Printanista Hub
Documento técnico

Version 1.3

Tabla de contenidos

Printanista

Visión general

El conjunto de productos Printanista ofrece una solución de impresión gestionada de clase empresarial que es bastante fácil de usar e implementar. Está diseñado y diseñado para aprovechar las características y ventajas avanzadas de la plataforma Microsoft .NET. Por lo tanto, ya no requiere técnicos calificados para instalar software, configurar y mantener el sistema. Los productos Printanista no pueden configurarse de ninguna manera para realizar una tarea más allá de aquellas para las que fueron diseñados. La transmisión de datos de los productos a fuentes externas está estrictamente restringida. Los productos no informan ningún otro detalle, excepto la información sobre el equipo que se está monitoreando (es decir, el tipo de equipo). Ninguna información confidencial se transmite fuera de la red a través de los productos Printanista. La suite consta de los siguientes componentes:

Printanista Hub: Un sitio web y sistema backend que alberga todos los datos recibidos de las herramientas de recopilación de datos de Printanista. Es un repositorio que le permite ver datos utilizando un navegador, generar informes, configurar flujos de trabajo y notificaciones de alerta y sincronizar datos con sus sistemas ERP para facturación o cumplimiento de suministros.

ECI DCA: Este nuevo Data Collection Agent-DCA ofrece grandes ventajas sobre el Onsite Data Collection Agent-DCA sin perder ninguna característica, incluido el soporte nativo completo multiplataforma de Windows, macOS, Linux y Raspberry Pi, cada uno con pasos de instalación únicos, documentación de soporte y personal de soporte capacitado en estas plataformas. ECI DCA también ofrece descubrimiento y escaneo continuos de dispositivos, capacidad mejorada de recolección de MIB Walk y Log, y ahora se recopilan muchos más tipos de medidores.

DCA in situ: una herramienta de agente de recopilación de datos heredada realiza automáticamente evaluaciones de impresión y supervisa los niveles de consumibles, el estado de la impresora y los registros de errores. Esta aplicación se instala en el sitio del cliente y puede realizar evaluaciones de impresión automáticamente de forma programada sin intervención humana. Los datos capturados se envían al sitio web de Printanista Hub utilizando HTTPS, HTTP o, si el cliente prefiere un archivo cifrado de propiedad.

WebAudit Assessment Tool: Una herramienta de recopilación de datos que forma parte de la aplicación Printanista Hub. Las evaluaciones de flotas se realizan directamente desde un navegador sin instalar ningún software. Los datos capturados se envían directamente a Printanista Hub.

El propósito de este documento es proporcionar una visión general de la línea de productos de la Suite de Productos Printanista desde una perspectiva técnica para ayudar a facilitar las respuestas a las preguntas más frecuentes que recibirán los equipos de Tecnología de la Información.

Printanista

Cómo funciona Printanista

El motor central del agente de recopilación de datos, que es el corazón de cada producto Printanista, identifica y extrae correctamente los datos de impresoras, copiadoras y MFP en red utilizando los protocolos compatibles con los dispositivos.

Printanista actualmente soporta (Simple Network Management Protocol) los protocolos SNMP v1, v2c y v3. SNMP v3 proporciona una mayor protección de paquetes para garantizar que la información y la comunicación se transmitan a través de fuentes confiables. A diferencia de SNMPv1 o v2, SNMP v3 está cifrado para mayor seguridad y requiere un nombre de usuario y una contraseña. Un beneficio de usar SNMP v3 es que los administradores de red pueden determinar el método de cifrado, así como un nombre de usuario y contraseña seguros.

SNMP es un protocolo de red que facilita el intercambio de información entre dispositivos de red que extraen datos de la Base de información de gestión (MIB) y otras ubicaciones dentro del dispositivo de impresión. La Base de información de administración (MIB) es una base de datos interna que la mayoría de los dispositivos conectados a la red tienen como parte de su anatomía. La Base de información de gestión (MIB) contiene datos como el nombre del modelo, los niveles de tóner y el estado actual de la impresora.

Requisitos de Printanista

Aplicación backend Printanista Hub

Printanista Hub Product Specifications

	Printanista Hub 5.0	ECI DCA 1.5	Onsite 4.1	Viewer 3	WebAudit on v4	Agent 4	Microsoft Support	Notes
Supported OSes[1]								
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 [3]	~~April 2018~~ ~~January 2023~~	
Windows 8.1 (32/64)	No	Yes	Yes	Yes	No	Partial [3]	~~April 2018~~ ~~January 2023~~	
Windows 10 (32/64)	No	Yes	Yes	Yes	No	Partial [3]	~~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

Utilice el siguiente enlace para ver las especificaciones completas actuales del producto Printanista: SysReq v3.0.html

Todos los datos recopilados se envían al servidor de Printanista Hub, donde están disponibles para informes y alertas. ECI DCA se conecta al servidor Printanista Hub mediante HTTPS (puerto **443/TCP).** Póngase en contacto con el administrador de la solución ECI para obtener información sobre los nombres de dominio y las direcciones IP utilizadas por su servidor. Esta conexión está protegida por **TLS** (Transport Layer Security) estándar de la industria. **Se recomienda TLS 1.2.** TLS 1.0 y TLS 1.1 son compatibles actualmente, pero no se recomiendan por motivos de seguridad. La compatibilidad con TLS 1.0 y TLS 1.1 dejará de ser admitida en el futuro.

Esta conexión permanece abierta todo el tiempo que ECI DCA se está ejecutando. Normalmente **se utiliza una conexión WebSocket**, pero en algunas situaciones ECI DCA puede recurrir al uso **de eventos enviados por el servidor** o **sondeos largos HTTP**.

NOTA IMPORTANTE: Se requieren varias conexiones salientes HTTPS seguras desde el servidor donde está instalado 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

Requisitos de la aplicación Printanista

Agente de recopilación de datos (ECI DCA)

Las impresoras, copiadoras y MFP deben tener habilitado el protocolo SNMP (puerto 161) para la detección y extracción de información. El protocolo SNMP es una parte estándar de la capa de aplicación de la suite TCP/IP.

Requisitos de PC/servidor para ECI DCA:

Microsoft Windows (x86/64)

Requisitos:

- Windows 7, 8, 10, Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, Server 2019 y Server 2021
  - .NET 4.5.2 superior

Linux (x86/64 or ARM)

Requisitos:

- Ubuntu 14.04, 16.04 or 18.04, Debian 9.5+, Raspbian Jessie or Stretch, RedHat Enterprise 7.5+, CentOS 7.5+, Fedora 28+
- Mono 5.4 o sup

macOS (x64)

Requisitos:

1. Sierra (10.12) o superior
2. Mono 5.4 o superior

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

Requisitos:

1. Tarjeta microSD en blanco de 8 GB o más
2. PC capaz de escribir en una tarjeta microSD

Consideraciones de firewall para ECI DCA:

Conexiones entrantes

No hay conexiones entrantes desde Internet a ECI DCA.

Conexiones salientes

Service	Port	Connection To
Carga de datos	**443/TCP** (HTTPS)	El servidor Printanista HUB
Actualizaciones de software	**443/TCP** (HTTPS)	Servidor de actualizaciones de ECI
Registro (reserva)	**53/UDP** (DNS)	Servidor DNS de red local (principal) Servidor de actualizaciones de ECI (reserva)

Servidor de actualizaciones de ECI

ECI Updates Server es un servicio ejecutado por ECI Device Management para facilitar el registro de DCA, las actualizaciones automáticas de software y las instalaciones de DCA (este sitio), y es necesario para la operación de ECI DCA. Nota: ECI DCA no envía ningún dispositivo recopilado ni datos de configuración al servidor de actualizaciones de ECI.

Actualizaciones de software

ECI DCA se actualiza automáticamente descargando actualizaciones publicadas en https://updates.printanista.net/ . Las conexiones siempre se realizan en el puerto HTTPS estándar **443/tcp**.

Registro

ECI DCA utiliza solicitudes DNS para `*.reg.pf-d.ca` para registrarse. Primero intentará hacer esto utilizando los servidores DNS de la red local y luego volverá a hablar directamente con las direcciones IP del servidor de actualizaciones de ECI (utilizando el puerto **53 / udp**). El firewall solo necesita permitir esta conexión al servidor de actualizaciones de ECI si los servidores DNS locales no resuelven las solicitudes de registro.

Región de servicio

ECI DCA se enruta a la región a la que tiene la latencia de red más baja y se basa en la disponibilidad del servicio. En ciertas ubicaciones, la región que se usa puede cambiar con el tiempo, ya que la actividad en la infraestructura global de Internet puede afectar la latencia.

Datos recopilados y cifrado

Cifrado Datos

Todos los paquetes de datos de ECI DCA y DCA in situ heredado están codificados y ofuscados. Printanista requiere el uso de HTTPS para la comunicación entre los DCA y Printanista Hub. ECI DCA requiere HTTPS para funcionar. Además, todas las configuraciones y trabajos confidenciales entre ECI DCA e Printanista se cifran utilizando el algoritmo de cifrado simétrico estándar AES256, utilizando una clave compartida protegida. Esto garantiza el cifrado de extremo a extremo, por lo que los datos están protegidos contra la lectura si son interceptados por un tercero, una instancia de Printanista competitiva o no autorizada.

Cuestiones de seguridad

ECI DCA y DCA in situ, heredado se comunican con Printanista Hub a través del protocolo HTTPS, utilizando **TLS 1.2** (Seguridad de la capa de transporte) estándar de la industria. Los datos confidenciales no son recopilados, vistos o guardados por ninguna aplicación de Printanista. Solo se recopilan y visualizan los datos relacionados con la impresora. ECI DCA o DCA in situ heredado no puede identificar ni recopilar ningún otro dato de red, excepto la dirección IP, la dirección MAC y el nombre de host.

ECI DCA y DCA in situ heredado no recopilan ni procesan ningún dato personal. La única forma en que el sistema recopilará este tipo de información es si usted o su(s) cliente(s) ingresan los datos en Printanista dentro de un campo o etiqueta como la ubicación o el nombre del cliente. ECI DCA y DCA in situ heredado le permiten supervisar dispositivos de red mediante el Protocolo simple de administración de red (SNMP). La aplicación se implementa dentro de la red del cliente y, desde allí, se comunica con los dispositivos para recopilar información operativa sobre el dispositivo que está disponible a través del firmware del dispositivo y una base de información de administración (MIB) SNMP. Los datos expuestos por el dispositivo varían según el fabricante y el modelo. Siempre es de naturaleza técnica u operativa y específica para el dispositivo en sí. En el nivel más básico, los datos expuestos por una impresora MIB están documentados en el IETF RFC 3805 (https://tools.ietf.org/html/rfc3805). El fabricante puede exponer información adicional del dispositivo a través de extensiones y MIB privadas (Base de información de gestión), pero la información es fundamentalmente técnica y específica del dispositivo.

Printanista Hub solo almacena:

1. Nombre de host
- Sistema operativo
- Dirección IP remota
- Arquitectura del sistema

Otra información de red/entorno se recopila y muestra mientras está conectado para solucionar problemas, pero nunca se almacena en Printanista.

Types of Information Collected

ECI DCA and legacy Onsite DCA attempts to collect the following information from networked printing devices during a network scan:

Atributos del dispositivo

1. Dirección IP (se puede enmascarar)
2. Fabricante
3. Número de serie
4. Número de activo
5. Dirección MAC
6. Descripción del dispositivo
7. Ubicación

Suministros

1. Número de serie del cartucho de tóner
2. Nivel de suministro del cartucho de tóner
3. Niveles de tambor
4. Niveles del kit de mantenimiento
5. Niveles de suministro sin tóner
6. Niveles varios
7. Detalles del suministro de impresoras basadas en etiquetas

Varios (específicos de la máquina)

1. Lectura LCD
2. Estado del dispositivo
3. Códigos de error
4. Firmware

Cobertura y medidores

1. Lecturas del medidor
2. Tipo de medidor
3. Nivel de cobertura
4. Identificación monocromática o de color

Descubrimiento de redes y recopilación de datos

Para aumentar la eficiencia del DCA, solo cuando haya datos nuevos o modificados de los dispositivos, esta información se enviará al servidor de concentradores de Printanista. Esto garantizará una carga de red mínima y eliminará la frecuencia de cualquier acumulación de envíos de datos del dispositivo. Además, el descubrimiento y el escaneo de dispositivos ahora son independientes para garantizar solo la dirección IP
(o nombre de host) de los dispositivos descubiertos previamente se están escaneando sobre la base establecida periódicamente en comparación con un escaneo de red completo (esto se completa inicialmente, periódicamente o cuando lo determina un usuario administrador).

Esto garantizará que la velocidad de envío de datos del dispositivo esté lo más actualizada posible. Esto permite a los usuarios ser notificados de dispositivos problemáticos en cuestión de minutos o incluso segundos en muchas situaciones. ECI DCA separa la detección de dispositivos de otros tipos de escaneo, lo que le permite establecer intervalos de escaneo personalizados para recuperar medidores, atributos de suministros y errores. Los valores predeterminados, mínimos y máximos para los intervalos de escaneo son:

Scan Function	Default	Minimum	Maximum
Discovery	60 minutes	10 minutes	7 days
Meters	24 hours	30 minutes	14 days
Supplies	4 hours	30 minutes	7 days
Errors	60 minutes	30 minutes	7 days
Attributes	24 hours	1 hour	14 days

Tenga en cuenta que los intervalos de escaneo (medidores, suministros, errores y atributos) solo están disponibles si un dispositivo tiene un archivo de definición de modelo (MDF). Si esto no está presente, se realizará un escaneo completo en el dispositivo en cuestión utilizando un intervalo predefinido.

Los administradores de Printanista Hub pueden administrar de forma remota ECI DCA que se han activado en el servidor. Puede activar de forma remota el DCA de ECI para ejecutar comandos predefinidos, como tareas de recopilación de datos, proporcionar registros de DCA de ECI, ejecutar caminatas MIB remotas o actualizar la configuración de DCA de ECI.

Nota: ECI DCA siempre inicia la comunicación con el servidor Printanista, y no al revés.

Nota: Solo cuando la información del medidor, el suministro o los errores se ha actualizado o cambiado, se produce la comunicación, lo que reduce el uso de ancho de banda.

Nota: HP JAMC solo funciona con DCA in situ heredado en la actualidad.

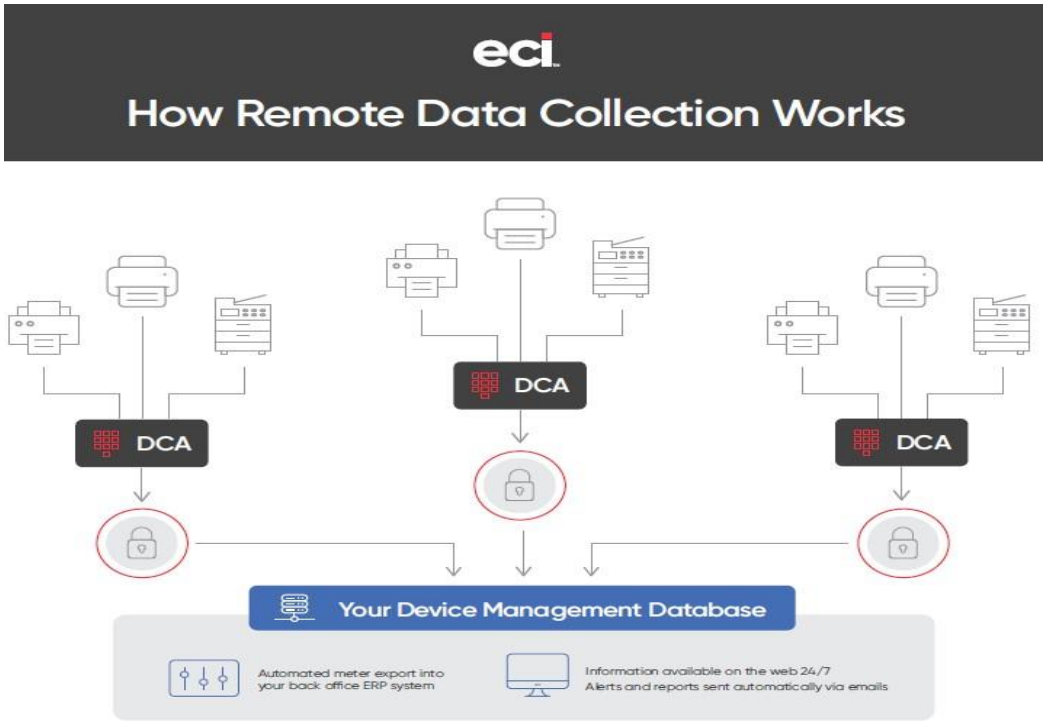
Impresoras locales

Flujo de trabajo

Printanista Workflow es una herramienta robusta de gestión de impresión. Printanista Workflow puede ayudar a sus clientes a reducir el costo de la producción de documentos, aumentar sus prácticas de seguridad de documentos y proporcionar métodos flexibles de recuperación de costos. Mediante un proceso de instalación simplificado, sus clientes pueden ver rápidamente toda su información de impresión en una sola ubicación. Empoderar a sus clientes para reducir costos al comprender cada documento que producen.

¿Qué es Printanista Workflow?

Printanista Workflow es la próxima generación de productos de gestión de usuarios utilizados para rastrear y administrar la impresión para cientos de organizaciones y empresas de todo el mundo. Si estaba familiarizado con la aplicación de administración de usuarios en el pasado, le complacerá ver que la instalación y configuración de la aplicación sigue siendo tan intuitiva como las versiones anteriores. Se han conservado los menús, las herramientas y la administración general del sistema. Si está actualizando desde una versión anterior, todo será familiar y fácil de navegar



Cómo funciona Printanista Workflow (a través de los datos de ECI DCA se recopilan de Workflow)

Printanista Workflow es la próxima generación de administración de dispositivos, esta función solo funciona con el ECI DCA. Printanista Workflow no funciona con DCA in situ.

-El cliente de flujo de trabajo se puede instalar en escritorios del sistema operativo MAC y Windows, lo que permite la recolección de medidores de dispositivos USB conectados localmente

-Los medidores se determinan utilizando datos de la cola de impresión, la aplicación y el controlador de impresión

-Almacenado en la base de datos de flujo de trabajo

-ECI DCA solicita la información del medidor del flujo de trabajo a través de la llamada API (interfaz de programación de aplicaciones) al servicio web

-ECI DCA proporciona datos a Printanista Hub para ....

-El flujo de trabajo a la conexión DCA de ECI está cifrado (https)

Printanista Workflow System Requirements

Server and Admin Tools

You can install the Printanista Workflow server components on computers running:

- Microsoft Windows Server 2012 R2 o posterior
- Windows 8 Professional or sup (64bit)

A full server installation requires:

- Un mínimo de 5 gigabytes de espacio libre para admitir el software Workflow
- Se requieren Base de datos SQL y SQL Express 2012. SQL Express 2012 se instalará si está ausente
- Se requiere Internet Information Service (IIS) y se instalará si está ausente
- .NET 4.5.2 es necesario y se instalará si está ausente.

1. De forma predeterminada, todos los trabajos y registros de datos de impresión se almacenan en este servidor

Importante: Los sistemas operativos Microsoft Home y Microsoft Small Business Server no son compatibles con ningún componente.

Requisitos del cliente de Windows y uso de memoria

Puede instalar el software emergente Printanista Workflow Client en equipos que ejecutan Microsoft Windows 8 o posterior.

- Una instalación completa del cliente requerirá aproximadamente 10-20 MB de espacio en disco. El cliente se compone de dos componentes: el cliente de escritorio y el Servicio al Cliente.
- El cliente de escritorio requiere entre 5 y 20 megabytes, dependiendo de la actividad.
- No se requiere software adicional.

Requisitos del sistema para Workflow Client para Mac®

- Workflow Client para Mac es compatible con sistemas operativos Mac®® siguiendo el modelo de soporte de Apple.
- El cliente Mac solo admitirá la versión más reciente y dos versiones anteriores de Mac®® OS.
- Haga clic en "Acerca de esta Mac" en su menú Apple, para encontrar qué versión de Mac®® OS se está ejecutando en la estación de trabajo.
- Workflow Client para Mac® también requiere un (1) equipo basado en Windows para hospedar Workflow Server y la base de datos.

Important: Printanista Workflow debe estar instalado en una red con al menos un equipo Windows.

Compatibilidad con servidores web de IIS

Workflow usa Internet Information Services (IIS) para comunicarse con dispositivos e internamente entre los componentes de Workflow. La instalación requiere la versión completa de IIS. El instalador determinará si tiene una instalación de IIS existente. De lo contrario, el instalador creará un nuevo sitio y grupo de aplicaciones mediante IIS.

Requisitos de red

Printanista Workflow utiliza la comunicación HTTP / SSL estándar a través de los puertos 80/443 para servicios web de forma predeterminada. Si estos puertos no están disponibles, Workflow utilizará 6320/6321. Sin embargo, puede cambiar los puertos de comunicación si hay un conflicto en su organización.

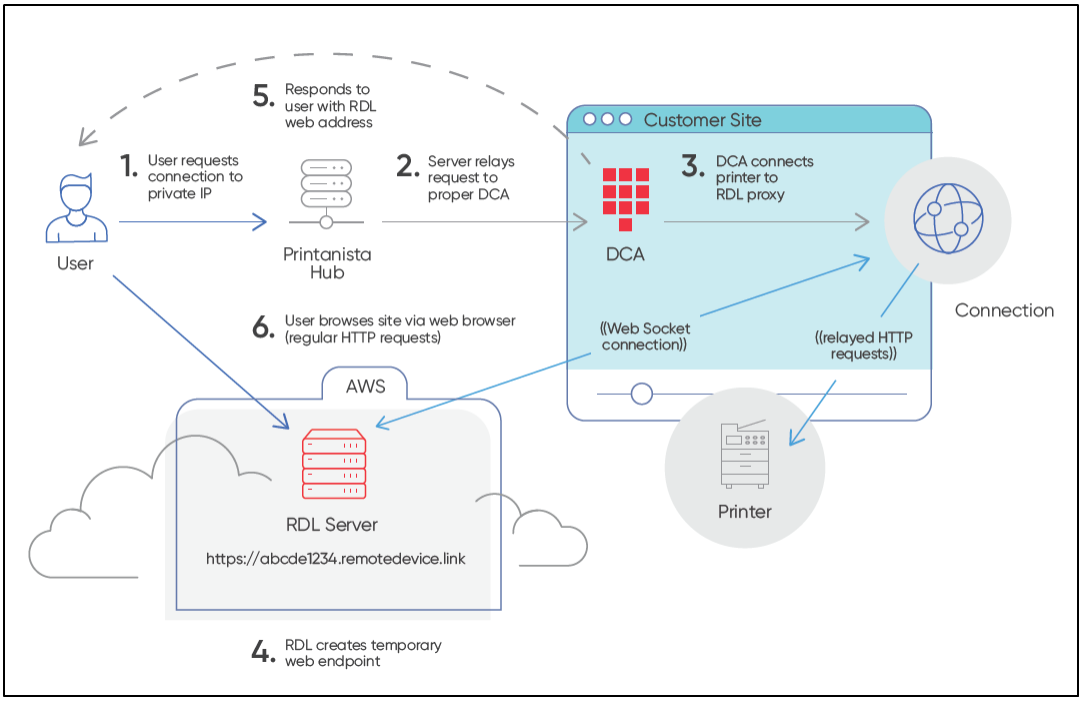
Datos suministrados a ECI DCA por Workflow Server:

Ejemplos de información de identificación de algunos de los dispositivos: fabricante, modelo, dirección IP, número de serie / activo, ubicación, páginas en color / monocromáticas, impresiones en color / monocromáticas, etc..

La documentación de ayuda de Printanista Workflow se puede encontrar aquí:

Printanista Workflow Help

Remote Device Link (RDL)



Descripción general del sistema: Remote device link (RDL)

Remote Device Link (RDL) es un servicio que permite a un **usuario final** remoto acceder a un extremo HTTP en una LAN privada. Hay 4 componentes principales para él:

1. El **usuario final** que accede al dispositivo
2. El **servidor de Remote Device Link**, en Internet público (a través de https://*.remotedevice.link URL)
3. El **cliente RDL** (incrustado en el DCA), que se ejecuta en la LAN privada
1. El **punto final HTTP (**impresora) al que se accede (que se ejecuta en la LAN privada)

Seguridad: Puertos y SSL (Secure Sockets Layer)

La ruta pública para RDL es siempre una dirección URL https:// en el puerto 443, independientemente del puerto del punto final o del estado SSL.

Habilitación y permisos

1. Opción de habilitación global por instancia de distribuidor
2. Habilitación local para cada cuenta de cliente final
3. Se requieren permisos para que un usuario pueda acceder a la característica

Capacidades de auditoría

1. Auditoría local de Printanista Hub de los detalles de cada sesión
- Informes de administración de Printanista Hub para la auditoría de enlace de dispositivo remoto (RDL)
2. Enlace de dispositivo remoto (RDL) Registro en la nube de AWS (Amazon Web Services) de todos los detalles de la sesión

Seguridad de enlace de dispositivo remoto (RDL)

La seguridad de Remote Device Link (RDL) fue una preocupación clave al desarrollar

esta herramienta.

Autorización:

- El usuario debe tener permiso desde Printanista Hub para acceder a la función Remote Device Link (RDL) en la cuenta.
- El Agente de recopilación de datos (DCA) solo aceptará solicitudes RDL (Remote Device Link) del servidor Printanista Hub, que es mutuamente autenticada.
- El Agente de recopilación de datos (DCA) solo establece una conexión RDL (Remote Device Link) con dispositivos de impresión conocidos y supervisados actualmente dentro del intervalo IP de detección de los agentes de recopilación de datos (DCA)
- Cada solicitud web individual debe ser a la misma IP: el agente de recopilación de datos (DCA) no seguirá redirecciones.

Seguridad de conexión:

- Todas las conexiones hacia y desde los servidores Remote Device Link (RDL) y Printanista Hub se cifran mediante TLS 1.2 estándar (Transport Layer Security)
- A cada conexión se le asigna un nombre de dominio único que utiliza un combinación alfa / numérico aleatorio de 19 caracteres (96 bits)
- Cada solicitud requiere un token de seguridad de 160 bits, almacenado como una cookie del navegador y solo configurado al inicio de la sesión protegida por encriptación TLS.
- El Agente de recopilación de datos (DCA) puede establecer una conexión HTTP no cifrada con el dispositivo de impresión a través de la red local, pero admite TLS 1.2 si el dispositivo lo soporta.

Límites de tiempo de sesión:

- Cada sesión individual de Remote Device Link (RDL) agota el tiempo de espera después de 20 minutos de inactividad de forma predeterminada con un máximo absoluto de 2 horas.

Implicaciones

La conexión entre ECI DCA y Printanista Hub está protegida por claves de autenticación que son específicas de la instalación de DCA, y la conexión requiere un certificado SSL de confianza válido para usar a través de una conexión TLS.

Todo el tráfico que transita desde el DCA a Internet está encriptado. Sin embargo, el DCA de ECI puede comunicarse con el dispositivo en la red local a través de conexiones HTTP simples si el dispositivo no admite conexiones seguras.

Printanista Hub Application

La funcionalidad de Printanista Hub es accesible a través de una interfaz de usuario

basada en web. Administración de usuarios basada en permisos

El acceso al front-end web de Printanista Hub se controla con la administración de usuarios basada en permisos. Los usuarios deben iniciar sesión en Printanista con un nombre de usuario y contraseña designados. A los usuarios se les asignan uno o más roles que especifican permisos y se les concede acceso a uno o más grupos de dispositivos. Los administradores con permiso total pueden especificar exactamente qué pantallas puede ver o interactuar cada usuario.

Acceso HTTPS

Printanista requiere que todos los sitios usen HTTPS con un certificado de seguridad SSL válido. Esto garantiza el cifrado de los datos que se transfieren a través de Internet.

Printanista lado a lado

Printanista Hub utiliza una base de datos de metadatos del modelo conocida como Side-by-Side (SBS), que tiene varios atributos del modelo, tales como: velocidades de impresión, cuándo se introdujo en el mercado o compatibilidades de números de pieza OEM, que se actualiza periódicamente a medida que los OEM lanzan modelos y versiones futuras. Printanista Hub se comunicará con Side-by-Side para buscar nuevas actualizaciones, así como recuperar metadatos del dispositivo para almacenarlos en caché localmente en cada sistema Printanista Hub.

Printanista Hub Alojamiento de aplicaciones

Printanista Hub está alojado por ECI Software Solutions dentro de centros de datos seguros y protegidos en diferentes regiones del mundo. ECI Software Solutions entiende que la confidencialidad, integridad y disponibilidad de la información de nuestros clientes es vital para sus operaciones comerciales y para nuestro propio éxito. Utilizamos un enfoque de múltiples capas para proteger esa información clave, monitoreando y mejorando constantemente nuestras aplicaciones, sistemas y procesos, para satisfacer las crecientes demandas y desafíos de seguridad.

Centros de datos seguros de ECI

Nuestro servicio se encuentra en espacios dedicados en centros de datos de primer nivel. Estas instalaciones

proporcionan soporte a nivel de operador. Haga clic en el siguiente enlace para obtener el documento detallado de

ECI relacionado con la seguridad de los centros de datos

ECI Cloud Security Overview 2021 (ecisolutions.com)

Gestión de versiones

Proceso de prueba y lanzamiento

Cada versión mayor y menor del software pasa por un proceso de control de calidad, en el que múltiples miembros del personal de Printanista probarán de regresión las partes alteradas del sistema para garantizar que no haya habido una degradación en la seguridad o funcionalidad del sistema, así como validar los nuevos aspectos funcionales. Las versiones principales pasan por un proceso de lanzamiento beta en el que los clientes seleccionados ejecutan los sistemas nuevos y antiguos en paralelo.

Seguridad del código fuente

El código fuente de Printanista se mantiene en un sistema de control de revisión seguro, accesible solo para personas autorizadas. Cada cambio en el código fuente requiere que dos desarrolladores autorizados aprueben los cambios antes de ser aceptados en el repositorio de código de producción donde se realiza un seguimiento de cada cambio, que incluye qué desarrollador realizó el cambio y por qué. Los productos se cifran y firman digitalmente con un certificado de firma de código de confianza antes del envío. Un depósito de depósito en garantía puede estar disponible bajo petición.

ECI contrata a un tercero independiente certificado por CREST, SOC 2, NSA-CIRA, CSA-STAR líder en la industria para realizar pruebas de penetración a nivel de aplicación y remediar los hallazgos basados en sus requisitos comerciales y marco interno de gestión de riesgos. Las pruebas de penetración se realizan al menos una vez al año o cuando se realizan cambios importantes en el
sistema. La política de ECI es utilizar esfuerzos comercialmente razonables para remediar todos los hallazgos críticos dentro de los 30 días o dentro de un plazo razonable con un caso de negocio proporcionado. ECI no revela detalles sobre nuestros controles de seguridad o los resultados de las pruebas de penetración, ya que esa información es patentada y confidencial y está en las manos equivocadas puede generar un mayor riesgo.

Data Privacy and Legislation

Reglamento General de Protección de Datos (RGPD)

A partir de mayo de 2018, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea entró en pleno efecto. El GDPR reemplaza la Directiva de Protección de Datos 95/46 / CE y está diseñado para fortalecer y unificar las leyes de privacidad de datos en toda Europa.

ECI ha implementado un programa de cumplimiento de GDPR estructurado y completo. El programa consiste, entre otras cosas, en capacitación del personal, auditoría y evaluación de riesgos en todo el negocio, políticas y procedimientos, gobierno y esfuerzos continuos de cumplimiento. Alentamos a nuestros clientes a tomar medidas similares para garantizar que sus propios negocios cumplan con GDPR y en los próximos años.

Los productos Printanista no procesan, monitorean ni administran ningún registro personal ni ningún registro o información específica de ninguna persona o grupo de personas.

Las aplicaciones de software de Printanista no recopilan, alojan ni transmiten ninguna información sobre el contenido de los trabajos de impresión.

Printanista no tiene forma de acceder, alojar o transmitir información de alto riesgo, incluso si esta información se imprime o se envía a dispositivos de impresión monitoreados por aplicaciones de software de Printanista.

Las aplicaciones de software de Printanista no almacenan, procesan ni transmiten datos del titular de la tarjeta ni información personal.

Las comunicaciones del motor del producto están controladas, utilizando acceso limitado a la dirección IP y / o rango específico del contacto.

Todas las comunicaciones deben originarse en los productos de Printanista, y no hay forma de contactar y acceder a los productos desde fuera de la red.

La comunicación fuera de la red utiliza un flujo de datos comprimido propietario que se envía mediante SSL a través de HTTPS estándar de la industria.

Para obtener información relacionada con el cumplimiento de leyes y/o regulaciones específicas, comuníquese con su gerente de cuenta de ECI.

El siguiente es un enlace a ECI Cloud Security: ECI Cloud Security Overview 2021 (ecisolutions.com)

Preguntas frecuentes (FAQs)

¿Los productos Printanista funcionan con proxies de Internet?
Sí, ECI DCA puede funcionar con la mayoría de los proxies. La configuración del proxy es necesaria en el sistema donde está instalado y opera el DCA de ECI.
¿Cuáles son los requisitos mínimos de Printanista Hub, ECI DCA, Onsite?
Por favor, consulte el Printanista Application Requirements de este documento.

¿Los productos Printanista son compatibles con entornos Mac, Linux o Raspberry Pi?
Este ECI DCA ofrece grandes ventajas sobre el DCA in situ sin perder ninguna característica, incluido el soporte multiplataforma nativo completo de Windows, macOS, Linux y Raspberry Pi. Cada uno con pasos de instalación únicos, documentación de soporte y personal de soporte capacitado en estas plataformas. El proceso de instalación también ha mejorado mucho y es mucho más intuitivo para todo tipo de usuarios.

¿ECI DCA requiere Microsoft Internet Information Services (IIS)?
No. ECI DCA y DCA in situ incluyen su propio servidor para alojar la interfaz de usuario (UI) basada en web y se configura automáticamente durante la instalación.

¿Se puede instalar ECI DCA en un equipo que ya hospeda otro sitio web de IIS?
Sí. Sin embargo, los puertos enumerados a continuación deben estar en la lista blanca para garantizar la conectividad de ECI DCA.

Service	Port	Connection To
Data Upload	**443/TCP** (HTTPS)	Your Printanista Hub Server
Software Updates	**443/TCP** (HTTPS)	ECI Updates Server
Registration (fallback)	**53/UDP** (DNS)	Local Network DNS server (primary) ECI Updates Server (fallback)

ECI DCA utiliza el puerto 31816 de forma predeterminada para la interfaz de usuario local basada en web de DCA.

¿Cuánto mantenimiento continuo requiere ECI DCA?
ECI DCA y DCA in situ es un servicio que se ejecuta en segundo plano y realiza auditorías y exportaciones a destinos configurados en horarios predefinidos. Se recomienda utilizar subredes (rangos de IP) en lugar de IP fijas. Al agregar nuevos dispositivos a la red, se descubrirán e incluirán en los resultados de la auditoría, lo que limitará la intervención manual.

¿Cómo funciona el proceso de la herramienta de evaluación WebAudit?
Desde Printanista Hub, el distribuidor especifica el ciclo de facturación aplicable del usuario final (sus clientes/clientes). En este momento, se genera automáticamente un correo electrónico y se envía al contacto adecuado informándole que es hora de recoger sus medidores. Las instrucciones incluyen una URL mediante la cual cuando el usuario final hace clic en el enlace, inicia automáticamente su navegador web, listo para realizar la acción. A continuación, el usuario final hace clic en "'inicio" y "'guardar"'. Hecho. No se instala ningún software en ningún momento. También se puede publicar un enlace a la página WebAudit en el sitio web existente de los distribuidores, es decir, la página web Enter Meter Readings. Esto permite al usuario automatizar la colección, en lugar de caminar manualmente de un dispositivo a otro, imprimir la página de configuración y transcribir los medidores.

¿Con qué marcas de equipos funcionará la supervisión de Remote Device Link (RDL)? ¿Cuáles son los requisitos para que funcione?
Todas las marcas con una página web incrustada son descubiertas por ECI DCA. La información en las páginas web incrustadas variará según el fabricante y el modelo. Los dispositivos locales no mostrarán la página web incrustada.

¿Hay problemas de seguridad adicionales con Remote Device Link (RDL)?
Se abre un canal seguro entre el dispositivo en la red local del cliente y un operador ubicado fuera de esa red. RDL solo informará sobre los dispositivos descubiertos y monitoreados activamente a través de ECI DCA. Aparece un mensaje que indica que la conexión del dispositivo no es compatible a través del DCA

Remote Device Link (RDL) parece un poco lento, ¿por qué?
Esto se puede esperar ya que la conexión debe ser tunelizada a través de nuestros servicios en la nube. Sin embargo, el principal factor de influencia es la rapidez con que los dispositivos responden a las solicitudes de la interfaz web de usuario (UI).
Hemos visto dispositivos que responden en décimas de segundos a los primeros intentos de conexión, a ser influenciados por el uso actual o los recursos disponibles para la interfaz de usuario (UI).

¿Qué funciones están disponibles con Remote Device Link (RDL)?
Se puede acceder a todas las opciones a las que el OEM proporciona acceso a través de la página web incrustada a través de Remote Device Link (RDL).

¿Se puede desactivar la función Vínculo de dispositivo remoto (RDL)?
Sí, existe la posibilidad de desactivar esta función por cuenta.
También es posible desactivar esta función por usuario, lo que le permite bloquear el acceso de un usuario a Remote Device Link (RDL).

¿Dónde puedo obtener información adicional para Printanista Hub, Printanista Workflow, ECI DCA, DCA in situ heredado, etc.? Se puede encontrar información adicional en el sitio web Printanista de ECI: https://www.ecisolutions.com/products/printanista-hub/

Información de DCA en el sitio heredada

Se recomienda utilizar ECI DCA con Printanista. Sin embargo, el DCA in situ heredado actualmente funciona con Printanista. Requisitos de PC/servidor para DCA in situ:

- 1 GB de RAM
- 400 MB de espacio en disco
- Microsoft .NET Framework 4.7.1 o posterior
- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- La versión 4.1.3 in situ y posterior es compatible con Windows Server 2022
- Internet Explorer 11.0 o posterior, Chrome, Firefox
- MDAC 2.8 o superior (normalmente se incluye cuando Windows está instalado)
- JET 4.0 o superior (normalmente se incluye cuando Windows está instalado)
- Cargado en una máquina que está activa las 24 horas del día, los 7 días de la semana o al menos todo el día hábil
- Debe haber iniciado sesión como administrador local (o equivalente) durante la instalación

Consideraciones sobre el firewall saliente (puerto 80 o 443)):

Transmisión de datos:

- https://(company_Printanista_FQDN)/WebServices/Onsite2Service.asmx
- Aplicación: fmaonsite.exe
- SOAP sobre HTTP(s) debe permitirse más allá del firewall

Requisitos de red:

El tráfico SNMP (puerto 161) debe ser enrutable a través de la LAN o WAN (redes de área amplia))

Utilice ECI DCA si los sistemas operativos macOS, Linux o Raspberry Pi son necesarios El Java Onsite heredado en sistemas Linux y macOS no funciona.

Requisitos de PC/impresora para utilizar el agente local (instalación opcional):

- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- Microsoft .NET Framework 4.7.1 o posterior
- Controlador actual para la impresora local (se recomienda UPD para dispositivos HP)
- La impresora debe admitir el lenguaje de trabajo de impresora (PJL) o el lenguaje de administración de
- impresoras (PML))
- Quitar los controladores de impresión no utilizados
- El soporte bidireccional del conductor está habilitado
- Modificaciones del Firewall de Windows: puerto 161/33333 entrante/saliente para TCP y UDP

Nota: Para las versiones recientes del sistema operativo que utilizan el modelo de controlador 4 (por ejemplo, Windows 10), actualmente solo se admiten los OEM de Kyocera y Ricoh, y sus variaciones.

Descubrimiento de redes y recolección de medidores y suministros (DCA in situ)

La configuración de descubrimiento automático de red patentada por Printanista utiliza una combinación de algoritmos para identificar los rangos de red donde se pueden ubicar los dispositivos de impresión y luego descubrir y comunicarse con los dispositivos que están en línea, enrutando a través de múltiples elementos de red, como estaciones de trabajo o servidores activos, enrutadores, concentradores, conmutadores y hardware de red adicional.

Los administradores de Printanista Hub pueden administrar de forma remota los DCA (Data Collection Agent) activados en el servidor, así como activar de forma remota el Onsite para ejecutar comandos predefinidos, como tareas de recopilación de datos, proporcionar registros in situ, ejecutar MIBWalks remotos, instalar HP JCM o actualizar la configuración in situ. Estos se explican con más detalle a continuación.:

Function	**Location**	**Description**
Tareas	Configuración in situ	Puede configurar de forma remota las tareas para que se ejecuten en una programación preestablecida, pero puede seleccionar tareas (caché, medidores, suministros, servicio) para que se ejecuten inmediatamente y recopilen datos del dispositivo bajo comando.
Caminatas MIB	Configuración in situ	Puede indicar ciertos nombres de host IPv4/IPv6/de dispositivos y activar el Onsite para iniciar la recopilación de los paseos MIB inmediatamente.
Registros (detallados)	Configuración in situ	Puede indicar al sitio que recopile los registros (críticos, error, advertencia, detalles, depuración) a partir de una fecha determinada.

Ninguno de estos comandos conduce a la recopilación de datos más allá de los tipos de información recopilada como se describió anteriormente. Los datos intercambiados entre DCA in situ y Printanista Hub se cifran mediante protocolos de cifrado sólidos que cumplen con FIPS. Onsite recibe actualizaciones de software seguras de los servidores de Printanista Updates.

El DCA in situ heredado se comunica con Printanista en un intervalo predefinido para determinar si hay acciones en cola que aún no se hayan ejecutado. Esto garantiza que las acciones se ejecuten de manera oportuna.

Nota: DCA in situ siempre inicia esta comunicación con el servidor Printanista, y no al revés.

Nota: HP JAMC solo es compatible con el DCA in situ heredado en el lanzamiento inicial de Printanista.

Tráfico de red

Las auditorías realizadas por el software utilizan un sistema inteligente para extraer información mínima para cada impresora, copiadora o MFP. A diferencia de productos similares que envían un conjunto fijo de consultas (un superconjunto de todas las consultas posibles) a cada dispositivo en red, Onsite DCA solo envía las consultas relevantes de acuerdo con los campos que admite el dispositivo de destino, y cada consulta de dispositivo no es más que unos pocos kilobytes de datos. Para reducir aún más la cantidad de ancho de banda de red utilizado, el DCA in situ se comunica con no más de 20 dispositivos a la vez. Se consultará cada IP dentro de los rangos configurados y, si no se recibe respuesta dentro del período de tiempo de espera configurado, pasará a la siguiente dirección IP. Una regla general es que Printanista recopilará información sobre aproximadamente 65,000 dispositivos en poco menos de una hora.

Agente USB local (SOLO funcional con DCA in situ)

El Agente USB local es la solución utilizada para extraer información de una o más impresoras locales conectadas a cualquier tipo de puerto de Windows, como USB y paralelo. El agente USB local no interrumpe el flujo de trabajos de impresión, solo
se activa cuando se le solicita una de las herramientas de aplicación de recopilación de Printanista, DCA in situ o WebAudit, y luego se cierra. El agente USB local recopila información específica que depende de los niveles de inteligencia del dispositivo del motor y no de la cola de impresión. Los atributos más comunes notificados son modelo, número de serie, medidores de tiempo de vida, cobertura de consumibles, nivel de consumibles y servicio. Printanista Local USB Agent se puede implementar en las estaciones de trabajo mediante una solución como Microsoft SMS. Es posible que sea necesario volver a configurar los firewalls antivirus o de software si se bloquea el puerto SNMP 161 o el puerto alternativo de reserva del agente 33333.

Soporte del fabricante

Los productos Printanista son neutrales con respecto al fabricante. Son compatibles con todos los principales fabricantes y familias de modelos. Algunos dispositivos tienen limitaciones que impiden la extracción de cierta información.

Preocupaciones sobre el virus

Los archivos de la aplicación Printanista se han firmado digitalmente para evitar la ejecución si la integridad del archivo se ve comprometida. Esto asegura que si algún virus puede estar presente no se active y evita la propagación del virus de una red a otra. Para mayor seguridad, recomendamos utilizar software antivirus en su red.

