



# White paper tecnico di Printanista Hub

Versione 1.10



# Indice

Panoramica .....	4
Printanista Hub progettato come applicazione ospitata .....	5
Data center sicuri ECI .....	5
Agente di raccolta dati (DCA) .....	5
<b>Applicazione backend Printanista Hub</b> .....	6
<b>Requisiti dell'applicazione Printanista</b> .....	7
<b>Agente di raccolta dati (ECI DCA)</b> .....	7
Requisiti PC/server per ECI DCA .....	7
Server aggiornamenti ECI .....	8
Aggiornamenti software .....	8
Registrazione .....	8
Area di assistenza .....	8
Dati raccolti e crittografia.....	9
<b>Crittografia dei dati</b> .....	9
<b>Questioni di sicurezza</b> .....	9
<b>Tipi di informazioni raccolte</b> .....	9
Collegamento remoto al dispositivo (RDL).....	11
<b>Panoramica del sistema – Remote Device Link (RDL)</b> .....	11
<b>Sicurezza: porte e SSL (Secure Sockets Layer)</b> .....	11
<b>Abilitazione e autorizzazioni</b> .....	11
<b>Funzionalità di auditing</b> .....	11
<b>Sicurezza del collegamento remoto ai dispositivi (RDL)</b> .....	12
La sicurezza del collegamento ai dispositivi remoti (RDL) è stata una preoccupazione fondamentale durante lo sviluppo di questo strumento.....	12
Applicazione Printanista Hub .....	13
Gestione utenti basata sui permessi .....	13
Accesso HTTPS.....	13
Printanista Side-By-Side.....	13
Hosting dell'applicazione Printanista Hub .....	13
Data center sicuri ECI .....	13
Gestione delle versioni .....	14
Processo di test e rilascio .....	14
Sicurezza del codice sorgente.....	14
Privacy dei dati e legislazione.....	15
<b>Regolamento generale sulla protezione dei dati (GDPR)</b> .....	15
Domande frequenti (FAQ).....	16
Informazioni sul DCA in loco legacy.....	18

Requisiti PC/server per DCA in loco:.....	18
Considerazioni sul firewall in uscita (porta 80 o 443).....	18
Requisiti di rete .....	18
La versione legacy di Java Onsite su sistemi Linux e macOS non è funzionante .....	18
Requisiti PC/stampante per l'utilizzo dell'agente locale (installazione opzionale).....	18
Rilevamento della rete e raccolta dei dati relativi a contatori e forniture (DCA Onsite).....	19
Traffico di rete .....	19
Assistenza del produttore .....	20
Preoccupazioni relative ai virus .....	20

**ECI fornirà servizi di assistenza esclusivamente per l'ultima versione del Software disponibile in commercio, nonché per la versione immediatamente precedente del Software. Questa politica si applica a tutti i prodotti ECI Device Management.**

**Microsoft®, .NET Framework®, Windows® e Windows Server® sono marchi registrati o marchi di Microsoft Corporation**

## Panoramica

---

La suite di prodotti Printanista offre una soluzione di gestione della stampa di classe enterprise molto facile da usare e da implementare. È stata progettata e realizzata per sfruttare le funzionalità avanzate e i vantaggi della piattaforma Microsoft .NET. Pertanto, non sono più necessari tecnici esperti per installare il software, configurare e mantenere il sistema. I prodotti Printanista non possono in alcun modo essere configurati per eseguire attività diverse da quelle per cui sono stati progettati. La trasmissione di dati dai prodotti a fonti esterne è strettamente limitata. I prodotti non riportano alcun altro dettaglio se non le informazioni relative alle apparecchiature monitorate (ad esempio, il tipo di apparecchiatura). Nessuna informazione riservata viene mai trasmessa al di fuori della rete tramite i prodotti Printanista. La suite è composta dai seguenti componenti:

**Printanista Hub:** un sito web e un sistema di backend che ospita tutti i dati ricevuti dagli strumenti di raccolta dati Printanista. Si tratta di un archivio che consente di visualizzare i dati utilizzando un browser, generare report, configurare flussi di lavoro di avviso e notifiche e sincronizzare i dati con i sistemi ERP per la fatturazione o l'evasione degli ordini.

**ECI DCA:** Questo nuovissimo agente di raccolta dati (DCA) offre notevoli vantaggi rispetto all'agente di raccolta dati in loco (DCA) senza rinunciare a nessuna funzionalità, tra cui il supporto multiplatforma nativo completo per Windows, macOS, Linux e Raspberry Pi, ciascuno con procedure di installazione specifiche, documentazione di supporto e personale di assistenza qualificato su queste piattaforme. ECI DCA garantisce inoltre il rilevamento e la scansione continui dei dispositivi, funzionalità migliorate di MIBWalk e raccolta dei log, oltre alla possibilità di acquisire dati da molti più tipi di contatori.

**DCA in loco:** uno strumento legacy di raccolta dati che esegue automaticamente valutazioni di stampa e monitora i livelli dei materiali di consumo, lo stato delle stampanti e i registri degli errori. Questa applicazione viene installata presso la sede del cliente ed è in grado di eseguire valutazioni di stampa in modo automatico e programmato senza l'intervento umano. I dati acquisiti vengono inviati al sito web Printanista Hub tramite HTTPS, HTTP o, se il cliente lo preferisce, un file crittografato proprietario.

Lo scopo di questo documento è fornire una panoramica della linea di prodotti Printanista Suite da un punto di vista tecnico, per aiutare a rispondere alle domande più frequenti che i team IT riceveranno.

## Come funziona Printanista

---

### Printanista Hub progettato come applicazione in hosting

Printanista Hub è ospitato da ECI Software Solutions all'interno di data center sicuri e protetti in diverse regioni del mondo. ECI Software Solutions è consapevole che la riservatezza, l'integrità e la disponibilità delle informazioni dei nostri clienti sono fondamentali per le loro operazioni aziendali e per il nostro stesso successo. Utilizziamo un approccio a più livelli per proteggere tali informazioni chiave, monitorando e migliorando costantemente la nostra applicazione, i nostri sistemi e i nostri processi, al fine di soddisfare le crescenti esigenze e sfide in materia di sicurezza.

### Data center sicuri di ECI

Il nostro servizio è collocato in spazi dedicati presso data center di prim'ordine. Queste strutture forniscono un supporto di livello carrier. Questo link rimanda al documento dettagliato di ECI relativo alla sicurezza dei data center.

[Panoramica sulla sicurezza del cloud ECI](#)

### Agente di raccolta dati (DCA)

Il motore centrale dell'agente di raccolta dati, che costituisce il cuore di ogni prodotto Printanista, identifica ed estrae correttamente i dati da stampanti, fotocopiatrici e dispositivi multifunzione collegati in rete, utilizzando i protocolli supportati dai dispositivi stessi.

Printanista attualmente supporta i protocolli SNMP (Simple Network Management Protocol) v1, v2c e v3. SNMP v3 offre una maggiore protezione dei pacchetti per garantire che le informazioni e le comunicazioni vengano trasmesse tramite fonti affidabili. A differenza di SNMP v1 o v2, SNMP v3 è crittografato per una maggiore sicurezza e richiede sia un nome utente che una password. Un vantaggio dell'utilizzo di SNMP v3 è che gli amministratori di rete possono determinare il metodo di crittografia, nonché un nome utente e una password sicuri.

SNMP è un protocollo di rete che facilita lo scambio di informazioni tra i dispositivi di rete estraendo dati dalla Management Information Base (MIB) e da altre posizioni all'interno del dispositivo di stampa. La Management Information Base (MIB) è un database interno che la maggior parte dei dispositivi connessi in rete possiede come parte della propria struttura. La Management Information Base (MIB) contiene dati quali il nome del modello, i livelli di toner e lo stato attuale della stampante.

## Requisiti di Printanista

### Applicazione backend di Printanista Hub

Tutti i dati raccolti vengono inviati al server Printanista Hub, dove vengono resi disponibili per la creazione di report e la generazione di avvisi.

ECI DCA si connette al server Printanista Hub utilizzando HTTPS (porta **443/TCP**). Si prega di contattare l'amministratore di ECI Solutions per informazioni sui nomi di dominio e sugli indirizzi IP utilizzati dal server.

Questa connessione è protetta dallo standard di settore **TLS** (Transport Layer Security).

**È richiesta la versione minima TLS 1.2.**

Questa connessione rimane aperta per tutto il tempo in cui ECI DCA è in esecuzione. Normalmente viene utilizzata una connessione **WebSocket**, ma in alcune situazioni ECI DCA potrebbe ricorrere all'utilizzo **di eventi inviati dal server** o **al long polling HTTP**.

**NOTA IMPORTANTE:** sono necessarie diverse connessioni in uscita HTTPS sicure dal server su cui è installato Printanista Hub:

- <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>

### Requisiti di sistema di Printanista Hub

Utilizza il seguente link per le specifiche di sistema complete e aggiornate del prodotto Printanista:

[Requisiti di sistema di Printanista Hub v4.0](#)

## Requisiti dell'applicazione Printanista

### Agente di raccolta dati (ECI DCA)

Stampanti, fotocopiatrici e dispositivi multifunzione devono avere il protocollo SNMP (Porta 161) abilitato per il rilevamento e l'estrazione delle informazioni. Il protocollo SNMP è una parte standard del livello applicativo della suite TCP/IP.

### Requisiti PC/server per ECI DCA:

#### Requisiti Microsoft Windows (x86/64):

- Microsoft .NET Framework 4.7.2. o versioni successive (consigliata: versione più recente)
- Versioni di Windows Server (ad eccezione delle edizioni Datacenter e Core) e di Windows
  - *Le versioni Microsoft non più supportate da Microsoft non sono supportate da ECI DCA.*
- Le impostazioni della rete locale e/o del firewall consentono [la connessione ai servizi del server degli aggiornamenti ECI e al server hub di Printanista](#)

#### Requisiti per Linux (x86/64 o ARM):

- Mono Framework 5.4 o superiore (consigliata: versione più recente)
- Le impostazioni della rete locale e/o del firewall consentono [la connessione ai servizi del server ECI Updates e al server Printanista Hub.](#)
- Sono ufficialmente supportate solo le versioni di Ubuntu LTS 20.04 e successive.

#### Requisiti per macOS (x64):

- Mono Framework 5.4 o superiore (consigliata: versione più recente)
- Da macOS® Sierra (10.12) a Sequoia (15.4). Le versioni più recenti non sono supportate.
- Le impostazioni della rete locale e/o del firewall consentono [la connessione ai servizi del server ECI Updates e al server Printanista Hub.](#)

#### Requisiti per Raspberry Pi:

- Raspberry Pi 3 Modello B o Pi 4 Rev 1.5. Le versioni più recenti non sono supportate.
- Scheda microSD vuota da 8 GB o superiore
- PC in grado di scrivere su scheda microSD
- Le impostazioni della rete locale e/o del firewall consentono [la connessione ai servizi del server ECI Updates e al server Printanista Hub.](#)

### Considerazioni sul firewall per ECI DCA:

**Connessioni in entrata** - Non ci sono connessioni in entrata da Internet verso ECI DCA.

#### Connessioni in uscita

Servizio	Porta	Connessione a
Caricamento dati	443/TCP (HTTPS)	Il tuo server Printanista Hub
Aggiornamenti software	443/TCP (HTTPS)	Server aggiornamenti ECI
Registrazione (fallback)	53/UDP (DNS)	Server DNS della rete locale (primario) Server aggiornamenti ECI (fallback)

## Server aggiornamenti ECI

ECI Updates Server è un servizio gestito da [ECI Device Management](#) per facilitare la registrazione dei dispositivi DCA, gli aggiornamenti automatici del software e l'installazione dei dispositivi DCA (questo sito) ed è necessario per il funzionamento dei dispositivi DCA di ECI. Nota: i dispositivi DCA di ECI non inviano all'ECI Updates Server alcun dato raccolto relativo ai dispositivi o alla configurazione.

## Aggiornamenti software

ECI DCA si aggiorna automaticamente scaricando gli aggiornamenti pubblicati su <https://updates.printanista.net/>. Le connessioni vengono sempre effettuate sulla porta HTTPS standard **443/tcp**.

## Registrazione

ECI DCA utilizza richieste DNS a [\\*.reg.pf-d.ca](#) per registrarsi. Proverà prima a farlo utilizzando i server DNS della rete locale, per poi ricorrere alla comunicazione diretta con gli indirizzi IP del server di aggiornamenti ECI (utilizzando la porta **53/udp**). Il firewall deve consentire questa connessione al server di aggiornamenti ECI solo se i server DNS locali non risolvono le richieste di registrazione.

## Area di servizio

ECI DCA viene indirizzato verso la regione che presenta la minore latenza di rete, in base alla disponibilità del servizio. In alcune località, la regione utilizzata potrebbe cambiare nel tempo, poiché l'attività sull'infrastruttura Internet globale può influire sulla latenza.

## Dati raccolti e crittografia

### Crittografia dei dati

Tutti i pacchetti di dati provenienti da ECI DCA e dal DCA Onsite legacy sono codificati e offuscati. Printanista richiede l'uso di HTTPS per la comunicazione tra i DCA e l'Hub Printanista. ECI DCA richiede HTTPS per funzionare. Inoltre, tutte le impostazioni e i lavori sensibili tra ECI DCA e Printanista sono crittografati utilizzando l'algoritmo di crittografia simmetrica standard AES256, con una chiave condivisa protetta. Ciò garantisce la crittografia end-to-end, in modo che i dati siano protetti dalla lettura se intercettati da terzi, da un'istanza Printanista concorrente o comunque non autorizzata.

### Questioni di sicurezza

ECI DCA e Onsite DCA legacy comunicano con Printanista Hub tramite il protocollo HTTPS, utilizzando lo standard industriale **TLS 1.2** (Transport Layer Security). I dati riservati non vengono raccolti, visualizzati o salvati da nessuna applicazione Printanista. Vengono raccolti e visualizzati solo i dati relativi alla stampante. Nessun altro dato di rete può essere identificato o raccolto da ECI DCA o Onsite DCA legacy, ad eccezione dell'indirizzo IP, dell'indirizzo MAC e del nome host.

ECI DCA e la versione precedente di Onsite DCA non raccolgono né trattano dati personali. L'unico caso in cui il sistema raccoglie questo tipo di informazioni è quando l'utente o i suoi clienti inseriscono i dati in Printanista in un campo o in un'etichetta, ad esempio la località o il nome del cliente. ECI DCA e Onsite DCA legacy consentono di monitorare i dispositivi di rete utilizzando il Simple Network Management Protocol (SNMP). L'applicazione viene distribuita all'interno della rete del cliente e da lì comunica con i dispositivi per raccogliere informazioni operative sul dispositivo rese disponibili tramite il firmware del dispositivo e una Management Information Base (MIB) SNMP. I dati esposti dal dispositivo variano a seconda del produttore e del modello. Sono sempre di natura tecnica o operativa e specifici del dispositivo stesso. Al livello più elementare, i dati esposti da una MIB della stampante sono documentati nell'IETF RFC 3805 (<https://tools.ietf.org/html/rfc3805>). Ulteriori informazioni sul dispositivo possono essere rese disponibili dal produttore tramite estensioni e MIB (Management Information Base) private, ma le informazioni sono fondamentalmente tecniche e specifiche del dispositivo.

### Printanista Hub memorizza solo:

- Nome host
- Sistema operativo
- Indirizzo IP remoto
- Architettura di sistema

*Altre informazioni relative alla rete e all'ambiente vengono raccolte e visualizzate durante la connessione a scopo di risoluzione dei problemi, ma non vengono mai memorizzate in Printanista.*

### Tipi di informazioni raccolte

ECI DCA e la versione precedente di Onsite DCA tentano di raccogliere le seguenti informazioni dai dispositivi di stampa collegati in rete durante una scansione della rete:

#### Attributi del dispositivo

- Indirizzo IP (può essere mascherato)
- Produttore
- Numero di serie
- Numero di inventario
- Indirizzo MAC
- Descrizione del dispositivo
- Ubicazione
- Varie (specifiche della macchina)

#### Assistenza

- Lettura LCD
- Stato del dispositivo
- Codici di errore
- Firmware

#### Materiali di consumo

- Numero di serie della cartuccia toner
- Livello di toner della cartuccia
- Livelli del tamburo
- Livelli del kit di manutenzione
- Livelli dei materiali di consumo non toner
- Livelli vari
- Dettagli sulle forniture per stampanti a etichette

#### Copertura e contatori

- Lettura contatori
- Tipo di contatore
- Livello di copertura
- Identificazione in bianco e nero o a colori

## Rilevamento della rete e raccolta dei dati

Per aumentare l'efficienza del DCA, le informazioni vengono inviate al server Printanista Hub solo quando sono presenti dati nuovi o modificati provenienti dai dispositivi. Ciò garantisce un carico di rete minimo ed elimina la frequenza di eventuali accumuli di invii di dati dei dispositivi. Inoltre, il rilevamento e la scansione dei dispositivi sono ora indipendenti per garantire che venga scansionato solo l'indirizzo IP

(o il nome host) dei dispositivi precedentemente rilevati venga sottoposto a scansione a intervalli periodici, anziché effettuare una scansione completa della rete (quest'ultima viene eseguita inizialmente, periodicamente o quando stabilito da un utente amministratore).

Ciò garantirà che la velocità di invio dei dati dei dispositivi sia il più aggiornata possibile. Ciò consente agli utenti di essere avvisati di dispositivi problematici in pochi minuti o addirittura secondi in molte situazioni. ECI DCA separa il rilevamento dei dispositivi da altri tipi di scansione, consentendo di impostare intervalli di scansione personalizzati per il recupero di contatori, attributi dei materiali di consumo ed errori. I valori predefiniti, minimi e massimi per gli intervalli di scansione sono:

Funzione di scansione	Predefinito	Minimo	Massimo
Rilevamento	60 minuti	10 minuti	7 giorni
Metri	24 ore	30 minuti	14 giorni
Rifornimenti	4 ore	30 minuti	7 giorni
Errori	60 minuti	30 minuti	7 giorni
Attributi	24 ore	1 ora	14 giorni

Si prega di notare che gli intervalli di scansione (contatori, forniture, errori e attributi) sono disponibili solo se un dispositivo dispone di un file di definizione del modello (MDF). In caso contrario, verrà eseguita una scansione completa sul dispositivo in questione utilizzando un intervallo predefinito.

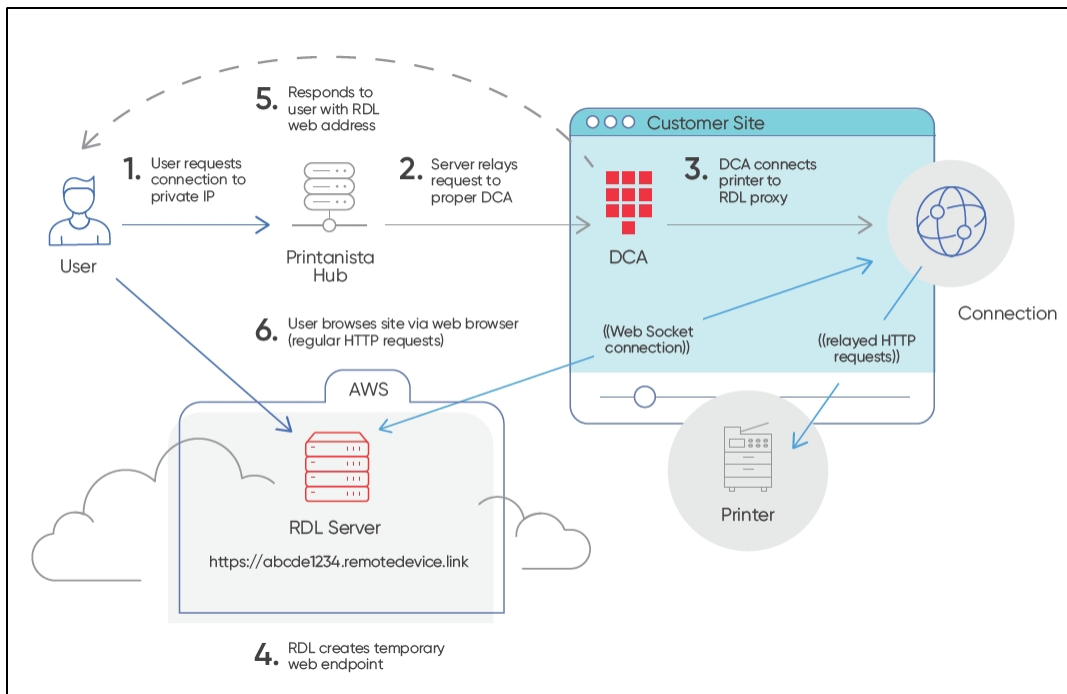
Gli amministratori di Printanista Hub possono gestire in remoto gli ECI DCA che sono stati attivati sul server. Possono attivare in remoto l'ECI DCA per eseguire comandi predefiniti quali attività di raccolta dati, fornitura di log ECI DCA, esecuzione di MIB Walk in remoto o aggiornamento delle impostazioni ECI DCA.

**Nota:** è sempre ECI DCA ad avviare la comunicazione con il server Printanista, e non viceversa.

**Nota:** la comunicazione avviene solo quando le informazioni relative al contatore, alle forniture o agli errori sono state aggiornate o modificate, riducendo così l'utilizzo della larghezza di banda.

**Nota:** al momento HP JAMC funziona solo con il DCA Onsite legacy.

## Collegamento dispositivo remoto (RDL)



### Panoramica del sistema – Remote Device Link (RDL)

**Remote Device Link (RDL)** è un servizio che consente a un **utente finale** remoto di accedere a un endpoint HTTP su una LAN privata. È costituito da 4 componenti principali:

1. L'**utente finale** che accede al dispositivo
2. Il **server Remote Device Link**, su Internet pubblico (tramite l'URL [https://\\*.remotedevice.link](https://*.remotedevice.link))
3. Il **client RDL** (integrato nel DCA), in esecuzione sulla LAN privata
4. L'**endpoint HTTP** (stampante) a cui si accede (in esecuzione sulla LAN privata)

### Sicurezza: porte e SSL (Secure Sockets Layer)

Il percorso pubblico per RDL è sempre un URL <https://> sulla porta 443, indipendentemente dalla porta dell'endpoint e/o dallo stato SSL.

### Abilitazione e autorizzazioni

1. Opzione di abilitazione globale per istanza del rivenditore
2. Abilitazione locale per ogni account del cliente finale
3. Sono necessarie delle autorizzazioni affinché un utente possa accedere alla funzionalità

### Funzionalità di auditing

1. Controllo locale di Printanista Hub dei dettagli di ogni sessione
  - a. Report di amministrazione di Printanista Hub per l'auditing di Remote Device Link (RDL)
2. Remote Device Link (RDL): registrazione su cloud AWS (Amazon Web Services) di tutti i dettagli della sessione

## Remote Device Link (RDL) - Sicurezza

La sicurezza di Remote Device Link (RDL) è stata una preoccupazione fondamentale durante lo sviluppo di questo strumento. Autorizzazione:

- L'utente deve disporre dell'autorizzazione all'interno di Printanista Hub per accedere alla funzionalità Remote Device Link (RDL) sull'account specifico
- L'agente di raccolta dati (DCA) accetterà solo le richieste Remote Device Link (RDL) provenienti dal server Printanista Hub che sia stato autenticato reciprocamente
- L'agente di raccolta dati (DCA) stabilisce una connessione RDL (Remote Device Link) solo con i dispositivi di stampa noti e attualmente monitorati che si trovano all'interno degli intervalli IP di rilevamento dell'agente di raccolta dati (DCA).
- Ogni singola richiesta web deve essere indirizzata allo stesso IP – L'agente di raccolta dati (DCA) non seguirà i reindirizzamenti

Sicurezza della connessione:

- Tutte le connessioni da e verso i server Remote Device Link (RDL) e Printanista Hub sono crittografate utilizzando la versione minima standard TLS 1.2 (Transport Layer Security)
- A ogni connessione viene assegnato un nome di dominio univoco che utilizza una combinazione alfanumerica casuale di 19 caratteri (96 bit)
- Ogni richiesta richiede un token di sicurezza a 160 bit, memorizzato come cookie del browser, che viene impostato solo all'inizio della sessione protetta dalla crittografia TLS
- L'agente di raccolta dati (DCA) può stabilire una connessione HTTP non crittografata con il dispositivo di stampa attraverso la rete locale, ma supporta la versione minima TLS 1.2 se il dispositivo la supporta

Limiti di tempo della sessione:

- Ogni singola sessione Remote Device Link (RDL) scade dopo 20 minuti di inattività per impostazione predefinita, con un massimo assoluto di 2 ore.

## Implicazioni

La connessione tra ECI DCA e Printanista Hub è protetta da chiavi di autenticazione specifiche per l'installazione di DCA e richiede un certificato SSL valido e attendibile per poter utilizzare una connessione TLS.

Tutto il traffico in transito dal DCA a Internet è crittografato. Tuttavia, l'ECI DCA può comunicare con il dispositivo nella rete locale tramite connessioni HTTP non crittografate se il dispositivo non supporta connessioni sicure.

## Applicazione Printanista Hub

---

È possibile accedere alle funzionalità di Printanista Hub tramite un'interfaccia utente basata

sul web. Gestione utenti basata su autorizzazioni

L'accesso all'interfaccia web di Printanista Hub è controllato tramite una gestione degli utenti basata sui permessi. Gli utenti devono effettuare l'accesso a Printanista utilizzando un nome utente e una password specifici. Agli utenti vengono assegnati uno o più ruoli che specificano i permessi e viene concesso l'accesso a uno o più gruppi di dispositivi. Gli amministratori con permessi completi possono specificare esattamente quali schermate ogni utente può visualizzare e/o con cui può interagire.

### Accesso HTTPS

Printanista richiede che tutti i siti utilizzino HTTPS con un certificato di sicurezza SSL valido. Ciò garantisce la crittografia dei dati trasferiti su Internet.

### Printanista Side-By-Side

Printanista Hub utilizza un database di metadati dei modelli noto come Side-by-Side (SBS), che contiene vari attributi dei modelli quali: velocità di stampa, data di introduzione sul mercato o compatibilità dei codici OEM, che viene aggiornato periodicamente man mano che i produttori OEM rilasciano nuovi modelli e versioni. Printanista Hub comunicherà con Side-by-Side per verificare la presenza di nuovi aggiornamenti e per recuperare i metadati dei dispositivi da memorizzare nella cache locale su ciascun sistema Printanista Hub.

### Hosting dell'applicazione Printanista Hub

Printanista Hub è ospitato da ECI Software Solutions all'interno di data center sicuri e protetti situati in diverse regioni del mondo. ECI Software Solutions è consapevole che la riservatezza, l'integrità e la disponibilità delle informazioni dei nostri clienti sono fondamentali per le loro attività aziendali e per il nostro stesso successo. Adottiamo un approccio a più livelli per proteggere tali informazioni chiave, monitorando e migliorando costantemente le nostre applicazioni, i nostri sistemi e i nostri processi, al fine di soddisfare le crescenti esigenze e sfide in materia di sicurezza.

### Data center sicuri ECI

Il nostro servizio è collocato in spazi dedicati presso data center di prim'ordine. Queste strutture forniscono un supporto di livello carrier. Clicca sul seguente link per ottenere il documento dettagliato di ECI relativo alla sicurezza dei data center

[Panoramica sulla sicurezza del cloud ECI](#)

## Gestione delle versioni

### Processo di test e rilascio dell'

Ogni versione principale e secondaria del software viene sottoposta a un processo di controllo qualità, in cui più membri del personale di Printanista eseguono test di regressione sulle parti modificate del sistema per garantire che non vi sia stato un peggioramento della sicurezza o della funzionalità del sistema, oltre a convalidare i nuovi aspetti funzionali. Le versioni principali vengono sottoposte a un processo di rilascio beta in cui alcuni clienti selezionati eseguono il nuovo e il vecchio sistema in parallelo.

### Sicurezza del codice sorgente

Il codice sorgente di Printanista è conservato in un sistema di controllo delle revisioni protetto, accessibile solo a persone autorizzate. Ogni modifica al codice sorgente richiede l'approvazione di due sviluppatori autorizzati prima di essere accettata nel repository del codice di produzione, dove ogni modifica viene tracciata, indicando chi l'ha apportata e il motivo. I prodotti vengono crittografati e firmati digitalmente con un certificato di firma del codice affidabile prima della spedizione. Su richiesta, è possibile disporre di un deposito a garanzia.

ECI si avvale di un ente terzo indipendente leader del settore, certificato CREST, SOC 2, NSA-CIRA e CSA-STAR, per condurre test di penetrazione a livello di applicazione e correggere i risultati in base ai propri requisiti aziendali e al proprio quadro interno di gestione dei rischi. I test di penetrazione vengono condotti almeno una volta all'anno o quando vengono apportate modifiche significative al sistema. La politica di ECI è quella di compiere ogni sforzo commercialmente ragionevole per correggere tutti i risultati critici entro 30 giorni o entro un lasso di tempo ragionevole, previa presentazione di un business case. ECI non divulga dettagli relativi ai propri controlli di sicurezza o ai risultati dei test di penetrazione, poiché tali informazioni sono proprietarie e riservate e, se finissero nelle mani sbagliate, potrebbero comportare un aumento del rischio.

## Privacy dei dati e legislazione

### Regolamento generale sulla protezione dei dati (GDPR)

A partire da maggio 2018, il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea è entrato pienamente in vigore. Il GDPR sostituisce la Direttiva 95/46/CE sulla protezione dei dati ed è stato concepito per rafforzare e unificare le leggi sulla privacy dei dati in tutta Europa.

ECI ha implementato un programma di conformità al GDPR strutturato e completo. Il programma comprende, tra le altre cose, la formazione del personale, l'audit e la valutazione dei rischi in tutta l'azienda, le politiche e le procedure, la governance e gli sforzi continui per garantire la conformità. Incoraggiamo i nostri clienti ad adottare misure simili per garantire che le loro aziende siano conformi al GDPR ora e negli anni a venire.

-----

I prodotti Printanista non elaborano, monitorano né gestiscono dati personali o informazioni specifiche relative a una singola persona o a un gruppo di persone.

Le applicazioni software Printanista non raccolgono, conservano o trasmettono alcuna informazione relativa al contenuto dei lavori di stampa.

Printanista non ha alcun modo di accedere, archiviare o trasmettere informazioni ad alto rischio, anche se tali informazioni vengono stampate o inviate in altro modo a dispositivi di stampa monitorati dalle applicazioni software Printanista.

Le applicazioni software Printanista non memorizzano, elaborano o trasmettono dati dei titolari di carte o informazioni personali.

Le comunicazioni del motore del prodotto sono controllate tramite un accesso limitato a indirizzi IP e/o intervalli specifici.

Tutte le comunicazioni devono provenire dai prodotti Printanista e non è possibile contattare o accedere ai prodotti dall'esterno della rete.

La comunicazione al di fuori della rete utilizza un flusso di dati compresso proprietario, inviato tramite HTTPS con protocollo SSL standard del settore.

-----

Per informazioni relative alla conformità a leggi e/o normative specifiche, si prega di contattare il proprio Account Manager ECI.

-----

Di seguito è riportato un link alla pagina dedicata alla sicurezza cloud di ECI: [Panoramica su ECI Cloud Security](#)

## Domande frequenti (FAQ)

### I prodotti Printanista funzionano con i proxy Internet?

Sì, ECI DCA funziona con la maggior parte dei proxy. È necessario configurare le impostazioni del proxy sul sistema in cui ECI DCA è installato e opera.

### Quali sono i requisiti minimi per Printanista Hub, ECI DCA e Onsite?

Fare riferimento alla sezione [Requisiti dell'applicazione Printanista](#) in questo documento.

### I prodotti Printanista sono compatibili con gli ambienti Mac, Linux o Raspberry Pi?

Questo ECI DCA offre notevoli vantaggi rispetto all'Onsite DCA senza perdere alcuna funzionalità, compreso il supporto multiplatforma nativo completo per Windows, macOS, Linux e Raspberry Pi. Ciascuna piattaforma dispone di procedure di installazione specifiche, documentazione di supporto e personale di assistenza qualificato. Anche il processo di installazione è stato notevolmente migliorato ed è molto più intuitivo per tutti i tipi di utenti.

### ECI DCA richiede Microsoft Internet Information Services (IIS)?

No. ECI DCA e Onsite DCA includono un proprio server per ospitare l'interfaccia utente (UI) basata sul web e vengono configurati automaticamente durante l'installazione.

### È possibile installare ECI DCA su un computer che ospita già un altro sito web IIS?

Sì. Tuttavia, è necessario inserire nella lista bianca le porte elencate di seguito per garantire la connettività di ECI DCA.

Servizio	Porta	Connessione a
Caricamento dati	443/TCP (HTTPS)	Il tuo server Printanista Hub
Aggiornamenti software	443/TCP (HTTPS)	Server aggiornamenti ECI
Registrazione (fallback)	53/UDP (DNS)	Server DNS della rete locale (primario) Server aggiornamenti ECI (fallback)

ECI DCA utilizza la porta 31816 per impostazione predefinita per l'interfaccia utente web DCA locale.

### Quanta manutenzione continua richiede ECI DCA?

ECI DCA e Onsite DCA sono servizi che operano in background ed eseguono controlli ed esportazioni verso destinazioni configurate secondo scadenze predefinite. Si consiglia di utilizzare sottoreti (intervalli di indirizzi IP) anziché indirizzi IP fissi. Quando si aggiungono nuovi dispositivi alla rete, questi vengono rilevati e inclusi nei risultati dei controlli, limitando così l'intervento manuale.

### Con quali marche di apparecchiature funziona il monitoraggio Remote Device Link (RDL)?

#### Quali sono i requisiti per il suo funzionamento?

Tutte le marche dotate di una pagina web incorporata vengono rilevate da ECI DCA. Le informazioni sulle pagine web incorporate variano a seconda del produttore e del modello. I dispositivi locali non mostreranno la pagina web incorporata.

### Esistono ulteriori preoccupazioni in materia di sicurezza con Remote Device Link (RDL)?

Viene aperto un canale sicuro tra il dispositivo sulla rete locale del cliente e un operatore situato al di fuori di tale rete. RDL segnalerà solo i dispositivi rilevati e monitorati attivamente tramite ECI DCA. Viene visualizzato un messaggio che indica che la connessione del dispositivo non è supportata tramite DCA

**Remote Device Link (RDL) sembra un po' lento, perché?**

Questo è prevedibile, poiché la connessione deve essere instradata attraverso i nostri servizi cloud. Tuttavia, il fattore principale che influisce è la velocità con cui i dispositivi rispondono alle richieste dell'interfaccia utente web (UI).

Abbiamo riscontrato che i dispositivi rispondono in pochi decimi di secondo ai primi tentativi di connessione, ma che la velocità può essere influenzata dall'utilizzo corrente o dalle risorse disponibili per l'interfaccia utente (UI).

**Quali funzionalità sono disponibili con Remote Device Link (RDL)?**

Tutte le opzioni a cui l'OEM consente l'accesso tramite la pagina web integrata sono accessibili tramite Remote Device Link (RDL).

**È possibile disattivare la funzione Remote Device Link (RDL)?**

Sì, è possibile disattivare questa funzione per ogni account.

È inoltre possibile disattivare questa funzione per singolo utente, consentendo di bloccare l'accesso di un utente a Remote Device Link (RDL).

**Dove posso trovare ulteriori informazioni su Printanista Hub, ECI DCA, Onsite DCA legacy, ecc.?**

Ulteriori informazioni sono disponibili sul sito web Printanista dell'ECI:

<https://www.ecisolutions.com/products/printanista-hub/>

## Informazioni su Onsite DCA legacy

Si consiglia di utilizzare ECI DCA con Printanista. Tuttavia, il vecchio Onsite DCA attualmente funziona con Printanista. Requisiti PC/server per Onsite DCA:

- 1 GB di RAM
- 400 MB di spazio su disco
- Microsoft .NET Framework 4.7.2 o versioni successive
- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- La versione 4.1.3 e successive di Onsite supportano Windows Server 2022
- Internet Explorer 11.0 o versioni successive, Chrome, Firefox
- MDAC 2.8 o versioni successive (normalmente incluso con l'installazione di Windows)
- JET 4.0 o versioni successive (normalmente incluso con l'installazione di Windows)
- Installato su un computer attivo 24 ore su 24, 7 giorni su 7, o almeno per l'intera giornata lavorativa
- È necessario effettuare l'accesso come amministratore locale (o equivalente) durante l'installazione

Considerazioni relative al firewall in uscita (porta 80 o 443):

Trasmissione dei dati:

- [https://\(company\\_Printanista\\_FQDN\)/WebServices/Onsite2Service.asmx](https://(company_Printanista_FQDN)/WebServices/Onsite2Service.asmx)
- Applicazione: fmaonsite.exe
- SOAP su HTTP(s) deve essere consentito oltre il firewall

Requisiti di rete:

Il traffico SNMP (Porta 161) deve essere instradabile attraverso la LAN o la WAN (Wide Area Networks)

Si prega di utilizzare ECI DCA se sono necessari sistemi operativi macOS, Linux o Raspberry Pi

Il Java Onsite legacy su sistemi Linux e macOS non è funzionante.

Requisiti PC/stampante per l'utilizzo dell'agente locale (installazione opzionale):

- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- Microsoft .NET Framework 4.7.2 o versione successiva
- Driver aggiornato per la stampante locale (si consiglia l'aggiornamento a HP Update)
- La stampante deve supportare il linguaggio PJI (Printer Job Language) o PML (Printer Management Language)
- Rimuovere eventuali driver di stampa inutilizzati
- Il supporto bidirezionale del driver è abilitato
- Modifiche al Firewall di Windows — Porta 161/33333 in entrata/in uscita sia per TCP che per UDP

*Versioni di Windows e Windows Server supportate da Microsoft. Le versioni non più supportate da Microsoft non sono supportate da ECI.*

**Nota:** per le versioni recenti del sistema operativo che utilizzano il modello di driver 4 (ad es. Windows 10), al momento sono supportati solo i modelli OEM Kyocera e Ricoh e le loro varianti.

Rilevamento della rete e raccolta dei dati di consumo e delle forniture (DCA in loco)

Le impostazioni di rilevamento automatico della rete brevettate da Printanista utilizzano una combinazione di algoritmi per identificare gli intervalli di rete in cui potrebbero trovarsi i dispositivi di stampa, quindi rilevano e comunicano con i dispositivi online, instradando il traffico attraverso diversi elementi di rete quali workstation o server attivi, router, hub, switch e hardware di rete aggiuntivo.

Gli amministratori di Printanista Hub possono gestire in remoto gli Onsite DCA (Data Collection Agent) attivati sul server, nonché attivare in remoto l'Onsite per eseguire comandi predefiniti quali attività di raccolta dati, fornitura di log Onsite, esecuzione di MIBWalk remoti, installazione di HP JAMC o aggiornamento delle impostazioni Onsite. Questi aspetti sono spiegati in maggior dettaglio di seguito:

Funzione	Posizione	Descrizione
Attività	Impostazioni Onsite	È possibile configurare da remoto l'esecuzione delle attività secondo una pianificazione prestabilita, ma è anche possibile selezionare alcune attività (Cache, Contatori, Materiali di consumo, Assistenza) da eseguire immediatamente e raccogliere i dati dei dispositivi su richiesta.
Percorsi MIB	Impostazioni Onsite	È possibile indicare determinati indirizzi IPv4/IPv6/nomi host dei dispositivi e far sì che Onsite avvii immediatamente la raccolta dei MIB Walk.
Registri (dettagliati)	Impostazioni Onsite	È possibile istruire Onsite a raccogliere i log (Critical, Error, Warning, Details, Debug) a partire da una determinata data.

Nessuno di questi comandi comporta la raccolta di dati oltre ai tipi di informazioni raccolte come descritto sopra. I dati scambiati tra Onsite DCA e Printanista Hub sono crittografati utilizzando protocolli di crittografia avanzati conformi allo standard FIPS. Onsite riceve aggiornamenti software sicuri dai server di aggiornamento Printanista.

Il sistema DCA Onsite legacy comunica con Printanista a intervalli prestabiliti per verificare se vi siano azioni in coda non ancora eseguite. Ciò garantisce che le azioni vengano eseguite tempestivamente.

**Nota:** è sempre Onsite DCA ad avviare questa comunicazione con il server Printanista, e non il contrario.

**Nota:** HP JAMC è supportato solo se utilizzato in combinazione con il sistema Onsite DCA legacy al momento del lancio iniziale di Printanista.

## Traffico di rete

Le verifiche condotte dal software utilizzano un sistema intelligente per estrarre solo le informazioni essenziali relative a ciascuna stampante, fotocopiatrice o dispositivo multifunzione. A differenza di prodotti simili che inviano una serie fissa di richieste (un insieme più ampio di tutte le richieste possibili) a ogni dispositivo collegato in rete, Onsite DCA invia solo le richieste pertinenti in base ai campi supportati dal dispositivo di destinazione, con ogni richiesta che non supera i pochi kilobyte di dati. Per ridurre ulteriormente la quantità di larghezza di banda di rete utilizzata, Onsite DCA comunica con non più di 20 dispositivi alla volta. Ogni IP all'interno degli intervalli configurati verrà interrogato e, se non viene ricevuta alcuna risposta entro il periodo di timeout configurato, si passerà all'indirizzo IP successivo. Come regola generale, Printanista raccoglierà informazioni su circa 65.000 dispositivi in poco meno di un'ora.

## Supporto dei produttori

I prodotti Printanista sono indipendenti dal produttore. Supportano tutti i principali produttori e famiglie di modelli. Alcuni dispositivi presentano limitazioni che impediscono l'estrazione di determinate informazioni.

## Preoccupazioni relative ai virus

I file dell'applicazione Printanista sono stati firmati digitalmente per impedire l'esecuzione qualora l'integrità del file fosse compromessa. Ciò garantisce che eventuali virus presenti non vengano attivati e impedisce la diffusione del virus da una rete all'altra. Per una maggiore sicurezza, si consiglia di utilizzare un software antivirus sulla propria rete.

**ECI fornirà servizi di assistenza esclusivamente per l'ultima versione del Software disponibile in commercio, nonché per la versione immediatamente precedente del Software. Questa politica si applica a tutti i prodotti ECI Device Management.**

**Microsoft®, .NET Framework®, Windows® e Windows Server® sono marchi registrati o marchi commerciali di Microsoft Corporation.**