ©2025 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Mit welchen Gerätemarken funktioniert die Remote Device Link (RDL)-Überwachung? Welche Voraussetzungen müssen erfüllt sein, damit es funktioniert?
Alle Marken mit einer eingebetteten Webseite werden von ECI DCA entdeckt. Die Informationen auf den eingebetteten Webseiten variieren je nach Hersteller und Modell. Lokale Geräte zeigen die eingebettete Webseite nicht an.

Gibt es zusätzliche Sicherheitsbedenken bei Remote Device Link (RDL)?
Es wird ein sicherer Kanal zwischen dem Gerät im lokalen Kundennetz und einem Betreiber außerhalb dieses Netzes geöffnet. RDL meldet nur Geräte zurück, die über ECI DCA entdeckt und aktiv überwacht werden. Es erscheint eine Meldung, die anzeigt, dass eine Geräteverbindung über DCA nicht unterstützt wird

Remote Device Link (RDL) scheint etwas langsam zu sein, woran liegt das?
Dies ist zu erwarten, da die Verbindung durch unsere Cloud-Dienste getunnelt werden muss. Der Haupteinflussfaktor ist jedoch, wie schnell die Geräte auf Anfragen der Web-Benutzeroberfläche (UI) reagieren.
Wir haben gesehen, dass Geräte innerhalb von Zehntelsekunden auf die ersten Verbindungsversuche reagieren, bis hin zur Beeinflussung durch die aktuelle Nutzung oder die für die Benutzeroberfläche (UI) verfügbaren Ressourcen.

Welche Funktionen sind mit Remote Device Link (RDL) verfügbar?
Alle Optionen, auf die der OEM über die eingebettete Webseite zugreift, sind über Remote Device Link (RDL) zugänglich.

Kann die Funktion Remote Device Link (RDL) ausgeschaltet werden?
Ja, es gibt die Möglichkeit, diese Funktion pro Konto auszuschalten.
Es ist auch möglich, diese Funktion pro Benutzer zu deaktivieren, so dass Sie den Zugriff eines Benutzers auf Remote Device Link (RDL) sperren können.

Wo erhalte ich zusätzliche Informationen zu Printanista Hub, Printanista Workflow, ECI DCA, Legacy Onsite DCA, usw.? Zusätzliche Informationen sind auf der Printanista-Website der ECI zu finden: https://www.ecisolutions.com/products/printanista-hub/

 ©2025 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Legacy Onsite DCA Informationen

ECI DCA wird für die Verwendung mit Printanista empfohlen. Das bisherige Onsite DCA funktioniert jedoch auch mit Printanista. PC/Server-Anforderungen für Onsite DCA:

- 1GB RAM
- 400 MB Festplattenspeicher
- Microsoft .NET Framework 4.7.2 oder neuere Version
- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- Onsite Version 4.1.3 und neuer unterstützt Windows Server 2022
- Internet Explorer 11.0 oder neuer, Chrome, Firefox
- MDAC 2.8 oder höher (normalerweise bei der Installation von Windows enthalten)
- JET 4.0 oder höher (normalerweise bei der Installation von Windows enthalten)
- Auf einem Rechner geladen, der rund um die Uhr oder zumindest den ganzen Arbeitstag in Betrieb ist
- Sie müssen während der Installation als lokaler Administrator (oder gleichwertig) angemeldet sein.

Überlegungen zur ausgehenden Firewall (Port 80 oder 443):

Datenübertragung:

- https://(Unternehmen_Printanista_FQDN)/WebServices/Onsite2Service.asmx
- Anwendung: fmaonsite.exe
- SOAP über HTTP(s) muss die Firewall passieren dürfen

Netzanforderungen:

Der SNMP-Datenverkehr (Port 161) muss über das LAN oder WAN (Wide Area Networks) geleitet werden können.

Bitte verwenden Sie ECI DCA, wenn macOS, Linux oder Raspberry Pi als Betriebssysteme benötigt werden. Das alte Java Onsite auf Linux und macOS Systemen ist nicht funktionsfähig.

PC-/Druckeranforderungen für die Verwendung des lokalen Agenten (optionale Installation):

- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- Microsoft .NET Framework 4.7.2 oder neuere Version
- Aktueller Treiber für den lokalen Drucker (UPD wird für HP-Geräte empfohlen)
- Der Drucker muss Printer Job Language (PJL) oder Printer Management Language (PML) unterstützen.
- Entfernen Sie alle nicht verwendeten Druckertreiber
- Die bidirektionale Unterstützung des Treibers ist aktiviert
- Änderungen der Windows-Firewall - Port 161/33333 eingehend/ausgehend für TCP und UDP *Microsoft-unterstützte Versionen von Windows und Windows Server. Versionen, die nicht mehr von Microsoft unterstützt werden, werden von ECI nicht unterstützt.*

Hinweis: Für aktuelle Betriebssystemversionen, die das Treibermodell 4 verwenden (z. B. Windows 10), werden derzeit nur Kyocera- und Ricoh-OEMs und deren Varianten unterstützt.

 ©2025 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Netzerkundung und Zähler- und Versorgungserfassung (Onsite DCA)

Die patentierten automatischen Netzwerkerkennungseinstellungen von Printanista verwenden eine Mischung aus Algorithmen, um die Netzwerkbereiche zu identifizieren, in denen sich Druckgeräte befinden können, und dann die Geräte zu erkennen und mit ihnen zu kommunizieren, die online sind, wobei mehrere Netzwerkelemente wie aktive Workstations oder Server, Router, Hubs, Switches und zusätzliche Netzwerkhardware durchlaufen werden.

Printanista Hub-Administratoren können aktivierte Onsite-DCAs (Data Collection Agent) auf dem Server aus der Ferne verwalten und die Onsite aus der Ferne veranlassen, vordefinierte Befehle auszuführen, wie z. B. Datenerfassungsaufgaben, die Bereitstellung von Onsite-Protokollen, die Ausführung von MIBWalks aus der Ferne, die Installation von HP JAMC oder die Aktualisierung von Onsite-Einstellungen. Diese werden im Folgenden näher erläutert:

Funktion	**Standort**	**Beschreibung**
Aufgaben	Vor-Ort-Einstellungen	Kann Aufgaben aus der Ferne so konfigurieren, dass sie nach einem voreingestellten Zeitplan ablaufen, kann aber auch Aufgaben (Cache, Zähler, Verbrauchsmaterial, Service) auswählen, die sofort ablaufen und auf Befehl Gerätedaten sammeln.
MIB-Spaziergänge	Vor-Ort-Einstellungen	Kann bestimmte IPv4/IPv6/Hostnamen von Geräten angeben und den Onsite veranlassen, sofort mit der Sammlung der MIB-Walks zu beginnen.
Protokolle (detailliert)	Vor-Ort-Einstellungen	Kann die Onsite anweisen, die Logs (Critical, Error, Warning, Details, Debug) ab einem bestimmten Datum zu sammeln.

Keiner dieser Befehle führt zu einer Datenerfassung, die über die oben beschriebenen Arten von erfassten Informationen hinausgeht. Die zwischen Onsite DCA und Printanista Hub ausgetauschten Daten werden mit starken Verschlüsselungsprotokollen verschlüsselt, die FIPS-konform sind. Onsite erhält sichere Software-Updates von den Printanista Updates-Servern.

Der bisherige Onsite-DCA kommuniziert in einem vordefinierten Intervall mit Printanista, um festzustellen, ob es in der Warteschlange stehende Aktionen gibt, die noch nicht ausgeführt wurden. Dadurch wird sichergestellt, dass die Aktionen rechtzeitig ausgeführt werden.

Hinweis: Onsite DCA initiiert immer diese Kommunikation mit dem Printanista-Server und nicht .

Hinweis: HP JAMC wird nur unterstützt, wenn es in Verbindung mit dem alten Onsite DCA bei der ersten Einführung von Printanista verwendet wird.

Netzverkehr

Die von der Software durchgeführten Audits verwenden ein intelligentes System, um minimale Informationen für jeden Drucker, Kopierer oder MFP zu extrahieren. Im Gegensatz zu ähnlichen Produkten, die einen festen Satz von Abfragen (eine Obermenge aller möglichen Abfragen) an jedes vernetzte Gerät senden, sendet Onsite DCA nur die relevanten Abfragen entsprechend den Feldern, die das Zielgerät unterstützt, wobei jede Geräteabfrage nicht mehr als ein paar Kilobytes an Daten umfasst. Um die beanspruchte Netzwerkbandbreite weiter zu reduzieren, kommuniziert Onsite DCA mit nicht mehr als 20 Geräten auf einmal. Jede IP-Adresse innerhalb der konfigurierten Bereiche wird abgefragt, und wenn innerhalb der konfigurierten Timeout-Periode keine Antwort eingeht, wird zur nächsten IP-Adresse gewechselt. Als Faustregel gilt, dass Printanista in knapp einer Stunde Informationen über etwa 65.000 Geräte sammelt.

 ©2025 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Lokaler USB-Agent (NUR funktionsfähig mit DCA vor Ort)

Der lokale USB-Agent ist die Lösung, die verwendet wird, um Informationen von einem oder mehreren lokalen Druckern zu extrahieren, die an einen beliebigen Windows-Anschlusstyp angeschlossen sind, z. B. USB und parallel. Der lokale USB-Agent unterbricht den Druckauftragsfluss nicht, er wird nur aktiviert, wenn er von einem der Printanista-Sammelanwendungs-Tools - Onsite DCA oder WebAudit - aufgerufen und dann geschlossen wird. Der lokale USB-Agent sammelt spezifische Informationen, die von der Intelligenz des Geräts abhängen, von der Engine und nicht vom Druckspooler. Die häufigsten Attribute, die gemeldet werden, sind Modell, Seriennummer, Lebensdauerzähler, Verbrauchsmaterialabdeckung, Verbrauchsmaterialstand und Service. Der Printanista Local USB Agent kann mit einer Lösung wie Microsoft SMS auf den Arbeitsstationen installiert werden. Eine Neukonfiguration von Antivirenprogrammen oder Software-Firewalls kann erforderlich sein, wenn der SNMP-Port 161 oder der alternative Agent-Fallback-Port 33333 blockiert wird.

Hersteller-Support

Printanista-Produkte sind herstellerneutral. Sie unterstützen alle wichtigen Hersteller und Modellfamilien. Einige Geräte haben Einschränkungen, die die Extraktion bestimmter Informationen verhindern.

Virus-Bedenken

Die Printanista-Anwendungsdateien wurden digital signiert, um die Ausführung zu verhindern, wenn die Integrität der Datei beeinträchtigt ist. Dies stellt sicher, dass ein eventuell vorhandener Virus nicht aktiviert wird und verhindert die Verbreitung des Virus von einem Netzwerk zum anderen. Für zusätzliche Sicherheit empfehlen wir die Verwendung von Antiviren-Software in Ihrem Netzwerk.

ECI erbringt Supportleistungen ausschließlich für die letzte im Handel erhältliche Version der Software sowie für die unmittelbar vorangegangene Version der Software. Diese Richtlinie gilt für alle ECI Device Management-Produkte.

Microsoft®, .NET Framework®, Windows® und Windows Server® sind entweder eingetragene Marken oder Marken der Microsoft Corporation.

 ©2025 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.