Printanista Hub Technisches Whitepaper

Version 1.8

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

Inhaltsverzeichnis

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

ECI bietet Support-Services ausschließlich für die neueste im Handel erhältliche Version der Software sowie für die unmittelbar vorhergehende Version der Software. Diese Richtlinie gilt für alle ECI-Produkte zur Geräteverwaltung.

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.

Übersicht

Die Printanista-Produktsuite bietet eine verwaltete Drucklösung 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 erfahrenen 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, für die sie nicht vorgesehen sind. Die Übertragung von Daten aus den Produkten an externe Quellen unterliegt strengen Beschränkungen. 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, in dem Sie Daten mit einem Browser anzeigen, Berichte erstellen, Alarm-Workflows und Benachrichtigungen konfigurieren und Daten mit Ihren ERP-Systemen für die Rechnungsstellung oder die Lieferabwicklung synchronisieren können.

ECI DCA: Dieser neueste Datenerfassungsagent (DCA) bietet gegenüber dem Onsite-Datenerfassungsagenten (DCA) erhebliche Vorteile, ohne dabei an Funktionen einzubüßen, darunter vollständige native plattformübergreifende Unterstützung für Windows, macOS, Linux und Raspberry Pi, jeweils mit individuellen Installationsschritten, Support-Dokumentation und geschultem Support-Personal für diese Plattformen. ECI DCA bietet außerdem eine kontinuierliche Erkennung und Überprüfung von Geräten, verbesserte MIBWalk- und Protokoll-Erfassungsfunktionen und die Erfassung einer Vielzahl weiterer Zählertypen.

Onsite DCA: Ein älteres Datenerfassungs-Agent-Tool führt automatisch Druckbewertungen durch und überwacht den Verbrauchsmaterialstand, den Druckerstatus und die Fehlerprotokolle. Diese Anwendung wird beim Kunden vor Ort installiert und kann automatisch und ohne menschliches Eingreifen zu festgelegten Zeiten Druckbewertungen durchführen. Die erfassten Daten werden über HTTPS, HTTP oder, wenn der Kunde dies bevorzugt, in einer proprietären verschlüsselten Datei an die Printanista Hub-Website gesendet.

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

 ©2025 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

Der 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 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 Sicherheit gerecht zu werden.

Sichere Rechenzentren von ECI

Unser Service wird in dedizierten Räumen in erstklassigen Rechenzentren bereitgestellt. Diese Einrichtungen bieten Support auf Carrier-Niveau. Dieser Link führt zu einem detaillierten Dokument von ECI zum Thema Sicherheit in Rechenzentren.
ECI Cloud Security Overview 2021 (ecisolutions.com)

Datenerfassungsagent (DCA)

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

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 für erhöhte 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 sicheres Passwort festlegen können.

SNMP ist ein Netzwerkprotokoll, das den Austausch von Informationen zwischen Netzwerkgeräten erleichtert, indem es Daten aus der Management Information Base (MIB) und anderen Speicherorten innerhalb des Druckgeräts extrahiert. Die Management Information Base (MIB) ist eine interne Datenbank, über die die meisten mit dem Netzwerk verbundenen Geräte verfügen. Die Management Information Base (MIB) enthält Daten wie Modellname, Tonerfüllstand und aktuellen Status des Druckers.

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

Anforderungen für Printanista

Printanista Hub Backend- -Anwendung

Alle gesammelten Daten werden an den Printanista Hub-Server gesendet, wo sie für Berichte und Warnmeldungen zur Verfügung stehen. ECI DCA verbindet sich über HTTPS (Port **443/TCP**) mit Ihrem Printanista Hub-Server. Informationen zu den von Ihrem Server verwendeten Domänennamen und IP-Adressen erhalten Sie von Ihrem ECI Solutions-Administrator.

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 **WebS**ocket-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

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

Anforderungen für die Printanista-Anwendung

Datenerfassungsagent (ECI DCA)

Drucker, Kopierer und Multifunktionsgeräte müssen über das SNMP-Protokoll (Port 161) verfügen, damit Informationen erkannt und extrahiert werden können. Das SNMP-Protokoll ist ein Standardbestandteil der Anwendungsschicht der TCP/IP-Suite.

PC-/Serveranforderungen für ECI DCA:

Anforderungen an Microsoft Windows (x86/64):

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

Anforderungen für Linux (x86/64 oder ARM):

- Mono Framework 5.4 oder höher (empfohlen: neueste Version)
- Lokale Netzwerk- und/oder Firewall-Einstellungen ermöglichen die Verbindung zu 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 lokalen Netzwerk- und/oder Firewall-Einstellungen ermöglichen die Verbindung zu den Diensten des ECI Updates Servers und dem Printanista Hub Server.

Anforderungen für Raspberry Pi:

- Raspberry Pi 3 Model B oder Pi 4 Rev 1.5. Neuere Versionen werden nicht unterstützt.
- Leere microSD-Karte mit mindestens 8 GB Speicherplatz
- PC, der auf microSD-Karten schreiben kann
- Lokale Netzwerk- und/oder Firewall-Einstellungen ermöglichen die Verbindung zu ECI Updates Server-Diensten und dem Printanista Hub-Server.

Firewall-Überlegungen 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)	Ihr 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)

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

ECI-Update-Server

Der ECI-Update-Server ist ein von ECI Device Management betriebener Dienst, der die DCA-Registrierung, automatische Software-Updates und DCA-Installationen (diese Website) erleichtert und für den Betrieb von ECI DCA erforderlich ist. Hinweis: ECI DCA sendet keine gesammelten Geräte- oder Konfigurationsdaten an den ECI-Update-Server.

Software-Updates

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.

Registrierung

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

Service-Region

ECI DCA wird an die Region weitergeleitet, in der die Netzwerklatenz am geringsten ist und die Dienstverfügbarkeit am besten ist. An bestimmten Standorten kann sich die verwendete Region im Laufe der Zeit ändern, da Aktivitäten in der globalen Internetinfrastruktur die Latenz beeinflussen können.

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

Verschlüsselung der gesammelten Daten und der Datenübertragung ( )

Datenverschlüsselung

Alle Datenpakete von ECI DCA und Legacy 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. 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, einem Wettbewerber oder einer anderen nicht autorisierten Printanista-Instanz abgefangen werden.

Sicherheits en

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, 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 älteren Onsite DCA identifiziert oder erfasst werden.

ECI DCA und Legacy Onsite DCA erfassen oder verarbeiten keine personenbezogenen Daten. Das System erfasst diese Art von Informationen nur, wenn Sie oder Ihre Kunden die Daten in Printanista in ein Feld oder eine Bezeichnung wie Standort oder Kundenname eingeben. ECI DCA und Legacy Onsite DCA ermöglichen Ihnen die Überwachung von Netzwerkgeräten mithilfe des Simple Network Management Protocol (SNMP). Die Anwendung wird im Netzwerk des Kunden bereitgestellt und kommuniziert von dort aus mit Geräten, um Betriebsinformationen über das Gerät zu sammeln, die über die Geräte-Firmware und eine SNMP Management Information Base (MIB) verfügbar gemacht werden. Die vom Gerät offengelegten Daten variieren je nach Hersteller und Modell. Sie sind immer technischer oder betrieblicher Natur und spezifisch für das Gerät selbst. 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, aber die Informationen sind grundsätzlich technischer Natur und gerätespezifisch.

Printanista Hub speichert nur:

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

Andere Netzwerk-/Umgebungsinformationen werden während der Verbindung zu Fehlerbehebungszwecken erfasst und angezeigt, jedoch niemals in Printanista gespeichert.

Arten von Informationen, die von der Netzwerk sammlung erfasst werden

ECI DCA und 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 (maschinenspezifisch)

Service

- LCD-Anzeige
- Gerätestatus
- Fehlercodes
- Firmware

Verbrauchsmaterial

- Seriennummer der Tonerkartusche
- Füllstand der Tonerkartusche
- Trommelfüllstand
- Wartungsset-Füllstand
- Füllstand von Nicht-Toner-Verbrauchsmaterialien
- Sonstige Füllstände
- Details zur Versorgung von Etikettendruckern

Abdeckung und Zähler

- Messgerätanzeigen
- Messgerätetyp
- Abdeckungsgrad
- Monochrom- oder Farberkennung

©2025 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 nur neue oder geänderte Daten von den Geräten an den Printanista Hub Server gesendet. Dadurch wird eine minimale Netzwerkbelastung gewährleistet und die Häufigkeit von Rückständen bei der Übermittlung von Gerätedaten beseitigt. Außerdem sind die Erkennung und das Scannen von Geräten nun unabhängig voneinander, um sicherzustellen, dass nur die IP-Adresse
(oder Hostname) zuvor erkannter Geräte werden in regelmäßigen Abständen gescannt, im Gegensatz zu einem vollständigen Netzwerkscan (dieser wird zu Beginn, in regelmäßigen Abständen oder nach Festlegung durch einen Administrator durchgeführt).

Dadurch wird sichergestellt, dass die Geschwindigkeit der Gerätedatenübermittlung so aktuell wie möglich ist. 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-Typen, sodass Sie benutzerdefinierte Scan-Intervalle für das Abrufen von Zählern, Verbrauchsmaterialattributen und Fehlern festlegen können. Die Standard-, Mindest- und Höchstwerte für die Scan-Intervalle sind:

Scan-Funktion	Standard	Minimum	Maximal
Erkennung	60 Minuten	10 Minuten	7 Tage
Messgeräte	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 (Zählerstände, Verbrauchsmaterialien, Fehler und Attribute) nur verfügbar sind, wenn für ein Gerät eine Modelldefinitionsdatei (MDF) vorhanden ist. Ist dies nicht der Fall, wird das betreffende Gerät in einem vordefinierten Intervall vollständig gescannt.

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

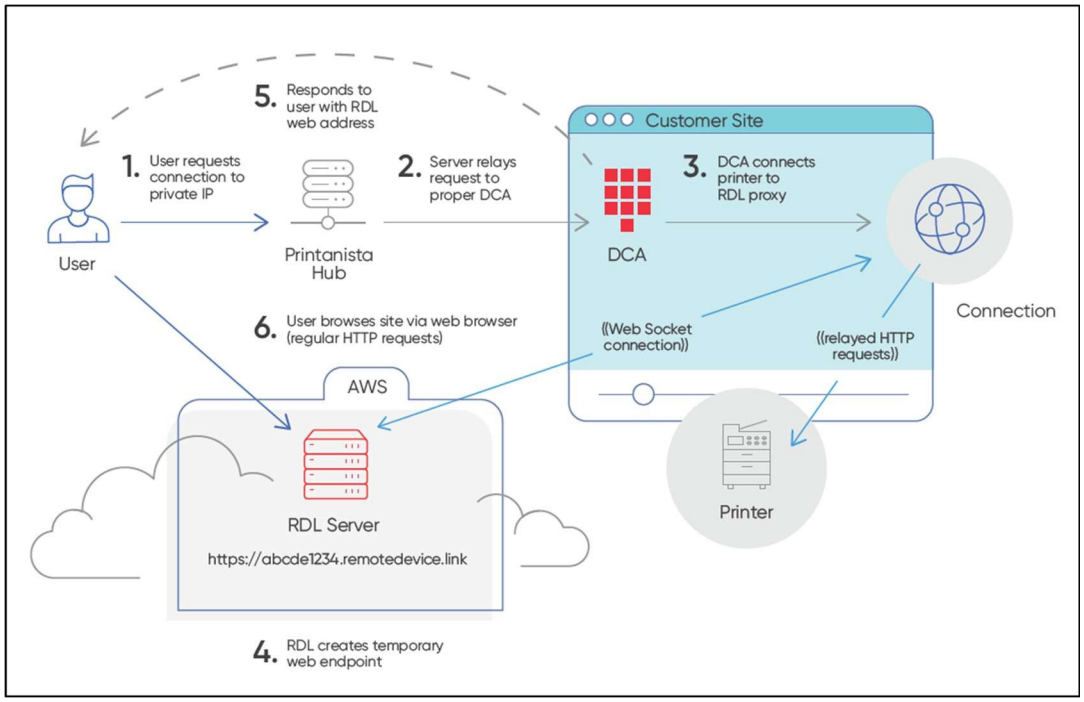
Hinweis: ECI DCA initiiert immer die Kommunikation mit dem Printanista-Server und nicht umgekehrt.

Hinweis: Die Kommunikation findet nur statt, wenn sich Informationen zu Zähler, Versorgung oder Fehlern aktualisiert oder geändert haben, wodurch die Bandbreitennutzung reduziert wird.

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

 ©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- en (RDL)

Remote Device Link (RDL) ist ein Dienst, mit dem ein Remote-**Endbenutzer** auf einen HTTP-Endpunkt in einem privaten LAN zugreifen kann. 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 die DCA eingebettet), der im privaten LAN ausgeführt wird
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 Endpunktport und/oder SSL-Status.

Aktivierungs- und Konfigurationsberechtigungen

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

Auditierungs sfunktionen

1. Lokale Überprüfung der Details jeder Sitzung durch 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

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

Sicherheit der Remote Device Link (RDL)-

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

zentrales Anliegen. Autorisierung:

- Der Benutzer muss über eine Berechtigung innerhalb von 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 Datenerfassungsagent (DCA) stellt nur eine Remote Device Link (RDL)-Verbindung zu bekannten und aktuell überwachten Druckgeräten innerhalb des IP-Bereichs (der IP-Bereiche) des Datenerfassungsagenten (DCA) her.
- Jede einzelne Webanfrage muss an dieselbe IP-Adresse gerichtet sein – der Datenerfassungsagent (DCA) folgt keinen Weiterleitungen.

Verbindungssicherheit:

- Alle Verbindungen zum und vom Remote Device Link (RDL) und den Printanista Hub-Servern werden mit der Standardversion 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 nur zu Beginn der durch TLS-Verschlüsselung gesicherten Sitzung gesetzt wird.
- Der Data Collection Agent (DCA) kann eine unverschlüsselte HTTP-Verbindung zum Druckgerät über das lokale Netzwerk herstellen, unterstützt jedoch die Mindestversion TLS 1.2, wenn das Gerät dies ebenfalls tut.

Sitzungszeitlimits:

- Jede einzelne Remote Device Link (RDL)-Sitzung läuft standardmäßig nach 20 Minuten Inaktivität ab, wobei die maximale Dauer 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 die Verbindung erfordert ein gültiges, vertrauenswürdiges SSL-Zertifikat, um über eine TLS-Verbindung genutzt werden zu können.

Der gesamte Datenverkehr vom DCA zum Internet wird verschlüsselt. Der ECI DCA kann jedoch über einfache HTTP-Verbindungen mit dem Gerät im lokalen Netzwerk 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- sanwendung

Die Funktionen von Printanista Hub sind über eine webbasierte Benutzeroberfläche

zugänglich. Berechtigungsbasierte Benutzerverwaltung

Der Zugriff auf das Web-Frontend des Printanista Hub wird durch eine berechtigungsbasierte Benutzerverwaltung kontrolliert. Benutzer müssen sich mit einem festgelegten Benutzernamen und Passwort bei Printanista anmelden. Benutzern werden eine oder mehrere Rollen zugewiesen, die ihre Berechtigungen festlegen, und sie erhalten Zugriff auf eine oder mehrere Gerätegruppen. Administratoren mit uneingeschränkten Berechtigungen können genau festlegen, welche Bildschirme jeder Benutzer anzeigen und/oder mit denen er interagieren kann.

HTTPS-Zugriff

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

Printanista Side-By-Side

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

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

Sichere Rechenzentren von ECI

Unser Service wird in dedizierten Räumen in erstklassigen Rechenzentren bereitgestellt. Diese Einrichtungen bieten Support auf

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

erhalten

[ECI Cloud Security Overview 2021 (ecisolutions.com)]

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

Versionsverwaltung Test- und

Freigabeprozess

Jede größere und kleinere Version der Software durchläuft einen Qualitätskontrollprozess, in dem mehrere Mitarbeiter von Printanista die geänderten Teile des Systems einem Regressionstest unterziehen, um sicherzustellen, dass es zu keiner Verschlechterung der Sicherheit oder Funktionalität des Systems gekommen ist, und um die neuen funktionalen Aspekte zu validieren. Größere Versionen 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 gespeichert, auf das nur autorisierte Personen Zugriff haben. Jede Änderung am Quellcode muss von zwei autorisierten Entwicklern genehmigt werden, bevor sie in das Produktionscode-Repository übernommen wird, in dem jede Änderung protokolliert wird, einschließlich des Entwicklers, der die Änderung vorgenommen hat, und des Grundes dafür. Die Produkte werden vor dem Versand verschlüsselt und mit einem vertrauenswürdigen Code-Signing-Zertifikat digital signiert. Auf Anfrage kann eine Treuhandhinterlegung vorgenommen werden.

ECI beauftragt einen branchenführenden, CREST-, SOC 2-, NSA-CIRA- und CSA-STAR-zertifizierten unabhängigen Dritten mit der Durchführung von Penetrationstests auf Anwendungsebene und behebt die Ergebnisse auf der Grundlage seiner Geschäftsanforderungen und seines internen Risikomanagement-Rahmens. Penetrationstests werden mindestens einmal jährlich oder bei größeren Änderungen am System durchgeführt. Die Richtlinie von ECI sieht vor, dass alle kritischen Ergebnisse innerhalb von 30 Tagen oder innerhalb eines angemessenen Zeitraums mit einem vorgelegten Business Case mit wirtschaftlich vertretbarem Aufwand behoben werden. 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.

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

Datenschutz und Datenschutz-

e 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 eingeführt. Das Programm umfasst unter anderem Mitarbeiterschulungen, Audits und Risikobewertungen im gesamten Unternehmen, Richtlinien und Verfahren, Governance sowie kontinuierliche Compliance-Maßnahmen. Wir empfehlen unseren Kunden, ähnliche Schritte zu unternehmen, um sicherzustellen, dass ihre eigenen Unternehmen die DSGVO auch in den kommenden Jahren einhalten.

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

Die Softwareanwendungen von Printanista sammeln, 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.

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

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

Die gesamte Kommunikation muss von den Printanista-Produkten ausgehen, und es gibt keine Möglichkeit, von außerhalb des Netzwerks auf die Produkte 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 bestimmter Gesetze und/oder Vorschriften wenden Sie sich bitte an Ihren ECI-Kundenbetreuer.

Hier ist ein Link zur ECI Cloud Security: ECI Cloud Security Overview 2021 (ecisolutions.com)

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

Häufig gestellte Fragen (FAQs) zu „ “

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 ausgeführt wird.
Was sind die Mindestanforderungen für Printanista Hub, ECI DCA und Onsite?
Bitte lesen Sie den Abschnitt „Anwendungsanforderungen für Printanista“ in diesem Dokument.

Sind Printanista-Produkte mit Mac-, Linux- oder Raspberry Pi-Umgebungen kompatibel?
Dieses ECI DCA bietet gegenüber Onsite DCA erhebliche Vorteile, ohne dass Funktionen verloren gehen, darunter die vollständige native plattformübergreifende Unterstützung von Windows, macOS, Linux und Raspberry Pi. Für jede dieser Plattformen gibt es eigene Installationsschritte, Support-Dokumentationen und geschulte Support-Mitarbeiter. Der Installationsprozess wurde ebenfalls erheblich 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 zum Hosten der webbasierten Benutzeroberfläche (UI), der während der Installation automatisch eingerichtet wird.

Können Sie ECI DCA auf einem Computer installieren, der bereits eine andere IIS-Website hostet?
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)	Ihr 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 ausgeführt wird und Audits durchführt und nach vordefinierten Zeitplänen 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 Auditergebnisse aufgenommen, wodurch manuelle Eingriffe begrenzt werden.

Mit welchen Gerätemarken funktioniert die Remote Device Link (RDL)-Überwachung? Was sind die Voraussetzungen dafür?
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 außerhalb dieses Netzwerks befindlichen Betreiber wird ein sicherer Kanal geöffnet. RDL meldet nur Geräte zurück, die über ECI DCA entdeckt und aktiv überwacht werden. Es erscheint eine Meldung, dass die Geräteverbindung über DCA nicht unterstützt wird.

 ©2025 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 festgestellt, dass Geräte innerhalb von Zehntelsekunden auf die ersten Verbindungsversuche reagieren, wobei sie von der aktuellen Nutzung oder den für die Benutzeroberfläche (UI) verfügbaren Ressourcen beeinflusst werden.

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

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

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

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

Informationen zu Legacy Onsite DCA

Es wird empfohlen, ECI DCA mit Printanista zu verwenden. Legacy Onsite DCA funktioniert jedoch derzeit auch 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
- 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 Computer installiert, der rund um die Uhr oder mindestens während der gesamten Geschäftszeiten in Betrieb ist
- Während der Installation muss als lokaler Administrator (oder gleichwertig) angemeldet sein

Überlegungen 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 sein

Netzwerkanforderungen:

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

Bitte verwenden Sie ECI DCA, wenn macOS-, Linux- oder Raspberry Pi-Betriebssysteme erforderlich sind. Das ältere 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 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 eingehend/ausgehend 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 aktuellen 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.

Netzwerkerkennung und Erfassung von Verbrauchsdaten (Onsite DCA)

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

Printanista Hub-Administratoren können aktivierte Onsite-DCAs (Data Collection Agent) auf dem Server aus der Ferne verwalten und Onsite aus der Ferne dazu veranlassen, vordefinierte Befehle auszuführen, z. B. Datenerfassungsaufgaben, Bereitstellung von Onsite-Protokollen, Ausführen von Remote-MIBWalks, Installieren von HP JAMC oder Aktualisieren 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 können jedoch auch Aufgaben (Cache, Zähler, Verbrauchsmaterialien, Service) ausgewählt werden, die sofort ausgeführt werden und auf Befehl Gerätedaten erfassen.
MIB-Walks	Einstellungen vor Ort	Es können bestimmte IPv4/IPv6/Hostnamen von Geräten angegeben und der Vor-Ort-Standort dazu veranlasst werden, die Erfassung der MIB-Walks sofort zu starten.
Protokolle (detailliert)	Einstellungen vor Ort	Kann Onsite anweisen, die Protokolle (kritisch, Fehler, Warnung, Details, Debug) ab einem bestimmten Datum zu sammeln.

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

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

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

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

Netzwerkverkehr

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 vom Zielgerät unterstützten Feldern, wobei jede Geräteabfrage nicht mehr als einige Kilobyte an Daten umfasst. Um die genutzte Netzwerkbandbreite weiter zu reduzieren, kommuniziert Onsite DCA mit nicht mehr als 20 Geräten gleichzeitig. Jede IP-Adresse innerhalb der konfigurierten Bereiche wird abgefragt, und wenn innerhalb der konfigurierten Zeitüberschreitung keine Antwort empfangen wird, wird zur nächsten IP-Adresse weitergegangen. Als Faustregel gilt, dass Printanista in knapp einer Stunde Informationen zu etwa 65.000 Geräten sammelt.

 ©2025 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 das Extrahieren bestimmter Informationen verhindern.

Virenproblematik

Die Printanista-Anwendungsdateien wurden digital signiert, um eine Ausführung zu verhindern, wenn die Dateiintegrität beeinträchtigt ist. Dadurch wird sichergestellt, dass eventuell vorhandene Viren nicht aktiviert werden und sich nicht von einem Netzwerk auf ein anderes ausbreiten können. Für zusätzliche Sicherheit empfehlen wir die Verwendung einer Antivirensoftware in Ihrem Netzwerk.

ECI bietet Support-Services ausschließlich für die neueste im Handel erhältliche Version der Software sowie für die unmittelbar vorhergehende Version der Software. Diese Richtlinie gilt für alle ECI-Produkte zur Geräteverwaltung.

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.