Technisches Whitepaper zum Printanista Hub

Version 1.10

©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Inhaltsverzeichnis

©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

ECI bietet Supportleistungen ausschließlich für die aktuellste im Handel erhältliche Version der Software sowie für die unmittelbar vorhergehende Version der Software an. 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

©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Übersicht

Die Printanista-Produktsuite bietet eine Managed-Print-Lösung der Enterprise-Klasse, die sehr einfach zu bedienen und zu implementieren ist. Sie wurde so konzipiert und entwickelt, dass sie die fortschrittlichen Funktionen und Vorteile der Microsoft .NET-Plattform nutzt. Daher sind keine qualifizierten Techniker mehr erforderlich, um die Software zu installieren, das System zu konfigurieren und zu warten. Die Printanista-Produkte können in keiner Weise so konfiguriert werden, dass sie Aufgaben ausführen, die über die vorgesehenen Funktionen hinausgehen. Die Übertragung von Daten aus den Produkten an externe Quellen ist streng eingeschränkt. Die Produkte melden keine weiteren Details außer Informationen zu den überwachten Geräten (d. h. Gerätetyp). Es werden niemals vertrauliche Informationen über Printanista-Produkte aus dem Netzwerk übertragen. Die Suite besteht aus den folgenden Komponenten:

Printanista Hub: Eine Website und ein Backend-System, in dem alle von den Printanista-Datenerfassungstools empfangenen Daten gespeichert werden. Es handelt sich um ein Repository, das es Ihnen ermöglicht, Daten über einen Browser einzusehen, Berichte zu erstellen, Alarm-Workflows und Benachrichtigungen zu konfigurieren sowie Daten mit Ihren ERP-Systemen für die Abrechnung oder die Auftragsabwicklung zu synchronisieren.

ECI DCA: Dieser neueste Data Collection Agent (DCA) bietet gegenüber dem Onsite Data Collection Agent (DCA) erhebliche Vorteile, ohne dabei auf Funktionen zu verzichten. Dazu gehören die vollständige native plattformübergreifende Unterstützung von Windows, macOS, Linux und Raspberry Pi, jeweils mit spezifischen Installationsschritten, Support-Dokumentation und geschultem Support-Personal für diese Plattformen. ECI DCA ermöglicht zudem die kontinuierliche Erkennung und Überprüfung von Geräten, verbesserte MIBWalk- und Protokoll-Erfassungsfunktionen sowie die Erfassung einer deutlich größeren Anzahl von Messgerätetypen.

Onsite DCA: Ein bewährtes Tool zur Datenerfassung führt automatisch Druckbewertungen durch und überwacht den Verbrauchsmaterialstand, den Druckerstatus sowie Fehlerprotokolle. Diese Anwendung wird beim Kunden vor Ort installiert und kann Druckbewertungen automatisch nach einem festgelegten Zeitplan ohne menschliches Eingreifen durchführen. Die erfassten Daten werden über HTTPS, HTTP oder, falls der Kunde dies bevorzugt, als proprietäre verschlüsselte Datei an die Printanista Hub-Website gesendet.

Der Zweck dieses Dokuments ist es, einen Überblick über die Produktpalette der Printanista-Produktfamilie aus technischer Perspektive zu geben, um Antworten auf die häufigsten Fragen zu erleichtern, die IT-Teams erhalten.

 ©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

So funktioniert Printanista

Printanista Hub – als gehostete Anwendung konzipiert

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 Daten unserer Kunden für deren Geschäftsbetrieb und für unseren eigenen Erfolg von entscheidender Bedeutung sind. Wir schützen diese wichtigen Daten mit einem mehrschichtigen Ansatz und überwachen und verbessern unsere Anwendung, Systeme und Prozesse kontinuierlich, um den wachsenden Anforderungen und Herausforderungen im Bereich der Sicherheit gerecht zu werden.

Sichere Rechenzentren von ECI

Unser Service wird in dedizierten Bereichen in erstklassigen Rechenzentren untergebracht. Diese Einrichtungen bieten Support auf Carrier-Niveau. Dieser Link führt zu dem ausführlichen Dokument von ECI zur Sicherheit von Rechenzentren.
Übersicht über die ECI-Cloud-Sicherheit

Data Collection Agent (DCA)

Die Kern-Engine des Datenerfassungsagenten, die das Herzstück jedes Printanista-Produkts bildet, identifiziert und extrahiert Daten von vernetzten Druckern, Kopierern und Multifunktionsgeräten korrekt, wobei sie die von den Geräten unterstützten Protokolle nutzt.

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

SNMP ist ein Netzwerkprotokoll, das den Informationsaustausch zwischen Netzwerkgeräten erleichtert, indem es Daten aus der Management Information Base (MIB) und anderen Speicherorten innerhalb des Druckgeräts abruft. Die Management Information Base (MIB) ist eine interne Datenbank, über die die meisten netzwerkfähigen Geräte verfügen. Die Management Information Base (MIB) enthält Daten wie den Modellnamen, den Tonerstand und den aktuellen Status des Druckers.

 ©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Anforderungen an Printanista

Printanista Hub-Backend-Anwendung

Alle erfassten Daten werden an den Printanista Hub-Server gesendet, wo sie für Berichte und Benachrichtigungen zur Verfügung stehen. ECI DCA verbindet sich über HTTPS (Port **443/TCP**) mit Ihrem Printanista Hub-Server. Bitte wenden Sie sich an Ihren ECI Solutions-Administrator, 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.
Es ist mindestens die Version TLS 1.2 erforderlich.

Diese Verbindung bleibt während der gesamten Laufzeit von ECI DCA offen. Normalerweise wird eine WebSocket-Verbindung verwendet, aber in einigen Situationen kann ECI DCA auf **Server-Sent-Events** oder **HTTP-Long-Polling** zurückgreifen.

WICHTIGER HINWEIS: Vom 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
- https://install.printanista.net

Systemanforderungen für Printanista Hub

Über den folgenden Link gelangen Sie zu den aktuellen vollständigen Systemspezifikationen für Printanista-

Produkte: Systemanforderungen für Printanista Hub v4.0

 ©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Anforderungen an die Printanista-Anwendung

Datenerfassungsagent (ECI DCA)

Drucker, Kopierer und Multifunktionsgeräte müssen das SNMP-Protokoll (Port 161) aktiviert haben, damit sie erkannt und Informationen von ihnen abgerufen werden können. Das SNMP-Protokoll ist ein Standardbestandteil der Anwendungsschicht der TCP/IP-Suite.

PC-/Server-Anforderungen für ECI DCA:

Anforderungen für Microsoft Windows (x86/64):

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

Linux (x86/64 oder ARM) Anforderungen:

- Mono Framework 5.4 oder höher (empfohlen: neueste Version)
- Die lokalen Netzwerk- und/oder Firewall-Einstellungen ermöglichen die Verbindung zu den Diensten des ECI Updates Servers und zum Printanista Hub-Server.
- Es werden offiziell nur Ubuntu LTS 20.04 und höher unterstützt.

Anforderungen für macOS (x64):

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

Anforderungen für Raspberry Pi:

- 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 auf die microSD-Karte schreiben kann
- Die Einstellungen des lokalen Netzwerks und/oder der Firewall ermöglichen die Verbindung zu den Diensten des ECI-Update-Servers und zum Printanista-Hub-Server.

Firewall-Hinweise für ECI DCA:

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

Dienst	Port	Verbindung zu
Daten-Upload	**443/TCP** (HTTPS)	Dein Printanista Hub-Server
Software-Updates	**443/TCP** (HTTPS)	ECI-Update-Server
Registrierung (Fallback)	**53/UDP** (DNS)	Lokaler Netzwerk-DNS-Server (primär) ECI-Update-Server (Fallback)

 ©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

ECI-Update-Server

Der ECI Updates Server ist ein von ECI Device Management betriebener Dienst, der die DCA-Registrierung, automatische Software-Updates und DCA-Installationen (auf dieser Website) ermöglicht und für den Betrieb von ECI DCA erforderlich ist. Hinweis: ECI DCA übermittelt keine erfassten Geräte- oder Konfigurationsdaten an den ECI Updates Server.

Software-Updates

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

Registrierung

ECI DCA verwendet DNS-Anfragen an `*.reg.pf-d.ca` zur Registrierung. Es versucht dies zunächst über die DNS-Server des lokalen Netzwerks und greift dann auf die direkte Kommunikation mit den IP-Adressen des ECI-Update-Servers zurück (über Port **53/udp**). Die Firewall muss diese Verbindung zum ECI-Update-Server nur zulassen, wenn die lokalen DNS-Server die Registrierungsanfragen nicht auflösen können.

Dienstregion

ECI DCA wird an die Region weitergeleitet, in der die Netzwerk-Latenz am geringsten ist, wobei die Verfügbarkeit der Dienste berücksichtigt wird. An bestimmten Standorten kann sich die verwendete Region im Laufe der Zeit ändern, da die Aktivität in der globalen Internetinfrastruktur die Latenz beeinflussen kann.

 ©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Erfasste Daten und Verschlüsselung

Datenverschlüsselung

Alle Datenpakete von ECI DCA und dem älteren Onsite DCA werden 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. Darüber hinaus werden alle sensiblen Einstellungen und Aufträge zwischen ECI DCA und Printanista mit dem symmetrischen Verschlüsselungsalgorithmus AES256 unter Verwendung eines geschützten gemeinsamen Schlüssels verschlüsselt. Dies gewährleistet eine End-to-End-Verschlüsselung, sodass die Daten vor dem Auslesen geschützt sind, falls sie von Dritten, einer konkurrierenden oder anderweitig nicht autorisierten Printanista-Instanz abgefangen werden.

Sicherheit

ECI DCA und das ältere Onsite DCA kommunizieren mit dem Printanista Hub über das HTTPS-Protokoll unter Verwendung des Industriestandards **TLS 1.2** (Transport Layer Security). Vertrauliche Daten werden von keiner Printanista-Anwendung erfasst, eingesehen oder gespeichert. Es werden ausschließlich druckerbezogene Daten erfasst und eingesehen. Mit Ausnahme von IP-Adresse, MAC-Adresse und Hostname können keine anderen Netzwerkdaten von ECI DCA oder dem älteren Onsite DCA identifiziert oder erfasst werden.

ECI DCA und das ältere Onsite DCA erfassen oder verarbeiten keine personenbezogenen Daten. Das System erfasst solche Informationen nur dann, wenn Sie oder Ihre Kunden diese Daten in Printanista in ein Feld oder auf ein Etikett eingeben, beispielsweise den Standort oder den Kundennamen. ECI DCA und das ältere Onsite DCA ermöglichen es Ihnen, Netzwerkgeräte mithilfe des Simple Network Management Protocol (SNMP) zu überwachen. Die Anwendung wird im Netzwerk des Kunden bereitgestellt und kommuniziert von dort aus mit den Geräten, um Betriebsinformationen über das Gerät zu erfassen, die über die Geräte-Firmware und eine SNMP Management Information Base (MIB) zur Verfügung gestellt werden. Die vom Gerät bereitgestellten Daten variieren je nach Hersteller und Modell. Sie sind stets technischer oder betrieblicher Natur und spezifisch für das jeweilige Gerät. Auf der grundlegendsten Ebene sind die von einer Drucker-MIB bereitgestellten Daten in der IETF RFC 3805 (https://tools.ietf.org/html/rfc3805) dokumentiert. Zusätzliche Geräteinformationen können vom Hersteller über Erweiterungen und private MIBs (Management Information Base) bereitgestellt werden, doch sind diese Informationen grundsätzlich technischer Natur und gerätespezifisch.

Printanista Hub speichert lediglich:

- Hostname
- Betriebssystem
- Remote-IP-Adresse
- Systemarchitektur

Weitere Netzwerk-/Umgebungsinformationen werden während der Verbindung zu Zwecken der Fehlerbehebung erfasst und angezeigt, jedoch niemals in Printanista gespeichert.

Arten der erfassten Informationen

ECI DCA und das ältere Onsite DCA versuchen, während eines Netzwerkscans die folgenden Informationen von vernetzten Druckgeräten zu erfassen:

Geräteattribute

- IP-Adresse (kann maskiert werden)
- Hersteller
- Seriennummer
- Asset-Nummer
- MAC-Adresse
- Gerätebeschreibung
- Standort
- Sonstiges (gerätespezifisch)

Service

- LCD-Anzeige
- Gerätestatus
- Fehlercodes
- Firmware

Verbrauchsmaterial

- Seriennummer der Tonerkartusche
- Füllstand der Tonerkartusche
- Trommelfüllstand
- Füllstand des Wartungssets
- Füllstand der Nicht-Toner-Verbrauchsmaterialien
- Sonstige Füllstände
- Details zum Verbrauchsmaterial bei Etikettendruckern

Abdeckung und Zähler

- Zählerstände
- Zählertyp
- Erfassungsgrad
- Monochrome oder farbige Kennzeichnung

©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Netzwerkerkennung und Datenerfassung

Um die Effizienz des DCA zu steigern, werden Informationen nur dann an den Printanista Hub Server gesendet, wenn neue oder geänderte Daten von den Geräten vorliegen. Dies gewährleistet eine minimale Netzwerkbelastung und verhindert häufige Rückstände bei der Übermittlung von Gerätedaten. Außerdem erfolgen die Erkennung und das Scannen von Geräten nun unabhängig voneinander, um sicherzustellen, dass nur die IP-Adresse
(oder der Hostname) zuvor erkannter Geräte in festgelegten Zeitabständen gescannt wird, anstatt einen vollständigen Netzwerkscan durchzuführen (dieser wird zu Beginn, in regelmäßigen Abständen oder nach Festlegung durch einen Administrator durchgeführt).

Dadurch wird sichergestellt, dass die übermittelten Gerätedaten so aktuell wie möglich sind. So können Benutzer in vielen Situationen innerhalb von Minuten oder sogar Sekunden über problematische Geräte benachrichtigt werden. ECI DCA trennt die Geräteerkennung von anderen Scan-Arten, sodass Sie benutzerdefinierte Scan-Intervalle für das Abrufen von Zählerständen, Verbrauchsmaterialien, Attributen und Fehlern festlegen können. Die Standard-, Minimal- und Maximalwerte für die Scan-Intervalle sind:

Scan-Funktion	Standard	Minimum	Maximal
Erkennung	60 Minuten	10 Minuten	7 Tage
Meter	24 Stunden	30 Minuten	14 Tage
Verbrauchsmaterial	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 Scan-Intervalle (Zähler, Verbrauchsmaterialien, Fehler und Attribute) nur verfügbar sind, wenn für ein Gerät eine Modelldefinitionsdatei (MDF) vorhanden ist. Ist dies nicht der Fall, wird ein vollständiger Scan des betreffenden Geräts in einem vordefinierten Intervall durchgeführt.

Printanista Hub-Administratoren können auf dem Server aktivierte ECI DCA-Geräte aus der Ferne verwalten. Sie können das ECI DCA-Gerät aus der Ferne anweisen, vordefinierte Befehle auszuführen, wie z. B. Datenerfassungsaufgaben, die Bereitstellung von ECI DCA-Protokollen, die Ausführung von Remote-MIB-Walks oder die Aktualisierung von ECI DCA-Einstellungen.

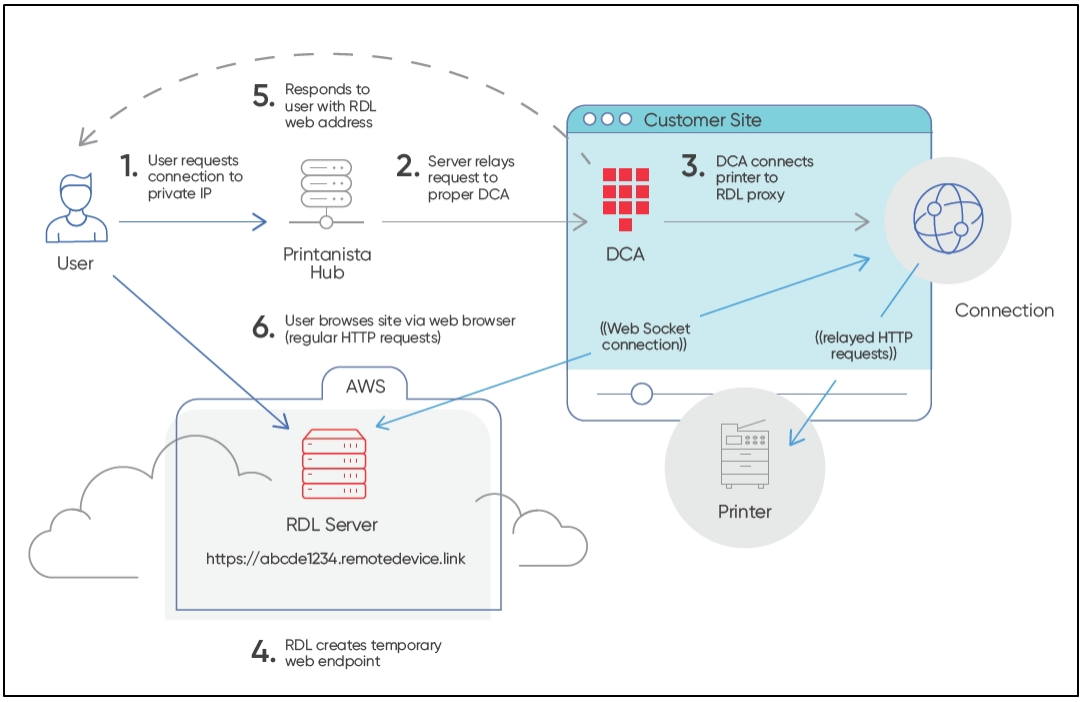
Hinweis**:** ECI DCA initiiert stets die Kommunikation mit dem Printanista-Server, nicht umgekehrt.

Hinweis: Eine Kommunikation findet nur statt, wenn sich Informationen zu Zählerstand, Verbrauchsmaterial oder Fehlern aktualisiert oder geändert haben, wodurch die Bandbreitennutzung reduziert wird.

Hinweis: HP JAMC funktioniert derzeit nur mit dem älteren Onsite DCA.

 ©2026 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 **Endbenutzer** an einem entfernten Standort ermöglicht, auf einen HTTP-Endpunkt in einem privaten LAN zuzugreifen. Er besteht aus vier Hauptkomponenten:

1. Der **Endbenutzer, der** auf das Gerät zugreift
2. Der **Remote Device Link-Server** im öffentlichen Internet (über die URL https://*.remotedevice.link)
3. Der **RDL-Client** (in den DCA eingebettet), 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 URL vom Typ https:// auf Port 443, unabhängig vom Endpunkt-Port und/oder dem SSL-Status.

Aktivierung und Berechtigungen

1. Globale Aktivierungsoption pro Händlerinstanz
2. Lokale Aktivierung für jedes Endkundenkonto
3. Für den Zugriff auf die Funktion sind Berechtigungen erforderlich

Auditierungsfunktionen

1. Lokale Überwachung der Details jeder Sitzung im Printanista Hub
    a. Printanista Hub-Verwaltungsberichte für die Überwachung von Remote Device Link (RDL)
2. Remote Device Link (RDL) – AWS (Amazon Web Services) Cloud-Protokollierung aller Sitzungsdetails

 ©2026 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 bei der Entwicklung dieses Tools ein zentrales Anliegen.

Autorisierung:

- Der Benutzer muss über eine Berechtigung innerhalb des Printanista Hub verfügen, um auf die Remote Device Link (RDL)-Funktion für das jeweilige Konto zugreifen zu können
- Der Data Collection Agent (DCA) akzeptiert nur Remote Device Link (RDL)-Anfragen vom Printanista Hub-Server, der gegenseitig authentifiziert ist
- Der Data Collection Agent (DCA) baut eine Remote Device Link (RDL)-Verbindung nur zu bekannten und aktuell überwachten Druckgeräten innerhalb des/der Erkennungs-IP-Bereiche(s) des Data Collection Agents (DCA) auf.
- Jede einzelne Webanfrage muss an dieselbe IP-Adresse gerichtet sein – der Data Collection Agent (DCA) folgt keinen Weiterleitungen

Verbindungssicherheit:

- Alle Verbindungen zu und von den Remote Device Link (RDL)- und Printanista Hub-Servern werden mit TLS 1.2 (Transport Layer Security) verschlüsselt
- Jede Verbindung erhält einen eindeutigen Domänennamen, der aus einer zufälligen 19-stelligen (96-Bit) alphanumerischen Kombination besteht
- Jede Anfrage erfordert ein 160-Bit-Sicherheitstoken, das als Browser-Cookie gespeichert und erst zu Beginn der durch TLS-Verschlüsselung gesicherten Sitzung gesetzt wird
- Der Data Collection Agent (DCA) kann über das lokale Netzwerk eine unverschlüsselte HTTP-Verbindung zum Druckgerät herstellen, unterstützt jedoch mindestens TLS 1.2, sofern das Gerät dies ebenfalls tut

Sitzungszeitlimits:

- Jede einzelne Remote Device Link (RDL)-Sitzung läuft standardmäßig nach 20 Minuten Inaktivität ab, wobei die absolute Höchstdauer 2 Stunden beträgt.

Auswirkungen

Die Verbindung zwischen ECI DCA und Printanista Hub wird durch Authentifizierungsschlüssel geschützt, die für die jeweilige DCA-Installation spezifisch sind, und erfordert ein gültiges, vertrauenswürdiges SSL-Zertifikat, um über eine TLS-Verbindung genutzt werden zu können.

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

 ©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Printanista Hub-Anwendung

Auf die Funktionen des Printanista Hub kann über eine webbasierte Benutzeroberfläche

zugegriffen werden. Berechtigungsbasierte Benutzerverwaltung

Der Zugriff auf das Printanista Hub-Web-Frontend wird über eine berechtigungsbasierte Benutzerverwaltung gesteuert. Benutzer müssen sich mit einem festgelegten Benutzernamen und Passwort bei Printanista anmelden. Den Benutzern werden eine oder mehrere Rollen zugewiesen, die ihre Berechtigungen festlegen, und sie erhalten Zugriff auf eine oder mehrere Gerätegruppen. Administratoren mit Vollzugriff können genau festlegen, welche Bildschirme jeder Benutzer anzeigen und/oder bedienen darf.

HTTPS-Zugriff

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

Printanista Side-By-Side

Printanista Hub nutzt eine Modell-Metadaten-Datenbank namens Side-by-Side (SBS), die verschiedene Modellattribute enthält, wie z. B.: Druckgeschwindigkeiten, Markteinführungsdatum oder Kompatibilität mit OEM-Teilenummern. Diese Datenbank wird regelmäßig aktualisiert, sobald neue Modelle und Versionen von den OEMs veröffentlicht werden. Printanista Hub kommuniziert mit Side-by-Side, um nach neuen Updates zu suchen sowie Gerätemetadaten abzurufen und diese lokal auf jedem Printanista Hub-System zwischenzuspeichern.

Hosting der Printanista Hub-Anwendung

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 Daten unserer Kunden für deren Geschäftsbetrieb und für unseren eigenen Erfolg von entscheidender Bedeutung sind. Wir schützen diese wichtigen Daten durch einen mehrschichtigen Ansatz und überwachen und verbessern unsere Anwendungen, Systeme und Prozesse kontinuierlich, um den wachsenden Anforderungen und Herausforderungen im Bereich der Sicherheit gerecht zu werden.

Sichere Rechenzentren von ECI

Unser Service wird in dedizierten Bereichen in erstklassigen Rechenzentren untergebracht. Diese Einrichtungen bieten Support auf

Carrier-Niveau. Klicken Sie auf den folgenden Link, um das detaillierte Dokument von ECI zur Sicherheit der Rechenzentren zu erhalten

Übersicht über die ECI-Cloud-Sicherheit

 ©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Versionsmanagement- -Test-

und Release-Prozess

Jede Haupt- und Nebenversion der Software durchläuft einen Qualitätskontrollprozess, in dem mehrere Printanista-Mitarbeiter Regressionstests an geänderten Teilen des Systems durchführen, um sicherzustellen, dass keine Verschlechterung der Sicherheit oder Funktionalität des Systems vorliegt, und um die neuen funktionalen Aspekte zu validieren. Hauptversionen 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 Versionskontrollsystem aufbewahrt, auf das nur autorisierte Personen Zugriff haben. Jede Änderung am Quellcode muss von zwei autorisierten Entwicklern genehmigt werden, bevor sie in das Produktions-Code-Repository übernommen wird, wo jede Änderung nachverfolgt wird, einschließlich der Angabe, welcher Entwickler die Änderung vorgenommen hat und warum. Die Produkte werden vor der Auslieferung verschlüsselt und mit einem vertrauenswürdigen Code-Signing-Zertifikat digital signiert. Auf Anfrage kann eine Treuhandhinterlegung bereitgestellt werden.

ECI beauftragt einen branchenführenden, nach CREST, SOC 2, NSA-CIRA und CSA-STAR zertifizierten unabhängigen Dritten mit der Durchführung von Penetrationstests auf Anwendungsebene und behebt die festgestellten Mängel auf der Grundlage seiner Geschäftsanforderungen und seines internen Risikomanagement-Rahmens. Penetrationstests werden mindestens einmal jährlich oder bei größeren Änderungen am System durchgeführt. Es ist die Politik von ECI, wirtschaftlich angemessene Anstrengungen zu unternehmen, um alle kritischen Befunde innerhalb von 30 Tagen oder innerhalb eines angemessenen Zeitraums mit einem vorgelegten Business Case zu beheben. ECI gibt keine Details zu unseren Sicherheitskontrollen oder den Ergebnissen von Penetrationstests bekannt, da diese Informationen urheberrechtlich geschützt und vertraulich sind und in den falschen Händen zu einem erhöhten Risiko führen können.

 ©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Datenschutz und Gesetzgebung

Datenschutz-Grundverordnung (DSGVO)

Im Mai 2018 trat die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union 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 DSGVO implementiert. Das Programm umfasst unter anderem Mitarbeiterschulungen, unternehmensweite Audits und Risikobewertungen, Richtlinien und Verfahren, Governance sowie fortlaufende Compliance-Maßnahmen. Wir empfehlen unseren Kunden, ähnliche Schritte zu unternehmen, um sicherzustellen, dass ihre eigenen Unternehmen die DSGVO einhalten – jetzt und in den kommenden Jahren.

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

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

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

Printanista-Softwareanwendungen speichern, verarbeiten oder übertragen keine Karteninhaberdaten oder personenbezogenen Daten.

Die Kommunikation der Produkt-Engine wird durch einen eingeschränkten Zugriff auf bestimmte IP-Adressen und/oder IP-Adressbereiche gesteuert.

Die gesamte Kommunikation muss von den Printanista-Produkten ausgehen, und es gibt keine Möglichkeit, von außerhalb des Netzwerks Kontakt zu den Produkten aufzunehmen oder auf diese zuzugreifen.

Die Kommunikation außerhalb des Netzwerks erfolgt über einen proprietären, komprimierten Datenstrom, der unter Verwendung des Industriestandards SSL über HTTPS gesendet wird.

Für Informationen zur Einhaltung spezifischer Gesetze und/oder Vorschriften wenden Sie sich bitte an Ihren ECI-Kundenbetreuer.

Hier ist ein Link zur ECI Cloud Security: ECI Cloud Security – Überblick

 ©2026 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 funktioniert mit den meisten Proxys. Die Konfiguration der Proxy-Einstellungen ist auf dem System erforderlich, auf dem ECI DCA installiert ist und läuft.

Was sind die Mindestanforderungen für den Printanista Hub, ECI DCA und die Vor-Ort-Installation?
Bitte beachten Sie den Abschnitt „Anwendungsanforderungen für Printanista“ in diesem Dokument.

Sind Printanista-Produkte mit Mac-, Linux- oder Raspberry-Pi-Umgebungen kompatibel?
Diese ECI DCA bietet gegenüber der Onsite DCA erhebliche Vorteile, ohne dass Funktionen verloren gehen, einschließlich vollständiger nativer plattformübergreifender Unterstützung für Windows, macOS, Linux und Raspberry Pi. Für jede dieser Plattformen gibt es eigene Installationsschritte, Support-Dokumentation und geschultes Support-Personal. Der Installationsprozess wurde zudem erheblich verbessert und ist für alle Arten von Benutzern wesentlich intuitiver.

Benötigt ECI DCA Microsoft Internet Information Services (IIS)?
Nein. ECI DCA und Onsite DCA verfügen über einen eigenen Server zum Hosten der webbasierten Benutzeroberfläche (UI), der während der Installation automatisch eingerichtet wird.

Kann man ECI DCA auf einem Computer installieren, auf dem bereits eine andere IIS-Website gehostet wird?
Ja. Allerdings müssen die unten aufgeführten Ports auf die Whitelist gesetzt werden, um die Konnektivität von ECI DCA sicherzustellen.

Dienst	Port	Verbindung zu
Daten-Upload	**443/TCP** (HTTPS)	Dein Printanista Hub-Server
Software-Updates	**443/TCP** (HTTPS)	ECI-Update-Server
Registrierung (Fallback)	**53/UDP** (DNS)	Lokaler Netzwerk-DNS-Server (primär) ECI-Update-Server (Fallback)

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

Wie viel laufende Wartung erfordert ECI DCA?
ECI DCA und Onsite DCA ist ein Dienst, der im Hintergrund läuft und nach vordefinierten Zeitplänen Überprüfungen durchführt sowie Daten an konfigurierte Ziele exportiert. Es wird empfohlen, Subnetze (IP-Bereiche) anstelle von festen IP-Adressen zu verwenden. Wenn neue Geräte zum Netzwerk hinzugefügt werden, werden diese erkannt und in die Überprüfungsergebnisse aufgenommen, wodurch manuelle Eingriffe auf ein Minimum reduziert werden.

Mit welchen Gerätemarken funktioniert die Remote Device Link (RDL)-Überwachung? Welche Voraussetzungen müssen erfüllt sein, damit sie funktioniert?
Alle Marken mit einer eingebetteten Webseite werden von ECI DCA erkannt. 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)?
Zwischen dem Gerät im lokalen Kundennetzwerk und einem Betreiber außerhalb dieses Netzwerks wird eine sichere Verbindung hergestellt. RDL meldet nur Geräte zurück, die über ECI DCA erkannt und aktiv überwacht werden. Es erscheint eine Meldung, dass die Geräteverbindung über DCA nicht unterstützt wird

 ©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Remote Device Link (RDL) scheint etwas langsam zu sein, woran liegt das?
Dies ist zu erwarten, da die Verbindung über unsere Cloud-Dienste getunnelt werden muss. Der wichtigste Einflussfaktor ist jedoch, wie schnell die Geräte auf Anfragen der Web-Benutzeroberfläche (UI) reagieren.
Wir haben beobachtet, dass Geräte bei den ersten Verbindungsversuchen innerhalb von Zehntelsekunden reagieren, wobei dies von der aktuellen Auslastung oder den für die Benutzeroberfläche (UI) verfügbaren Ressourcen beeinflusst wird.

Welche Funktionen stehen mit Remote Device Link (RDL) zur Verfügung?
Alle Optionen, auf die der OEM über die integrierte Webseite Zugriff gewährt, sind über Remote Device Link (RDL) zugänglich.

Kann die Remote Device Link (RDL)-Funktion deaktiviert werden?
Ja, es besteht die Möglichkeit, diese Funktion pro Konto zu deaktivieren.
Es ist auch möglich, diese Funktion pro Benutzer zu deaktivieren, sodass Sie den Zugriff eines Benutzers auf Remote Device Link (RDL) sperren können.

Wo finde ich weitere Informationen zu Printanista Hub, ECI DCA, dem alten Onsite DCA usw.? Weitere Informationen finden Sie auf der Printanista-Website der ECI:
https://www.ecisolutions.com/products/printanista-hub/

 ©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Informationen zum älteren Onsite DCA

Es wird empfohlen, ECI DCA zusammen mit Printanista zu verwenden. Das ältere Onsite DCA funktioniert jedoch derzeit mit Printanista. PC-/Serveranforderungen für Onsite DCA:

- 1 GB RAM
- 400 MB Festplattenspeicher
- Microsoft .NET Framework 4.7.2 oder neuer
- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- Die Onsite-Version 4.1.3 und höher 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)
- Installiert auf einem Rechner, der rund um die Uhr oder zumindest während des gesamten Arbeitstages in Betrieb ist
- Muss während der Installation als lokaler Administrator (oder gleichwertig) angemeldet sein

Hinweise zur ausgehenden Firewall (Port 80 oder 443):

Datenübertragung:

- https://(company_Printanista_FQDN)/WebServices/Onsite2Service.asmx
- Anwendung: fmaonsite.exe
- SOAP über HTTP(s) muss durch die Firewall zugelassen werden

Netzwerkanforderungen:

SNMP-Datenverkehr (Port 161) muss über das LAN oder WAN (Wide Area Networks) routbar sein

Bitte verwenden Sie ECI DCA, wenn Betriebssysteme wie macOS, Linux oder Raspberry Pi erforderlich sind: Das ältere Java Onsite auf Linux- und macOS-Systemen ist nicht funktionsfähig.

PC-/Druckeranforderungen für die Verwendung des Local Agent (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 neuer
- Aktueller Treiber für den lokalen Drucker (für HP-Geräte wird UPD 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 an der Windows-Firewall – Port 161/33333 für eingehenden und ausgehenden Datenverkehr für TCP und UDP *Von Microsoft unterstützte Versionen von Windows und Windows Server. Versionen, die von Microsoft nicht mehr unterstützt werden, werden auch von ECI nicht unterstützt.*

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

 ©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Netzwerkerkennung und Erfassung von Zählerständen und Verbrauchsmaterialien (Onsite DCA)

Die von Printanista patentierten Einstellungen zur automatischen Netzwerkerkennung nutzen eine Kombination aus Algorithmen, um die Netzwerkbereiche zu identifizieren, in denen sich Druckgeräte befinden könnten, und anschließend die online befindlichen Geräte zu erkennen und mit ihnen zu kommunizieren, wobei die Kommunikation über mehrere Netzwerkelemente wie aktive Workstations oder Server, Router, Hubs, Switches und weitere Netzwerkhardware geleitet wird.

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

Funktion	**Standort**	**Beschreibung**
Aufgaben	Onsite-Einstellungen	Aufgaben können per Fernzugriff so konfiguriert werden, dass sie nach einem voreingestellten Zeitplan ausgeführt werden; es ist jedoch möglich, bestimmte Aufgaben (Cache, Zählerstände, Verbrauchsmaterialien, Wartung) so auszuwählen, dass sie sofort ausgeführt werden und Gerätedaten auf Befehl erfasst werden.
MIB-Walks	Einstellungen vor Ort	Es können bestimmte IPv4-/IPv6-Adressen oder Hostnamen von Geräten angegeben werden, um Onsite dazu zu veranlassen, die Erfassung der MIB-Walks sofort zu starten.
Protokolle (detailliert)	Onsite-Einstellungen	Sie können Onsite anweisen, die Protokolle (Kritisch, Fehler, Warnung, Details, Debug) ab einem bestimmten Datum zu erfassen.

Keiner dieser Befehle führt zu einer Datenerfassung, die über die oben beschriebenen Arten von Informationen hinausgeht. Der Datenaustausch zwischen Onsite DCA und dem Printanista Hub wird mit starken, FIPS-konformen Verschlüsselungsprotokollen verschlüsselt. Onsite erhält sichere Software-Updates von den Printanista-Update-Servern.

Der ältere Onsite-DCA kommuniziert in festgelegten Intervallen mit Printanista, um festzustellen, ob noch nicht ausgeführte Aktionen in der Warteschlange stehen. Dadurch wird sichergestellt, dass die Aktionen zeitnah ausgeführt werden.

Hinweis**:** Onsite DCA initiiert diese Kommunikation immer zum Printanista-Server, nicht umgekehrt.

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

Netzwerkverkehr

Die von der Software durchgeführten Audits nutzen ein intelligentes System, um für jeden Drucker, Kopierer oder Multifunktionsdrucker nur ein Minimum an Informationen zu erfassen. 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 vom Zielgerät unterstützten Feldern, wobei jede Geräteabfrage nicht mehr als einige Kilobyte an Daten umfasst. Um die beanspruchte Netzwerkbandbreite weiter zu reduzieren, kommuniziert Onsite DCA gleichzeitig mit maximal 20 Geräten. Jede IP-Adresse innerhalb der konfigurierten Bereiche wird abgefragt, und wenn innerhalb der festgelegten Zeitüberschreitung keine Antwort eingeht, wird zur nächsten IP-Adresse übergegangen. Als Faustregel gilt, dass Printanista in knapp einer Stunde Informationen zu etwa 65.000 Geräten sammelt.

 ©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.

Herstellerunterstützung

Printanista-Produkte sind herstellerneutral. Sie unterstützen alle großen Hersteller und Modellfamilien. Bei einigen Geräten gibt es Einschränkungen, die die Extraktion bestimmter Informationen verhindern.

Bedenken hinsichtlich Viren

Die Dateien der Printanista-Anwendung wurden digital signiert, um eine Ausführung zu verhindern, falls die Dateiintegrität beeinträchtigt ist. Dadurch wird sichergestellt, dass eventuell vorhandene Viren nicht aktiviert werden, und eine Ausbreitung des Virus von einem Netzwerk auf ein anderes verhindert. Zur zusätzlichen Sicherheit empfehlen wir den Einsatz von Antivirensoftware in Ihrem Netzwerk.

ECI bietet Supportleistungen ausschließlich für die aktuellste im Handel erhältliche Version der Software sowie für die unmittelbar vorhergehende Version der Software an. 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.

 ©2026 ECI und das ECI-Logo sind eingetragene Marken von ECI Software Solutions, Inc. Alle Rechte vorbehalten.