



Carta bianca tecnica di Printanista Hub

Versione 1.5



Indice dei contenuti

Panoramica	4
Come funziona Printanista	5
Requisiti di Printanista	6
Applicazione backend Hub Printanista	6
Requisiti per l'applicazione di Printanista	7
Agente di raccolta dati (ECI DCA)	7
Requisiti del PC/server per ECI DCA.....	7
L'ECI aggiorna il server	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 dispositivo remoto (RDL).....	13
Panoramica del sistema - Collegamento dispositivo remoto (RDL)	13
Sicurezza: Porte e SSL (Secure Sockets Layer)	13
Abilitazione e permessi	13
Capacità di audit	13
Sicurezza del collegamento remoto dei dispositivi (RDL)	14
La sicurezza del Remote Device Link (RDL) è stata una preoccupazione fondamentale nello sviluppo di questo strumento.....	14
Applicazione Hub Printanista	15
Gestione degli utenti basata sui permessi.....	15
Accesso HTTPS	15
Printanista Side-By-Side	15
Hosting dell'applicazione Printanista Hub	15
Centri dati sicuri ECI.....	15
Gestione delle versioni	16
Processo di collaudo e rilascio	16
Sicurezza del codice sorgente.....	16
Privacy dei dati e legislazione	17

Regolamento generale sulla protezione dei dati (GDPR)	17
Domande frequenti (FAQ)	18
Informazioni sul DCA in loco Legacy	20
Requisiti del PC/server per DCA Onsite	20
Considerazioni sul firewall in uscita (porta 80 o 443).....	20
Requisiti di rete	20
Java Onsite su sistemi Linux e macOS non è funzionante	20
Requisiti del 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 loco)	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, 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 richiede più l'intervento di tecnici specializzati per l'installazione del software, la configurazione e la manutenzione del sistema. I prodotti Printanista non possono in alcun modo essere configurati per svolgere 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 altri dettagli, ad eccezione delle informazioni sull'apparecchiatura monitorata (ad esempio, il tipo di apparecchiatura). I prodotti Printanista non trasmettono mai informazioni riservate al di fuori della rete. La suite è composta dai seguenti componenti:

Hub di Printanista: Un sito web e un sistema backend che ospita tutti i dati ricevuti dagli strumenti di raccolta dati di Printanista. Si tratta di un repository che consente di visualizzare i dati tramite un browser, generare report, configurare flussi di lavoro e notifiche di avviso 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 grandi vantaggi rispetto all'Onsite Data Collection Agent-DCA, senza perdere alcuna funzionalità, tra cui 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. ECI DCA offre anche il rilevamento e la scansione continua dei dispositivi, una migliore capacità di raccolta di MIBWalk e di log e la raccolta di molti più tipi di contatori.

DCA in loco: uno strumento 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 alcun intervento umano. I dati acquisiti vengono inviati al sito web di Printanista Hub tramite HTTPS, HTTP o, se il cliente lo preferisce, tramite un file crittografato.

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 Printanista da un punto di vista tecnico, per facilitare le risposte alle domande più frequenti che i team di Information Technology ricevono.

Come funziona Printanista

Il motore centrale dell'agente di raccolta dati, che è 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.

Printanista supporta attualmente il protocollo SNMP v1, v2c e v3 (Simple Network Management Protocol). SNMP v3 offre una maggiore protezione dei pacchetti per garantire che le informazioni e le comunicazioni siano trasmesse da fonti affidabili. A differenza di SNMPv1 o v2, SNMP v3 è criptato per una maggiore sicurezza e richiede sia un nome utente che una password. Un vantaggio dell'uso di SNMP v3 è che gli amministratori di rete possono determinare il metodo di crittografia, nonché un nome utente e una password forti.

SNMP è un protocollo di rete che facilita lo scambio di informazioni tra i dispositivi di rete estraendo i 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 alla rete possiede come parte della propria anatomia. La Management Information Base (MIB) contiene dati quali il nome del modello, i livelli di toner e lo stato attuale della stampante.

Printanista Requisiti

Applicazione Printanista Hub Backend 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	
Supported OSes¹								
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 ²	April-2018 January 2023	
Windows 8.1 (32/64)	No	Yes	Yes	Yes	No	Partial ²	April-2018 January 2023	
Windows 10 (32/64)	No	Yes	Yes	Yes	No	Partial ²	October-2020 October 2025	
Windows Server 2003 (32/64) Internet Information Services 6 ²	No	No	No	Yes	Yes	Yes	April-2010 April-2015	
Windows Server 2008 (32/64) Internet Information Services 7.0	No	No	No	Yes	Yes	Yes	April-2015 January 2020	
Windows Server 2008 R2 (32/64) Internet Information Services 7.5	No	Yes	Yes	Yes	Yes	Yes	April-2015 January 2020	
Windows Server 2012 Internet Information Services 8.0	No	Yes	Yes	Yes	Yes	Yes	October-2018 January 2023	
Windows Server 2012 R2 Internet Information Services 8.5	No	Yes	Yes	Yes	Yes	Yes	October-2018 October 2023	
Windows Server 2016 Internet Information Services 10	Yes	Yes	Yes	Yes	Yes	Yes	January 2022 January 2027	Recommended by ECI
Windows Server 2019 Internet Information Services 10	Yes	Yes	Yes	Yes	Yes	Yes	January 2024 January 2029	Recommended by ECI
Linux (x86/64 or ARM) Debian, Ubuntu and similar distributions	N/A	Yes	No	No	No	No	---	Mono 5.4 or higher required
macOS (x64) Sierra (10.12 or higher)	N/A	Yes	No	No	No	No	---	Mono 5.4 or higher required
Raspberry Pi 4B, 3B+, 3B, 2B	N/A	Yes	No	No	No	No	---	8GB or larger SD card required

Utilizzate il seguente link per le specifiche complete 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 sono disponibili per la creazione di report e avvisi. ECI DCA si collega al vostro server Printanista Hub utilizzando HTTPS (porta **443/TCP**). Contattare l'amministratore della soluzione ECI per informazioni sui nomi di dominio e sugli indirizzi IP utilizzati dal 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 sono consigliati per motivi di sicurezza. Il supporto per TLS 1.0 e TLS 1.1 sarà interrotto in futuro.

Questa connessione rimane aperta per tutto il tempo di funzionamento di ECI DCA. Normalmente viene utilizzata una connessione **WebSocket**, ma in alcune situazioni ECI DCA può tornare a utilizzare gli **eventi inviati dal server** o il **polling lungo HTTP**.

NOTA IMPORTANTE: Sono necessarie diverse connessioni HTTPS sicure in uscita dal server in 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>

Applicazione Printanista Requisiti

Agente di raccolta dati (ECI DCA)

Le stampanti, le fotocopiatrici e i 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 di applicazione della suite TCP/IP.

Requisiti del PC/server per ECI DCA:

Microsoft Windows (x86/64)

Requisiti:

- Windows 10 o superiore
- 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+, Fedora 28+
- Mono 5.4 o

superiore macOS (x64)

Requisiti:

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

Raspberry Pi 2 Model B, Raspberry P 3 Model B, Raspberry Pi 3 Model B+, e Raspberry Pi 4 Model

Requisiti:

- Scheda microSD vuota da 8 GB o più grande
- PC in grado di scrivere sulla scheda microSD

Considerazioni sul firewall per ECI DCA:

Connessioni in entrata

Non ci sono connessioni in entrata da Internet all'ECI DCA.

Connessioni in uscita

Servizio	Porto	Connessione a
Caricamento dei dati	443/TCP (HTTPS)	Il vostro server Hub Printanista
Aggiornamenti software	443/TCP (HTTPS)	L'ECI aggiorna il server
Registrazione (fallback)	53/UDP (DNS)	Server DNS di rete locale (primario) Server aggiornamenti ECI

		(fallback)
--	--	------------

L'ECI aggiorna il server

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

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 le richieste DNS a `*.reg.pf-d.ca` per registrarsi. In un primo momento cercherà di farlo utilizzando i server DNS della rete locale, per poi tornare a parlare direttamente con gli indirizzi IP di ECI Updates Server (utilizzando la porta **53/udp**). Il firewall deve consentire questa connessione a ECI Updates Server solo se i server DNS locali non risolvono le richieste di registrazione.

Regione di servizio

L'ECI DCA viene instradato verso la regione con la latenza di rete più bassa e in base alla disponibilità del servizio. In alcune località, la regione utilizzata può 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 dai DCA ECI e dai DCA Onsite legacy sono codificati e offuscati. Printanista richiede l'utilizzo di HTTPS per la comunicazione tra i DCA e l'Hub di Printanista. ECI DCA richiede HTTPS per funzionare. Inoltre, tutte le impostazioni e i lavori sensibili tra ECI DCA e Printanista vengono crittografati con l'algoritmo di crittografia simmetrica standard AES256, utilizzando 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 di Printanista concorrente o comunque non autorizzata.

Sicurezza Questioni di sicurezza

Il DCA ECI e il DCA Onsite 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 dal DCA ECI o dal DCA Onsite legacy, ad eccezione di indirizzo IP, indirizzo MAC e nome host.

ECI DCA e legacy Onsite DCA non raccolgono né elaborano alcun dato personale. L'unico modo in cui il sistema raccoglie questo tipo di informazioni è se voi o i vostri clienti inserite i dati in Printanista all'interno di un campo o di un'etichetta, come ad esempio la località o il nome del cliente. Il DCA ECI e il DCA Onsite 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 base di informazioni di gestione SNMP (MIB). 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 di una stampante sono documentati nell'IETF RFC 3805 (<https://tools.ietf.org/html/rfc3805>). Il produttore può esporre ulteriori informazioni sul dispositivo tramite estensioni e MIB privati (Management Information Base), ma le informazioni sono fondamentalmente tecniche e specifiche del dispositivo.

Printanista Hub è solo negozi:

- Hostname
- Sistema operativo
- Indirizzo IP remoto
- Architettura del sistema

Altre informazioni sulla rete e sull'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 da

Il DCA ECI e il DCA Onsite 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 attività
- Indirizzo MAC
- Descrizione del dispositivo
- Posizione

Servizio

Forniture

- Numero di serie della cartuccia del toner
- Livello di alimentazione della cartuccia del toner
- Livelli del tamburo
- Livelli del kit di manutenzione
- Livelli di fornitura non toner
- Livelli vari
- Dettagli sulla fornitura delle stampanti per etichette
- Varie (specifiche della macchina)

- Lettura LC D
 - Stato del dispositivo
 - Codice errore
 - Firmware
- Copertura e contatori
- Lettura del contatore
 - Tipo di contatore
 - Livello di copertura
 - Identificazione monocromatica o a colori

Rilevamento della rete e raccolta dei dati

Per aumentare l'efficienza del DCA, solo quando ci sono dati nuovi o modificati dai dispositivi, queste informazioni vengono inviate al Printanista Hub Server. In questo modo si garantisce un carico di rete minimo e si elimina la frequenza degli arretrati nell'invio dei dati dei dispositivi. Inoltre, il rilevamento e la scansione dei dispositivi sono ora indipendenti, in modo da garantire che solo l'indirizzo IP (o il nome dell'host) dei dispositivi rilevati in precedenza vengono scansionati su base periodica rispetto a una scansione completa della rete (completata inizialmente, periodicamente o quando stabilito da un utente amministratore).

In questo modo si garantisce che la velocità di invio dei dati dei dispositivi sia il più possibile aggiornata. In questo modo gli utenti possono essere avvisati di dispositivi problematici entro pochi minuti o addirittura secondi in molte situazioni. ECI DCA separa il rilevamento dei dispositivi dagli altri tipi di scansione, consentendo di impostare intervalli di scansione personalizzati per il recupero di contatori, attributi delle forniture ed errori. I valori predefiniti, minimi e massimi 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

Gli intervalli di scansione (contatori, forniture, errori e attributi) sono disponibili solo se il dispositivo dispone di un Model Definition File (MDF). Se questo non è presente, verrà eseguita una scansione completa del dispositivo in questione utilizzando un intervallo predefinito.

Gli amministratori di Printanista Hub possono gestire da remoto gli ECI DCA attivati sul server. Possono attivare da remoto l'ECI DCA per eseguire comandi predefiniti come attività di raccolta dati, fornire log ECI DCA, eseguire MIB Walks remoti o aggiornare le impostazioni ECI DCA.

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

Nota: la comunicazione avviene solo quando le informazioni su contatori, forniture o errori vengono aggiornate o modificate, riducendo l'utilizzo della larghezza di banda.

Nota: attualmente HP JAMC funziona solo con il DCA Onsite legacy.

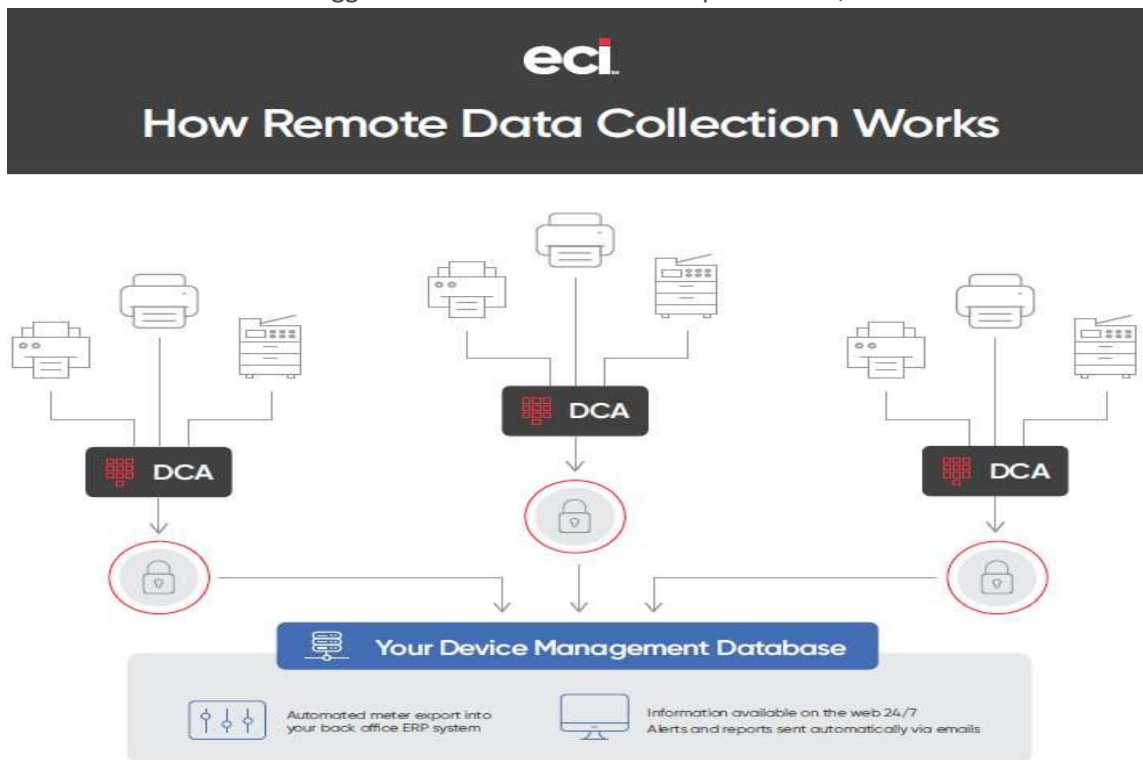
Stampanti locali

Flusso di lavoro di Printanista

Printanista Workflow è un solido strumento di gestione della stampa. Printanista Workflow può aiutare i vostri clienti a ridurre i costi di produzione dei documenti, ad aumentare le pratiche di sicurezza dei documenti e a fornire metodi flessibili di recupero dei costi. Grazie a un processo di installazione semplificato, i vostri clienti possono vedere rapidamente tutte le loro informazioni di stampa in un'unica posizione. I vostri clienti potranno ridurre i costi grazie alla comprensione di tutti i documenti che producono.

Che cos'è il flusso di lavoro di Printanista?

Printanista Workflow è la nuova generazione di prodotti per la gestione degli utenti utilizzati per tracciare e gestire la stampa per centinaia di organizzazioni e aziende in tutto il mondo. Chi aveva già familiarità con l'applicazione di gestione degli utenti in passato, sarà lieto di constatare che l'installazione e la configurazione dell'applicazione sono ancora intuitive come nelle versioni precedenti. I menu, gli strumenti e l'amministrazione generale del sistema sono stati mantenuti. Se si sta effettuando l'aggiornamento da una versione precedente, tutto risulterà familiare e facile da



navigare.

Come funziona il Workflow di Printanista (attraverso i dati ECI DCA raccolti dal Workflow)

Essendo Printanista Workflow la nuova generazione di gestione dei dispositivi, questa funzione funziona solo con l'ECI DCA. Printanista Workflow non funziona con il DCA Onsite.

- Il clientWorkflow può essere installato sui desktop dei sistemi operativi MAC e Windows, consentendo la raccolta di contatori da dispositivi USB collegati localmente.
- I parametri vengono determinati utilizzando i dati provenienti dallo spooler, dall'applicazione e dal driver di stampa.
- Memorizzato nel database del flusso di lavoro
- Il DCA richiede le informazioni sul contatore al Workflow tramite una chiamata API (Application Programming Interface) al

servizio web.

-Il DCA dell'ICE fornisce i dati all'Hub di Printanista per

-La connessione del flusso di lavoro all'ECI DCA è crittografata (https).

Requisiti di sistema del flusso di lavoro di Printanista

Server e strumenti di amministrazione

I componenti del server Printanista Workflow possono essere installati su computer in esecuzione:

- Microsoft Windows Server 2012 R2 o successivo
- Windows 8 Professional o più recente

(64bit) Un'installazione completa del server richiede:

- Almeno 5 Gigabyte di spazio libero per supportare il software Workflow.
- Sono necessari SQL Database e SQL Express 2012. SQL Express 2012 verrà installato se assente
- Internet Information Service (IIS) è necessario e verrà installato se assente.
- Microsoft .NET Framework 4.7.2 è necessario e verrà installato se assente.
- Per impostazione predefinita, tutti i lavori di stampa e i log vengono memorizzati su questo server.

Importante: i sistemi operativi Microsoft Home e Microsoft Small Business Server non sono supportati per nessun componente.

Requisiti del client Windows e utilizzo della memoria

È possibile installare il software Printanista Workflow Client Popup su computer con sistema operativo Microsoft Windows 8 o successivo.

- Un'installazione completa del client richiede circa 10-20 MB di spazio su disco. Il client è costituito da due componenti: il client desktop e il servizio client.
- Il client desktop richiede tra i 5 e i 20 Megabyte, a seconda dell'attività svolta.
- Non è necessario alcun software aggiuntivo.

Requisiti di sistema per Workflow Client per Mac

- Workflow Client per Mac® è supportato dai sistemi operativi Mac® secondo il modello di supporto Apple.
- Il client Mac® supporterà solo la versione più recente e due precedenti di Mac® OS.
- Cliccate su "Informazioni su questo Mac® " nel menu Apple, per scoprire quale versione di Mac® OS è in esecuzione sulla workstation.
- Workflow Client per Mac® richiede anche un (1) PC basato su Windows per ospitare il Workflow Server e il database.

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

Supporto per il server web IIS

Workflow utilizza Internet Information Services (IIS) per comunicare con i dispositivi e internamente tra i componenti di Workflow. L'installazione richiede la versione completa di IIS. Il programma di installazione determina se si dispone 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

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

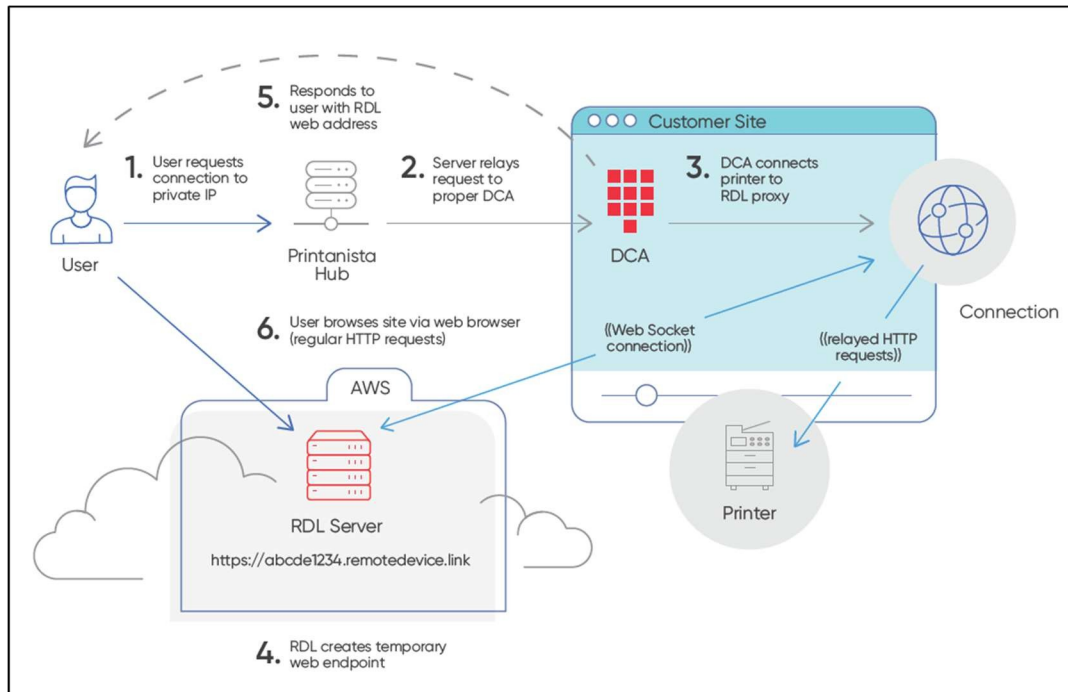
Dati forniti all'ECI DCA dal Workflow Server:

Esempi di alcune informazioni di identificazione dei dispositivi: Produttore, modello, indirizzo IP, numero di serie/asset, posizione, pagine a colori/monocromatiche, impressioni a colori/monocromatiche, ecc.

La documentazione della Guida al flusso di lavoro di Printanista è disponibile qui:

[Guida al flusso di lavoro di 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. Sono presenti 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`)
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.

Permessi di abilitazione e

1. Opzione di abilitazione globale per istanza del concessionario
2. Abilitazione locale per ogni cliente finale
3. Le autorizzazioni sono necessarie per consentire all'utente di accedere alla funzione.

Capacità di audit

1. Audit locale di Printanista Hub per i dettagli di ogni sessione
 - a. Rapporti di amministrazione di Printanista Hub per l'audit di Remote Device Link (RDL)
2. Remote Device Link (RDL) AWS (Amazon Web Services) registrazione in cloud di tutti i dettagli delle sessioni.

Remote Device Link (RDL) Sicurezza

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

- L'utente deve avere l'autorizzazione dall'interno di Printanista Hub per accedere alla funzione Remote Device Link (RDL) sull'account specifico.
- Il Data Collection Agent (DCA) accetterà le richieste di Remote Device Link (RDL) solo dal server Printanista Hub 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 all'interno dell'intervallo IP di rilevamento degli agenti di raccolta dati (DCA).
- Ogni singola richiesta web deve essere indirizzata allo stesso IP - Il Data Collection Agent (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 lo standard TLS 1.2 (Transport Layer Security).
- A ogni connessione viene assegnato un nome di dominio univoco che utilizza una combinazione alfa/numerica casuale di 19 caratteri (96 bit).
- 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.
- Il Data Collection Agent (DCA) può stabilire una connessione HTTP non crittografata al dispositivo di stampa attraverso la rete locale, ma supporta TLS 1.2 se il dispositivo

Limiti di tempo della sessione:

- Per impostazione predefinita, ogni sessione di Remote Device Link (RDL) viene interrotta 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 per l'installazione di DCA e richiede un certificato SSL attendibile valido da utilizzare su una connessione TLS.

Tutto il traffico che transita dal DCA a Internet è criptato. Tuttavia, il DCA ECI può parlare con il dispositivo nella rete locale tramite connessioni HTTP semplici se il dispositivo non supporta connessioni sicure.

Applicazione Printanista Hub

Le funzionalità di Printanista Hub sono accessibili tramite un'interfaccia utente

basata sul Web. Gestione degli utenti basata sui permessi

L'accesso al front-end web di Printanista Hub è controllato con una gestione degli utenti basata sui permessi. 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 l'accesso a uno o più gruppi di dispositivi. Gli amministratori con pieni permessi possono specificare esattamente le schermate che ogni utente può visualizzare e/o con cui può interagire.

Accesso HTTPS

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

Printanista Side-By-Side

Printanista Hub utilizza un database di metadati del modello noto come Side-by-Side (SBS), che contiene vari attributi del modello come: velocità di stampa, data di introduzione sul mercato o compatibilità con i numeri di parte degli OEM, e che viene aggiornato periodicamente man mano che gli OEM rilasciano modelli e versioni futuri. Printanista Hub comunicherà con Side-by-Side per verificare la presenza di nuovi aggiornamenti e recuperare i metadati del dispositivo per memorizzarli localmente su ciascun sistema Printanista Hub.

Hosting dell'applicazione Printanista Hub

Printanista Hub è ospitato da ECI Software Solutions all'interno di datacenter 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 commerciali e per il nostro stesso successo. Utilizziamo un approccio a più livelli per proteggere queste informazioni chiave, monitorando e migliorando costantemente le nostre applicazioni, i nostri sistemi e i nostri processi, per rispondere alle crescenti esigenze e sfide della sicurezza.

Centri dati sicuri ECI

Il nostro servizio è collocato in spazi dedicati presso centri dati di alto livello. Queste strutture forniscono un supporto di livello carrier. Fate clic sul seguente link per ottenere il documento dettagliato di ECI relativo alla sicurezza dei centri dati.

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

Gestione delle versioni

Processo di test e rilascio

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

Sicurezza del codice sorgente

Il codice sorgente di Printanista è conservato in un sistema di controllo delle revisioni protetto, accessibile solo alle 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 quale sviluppatore ha apportato la modifica e perché. Prima della spedizione, i prodotti vengono crittografati e firmati digitalmente con un certificato di firma del codice affidabile. Su richiesta, è possibile richiedere un deposito a garanzia.

L'ECI si avvale di una terza parte indipendente certificata CREST, SOC 2, NSA-CIRA e CSA-STAR, leader del settore, per condurre test di penetrazione a livello di applicazione e rimediare ai 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 prevede di compiere sforzi commercialmente ragionevoli per rimediare a tutti i risultati critici entro 30 giorni o entro un lasso di tempo ragionevole con una motivazione commerciale fornita. L'ECI non divulga i dettagli relativi ai controlli di sicurezza o ai risultati dei test di penetrazione, poiché si tratta di informazioni proprietarie e riservate che, nelle mani sbagliate, possono comportare un aumento del rischio.

Privacy dei dati e legislazione

Regolamento generale sulla protezione dei dati (GDPR)

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

L'ECI ha implementato un programma di conformità al GDPR strutturato e completo. Il programma comprende, tra l'altro, la formazione del personale, l'audit e la valutazione del rischio in tutta l'azienda, le politiche e le procedure, la governance e l'impegno costante per la conformità. Incoraggiamo i nostri clienti ad adottare misure simili per garantire che le loro aziende 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 persona o di un gruppo di persone.

Le applicazioni software di Printanista non raccolgono, memorizzano o trasmettono informazioni sul contenuto dei lavori di stampa.

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

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

Le comunicazioni del motore del prodotto sono controllate, utilizzando un accesso limitato a un indirizzo IP specifico e/o a un intervallo di contatti.

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

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

Per informazioni sulla conformità a leggi e/o regolamenti specifici, contattate il vostro Account Manager ECI.

Di seguito è riportato il link al documento ECI Cloud Security: [Panoramica sulla sicurezza del cloud ECI 2021 \(ecisolutions.com\)](https://ecisolutions.com/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 del proxy è necessaria sul sistema in cui è installato e funziona ECI DCA.

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

Consultare la sezione [Requisiti per la candidatura di Printanista](#) in questo documento.

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

Questo DCA ECI offre grandi vantaggi rispetto al DCA Onsite senza perdere alcuna funzionalità, tra cui il supporto nativo di Windows, macOS, Linux e Raspberry Pi. Ciascuna di queste piattaforme è dotata di passaggi di installazione, documentazione di supporto e personale di supporto 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. L'ECI DCA e l'Onsite DCA includono il proprio server per ospitare l'interfaccia utente (UI) basata sul web e viene impostata 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 whitelist per garantire la connettività di ECI DCA.

Servizio	Porto	Connessione a
Caricamento dei dati	443/TCP (HTTPS)	Il vostro server Hub Printanista
Aggiornamenti software	443/TCP (HTTPS)	L'ECI aggiorna il server
Registrazione (fallback)	53/UDP (DNS)	Server DNS di rete locale (primario) Server aggiornamenti ECI (fallback)

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

Quanto richiede la manutenzione continua di ECI DCA?

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

Come funziona il processo del WebAudit Assessment Tool?

Da Printanista Hub, il rivenditore specifica il ciclo di fatturazione applicabile dell'utente finale (i vostri clienti). A questo punto, viene generata automaticamente un'e-mail che viene inviata al contatto corretto per informarlo che è giunto il momento di ritirare i contatori. Le istruzioni includono un URL che, quando l'utente finale fa clic sul link, avvia automaticamente il suo browser web, pronto a eseguire l'azione. L'utente finale fa quindi clic su "inizia" e "salva". Fatto. Non viene installato alcun software. Un link alla pagina WebAudit può anche essere pubblicato sul sito web esistente del concessionario, ad esempio sulla pagina web Enter Meter Readings. In questo modo l'utente può automatizzare la raccolta, anziché andare manualmente da un dispositivo all'altro, stampare la pagina di configurazione e trascrivere i contatori.

Con quali marche di apparecchiature funziona il monitoraggio Remote Device Link (RDL)? Quali sono i requisiti per il funzionamento?

Tutti i marchi con una pagina web incorporata sono scoperti da ECI DCA. Le informazioni contenute nelle pagine web integrate variano a seconda del produttore e del modello. I dispositivi locali non mostrano la pagina web incorporata.

Ci sono ulteriori problemi di sicurezza con il 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 riporta solo i dispositivi rilevati e monitorati attivamente tramite ECI DCA. Viene visualizzato un messaggio che indica che la connessione del dispositivo non è supportata dal DCA.

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

Questo è prevedibile in quanto la connessione deve essere collegata tramite tunnel ai nostri servizi cloud. Tuttavia, il principale fattore di influenza è la velocità con cui i dispositivi rispondono alle richieste dell'interfaccia utente (UI). Abbiamo visto dispositivi rispondere in decimi di secondo ai primi tentativi di connessione, essere influenzati dall'utilizzo corrente o dalle risorse disponibili per l'interfaccia utente (UI).

Quali sono le funzioni disponibili con Remote Device Link (RDL)?

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

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

Sì, è possibile disattivare questa funzione per ogni account.

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

Dove posso trovare ulteriori informazioni per Printanista Hub, Printanista Workflow, ECI DCA, legacy Onsite DCA, ecc. Ulteriori informazioni sono disponibili sul sito web di Printanista dell'ECI:

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

Informazioni su Legacy Onsite DCA

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

- 1 GB DI RAM
- 400 MB di spazio su disco
- Microsoft .NET Framework 4.7.2 o più recente
- 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 supporta Windows Server 2022.
- Internet Explorer 11.0 o più recente, Chrome, Firefox
- MDAC 2.8 o superiore (normalmente incluso nell'installazione di Windows)
- JET 4.0 o superiore (normalmente incluso nell'installazione di Windows)
- Caricato su una macchina attiva 24 ore su 24, 7 giorni su 7, o almeno per l'intera giornata lavorativa.
- Durante l'installazione è necessario accedere come Amministratore locale (o equivalente).

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

Trasmissione dati:

- [https://\(azienda_Printanista_FQDN\)/WebServices/Onsite2Service.asmx](https://(azienda_Printanista_FQDN)/WebServices/Onsite2Service.asmx)
- Applicazione: fmaonsite.exe
- SOAP su HTTP deve essere autorizzato ad oltrepassare il firewall.

Requisiti di rete:

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

Si prega di utilizzare ECI DCA se sono necessari i sistemi operativi macOS, Linux o Raspberry Pi. Il sistema Java Onsite su Linux e macOS non è funzionante.

Requisiti del PC/stampante per l'utilizzo dell'Agente locale (installazione facoltativa):

- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- Microsoft .NET Framework 4.7.2 o più recente
- Driver corrente per la stampante locale (UPD è consigliato per i dispositivi HP)
- La stampante deve supportare il Printer Job Language (PJM) o il Printer Management Language (PML).
- Rimuovere i driver di stampa inutilizzati
- Il supporto bidirezionale del driver è attivato
- Modifiche al firewall di Windows - Porta 161/33333 in entrata/uscita per TCP e 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 loro varianti.

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

Le impostazioni di rilevamento automatico della rete brevettate da Printanista utilizzano una serie di algoritmi per identificare gli intervalli di rete in cui si trovano i dispositivi di stampa e quindi scoprire e comunicare con i dispositivi in linea, passando attraverso diversi elementi di rete come workstation o server attivi, router, hub, switch e hardware di rete aggiuntivo.

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

Funzione	Posizione	Descrizione
Compiti	Impostazioni in loco	È possibile configurare in remoto le attività da eseguire in base a un programma predefinito, ma anche selezionare le attività (Cache, Contatori, Forniture, Assistenza) da eseguire immediatamente e raccogliere i dati del dispositivo su comando.
Passeggiate MIB	Impostazioni in loco	Può indicare determinati IPv4/IPv6/nomi di host dei dispositivi e attivare l'Onsite per avviare immediatamente la raccolta dei MIB Walks.
Registri (dettagliati)	Impostazioni in loco	Può istruire l'Onsite a raccogliere i registri (Critico, Errore, Avviso, Dettagli, Debug) a partire da una certa 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 criptati utilizzando protocolli di crittografia forti e conformi a FIPS. Onsite riceve aggiornamenti software sicuri dai server di Printanista Updates.

Il DCA Onsite legacy comunica con Printanista a un intervallo predefinito per determinare se ci sono azioni in coda non ancora eseguite. In questo modo si garantisce che le azioni vengano eseguite in modo tempestivo.

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

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

Traffico di rete

Le verifiche condotte dal software utilizzano un sistema intelligente per estrarre informazioni minime per ogni 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, e ogni query del dispositivo non supera i pochi kilobyte di dati. Per ridurre ulteriormente la quantità di banda di rete utilizzata, Onsite DCA comunica con non più di 20 dispositivi alla volta. Ogni IP all'interno degli intervalli configurati viene interrogato e se non si riceve alcuna risposta entro il periodo di timeout configurato, si passa all'indirizzo IP successivo. Secondo una regola generale, Printanista raccoglie informazioni su circa 65.000 dispositivi in poco meno di un'ora.

Agente USB locale (funzionante SOLO con DCA Onsite)

L'Agente USB locale è la soluzione utilizzata per estrarre informazioni da una o più stampanti locali collegate a qualsiasi tipo di porta di Windows, come USB e parallela. L'Agente USB locale non interrompe il flusso dei lavori di stampa, ma si attiva solo quando viene richiamato da uno degli strumenti applicativi di raccolta di Printanista - DCA in loco o WebAudit - e poi si chiude. L'Agente USB locale raccoglie informazioni specifiche a seconda dei livelli di intelligenza della periferica dal motore e non dallo spooler di stampa. Gli attributi più comuni riportati sono il modello, il numero di serie, i contatori di durata, la copertura dei materiali di consumo, il livello dei materiali di consumo e l'assistenza. L'agente USB locale di Printanista può essere distribuito alle postazioni di lavoro utilizzando una soluzione come Microsoft SMS. Se la porta SNMP 161 o la porta alternativa di fallback dell'Agente 33333 vengono bloccate, potrebbe essere necessaria una riconfigurazione dell'antivirus o dei firewall software.

Supporto del produttore

I prodotti Printanista sono neutrali rispetto ai produttori. Supportano tutti i principali produttori e famiglie di modelli. Alcuni dispositivi hanno limitazioni che impediscono l'estrazione di determinate informazioni.

Preoccupazioni per i virus

I file dell'applicazione Printanista sono stati firmati digitalmente per impedire l'esecuzione se l'integrità del file è 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 rete.