



# Centro Printanista

# Libro bianco tecnico

Versione 1.5



# Sommario

Panoramica.....	4
Come funziona Printanista.....	5
Requisiti del Printanista.....	6
Applicazione back-end Printanista Hub.....	6
Requisiti per la candidatura a Printanista.....	7
Agente di raccolta dati (ECI DCA) .....	7
Requisiti PC/Server per ECI DCA: .....	7
Server degli aggiornamenti ECI .....	8
Aggiornamenti software .....	8
Registrazione .....	8
Regione di servizio.....	8
Dati raccolti e crittografia.....	9
Crittografia dei dati .....	9
Questioni di sicurezza.....	9
Tipi di informazioni raccolte.....	9
Stampanti locali.....	11
Flusso di lavoro di Printanista.....	11
Collegamento al dispositivo remoto (RDL) .....	13
Panoramica del sistema – Collegamento al dispositivo remoto (RDL) .....	13
Sicurezza: porte e SSL (Secure Sockets Layer) .....	13
Abilitazione e autorizzazioni.....	13
Capacità di controllo.....	13
Sicurezza del collegamento al dispositivo remoto (RDL) .....	14
La sicurezza di Remote Device Link (RDL) è stata una delle principali preoccupazioni durante lo sviluppo di questo strumento. ....	14
Applicazione Printanista Hub.....	15
Gestione utenti basata sui permessi.....	15
Accesso HTTPS.....	15
Printanista fianco a fianco.....	15
Hosting di applicazioni Printanista Hub .....	15
Centri dati sicuri ECI.....	15
Gestione delle versioni.....	16
Processo di test e rilascio.....	16
Sicurezza del codice sorgente.....	16
Privacy e legislazione sui dati.....	17
Regolamento generale sulla protezione dei dati (GDPR).....	17

Domande frequenti (FAQ).....18

Informazioni sui DCA in sede preesistenti..... 20

    Requisiti PC/Server per DCA in sede: .....20

    Considerazioni sul firewall in uscita (porta 80 o 443): .....20

    Requisiti di rete: ..... 20

    La versione legacy di Java Onsite sui sistemi Linux e macOS non è funzionante. ....20

    Requisiti PC/stampante per l'utilizzo dell'agente locale (installazione opzionale): ..... 20

    Individuazione della rete e raccolta di contatori e forniture (DCA in loco) .....21

    Traffico di rete .....21

    Agente USB locale (funzionante SOLO con DCA in sede) .....22

    Supporto del produttore..... 22

    Preoccupazioni per i virus.....22

## Panoramica

---

La suite di prodotti Printanista offre una soluzione di stampa gestita di livello aziendale che è abbastanza facile da utilizzare e implementare. È architettato e progettato per sfruttare le funzionalità avanzate e i vantaggi della piattaforma Microsoft .NET.

Pertanto, non sono più necessari tecnici specializzati per l'installazione del software, la configurazione e la manutenzione del sistema.

Il prodotto Printanista non può in alcun modo essere configurato per svolgere un compito oltre a quelli per cui è stato progettato. La trasmissione dei dati dai prodotti a fonti esterne è strettamente limitata. I prodotti non riportano altri dettagli se non le informazioni sulle apparecchiature monitorate (es. tipologia di apparecchiatura). Nessuna informazione riservata viene mai trasmessa fuori dalla rete tramite i prodotti Printanista. La suite è composta dai seguenti componenti:

**Printanista Hub:** un sito Web e un sistema backend che ospita tutti i dati ricevuti dagli strumenti di raccolta dati Printanista.

Si tratta di un repository che consente di visualizzare i dati utilizzando un browser, generare report, configurare flussi di lavoro di avvisi e notifiche e sincronizzare i dati con i sistemi ERP per la fatturazione o l'evasione delle forniture.

**ECI DCA:** questo nuovissimo Data Collection Agent-DCA offre importanti vantaggi rispetto a Onsite Data Collection Agent-DCA senza perdere alcuna funzionalità, incluso il supporto multipiattaforma nativo completo di Windows, macOS, Linux e Raspberry Pi, ciascuno con passaggi di installazione unici, documentazione di supporto e personale di supporto formato su queste piattaforme. ECI DCA offre inoltre il rilevamento e la scansione continua dei dispositivi, una migliore funzionalità MIBWalk e di raccolta dei registri e ora vengono raccolti molti altri tipi di contatori.

**DCA in sede:** uno strumento agente di raccolta dati legacy esegue automaticamente valutazioni di stampa e monitora i livelli dei materiali di consumo, lo stato della stampante e i registri degli errori. Questa applicazione viene installata presso la sede del cliente ed è in grado di eseguire automaticamente valutazioni di stampa su base programmata senza intervento umano. I dati acquisiti vengono inviati al sito Web Printanista Hub utilizzando HTTPS, HTTP o, se il cliente preferisce, un file crittografato proprietario.

**Strumento di valutazione WebAudit:** uno strumento di raccolta dati che fa parte dell'applicazione Printanista Hub. Le valutazioni della flotta vengono eseguite direttamente da un browser senza installare alcun software. I dati acquisiti vengono inviati direttamente a Printanista Hub.

Lo scopo di questo documento è fornire una panoramica della linea di prodotti della suite di prodotti Printanista da un punto di vista tecnico per facilitare le risposte alle domande più frequenti che i team IT riceveranno.

## Come funziona Printanista

---

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

Printanista attualmente supporta il protocollo SNMP v1, v2c e v3 (Simple Network Management Protocol). SNMP v3 fornisce una maggiore protezione dei pacchetti per garantire che le informazioni e le comunicazioni vengano trasmesse tramite fonti affidabili. A differenza di SNMPv1 o v2, SNMP v3 è crittografato per una maggiore sicurezza e richiede sia un nome utente che una password. Un vantaggio derivante dall'utilizzo di SNMP v3 è che gli amministratori di rete possono determinare il metodo di crittografia nonché un nome utente e una password complessi.

SNMP è un protocollo di rete che facilita lo scambio di informazioni tra dispositivi di rete che estraggono dati dal Management Information Base (MIB) e altre posizioni all'interno del dispositivo di stampa. Il Management Information Base (MIB) è un database interno che la maggior parte dei dispositivi connessi alla rete fa parte della loro anatomia. Il Management Information Base (MIB) contiene dati come il nome del modello, i livelli di toner e lo stato corrente della stampante.

## Requisiti del Printanista

Applicazione back-end Printanista Hub  
Printanista Hub Product Specifications

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

Utilizzare il seguente collegamento per le specifiche complete attuali del prodotto Printanista: [SysReq v3.0.html](https://www.printanista.com/SysReq_v3.0.html)

Tutti i dati raccolti vengono inviati al server Printanista Hub dove vengono resi disponibili per reporting e avvisi.

ECI DCA si connette al tuo server Printanista Hub utilizzando HTTPS (porta 443/TCP). Contatta l'amministratore della tua soluzione ECI per informazioni sui nomi di dominio e sugli indirizzi IP utilizzati dal tuo server. Questa connessione è protetta dallo standard industriale TLS (Transport Layer Security). Si consiglia TLS 1.2. TLS 1.0 e TLS 1.1 sono attualmente supportati ma non consigliati per motivi di sicurezza. Il supporto per TLS 1.0 e TLS 1.1 verrà interrotto in futuro.

Questa connessione rimane aperta per tutta la durata dell'esecuzione dell'ECI DCA. Normalmente viene utilizzata una connessione WebSocket, ma in alcune situazioni ECI DCA potrebbe ricorrere all'utilizzo di eventi inviati dal server o di polling lungo HTTP.

**NOTA IMPORTANTE:** sono necessarie diverse connessioni HTTPS sicure in uscita 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>

## Requisiti per l'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 dell'Application Layer della suite TCP/IP.

Requisiti PC/Server per ECI DCA:

### Microsoft Windows (x86/64)

Requisiti:

- Windows 10 o versioni successive
- Windows Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, Server 2019 e Server 2022
- Microsoft .NET Framework 4.7.2. o più recente

### Linux (x86/64 o ARM)

Requisiti:

- Ubuntu 14.04, 16.04 o 18.04, Debian 9.5+, Raspbian Jessie o Stretch, RedHat Enterprise 7.5+, CentOS 7.5+, Fedora28+
- Mono 5.4 o successiva

### macOS (x64)

Requisiti:

- Sierra (10.12) o successiva
- Mono 5.4 o successiva

### Raspberry Pi 2 Modello B, Raspberry P 3 Modello B, Raspberry Pi 3 Modello B+ e Raspberry Pi 4 Modello

Requisiti:

- Scheda microSD vuota da 8 GB o superiore
- PC in grado di scrivere su scheda microSD

Considerazioni sul firewall per ECI DCA:

Connessioni in entrata

Non sono presenti collegamenti in entrata da Internet a ECI DCA.

Connessioni in uscita

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

## Server degli aggiornamenti ECI

ECI Updates Server è un servizio gestito da [ECI Device Management](#) per facilitare la registrazione DCA, gli aggiornamenti automatici del software e le installazioni DCA (questo sito) ed è necessario per il funzionamento di ECI DCA. Nota: ECI DCA non invia alcun dispositivo raccolto o dati di configurazione al server degli aggiornamenti ECI.

## Aggiornamenti software

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

## Registrazione

ECI DCA utilizza le richieste DNS a [\\*.reg.pf-d.ca](#) per registrarsi. Inizialmente proverà a farlo utilizzando i server DNS della rete locale, quindi tornerà a comunicare direttamente con gli indirizzi IP del server di aggiornamento ECI (utilizzando la porta 53/udp). Il firewall deve consentire questa connessione al server degli aggiornamenti ECI solo se i server DNS locali non risolvono le richieste di registrazione.

## Regione di servizio

L'ECI DCA viene instradato verso la regione verso la quale ha la latenza di rete più bassa e 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 di ECI DCA e Onsite DCA legacy sono codificati e offuscati. Printanista richiede l'utilizzo di HTTPS per la comunicazione tra i DCA e Printanista Hub. ECI DCA richiede HTTPS per funzionare. Inoltre, tutte le impostazioni e i lavori sensibili tra ECI DCA e Printanista vengono crittografati utilizzando l'algoritmo di crittografia simmetrica standard AES256, utilizzando una chiave condivisa protetta. Ciò garantisce la crittografia end-to-end, quindi i dati sono protetti dalla lettura se intercettati da terze parti, da un'istanza Printanista competitiva o altrimenti.

### La sicurezza è importante

ECI DCA e Onsite DCA legacy comunicano con Printanista Hub tramite il protocollo HTTPS, utilizzando lo standard di settore TLS 1.2 (Sicurezza del livello di trasporto). 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 Onsite DCA legacy non raccolgono né trattano alcun dato personale. L'unico modo in cui il sistema raccoglierà questo tipo di informazioni è se tu o i tuoi clienti inserite i dati in Printanista all'interno di un campo o un'etichetta come la posizione o il nome del cliente. ECI DCA e Onsite DCA legacy consentono di monitorare i dispositivi di rete utilizzando il protocollo SNMP (Simple Network Management Protocol). 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 un Management Information Base (MIB) SNMP. I dati esposti dal dispositivo variano in base al produttore e al modello. È sempre di natura tecnica o operativa e specifica del dispositivo stesso. Al livello più elementare, i dati esposti da una stampante MIB sono documentati nell'IETF RFC 3805 (<https://tools.ietf.org/html/rfc3805>). Ulteriori informazioni sul dispositivo possono essere esposte dal produttore tramite estensioni e MIB privati (Management Information Base), ma le informazioni sono fondamentalmente tecniche e specifiche del dispositivo.

### Printanista Hub memorizza solo:

- Nome host
- Sistema operativo Altre
- Indirizzo IP remoto
- Architettura del sistema

informazioni sulla rete/ambiente vengono raccolte e visualizzate durante la connessione per scopi di risoluzione dei problemi, ma non vengono mai archiviate in Printanista.

### Tipi di informazioni raccolte

ECI DCA e Onsite DCA legacy tentano di raccogliere le seguenti informazioni dai dispositivi di stampa in rete durante una scansione di rete:

#### Attributi del dispositivo

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

#### Servizio

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

#### Forniture

- Numero di serie della cartuccia del toner.
- Livello di fornitura della cartuccia del toner
- Livelli del tamburo
- Livelli del kit di manutenzione
- Livelli di fornitura diversi dal toner
- Livelli vari
- Le stampanti basate su etichette forniscono dettagli

#### Copertura e metri

- Letture del contatore
- Tipo di contatore
- Livello di copertura
- Identificazione monocromatica o a colori

## Individuazione della rete e raccolta dati

Per aumentare l'efficienza del DCA, solo quando ci sono dati nuovi o modificati dai dispositivi queste informazioni verranno inviate al Printanista Hub Server. Ciò garantirà un carico di rete minimo ed eliminerà la frequenza di eventuali arretrati nell'invio di dati del dispositivo. 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 rilevati in precedenza sulla base impostata periodicamente rispetto a una scansione di rete completa (questa viene completata inizialmente, periodicamente o quando determinata da un utente amministratore).

Ciò garantirà che la velocità di invio dei dati del dispositivo sia quanto più aggiornata possibile. Ciò consente agli utenti di essere avvisati dei 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, minimo e massimo per gli intervalli di scansione sono:

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

Tieni presente che gli intervalli di scansione (contatori, materiali di consumo, errori e attributi) sono disponibili solo se un dispositivo dispone di un file di definizione del modello (MDF). Se questo non è presente, verrà effettuata una scansione completa sul dispositivo in questione utilizzando un intervallo

Gli amministratori di Printanista Hub possono gestire da remoto gli ECI DCA che sono stati attivati sul server. Può attivare in remoto l'ECI DCA per eseguire comandi predefiniti come attività di raccolta dati, fornire registri ECI DCA, eseguire passeggiate MIB remote o aggiornare le impostazioni ECI DCA.

**Nota:** ECI DCA avvia sempre la comunicazione con il server Printanista e non viceversa.

**Nota:** solo quando le informazioni sul contatore, sulla fornitura o sugli errori vengono aggiornate o modificate avviene la comunicazione, riducendo l'utilizzo della larghezza di banda.

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

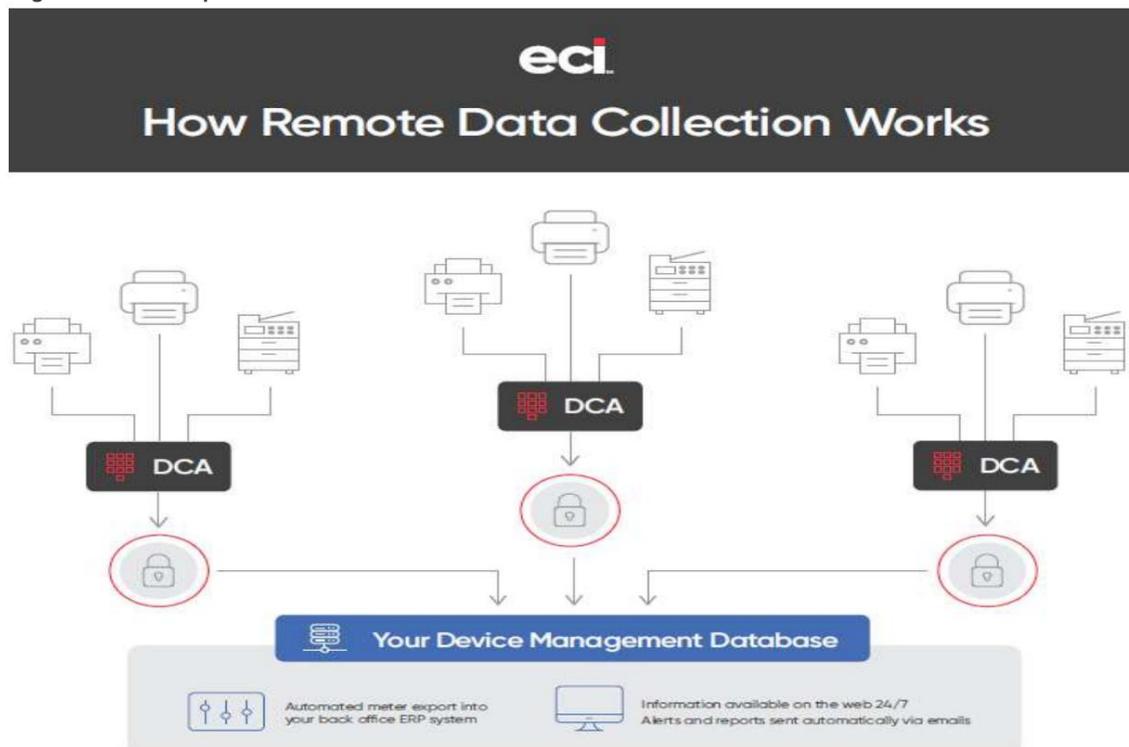
## Stampanti locali

### Flusso di lavoro Printanista

Printanista Workflow è un robusto strumento di gestione della stampa. Printanista Workflow può aiutare i tuoi clienti a ridurre il costo dell'output dei documenti, aumentare le pratiche di sicurezza dei documenti e fornire metodi flessibili di recupero dei costi. Utilizzando un processo di installazione semplificato, i tuoi clienti potranno visualizzare rapidamente tutte le informazioni di stampa in un'unica posizione. Consenti ai tuoi clienti di ridurre i costi comprendendo ogni documento che producono.

### Cos'è il flusso di lavoro Printanista?

Printanista Workflow è la prossima generazione di prodotti di gestione degli utenti utilizzati per monitorare e gestire la stampa per centinaia di organizzazioni e aziende in tutto il mondo. Se in passato avevi familiarità con l'applicazione Gestione utenti, sarai felice di vedere che l'installazione e la configurazione dell'applicazione sono ancora intuitive come le versioni precedenti. I menu, gli strumenti e l'amministrazione generale del sistema sono stati mantenuti. Se stai effettuando l'aggiornamento da una versione precedente, tutto ti sarà familiare e la navigazione sarà semplice.



### Come funziona Printanista Workflow (tramite l'ECI DCA i dati vengono raccolti dal flusso di lavoro)

Essendo Printanista Workflow la prossima generazione di gestione dei dispositivi, questa funzione funziona solo con ECI DCA.

Printanista Workflow non funziona con Onsite DCA.

-Il client del flusso di lavoro può essere installato su desktop MAC e con sistema operativo Windows consentendo la raccolta dei contatori del dispositivo USB connesso localmente

-I contatori vengono determinati utilizzando i dati dello spooler, dell'applicazione e del driver di stampa -Memorizzati nel database

del flusso di lavoro -ECI DCA richiede le informazioni sul contatore dal flusso di lavoro tramite una chiamata API (Application Programming Interface) al servizio web -ECI DCA fornisce i dati a Printanista Hub per....

-Il flusso di lavoro per la connessione ECI DCA è crittografato (https)

## Requisiti di sistema del flusso di lavoro Printanista

### Server e strumenti di amministrazione

È possibile installare i componenti del server Printanista Workflow sui computer che eseguono:

- Microsoft Windows Server 2012 R2 o versione successiva
- Windows 8 Professional o successivo (64 bit)

L'installazione completa del server richiede:

- Un minimo di 5 Gigabyte di spazio libero per supportare il software Workflow.
- Sono richiesti il database SQL e SQL Express 2012. Se assente verrà installato SQL Express 2012
- Internet Information Service (IIS) è richiesto e verrà installato se assente
- Microsoft .NET Framework 4.7.2 è obbligatorio e verrà installato se assente.
- Per impostazione predefinita, tutti i processi e i registri dei dati di stampa vengono archiviati su questo server. Importante: i sistemi operativi Microsoft Home e Microsoft Small Business Server non sono supportati per alcun componente.

### Requisiti del client Windows e utilizzo della memoria

È possibile installare il software Printanista Workflow Client Popup su computer che eseguono Microsoft Windows 8 o versioni successive.

- Un'installazione client completa richiederà circa 10-20 MB di spazio su disco.

Il Client è composto da due componenti: il Client Desktop e il Servizio Client.

- Il client desktop richiede tra 5 e 20 megabyte, a seconda dell'attività.
- Non è necessario alcun software aggiuntivo.

### Requisiti di sistema per Workflow Client per Mac®

- Workflow Client per Mac® è supportato sui sistemi operativi Mac® seguendo il modello di supporto di Apple.
- Il client Mac® supporterà solo la versione più recente e le due versioni precedenti del sistema operativo Mac®.
- Fare clic su "Informazioni su questo Mac®" nel menu Apple per scoprire quale versione del sistema operativo Mac® è in esecuzione sulla workstation.
- Workflow Client per Mac® richiede inoltre un (1) PC basato su Windows per ospitare Workflow Server e il database.

Importante: Printanista Workflow deve essere installato su una rete con almeno un computer Windows.

### Il flusso di lavoro di supporto

del server Web IIS utilizza Internet Information Services (IIS) per comunicare con i dispositivi e internamente tra i componenti del flusso di lavoro.

L'installazione richiede la versione completa di IIS. Il programma di installazione determinerà se disponi di un'installazione IIS esistente. In caso contrario, il programma di installazione creerà un nuovo sito e un pool di applicazioni utilizzando IIS.

### Requisiti di rete Printanista

Workflow utilizza per impostazione predefinita la comunicazione HTTP/SSL standard tramite le porte 80/443 per i servizi web. Se queste porte non sono disponibili, Workflow utilizzerà 6320/6321. Tuttavia, puoi modificare le porte di comunicazione in caso di conflitto nella tua organizzazione.

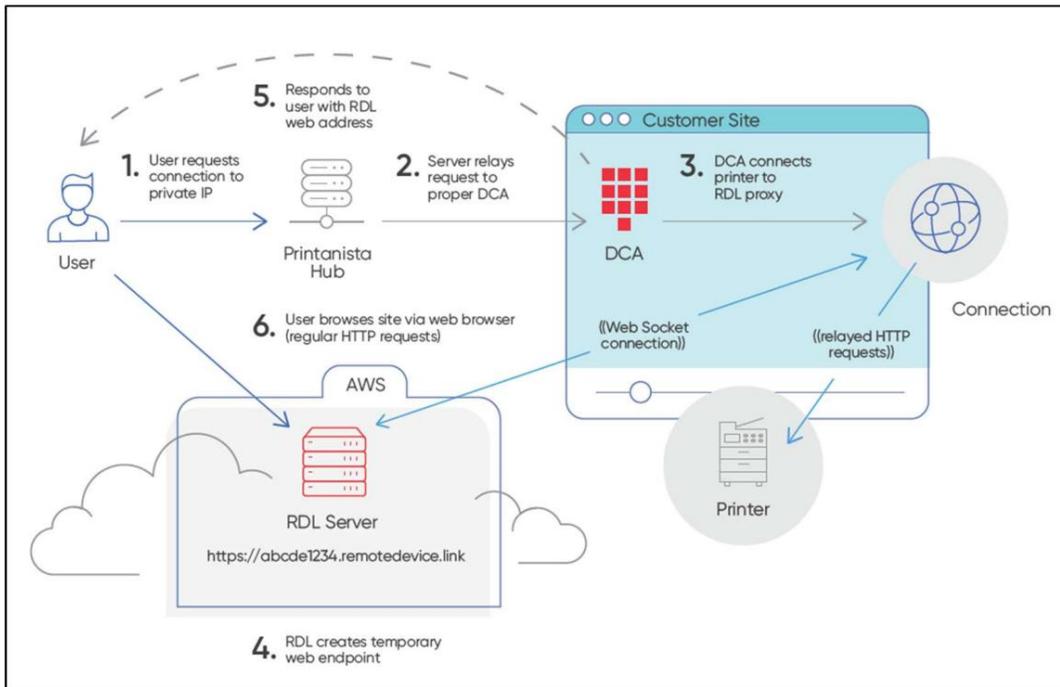
### Dati forniti a ECI DCA dal server del flusso di lavoro: esempi

di informazioni identificative di alcuni dispositivi: produttore, modello, indirizzo IP, numero di serie/risorsa, posizione, pagine a colori/monocromatiche, impressioni a colori/monocromatiche, ecc.

La documentazione della Guida al flusso di lavoro di Printanista può essere trovata qui:

[Guida al flusso di lavoro Printanista](#)

## Collegamento dispositivo remoto (RDL)



### Panoramica del sistema – Collegamento dispositivo remoto (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.

Ci sono 4 componenti principali:

1. L'utente finale che accede al dispositivo
2. Il server Remote Device Link, su Internet pubblica (tramite URL [https://\\*.remotedevice.link](https://*.remotedevice.link))
3. Il client RDL (incorporato 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 ciascun account cliente finale
3. Sono necessarie autorizzazioni affinché un utente possa accedere alla funzionalità

Capacità di controllo

1. Controllo locale di Printanista Hub dei dettagli di ciascuna sessione a. Report di amministrazione di Printanista Hub per il controllo di Remote Device Link (RDL)
2. Registrazione nel cloud AWS (Amazon Web Services) di Remote Device Link (RDL) di tutti i dettagli della sessione

Sicurezza del collegamento al dispositivo remoto (RDL).

La sicurezza di Remote Device Link (RDL) è stata una delle principali preoccupazioni durante lo sviluppo di questo strumento.

**Autorizzazione:**

- **L'utente deve disporre dell'autorizzazione da Printanista Hub per accedere alla funzione Remote Device Link (RDL) su conto specifico**
- **L'agente di raccolta dati (DCA) accetterà solo richieste di collegamento al dispositivo remoto (RDL) dal server Printanista Hub che è reciprocamente autenticato** • **L' agente di raccolta dati (DCA) stabilisce solo una connessione di collegamento al dispositivo remoto (RDL) ai sistemi di stampa noti e attualmente monitorati dispositivi all'interno degli intervalli IP di rilevamento degli agenti di raccolta dati (DCA) .**
- **Ogni singola richiesta Web deve avere lo stesso IP: l' agente di raccolta dati (DCA) non seguirà reindirizzamenti**

**Sicurezza della connessione:**

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

**Limiti di tempo della sessione:**

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

**Implicazioni**

La connessione tra ECI DCA e Printanista Hub è protetta da chiavi di autenticazione specifiche dell'installazione DCA e la connessione richiede un certificato SSL attendibile valido da utilizzare su 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 semplici connessioni HTTP se il dispositivo non supporta connessioni sicure.

## Applicazione Printanista Hub

---

La funzionalità Printanista Hub è accessibile tramite un'interfaccia utente basata sul web.

### Gestione utenti basata sui permessi

L'accesso al front-end web di Printanista Hub è controllato con la gestione degli utenti basata sulle autorizzazioni. Gli utenti devono accedere a Printanista utilizzando un nome utente e una password designati. Agli utenti vengono assegnati uno o più ruoli che specificano le autorizzazioni e viene loro concesso l'accesso a uno o più gruppi di dispositivi. Gli amministratori con autorizzazione completa possono specificare esattamente quali schermate ciascun utente può visualizzare e/o con cui 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 fianco a fianco

Printanista Hub utilizza un database di metadati del modello noto come Side-by-Side (SBS), che ha vari attributi del modello come: velocità di stampa, quando è stato introdotto sul mercato o compatibilità dei codici OEM, che viene periodicamente aggiornato come modelli e versioni futuri vengono rilasciati dagli OEM. Printanista Hub comunicherà con Side-by-Side per verificare la presenza di nuovi aggiornamenti e recuperare i metadati del dispositivo per memorizzarli nella cache locale su ciascun sistema Printanista Hub.

### Hosting di applicazioni Printanista Hub

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 vitali per le loro operazioni aziendali e per il nostro successo. Utilizziamo un approccio multilivello per proteggere le informazioni chiave, monitorando e migliorando costantemente le nostre applicazioni, sistemi e processi, per soddisfare le crescenti richieste e sfide di sicurezza.

### Centri dati sicuri ECI

Il nostro servizio è collocato in spazi dedicati presso data center di alto livello. Queste strutture forniscono supporto a livello di operatore.

Clicca sul seguente link per ottenere il documento dettagliato dell'ICE relativo alla Sicurezza dei Data Center

[Panoramica sulla sicurezza del cloud ECI 2021 \(ecisolutions.com\)](https://www.ecisolutions.com/it/risorse/panoramica-sulla-sicurezza-del-cloud-eci-2021)

## Gestione delle versioni

### Processo di test e rilascio

Ogni versione maggiore e minore del software passa attraverso un processo di controllo qualità, in cui più membri del personale Printanista effettueranno test di regressione su parti alterate del sistema per garantire che non si sia verificato un downgrade nella sicurezza o nella funzionalità del sistema, oltre a convalidare la nuova versione. aspetti funzionali. Le versioni principali passano attraverso un processo di rilascio beta in cui client 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 di revisione protetto, accessibile solo alle persone autorizzate. Ogni modifica al codice sorgente richiede che due sviluppatori autorizzati approvino le modifiche prima di essere accettate nel repository del codice di produzione dove viene tracciata ogni modifica, che include quale sviluppatore ha apportato la modifica e perché. I prodotti vengono crittografati e firmati digitalmente con un certificato di firma del codice affidabile prima della spedizione. Un deposito a garanzia può essere reso disponibile in base alla richiesta.

ECI coinvolge una terza parte indipendente certificata CREST, SOC 2, NSA-CIRA, CSA-STAR leader del settore per condurre test di penetrazione a livello di applicazione e correggere i risultati in base ai requisiti aziendali e al quadro interno di gestione del rischio. I test di penetrazione vengono condotti almeno una volta all'anno o quando vengono apportate modifiche importanti al sistema. La politica di ECI è quella di compiere sforzi commercialmente ragionevoli per porre rimedio a tutti i risultati critici entro 30 giorni o entro un periodo di tempo ragionevole con un caso aziendale fornito. ECI non divulga dettagli riguardanti i nostri controlli di sicurezza o i risultati dei test di penetrazione poiché tali informazioni sono proprietarie e riservate e nelle mani sbagliate possono comportare un aumento del rischio.

## Privacy e legislazione sui dati

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

Da maggio 2018 è entrato in pieno vigore il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea. Il GDPR sostituisce la Direttiva sulla protezione dei dati 95/46/CE ed è progettato 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 prevede, tra le altre cose, formazione del personale, audit e valutazione del rischio in tutta l'azienda, politiche e procedure, governance e sforzi continui di conformità. Incoraggiamo i nostri clienti ad adottare misure simili per garantire che le proprie attività siano conformi al GDPR e per gli anni a venire.

---

I prodotti Printanista non elaborano, monitorano o gestiscono alcun record personale o alcun record o informazione specifica di una qualsiasi persona o gruppo di persone.

Le applicazioni software Printanista non raccolgono, ospitano o trasmettono alcuna informazione riguardante il contenuto dei lavori di stampa.

Printanista non ha modo di accedere, ospitare 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 i dati dei titolari di carta o informazioni personali.

Le comunicazioni del motore del prodotto sono controllate, utilizzando l'accesso limitato all'indirizzo IP e/o all'intervallo specifico del contatto.

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

La comunicazione all'esterno della rete utilizza un flusso di dati compresso proprietario che viene inviato utilizzando SSL standard del settore su HTTPS.

---

Per informazioni relative alla conformità a leggi e/o regolamenti specifici, contattare il proprio account manager ECI.

---

Di seguito è riportato il collegamento all'ECI Cloud Security: [Panoramica sulla sicurezza del cloud ECI 2021 \(ecisolutions.com\)](https://www.ecisolutions.com/it/panoramica-sulla-sicurezza-del-cloud-eci-2021)

## Domande frequenti (FAQ)

I prodotti Printanista funzionano con i proxy Internet?

Sì, ECI DCA può funzionare con la maggior parte dei proxy. La configurazione delle impostazioni proxy è richiesta sul sistema in cui è installato e funziona l'ECI DCA.

Quali sono i requisiti minimi di Printanista Hub, ECI DCA, Onsite?

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

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

Questo ECI DCA apporta importanti vantaggi rispetto a Onsite DCA senza perdere alcuna funzionalità, incluso il supporto multiplatforma nativo completo di Windows, macOS, Linux e Raspberry Pi. Ciascuno con passaggi di installazione unici, documentazione di supporto e personale di supporto qualificato su queste piattaforme. Anche il processo di installazione è notevolmente migliorato ed è molto più intuitivo per tutti i tipi di utenti.

L'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, le porte elencate di seguito devono essere inserite nella lista bianca per garantire la connettività di ECI DCA.

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

ECI DCA utilizza la porta 31816 per impostazione predefinita per l'interfaccia utente locale basata sul Web DCA.

Quanta manutenzione continua richiede l'ECI DCA?

ECI DCA e Onsite DCA è un servizio che viene eseguito in background ed esegue controlli ed esportazioni verso destinazioni configurate secondo pianificazioni predefinite. Si consiglia di utilizzare sottoreti (intervalli IP) anziché IP fissi. Quando si aggiungono nuovi dispositivi alla rete, questi verranno rilevati e inclusi nei risultati dell'audit, limitando l'intervento manuale.

Come funziona il processo dello strumento di valutazione WebAudit?

Da Printanista Hub, il rivenditore specifica il ciclo di fatturazione applicabile all'utente finale (i tuoi clienti/clienti). A questo punto, viene generata automaticamente un'e-mail e inviata al contatto appropriato informandolo che è ora di ritirare i contatori. Le istruzioni includono un URL in base al quale quando l'utente finale fa clic sul collegamento, avvia automaticamente il browser Web, pronto per eseguire l'azione. L'utente finale fa quindi clic su "avvia" e "salva". Fatto. Nessun software viene installato in nessun momento. Un collegamento alla pagina WebAudit può anche essere pubblicato sul sito Web esistente dei rivenditori, ad esempio la pagina Web Immetti letture contatori. Ciò consente all'utente di automatizzare la raccolta, anziché camminare manualmente da un dispositivo all'altro, stampare la pagina di configurazione e trascrivere i contatori.

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

Quali sono i requisiti affinché funzioni?

Tutti i marchi con una pagina Web incorporata vengono rilevati da ECI DCA. Le informazioni sulle pagine Web integrate varieranno in base al produttore e al modello. I dispositivi locali non mostreranno la pagina Web incorporata.

Esistono ulteriori problemi 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 riporterà 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?

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

Abbiamo visto dispositivi rispondere in decine di secondi ai primi tentativi di connessione, influenzati 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 fornisce l'accesso tramite la pagina Web incorporata sono accessibili tramite Remote Device Link (RDL).

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

Sì, esiste la possibilità di disattivare questa funzionalità per ogni account.

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

Dove posso ottenere ulteriori informazioni su Printanista Hub, Printanista Workflow, ECI DCA, Onsite DCA legacy, ecc.?

Ulteriori informazioni sono disponibili sul sito web Printanista dell'ECI: <https://>

[www.ecisolutions.com/products/printanista-hub/](https://www.ecisolutions.com/products/printanista-hub/)

## Informazioni sui DCA in sede preesistenti

Si consiglia di utilizzare ECI DCA con Printanista. Tuttavia, la versione legacy di Onsite DCA attualmente funziona con Printanista.

Requisiti PC/server per DCA in loco:

- 1 GB di RAM
- 400 MB di spazio su disco Microsoft .NET Framework 4.7.2 o versione successiva
- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022 Onsite
- Versione 4.1.3 e successive supportano Windows Server 2022 Internet Explorer 11.0 o successive, Chrome, Firefox MDAC 2.8 o successive (normalmente incluso quando è installato Windows)
- JET 4.0 o successiva (normalmente inclusa quando è installato Windows)
- Caricato su una macchina attiva 24 ore su 24, 7 giorni su 7 o almeno per l'intero giorno lavorativo È necessario accedere come amministratore locale (o equivalente) durante l'installazione

Considerazioni sul firewall in uscita (porta 80 o 443):

Trasmissione 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 WAN (Wide Area Network)

**Utilizzare ECI DCA se sono necessari i sistemi operativi macOS, Linux o Raspberry Pi. Il legacy Java Onsite 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
- corrente per la stampante locale (UPD è consigliato per i dispositivi HP)
- La stampante deve supportare Printer Job Language (PJM) o Printer Management Language (PML)
- Rimuovere eventuali driver di stampa inutilizzati Il supporto bidirezionale del driver
- è abilitato Modifiche di Windows Firewall: porta 161/33333 in entrata/uscita sia per TCP che per UDP

Nota: per le versioni recenti del sistema operativo che utilizzano il modello di driver 4 (ad esempio, Windows 10), attualmente sono supportati solo gli OEM Kyocera e Ricoh e le relative varianti.

## Individuazione della rete e raccolta di contatori e forniture (DCA in loco)

Le impostazioni di rilevamento automatico della rete brevettate Printanista utilizzano una combinazione di algoritmi per identificare gli intervalli di rete in cui possono essere posizionati i dispositivi di stampa e quindi scoprire e comunicare con i dispositivi che sono online, instradando attraverso più elementi di rete come 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 Onsite per eseguire comandi predefiniti come attività di raccolta dati, fornire registri Onsite, eseguire MIBWalks remoti, installare HP JAMC o aggiornare le impostazioni Onsite. Questi sono spiegati più dettagliatamente di seguito:

Funzione	Posizione	Descrizione
Compiti	Impostazioni in loco	Può configurare in remoto le attività da eseguire secondo una pianificazione preimpostata, ma può selezionare attività (cache, contatori, forniture, servizio) da eseguire immediatamente e raccogliere i dati del dispositivo su comando.
MIB cammina	Impostazioni in loco	Può indicare determinati IPv4/IPv6/nomi host di dispositivi e attivare Onsite per avviare immediatamente la raccolta delle passeggiate MIB.
Registri (dettagliati)	Impostazioni in loco	Può istruire Onsite a raccogliere i registri (critici, errori, avvisi, dettagli, debug) da una determinata data.

Nessuno di questi comandi porta alla raccolta di dati oltre ai tipi di informazioni raccolte come descritto sopra. I dati scambiati tra Onsite DCA e Printanista Hub vengono crittografati utilizzando protocolli di crittografia avanzati conformi a FIPS. Onsite riceve aggiornamenti software sicuri dai server Printanista Updates.

Il legacy Onsite DCA comunica con Printanista a intervalli predefiniti per determinare se sono presenti azioni in coda non ancora eseguite. Ciò garantisce che le azioni vengano eseguite in modo tempestivo.

**Nota:** Onsite DCA avvia sempre questa comunicazione con il server Printanista e non viceversa.

**Nota:** HP JAMC è supportato solo se utilizzato insieme al legacy Onsite DCA al lancio iniziale di Printanista.

## Traffico di rete

I controlli condotti dal software utilizzano un sistema intelligente per estrarre informazioni minime per ciascuna stampante, fotocopiatrice o multifunzione. A differenza di prodotti simili che inviano un set fisso di query (un superset di tutte le query possibili) a ogni dispositivo collegato in rete, Onsite DCA invia solo le query pertinenti in base ai campi supportati dal dispositivo di destinazione, con ciascuna query del dispositivo non superiore a 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 contemporaneamente. Verrà interrogata ogni IP all'interno degli intervalli configurati e se non viene ricevuta alcuna risposta entro il periodo di timeout configurato, verrà spostato all'indirizzo IP successivo. Una regola pratica è che Printanista raccoglierà informazioni su circa 65.000 dispositivi in poco meno di un'ora.

## Agente USB locale (funzionante SOLO con DCA in sede)

L'agente USB locale è la soluzione utilizzata per estrarre informazioni da una o più stampanti locali collegate a qualsiasi tipo di porta Windows, come USB e parallela. L'agente USB locale non interrompe il flusso del lavoro di stampa, si attiva solo quando richiesto da uno degli strumenti applicativi di raccolta di Printanista (Onsite DCA o WebAudit) e quindi si chiude. L'agente USB locale raccoglie informazioni specifiche in base ai livelli di intelligenza del dispositivo dal motore e non dallo spooler di stampa. Gli attributi più comuni riportati sono modello, numero di serie, contatori della durata, copertura dei materiali di consumo, livello dei materiali di consumo e servizio. Printanista Local USB Agent può essere distribuito sulle workstation utilizzando una soluzione come Microsoft SMS. Potrebbe essere necessaria la riconfigurazione dell'antivirus o dei firewall software se si blocca la porta SNMP 161 o la porta di fallback alternativa dell'agente 33333.

## Supporto del produttore

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 per i virus

I file dell'applicazione Printanista sono stati firmati digitalmente per impedirne l'esecuzione se l'integrità del file è compromessa. Ciò garantisce che eventuali virus non vengano attivati e impediscono la diffusione del virus da una rete all'altra. Per maggiore sicurezza, ti consigliamo di utilizzare un software antivirus sulla tua rete.