



Documento técnico de Printanista Hub

Versión 1.8



Índice

Descripción general.....	4
Printanista Hub diseñado como una aplicación alojada.....	5
Centros de datos seguros de ECI	5
Agente de recopilación de datos (DCA).....	5
Aplicación backend de Printanista Hub	6
Requisitos de la aplicación Printanista	7
Agente de recopilación de datos (ECI DCA)	7
Requisitos del PC/servidor para ECI DCA.....	7
Servidor de actualizaciones ECI	8
Actualizaciones de software	8
Registro	8
Región de servicio	8
Datos recopilados y cifrado	9
Cifrado de datos	9
Cuestiones de seguridad	9
Tipos de información recopilada	9
Enlace remoto de dispositivos (RDL).....	11
Descripción general del sistema: Remote Device Link (RDL)	11
Seguridad: puertos y SSL (capa de sockets seguros)	11
Habilitación y permisos	11
Capacidades de auditoría	11
Seguridad de Remote Device Link (RDL)	12
La seguridad del enlace remoto de dispositivos (RDL) fue una preocupación clave durante el desarrollo de esta herramienta.	12
Aplicación Printanista Hub.....	13
Gestión de usuarios basada en permisos	13
Acceso HTTPS	13
Printanista Side-By-Side	13
Alojamiento de aplicaciones Printanista Hub	13
Centros de datos seguros de ECI	13
Gestión de versiones.....	14
Proceso de pruebas y lanzamiento.....	14
Seguridad del código fuente	14
Privacidad de datos y legislación.....	15
Reglamento General de Protección de Datos (RGPD)	15
Preguntas frecuentes (FAQ)	16
Información sobre el antiguo DCA in situ	18
Requisitos del PC/servidor para DCA in situ	18

Consideraciones sobre el firewall saliente (puerto 80 o 443)18

Requisitos de red18

La versión heredada de Java Onsite en sistemas Linux y macOS no funciona.18

Requisitos del PC/impresora para utilizar el agente local (instalación opcional)18

Detección de redes y recopilación de medidores y suministros (DCA in situ)19

Tráfico de red19

Asistencia del fabricante20

Preocupaciones relacionadas con los virus20

ECI proporcionará servicios de asistencia exclusivamente para la última versión comercialmente disponible del Software, así como para la versión inmediatamente anterior del mismo. Esta política se aplica a todos los productos de gestión de dispositivos de ECI.

Microsoft®, .NET Framework®, Windows® y Windows Server® son marcas comerciales registradas o marcas comerciales de Microsoft Corporation.

Descripción general

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

Printanista Hub: un sitio web y un sistema backend que alberga todos los datos recibidos de las herramientas de recopilación de datos de Printanista. Se trata de un repositorio que permite ver los datos mediante un navegador, generar informes, configurar flujos de trabajo de alertas y notificaciones, y sincronizar los datos con sus sistemas ERP para la facturación o el cumplimiento de los suministros.

ECI DCA: este nuevo agente de recopilación de datos (DCA) ofrece importantes ventajas con respecto al agente de recopilación de datos in situ (DCA) sin perder ninguna de sus funciones, incluida la compatibilidad nativa con múltiples plataformas, como Windows, macOS, Linux y Raspberry Pi, cada una con sus propios pasos de instalación, documentación de soporte y personal de soporte cualificado para estas plataformas. ECI DCA también ofrece detección y escaneo continuos de dispositivos, una capacidad mejorada de recopilación de MIBWalk y registros, y ahora recopila 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 las instalaciones 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 mediante HTTPS, HTTP o, si el cliente lo prefiere, un archivo cifrado propietario.

El objetivo de este documento es ofrecer una descripción general de la línea de productos Printanista Suite desde una perspectiva técnica para ayudar a responder a las preguntas más frecuentes que reciben los equipos de tecnología de la información.

Cómo funciona Printanista

Printanista Hub está diseñado como una aplicación alojada

Printanista Hub está alojado por ECI Software Solutions en 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 multicapa para proteger esa información clave, supervisando y mejorando constantemente nuestra aplicación, nuestros sistemas y nuestros procesos, con el fin de satisfacer las crecientes demandas y retos de seguridad.

Centros de datos seguros de ECI

Nuestro servicio se encuentra ubicado en espacios dedicados en centros de datos de primer nivel. Estas instalaciones proporcionan soporte a nivel de operador. Este enlace lleva al documento detallado de ECI relacionado con la seguridad de los centros de datos. [Descripción general de la seguridad en la nube de ECI 2021 \(ecisolutions.com\)](https://ecisolutions.com)

Agente de recopilación de datos (DCA)

El motor central del agente de recopilación de datos, que es el corazón de todos los productos Printanista, identifica y extrae correctamente los datos de las impresoras, copiadoras y equipos multifunción conectados en red utilizando los protocolos que admiten los dispositivos.

Printanista es actualmente compatible con los protocolos SNMP v1, v2c y v3 (Protocolo simple de administración de redes). SNMP v3 proporciona una mayor protección de los paquetes para garantizar que la información y las comunicaciones se transmitan a través de fuentes fiables. A diferencia de SNMPv1 o v2, SNMP v3 está cifrado para mayor seguridad y requiere tanto un nombre de usuario como una contraseña. Una ventaja de utilizar SNMP v3 es que los administradores de red pueden determinar el método de cifrado, así como un nombre de usuario y una contraseña seguros.

SNMP es un protocolo de red que facilita el intercambio de información entre dispositivos de red, extrayendo datos de la Base de Información de Gestión (MIB) y otras ubicaciones dentro del dispositivo de impresión. La Base de Información de Gestión (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

Backend de Printanista Hub Aplicación

Todos los datos recopilados se envían al servidor Printanista Hub, donde se ponen a disposición para la generación de informes y alertas. ECI DCA se conecta a su servidor Printanista Hub mediante HTTPS (puerto **443/TCP**). Póngase en contacto con su administrador de ECI Solutions para obtener información sobre los nombres de dominio y las direcciones IP que utiliza su servidor.

Esta conexión está protegida por **el protocolo TLS** (Transport Layer Security), estándar del sector.

Se requiere la versión mínima TLS 1.2.

Esta conexión permanece abierta mientras ECI DCA está en funcionamiento. Normalmente se utiliza una conexión **WebSocket**, pero en algunas situaciones ECI DCA puede recurrir al uso **de eventos enviados por el servidor o al sondeo largo HTTP**.

NOTA IMPORTANTE: Se requieren varias conexiones salientes HTTPS seguras desde el servidor en el que 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>
- <https://install.printanista.net>

Requisitos para la solicitud de Printanista

Agente de recopilación de datos (ECI DCA)

Las impresoras, fotocopadoras y equipos multifunción 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 del conjunto TCP/IP.

Requisitos del PC/servidor para ECI DCA:

Requisitos de Microsoft Windows (x86/64):

- Microsoft .NET Framework 4.7.2. o superior (recomendado: última versión)
- Las versiones de Windows Server (excepto las ediciones Datacenter y Core) y Windows totalmente liberadas y compatibles con Microsoft
 - *Las versiones de Microsoft que ya no son compatibles con Microsoft no son compatibles con ECI DCA.*
- La configuración de la red local y/o del cortafuegos permite [la conexión a los servicios del servidor de actualizaciones de ECI y al servidor Printanista Hub.](#)

Requisitos de Linux (x86/64 o ARM):

- Mono Framework 5.4 o superior (recomendado: última versión)
- La configuración de la red local y/o del cortafuegos permite [la conexión a los servicios del servidor de actualizaciones de ECI y al servidor Printanista Hub.](#)
- Solo Ubuntu LTS 20.04 y superior son oficialmente compatibles.

Requisitos de macOS (x64):

- Mono Framework 5.4 o superior (recomendado: última versión)
- macOS® Sierra (10.12) hasta Sequoia (15.4). Las versiones más recientes no son compatibles.
- La configuración de la red local y/o del cortafuegos permite [la conexión a los servicios del servidor de actualizaciones ECI y al servidor Printanista Hub.](#)

Requisitos de Raspberry Pi:

- Raspberry Pi 3 Modelo B o Pi 4 Rev 1.5. No se admiten versiones más recientes.
- Tarjeta microSD en blanco de 8 GB o más.
- PC capaz de escribir en tarjetas microSD
- La configuración de la red local y/o del cortafuegos permite [la conexión a los servicios del servidor de actualizaciones de ECI y al servidor Printanista Hub.](#)

Consideraciones sobre el cortafuegos para ECI DCA:

Conexiones entrantes: no hay conexiones entrantes desde Internet a ECI DCA.

Conexiones salientes

Servicio	Puerto	Conexión a
Carga de datos	443/TCP (HTTPS)	Su servidor Printanista Hub
Actualizaciones de software	443/TCP (HTTPS)	Servidor de actualizaciones ECI
Registro (reserva)	53/UDP (DNS)	Servidor DNS de red local (primario) Servidor de actualizaciones ECI (reserva)

Servidor de actualizaciones ECI

El servidor de actualizaciones ECI es un servicio gestionado 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 el funcionamiento de ECI DCA. Nota: ECI DCA no envía ningún dato recopilado sobre dispositivos o configuraciones al servidor de actualizaciones ECI.

Actualizaciones de software

ECI DCA se actualiza automáticamente descargando las 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 a `*.reg.pf-d.ca` para registrarse. Primero intentará hacerlo utilizando los servidores DNS de la red local y, a continuación, recurrirá a comunicarse directamente con las direcciones IP del servidor de actualizaciones de ECI (utilizando el puerto **53/udp**). El cortafuegos 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 que tiene la menor latencia de red y en función de la disponibilidad del servicio. En determinadas ubicaciones, la región utilizada puede cambiar con el tiempo, ya que la actividad en la infraestructura global de Internet puede afectar a la latencia.

Datos recopilados y cifrado de E

Cifrado de datos

Todos los paquetes de datos de ECI DCA y Onsite DCA 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, todos los ajustes y trabajos confidenciales entre ECI DCA y Printanista se cifran utilizando el algoritmo de cifrado simétrico estándar AES256, con una clave compartida protegida. Esto garantiza el cifrado de extremo a extremo, de modo que los datos están protegidos contra su lectura si son interceptados por un tercero, un competidor o una instancia de Printanista no autorizada.

La seguridad es importante para e

ECI DCA y el antiguo Onsite DCA se comunican con Printanista Hub a través del protocolo HTTPS, utilizando el estándar industrial **TLS 1.2** (Transport Layer Security). Ninguna aplicación de Printanista recopila, visualiza ni guarda datos confidenciales. Solo se recopilan y visualizan datos relacionados con la impresora. ECI DCA o el antiguo Onsite DCA no pueden identificar ni recopilar ningún otro dato de red, excepto la dirección IP, la dirección MAC y el nombre de host.

ECI DCA y el antiguo Onsite DCA no recopilan ni procesan ningún dato personal. La única forma en que el sistema recopilará este tipo de información es si usted o sus clientes introducen los datos en Printanista en un campo o etiqueta, como la ubicación o el nombre del cliente. ECI DCA y el antiguo Onsite DCA le permiten supervisar los dispositivos de red mediante el Protocolo simple de administración de redes (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 se pone a disposición 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 son de naturaleza técnica u operativa y específicos del propio dispositivo. En el nivel más básico, los datos expuestos por una MIB de impresora se documentan en el IETF RFC 3805 (<https://tools.ietf.org/html/rfc3805>). El fabricante puede exponer información adicional sobre el dispositivo a través de extensiones y MIB (base de información de gestión) privadas, pero la información es fundamentalmente técnica y específica del dispositivo.

Printanista Hub solo almacena:

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

Se recopila y muestra otra información de red/entorno mientras se está conectado con fines de resolución de problemas, pero nunca se almacena en Printanista.

Tipos de información recopilada por

ECI DCA y el antiguo Onsite DCA intentan recopilar la siguiente información de los dispositivos de impresión en red durante un escaneo de red:

Atributos del dispositivo	Suministros
• Dirección IP (puede estar enmascarada) • Fabricante • Número de serie • Número de activo • Dirección MAC • Descripción del dispositivo • Ubicación • Varios (específicos de la máquina)	• Número de serie del cartucho de tóner • Nivel de suministro del cartucho de tóner • Niveles del tambor • Niveles del kit de mantenimiento • Niveles de suministro de productos distintos al tóner • Niveles varios • Detalles de suministro de impresoras basadas en etiquetas
Servicio	Cobertura y medidores
• Lectura de la pantalla LCD • Estado del dispositivo • Códigos de error • Firmware	• Lecturas del medidor • Tipo de medidor • Nivel de cobertura • Identificación monocroma o en color

Detección de redes y recopilación de datos

Para aumentar la eficiencia del DCA, solo cuando haya datos nuevos o modificados de los dispositivos se enviará esta información al servidor Printanista Hub. Esto garantizará una carga mínima de la red y eliminará la frecuencia de los retrasos en el envío de datos de los dispositivos. Además, la detección y el escaneo de dispositivos ahora son independientes para garantizar que solo se envíe la dirección IP.

(o nombre de host) de los dispositivos detectados anteriormente se analizan periódicamente, en lugar de realizar un análisis completo de la red (que se completa inicialmente, periódicamente o cuando lo determina un usuario administrador).

Esto garantizará que la velocidad de envío de datos de los dispositivos sea lo más actualizada posible. De este modo, los usuarios pueden recibir notificaciones sobre dispositivos problemáticos en cuestión de minutos o incluso segundos en muchas situaciones. ECI DCA separa la detección de dispositivos de otros tipos de análisis, lo que le permite establecer intervalos de análisis personalizados para recuperar medidores, atributos de suministros y errores. Los valores predeterminados, mínimos y máximos para los intervalos de análisis son:

Función de escaneo	Predeterminado	Mínimo	Máximo
Detección	60 minutos	10 minutos	7 días
Medidores	24 horas	30 minutos	14 días
Suministros	4 horas	30 minutos	7 días
Errores	60 minutos	30 minutos	7 días
Atributos	24 horas	1 hora	14 días

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

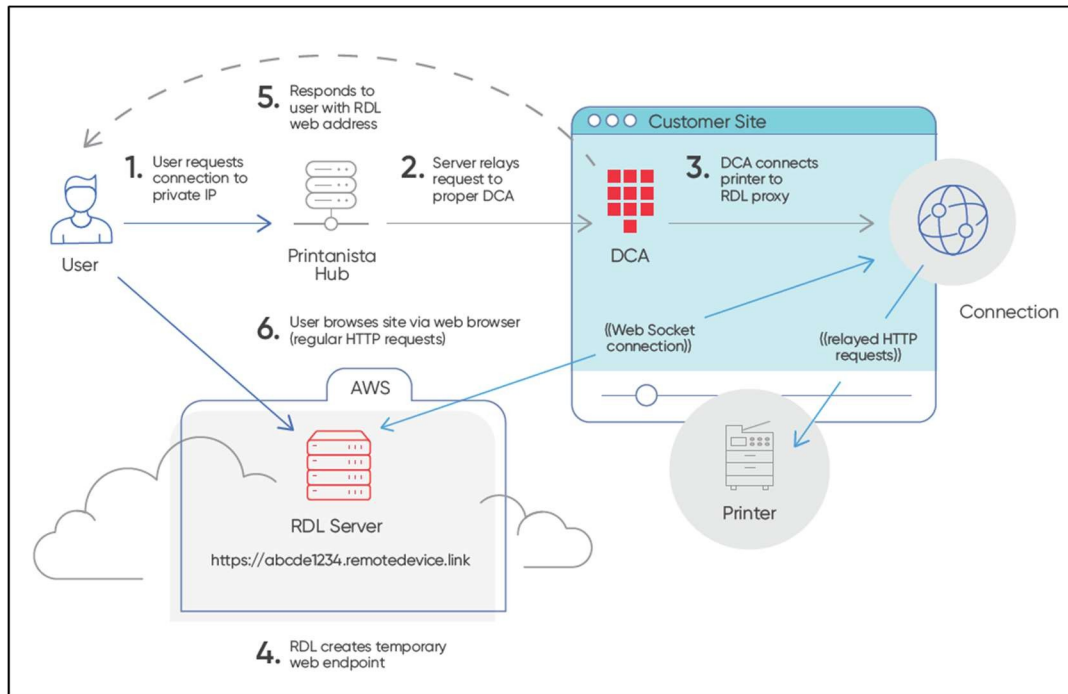
Los administradores de Printanista Hub pueden gestionar de forma remota los ECI DCA que se han activado en el servidor. Pueden activar de forma remota el ECI DCA para ejecutar comandos predefinidos, como tareas de recopilación de datos, proporcionar registros ECI DCA, ejecutar MIB Walks remotos o actualizar la configuración ECI DCA.

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

Nota: La comunicación solo se produce cuando se actualiza o cambia la información del contador, el suministro o los errores, lo que reduce el uso del ancho de banda.

Nota: HP JAMC solo funciona con el DCA local heredado en la actualidad.

Enlace de dispositivos remotos (, RDL)



Descripción general del sistema: enlace de dispositivo remoto (, RDL)

Remote Device Link (RDL) es un servicio que permite a un **usuario final** remoto acceder a un punto final HTTP en una LAN privada. Consta de cuatro componentes principales:

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

Seguridad: puertos y SSL (capa de conexión segura)

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

Habilitación y permisos de

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 función

Funciones de auditoría de

1. Auditoría local de Printanista Hub de los detalles de cada sesión
 - a. Informes de administración de Printanista Hub para la auditoría de Remote Device Link (RDL)
2. Remote Device Link (RDL) Registro en la nube de AWS (Amazon Web Services) de todos los detalles de la sesión

Seguridad de Remote Device Link (RDL)

La seguridad de Remote Device Link (RDL) fue una preocupación clave durante el desarrollo

de esta herramienta. Autorización:

- El usuario debe tener permiso desde Printanista Hub para acceder a la función Remote Device Link (RDL) en la cuenta específica.
- El agente de recopilación de datos (DCA) solo aceptará solicitudes de enlace de dispositivo remoto (RDL) del servidor Printanista Hub que estén autenticadas mutuamente.
- El agente de recopilación de datos (DCA) solo establece conexiones de enlace remoto con dispositivos (RDL) a dispositivos de impresión conocidos y supervisados actualmente dentro del rango o rangos de direcciones IP de descubrimiento de los agentes de recopilación de datos (DCA).
- Cada solicitud web individual debe dirigirse a la misma IP: el agente de recopilación de datos (DCA) no seguirá las redirecciones.

Seguridad de la conexión:

- Todas las conexiones hacia y desde los servidores Remote Device Link (RDL) y Printanista Hub se cifran utilizando la versión mínima estándar TLS 1.2 (Transport Layer Security).
- A cada conexión se le asigna un nombre de dominio único que utiliza una combinación aleatoria de 19 caracteres (96 bits) alfanuméricos.
- Cada solicitud requiere un token de seguridad de 160 bits, almacenado como una cookie del navegador, y solo se establece al inicio de la sesión protegida por el cifrado 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 la versión mínima TLS 1.2 si el dispositivo lo hace.

Límites de tiempo de sesión:

- Cada sesión individual de Remote Device Link (RDL) caduca tras 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 específicas de la instalación de DCA, y la conexión requiere un certificado SSL válido y de confianza para poder utilizarse a través de una conexión TLS.

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

Aplicación Printanista Hub

Se puede acceder a la funcionalidad de Printanista Hub a través de una interfaz de usuario

basada en web. Gestión de usuarios basada en permisos

El acceso a la interfaz web de Printanista Hub se controla mediante una gestión de usuarios basada en permisos. Los usuarios deben iniciar sesión en Printanista con un nombre de usuario y una contraseña designados. A los usuarios se les asignan una o varias funciones que especifican los permisos y se les concede acceso a uno o varios grupos de dispositivos. Los administradores con permisos completos pueden especificar exactamente qué pantallas puede ver y/o con cuáles puede interactuar cada usuario.

Acceso HTTPS

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

Printanista Side-By-Side

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

Alojamiento de la aplicación Printanista Hub

Printanista Hub está alojado por ECI Software Solutions en 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 multicapa para proteger esa información clave, supervisando y mejorando constantemente nuestras aplicaciones, sistemas y procesos, con el fin de satisfacer las crecientes demandas y retos de seguridad.

Centros de datos seguros de ECI

Nuestro servicio se encuentra ubicado 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

[Descripción general de la seguridad en la nube de ECI 2021 \(ecisolutions.com\)](https://ecisolutions.com/Descrición-general-de-la-seguridad-en-la-nube-de-ECI-2021)

Proceso de pruebas y lanzamiento de la gestión de versiones

Cada lanzamiento mayor y menor del software pasa por un proceso de control de calidad, en el que varios miembros del personal de Printanista realizan pruebas de regresión en las partes modificadas del sistema para garantizar que no se ha producido una disminución de la seguridad o la funcionalidad del sistema, así como para validar los nuevos aspectos funcionales. Los lanzamientos importantes pasan por un proceso de lanzamiento beta en el que clientes seleccionados ejecutan los sistemas nuevo y antiguo en paralelo.

Seguridad del código fuente

El código fuente de Printanista se almacena en un sistema de control de revisiones seguro, al que solo pueden acceder personas autorizadas. Cada cambio en el código fuente requiere la aprobación de dos desarrolladores autorizados antes de ser aceptado en el repositorio de código de producción, donde se realiza un seguimiento de cada cambio, incluyendo qué desarrollador lo ha realizado y por qué. Los productos se cifran y se firman digitalmente con un certificado de firma de código de confianza antes de su envío. Se puede disponer de un depósito en garantía previa solicitud.

ECI contrata a una empresa independiente líder en el sector, certificada por CREST, SOC 2, NSA-CIRA y CSA-STAR, para que realice pruebas de penetración a nivel de aplicación y corrija los resultados en función de sus requisitos empresariales y su marco interno de gestión de riesgos. Las pruebas de penetración se realizan al menos una vez al año o cuando se producen cambios importantes en el sistema. La política de ECI es realizar todos los esfuerzos comercialmente razonables para corregir todos los hallazgos críticos en un plazo de 30 días o en un plazo razonable con un caso de negocio proporcionado. ECI no divulga detalles sobre nuestros controles de seguridad ni los resultados de las pruebas de penetración, ya que esa información es privada y confidencial y, en manos equivocadas, puede aumentar el riesgo.

Legislación sobre privacidad de datos y el Reglamento General de Protección de Datos ()

Reglamento General de Protección de Datos (RGPD)

En mayo de 2018 entró en vigor el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. El RGPD sustituye a la Directiva 95/46/CE sobre protección de datos y tiene por objeto reforzar y unificar las leyes de protección de datos en toda Europa.

ECI ha implementado un programa estructurado y completo de cumplimiento del RGPD. El programa consiste, entre otras cosas, en la formación del personal, la auditoría y la evaluación de riesgos en toda la empresa, las políticas y procedimientos, la gobernanza y los esfuerzos continuos de cumplimiento. Animamos a nuestros clientes a que tomen medidas similares para garantizar que sus propias empresas cumplan con el RGPD y en los años venideros.

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

Las aplicaciones de software de Printanista no recopilan, almacenan ni transmiten ninguna información relativa al contenido de los trabajos de impresión.

Printanista no tiene forma de acceder, almacenar ni transmitir información de alto riesgo, incluso si dicha información se imprime o se envía de otro modo a dispositivos de impresión supervisados por las aplicaciones de software de Printanista.

Las aplicaciones de software de Printanista no almacenan, procesan ni transmiten datos de titulares de tarjetas ni información personal.

Las comunicaciones del motor del producto se controlan mediante un acceso limitado a direcciones IP específicas y/o rangos de direcciones IP.

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

Las comunicaciones fuera de la red utilizan un flujo de datos comprimido y patentado que se envía mediante el protocolo SSL estándar de la industria a través de HTTPS.

Para obtener información relacionada con el cumplimiento de leyes y/o normativas específicas, póngase en contacto con su gestor de cuentas de ECI.

El siguiente es un enlace a ECI Cloud Security:

[Descripción general de ECI Cloud Security 2021 \(ecisolutions.com\)](https://ecisolutions.com/Descrpcion-general-de-ECI-Cloud-Security-2021)

Preguntas frecuentes (FAQ)

¿Los productos Printanista funcionan con proxies de Internet?

Sí, ECI DCA puede funcionar con la mayoría de los proxies. Es necesario configurar los ajustes del proxy en el sistema en el que está instalado y funciona ECI DCA.

¿Cuáles son los requisitos mínimos de Printanista Hub, ECI DCA y Onsite?

Consulte la sección [Requisitos de la aplicación Printanista](#) de este documento.

¿Los productos Printanista son compatibles con entornos Mac, Linux o Raspberry Pi?

Este ECI DCA ofrece importantes ventajas con respecto al DCA in situ sin perder ninguna de sus funciones, incluida la compatibilidad multiplataforma nativa completa con Windows, macOS, Linux y Raspberry Pi. Cada uno de ellos cuenta con pasos de instalación únicos, documentación de soporte y personal de soporte cualificado en estas plataformas. El proceso de instalación también ha mejorado considerablemente y es mucho más intuitivo para todo tipo de usuarios.

¿ECI DCA requiere Microsoft Internet Information Services (IIS)?

No. ECI DCA y Onsite DCA incluyen su propio servidor para alojar la interfaz de usuario (UI) basada en web y se configuran automáticamente durante la instalación.

¿Se puede instalar ECI DCA en un ordenador que ya aloja otro sitio web IIS?

Sí. Sin embargo, los puertos que se enumeran a continuación deben incluirse en la lista blanca para garantizar la conectividad de ECI DCA.

Servicio	Puerto	Conexión a
Carga de datos	443/TCP (HTTPS)	Su servidor Printanista Hub
Actualizaciones de software	443/TCP (HTTPS)	Servidor de actualizaciones ECI
Registro (reserva)	53/UDP (DNS)	Servidor DNS de red local (primario) Servidor de actualizaciones ECI (reserva)

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

¿Cuánto mantenimiento continuo requiere ECI DCA?

ECI DCA y Onsite DCA es un servicio que se ejecuta en segundo plano y realiza auditorías y exportaciones a destinos configurados según calendarios predefinidos. Se recomienda utilizar subredes (rangos de IP) en lugar de IP fijas. Cuando se añaden nuevos dispositivos a la red, estos se detectan y se incluyen en los resultados de la auditoría, lo que limita la intervención manual.

¿Con qué marcas de equipos funciona la supervisión de Remote Device Link (RDL)?

¿Cuáles son los requisitos para que funcione?

ECI DCA detecta todas las marcas con una página web integrada. La información de las páginas web integradas variará según el fabricante y el modelo. Los dispositivos locales no mostrarán la página web integrada.

¿Existen problemas de seguridad adicionales con Remote Device Link (RDL)?

Se abre un canal seguro entre el dispositivo de la red local del cliente y un operador situado fuera de dicha red. RDL solo informará de los dispositivos detectados y supervisados activamente a través de ECI DCA. Aparece un mensaje indicando que la conexión del dispositivo no es compatible con DCA.

Remote Device Link (RDL) parece un poco lento, ¿por qué?

Esto es de esperar, ya que la conexión debe pasar por nuestros servicios en la nube. Sin embargo, el principal factor que influye es la rapidez con la que los dispositivos responden a las solicitudes de la interfaz de usuario web (UI).

Hemos observado que los dispositivos responden en décimas de segundo a los primeros intentos de conexión, dependiendo del uso actual o de los recursos disponibles para la interfaz de usuario (UI).

¿Qué funciones están disponibles con Remote Device Link (RDL)?

Todas las opciones a las que el fabricante de equipos originales (OEM) proporciona acceso a través de la página web integrada son accesibles a través de Remote Device Link (RDL).

¿Se puede desactivar la función Remote Device Link (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 sobre Printanista Hub, ECI DCA, el antiguo Onsite DCA, etc.? Puede encontrar información adicional en el sitio web de Printanista de ECI:

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

Información sobre el antiguo Onsite DCA

Se recomienda utilizar ECI DCA con Printanista. Sin embargo, el antiguo Onsite DCA funciona actualmente con Printanista. Requisitos del PC/servidor para Onsite DCA:

- 1 GB de RAM
- 400 MB de espacio en disco
- Microsoft .NET Framework 4.7.2 o superior
- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- La versión 4.1.3 y posteriores in situ son compatibles con Windows Server 2022.
- Internet Explorer 11.0 o posterior, Chrome, Firefox
- MDAC 2.8 o superior (normalmente incluido al instalar Windows)
- JET 4.0 o superior (normalmente incluido al instalar Windows)
- Cargado en un equipo que esté encendido las 24 horas del día, los 7 días de la semana, o al menos durante toda la jornada laboral
- Debe iniciar 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](https://(company_Printanista_FQDN)/WebServices/Onsite2Service.asmx)
- Aplicación: fmaonsite.exe
- Se debe permitir el paso de SOAP sobre HTTP(s) a través del firewall.

Requisitos de red:

El tráfico SNMP (puerto 161) debe poder enrutarse a través de la LAN o WAN (redes de área amplia).

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

Requisitos del 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 4.7.2 o posterior
- Controlador actual para la impresora local (se recomienda UPD para dispositivos HP)
- La impresora debe ser compatible con el lenguaje de trabajo de impresora (PJM) o el lenguaje de gestión de impresora (PML).
- Elimine cualquier controlador de impresión que no utilice.
- La compatibilidad bidireccional del controlador está habilitada.
- Modificaciones del Firewall de Windows: puerto 161/33333 entrante/saliente tanto para TCP como para UDP.

Versiones de Windows y Windows Server compatibles con Microsoft. Las versiones que ya no son compatibles con Microsoft tampoco lo son con ECI.

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

Detección de redes y recopilación de datos de medidores y suministros (DCA in situ)

La configuración patentada de detección automática de redes de Printanista utiliza una combinación de algoritmos para identificar los rangos de red en los que pueden encontrarse los dispositivos de impresión y, a continuación, detectar 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 gestionar de forma remota los DCA (agentes de recopilación de datos) activados en el servidor, así como activar de forma remota el Onsite para ejecutar comandos predefinidos, como tareas de recopilación de datos, proporcionar registros de Onsite, ejecutar MIBWalks remotos, instalar HP JAMC o actualizar la configuración de Onsite. A continuación se explica con más detalle:

Función	Ubicación	Descripción
Tareas	Configuración de Onsite	Puede configurar de forma remota tareas para que se ejecuten según un programa preestablecido, pero puede seleccionar tareas (caché, medidores, suministros, servicio) para que se ejecuten inmediatamente y recopilar datos del dispositivo cuando lo desee.
Recorridos MIB	Configuración in situ	Puede indicar determinados IPv4/IPv6/nombres de host de dispositivos y activar el Onsite para que inicie la recopilación de los recorridos MIB inmediatamente.
Registros (detallados)	Configuración in situ	Puede indicar a Onsite que recopile los registros (críticos, de error, de advertencia, detallados y de depuración) a partir de una fecha determinada.

Ninguno de estos comandos da lugar a la recopilación de datos más allá de los tipos de información recopilados tal y como se ha descrito anteriormente. Los datos intercambiados entre Onsite DCA y Printanista Hub se cifran mediante protocolos de cifrado robustos que cumplen con la norma FIPS. Onsite recibe actualizaciones de software seguras desde los servidores de actualizaciones de Printanista.

El antiguo Onsite DCA se comunica con Printanista a intervalos predefinidos para determinar si hay alguna acción en cola que aún no se haya ejecutado. Esto garantiza que las acciones se ejecuten de manera oportuna.

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

Nota: HP JAMC solo es compatible cuando se utiliza junto con el DCA local heredado en el lanzamiento inicial de Printanista.

Tráfico de red

Las auditorías realizadas por el software utilizan un sistema inteligente para extraer la información mínima necesaria de cada impresora, copiadora o impresora multifunción. A diferencia de otros productos similares que envían un conjunto fijo de consultas (un superconjunto de todas las consultas posibles) a todos los dispositivos conectados a la red, Onsite DCA solo envía las consultas relevantes según los campos que admite el dispositivo de destino, y cada consulta de dispositivo no supera unos pocos kilobytes de datos. Para reducir aún más la cantidad de ancho de banda de red utilizado, Onsite DCA 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 ninguna respuesta dentro del período de tiempo de espera configurado, se pasará a la siguiente dirección IP. Como regla general, Printanista recopilará información sobre aproximadamente 65 000 dispositivos en menos de una hora.

Asistencia del fabricante

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

Preocupaciones relacionadas con los virus

Los archivos de la aplicación Printanista han sido firmados digitalmente para impedir su ejecución si se ve comprometida la integridad del archivo. Esto garantiza que, si hay algún virus presente, no se active y se impida su propagación de una red a otra. Para mayor seguridad, recomendamos utilizar un software antivirus en su red.

ECI proporcionará servicios de asistencia exclusivamente para la última versión comercialmente disponible del Software, así como para la versión inmediatamente anterior del mismo. Esta política se aplica a todos los productos de gestión de dispositivos de ECI.

Microsoft®, .NET Framework®, Windows® y Windows Server® son marcas comerciales registradas o marcas comerciales de Microsoft Corporation.