Documento técnico de Printanista Hub

Versión 1.10

Índice

ECI prestará 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.

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 concebida y diseñada 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 comunican ningún otro detalle, salvo la información sobre el equipo que se está supervisando (es decir, el tipo de equipo). Nunca se transmite información confidencial fuera de la red a través de los productos Printanista. La suite 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 visualizar datos mediante un navegador, generar informes, configurar flujos de trabajo de alertas y notificaciones, y sincronizar 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, incluyendo compatibilidad nativa multiplataforma completa con Windows, macOS, Linux y Raspberry Pi, cada una con sus propios pasos de instalación, documentación de apoyo y personal de asistencia técnico especializado en estas plataformas. ECI DCA también ofrece detección y análisis continuos de dispositivos, una capacidad mejorada de MIBWalk y recopilación de registros, y ahora recopila muchos más tipos de medidores.

DCA in situ: Una herramienta de agente de recopilación de datos heredada que realiza automáticamente evaluaciones de impresión y supervisa los niveles de consumibles, el estado de las impresoras y los registros de errores. Esta aplicación se instala en las instalaciones del cliente y puede realizar evaluaciones de impresión de forma automática y 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 propio.

El objetivo de este documento es ofrecer una visión general de la gama de productos Printanista Suite desde una perspectiva técnica para ayudar a dar respuesta a las preguntas más frecuentes que recibirán los equipos de tecnologías de la información.

Cómo funciona Printanista

Printanista Hub, 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 de múltiples capas 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 aloja en espacios dedicados en centros de datos de primer nivel. Estas instalaciones ofrecen soporte de nivel de operador. Este enlace lleva al documento detallado de ECI sobre la seguridad de los centros de datos.
Descripción general de la seguridad en la nube de ECI

Agente de recopilación de datos (DCA)

El motor central del agente de recopilación de datos, que constituye el núcleo de todos los productos de Printanista, identifica y extrae correctamente los datos de impresoras, fotocopiadoras y equipos multifunción conectados en red utilizando los protocolos compatibles con dichos dispositivos.

Actualmente, Printanista es compatible con los protocolos SNMP (Protocolo simple de gestión de redes) v1, v2c y v3. SNMP v3 ofrece una mayor protección de los paquetes para garantizar que la información y la comunicación se transmitan a través de fuentes fiables. A diferencia de SNMP v1 o v2, SNMP v3 está encriptado 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 encriptación, así como establecer 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 estructura. 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 de backend de Printanista Hub

Todos los datos recopilados se envían al servidor Printanista Hub, donde quedan disponibles 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 como mínimo la versión TLS 1.2.

Esta conexión permanece abierta mientras ECI DCA esté en ejecución. 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 prolongado 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 del sistema Printanista Hub

Utilice el siguiente enlace para consultar las especificaciones completas y actualizadas del sistema del

producto Printanista: Requisitos del sistema Printanista Hub v4.0

Requisitos de la aplicación Printanista

Agente de recopilación de datos (ECI DCA)

Las impresoras, fotocopiadoras y equipos multifunción deben tener habilitado el protocolo SNMP (puerto 161) para la detección y extracción de información. El protocolo SNMP forma parte estándar de la capa de aplicación del conjunto TCP/IP.

Requisitos de PC/servidor para ECI DCA:

Requisitos de Microsoft Windows (x86/64):

- Microsoft .NET Framework 4.7.2. o posterior (recomendado: última versión)
- Versiones de Windows Server (excepto las ediciones Datacenter y Core) y Windows
  - *Las versiones de Microsoft que ya no cuentan con soporte técnico de Microsoft tampoco 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
  .

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 se admiten oficialmente las versiones de Ubuntu LTS 20.04 y posteriores.

Requisitos para macOS (x64):

- Mono Framework 5.4 o superior (recomendado: última versión)
- macOS® Sierra (10.12) hasta Sequoia (15.4). No se admiten versiones más recientes.
- 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 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)	Tu servidor Printanista Hub
Actualizaciones de software	**443/TCP** (HTTPS)	Servidor de actualizaciones de ECI
Registro (alternativa)	**53/UDP** (DNS)	Servidor DNS de la red local (principal) Servidor de actualizaciones de ECI (de reserva)

Servidor de actualizaciones de ECI

El servidor ECI Updates Server 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 al servidor ECI Updates Server ningún dato recopilado sobre los dispositivos o la configuración.

Actualizaciones de software

ECI DCA se actualiza automáticamente descargando las actualizaciones publicadas en https://updates.printanista.net/. Las conexiones se realizan siempre a través del 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 tiene que permitir esta conexión con el servidor de actualizaciones de ECI si los servidores DNS locales no resuelven las solicitudes de registro.

Región de servicio

ECI DCA se redirige a la región en la que presenta la menor latencia de red, teniendo en cuenta 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

Cifrado de datos

Todos los paquetes de datos de ECI DCA y del DCA local heredado se codifican y se ofuscan. 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, una instancia de Printanista de la competencia o cualquier otra instancia no autorizada.

Cuestiones de seguridad

ECI DCA y el DCA local heredado 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 DCA local heredado 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 Onsite DCA (versión anterior) no recopilan ni tratan 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 dispositivos de red mediante el Protocolo simple de gestión 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 gestión (MIB) SNMP. Los datos que expone 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 que expone la MIB de una impresora se documentan en el RFC 3805 del IETF (https://tools.ietf.org/html/rfc3805). El fabricante puede exponer información adicional del 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

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

Atributos del dispositivo

- Dirección IP (puede ocultarse)
- Fabricante
- Número de serie
- Número de activo
- Dirección MAC
- Descripción del dispositivo
- Ubicación
- Varios (específico de la máquina)

Servicio

- Lectura de la pantalla LCD
- Estado del dispositivo
- Códigos de error
- Firmware

Consumibles

- Número de serie del cartucho de tóner
- Nivel de suministro del cartucho de tóner
- Niveles del tambor
- Niveles del kit de mantenimiento
- Niveles de consumibles distintos del tóner
- Niveles varios
- Detalles de los consumibles de las impresoras de etiquetas

Cobertura y contadores

- Lecturas de contadores
- Tipo de contador
- Nivel de cobertura
- Identificación en blanco y negro o en color

Detección de dispositivos 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 en 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 escanee la dirección IP
(o el nombre de host) de los dispositivos detectados anteriormente se escaneen de forma periódica, en lugar de realizar un escaneo completo de la red (esto se lleva a cabo inicialmente, de forma periódica o cuando lo determine un usuario administrador).

Esto garantizará que la velocidad de envío de datos de los dispositivos sea lo más actualizada posible. Esto permite que los usuarios sean 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 contadores, atributos de consumibles y errores. Los valores predeterminados, mínimos y máximos para los intervalos de escaneo son:

Función de escaneo	Predeterminado	Mínimo	Máximo
Detección	60 minutos	10 minutos	7 días
Metros	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 escaneo (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 un escaneo completo del dispositivo en cuestión utilizando un intervalo predefinido.

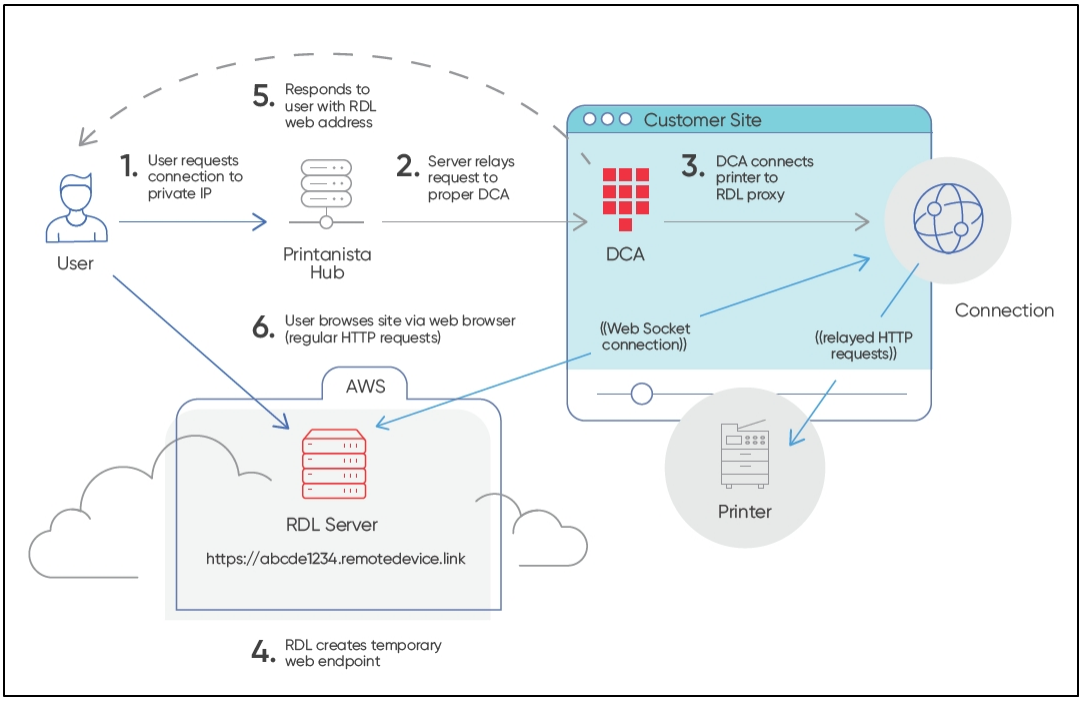
Los administradores de Printanista Hub pueden gestionar de forma remota los ECI DCA que se hayan activado en el servidor. Pueden activar de forma remota el ECI DCA para ejecutar comandos predefinidos, como tareas de recopilación de datos, proporcionar registros del ECI DCA, ejecutar MIB Walks remotos o actualizar la configuración del 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 ha actualizado o modificado la información sobre el contador, los consumibles o los errores, lo que reduce el uso del ancho de banda.

Nota: HP JAMC solo funciona con el DCA Onsite heredado en este momento.

Enlace de dispositivo remoto (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** de **Remote Device Link**, en la 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 (que se ejecuta en la LAN privada)

Seguridad: puertos y SSL (Secure Sockets Layer)

La ruta de acceso público para RDL es siempre una URL https:// en el puerto 443, independientemente del puerto del punto final y/o del estado del 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 función

Capacidades de auditoría

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

Remote Device Link (RDL): seguridad

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 Remote Device Link (RDL) procedentes del servidor de Printanista Hub que haya sido autenticado mutuamente
- El agente de recopilación de datos (DCA) solo establece una conexión RDL (Remote Device Link) con los dispositivos de impresión conocidos y que se están supervisando actualmente dentro de los rangos de direcciones IP de detección del agente 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 de 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 que solo se establece al inicio de la sesión protegida mediante 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 como mínimo la versión TLS 1.2 si el dispositivo también 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 requiere un certificado SSL válido y de confianza para funcionar a través de una conexión TLS.

Todo el tráfico que transita desde el DCA hacia Internet está cifrado. Sin embargo, el ECI DCA puede comunicarse con el dispositivo de la red local a través de conexiones HTTP sin cifrar 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 utilizando un nombre de usuario y una contraseña específicos. A los usuarios se les asignan uno o varios roles que especifican sus 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 contiene diversos atributos de los modelos, tales como: velocidades de impresión, fecha de lanzamiento al mercado o compatibilidades de números de pieza de los fabricantes de equipos originales (OEM), y que se actualiza periódicamente a medida que los fabricantes 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 ubicados en diferentes regiones del mundo. ECI Software Solutions es consciente de que la confidencialidad, la integridad y la disponibilidad de la información de nuestros clientes son fundamentales para sus operaciones comerciales y para nuestro propio éxito. Utilizamos un enfoque de múltiples capas para proteger esa información clave, supervisando y mejorando constantemente nuestra aplicación, nuestros sistemas y nuestros procesos, con el fin de satisfacer las crecientes exigencias y retos en materia de seguridad.

Centros de datos seguros de ECI

Nuestro servicio se aloja en espacios dedicados en centros de datos de primer nivel. Estas instalaciones ofrecen soporte de nivel

de operador. Haga clic en el siguiente enlace para obtener el documento detallado de ECI sobre la seguridad de los centros de

datos

Descripción general de la seguridad en la nube de ECI

Gestión de versiones: proceso de pruebas y lanzamiento de

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 en la seguridad o la funcionalidad del sistema, así como para validar los nuevos aspectos funcionales. Los lanzamientos mayores pasan por un proceso de lanzamiento beta en el que clientes seleccionados ejecutan los sistemas nuevos y antiguos en paralelo.

Seguridad del código fuente

El código fuente de Printanista se almacena en un sistema de control de versiones seguro, al que solo pueden acceder personas autorizadas. Cada modificación del código fuente requiere la aprobación de dos desarrolladores autorizados antes de ser aceptada en el repositorio de código de producción, donde se realiza un seguimiento de cada cambio, incluyendo quién lo realizó 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 entidad independiente líder en el sector, certificada por CREST, SOC 2, NSA-CIRA y CSA-STAR, para llevar a cabo pruebas de penetración a nivel de aplicación y subsanar los hallazgos 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 introducen cambios importantes en el sistema. La política de ECI es realizar todos los esfuerzos comercialmente razonables para subsanar todos los hallazgos críticos en un plazo de 30 días o en un plazo razonable, siempre que se presente un caso de negocio. ECI no divulga detalles sobre nuestros controles de seguridad ni los resultados de las pruebas de penetración, ya que dicha información es privada y confidencial y, en manos equivocadas, puede suponer un mayor riesgo.

Privacidad de datos y legislación

Reglamento General de Protección de Datos (RGPD)

En mayo de 2018 entró plenamente 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 la legislación en materia de protección de datos en toda Europa.

ECI ha implementado un programa de cumplimiento del RGPD estructurado y exhaustivo. 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 las iniciativas de cumplimiento continuas. Animamos a nuestros clientes a que adopten medidas similares para garantizar que sus propias empresas cumplan con el RGPD ahora y en los años venideros.

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

Las aplicaciones de software de Printanista no recopilan, almacenan ni transmiten información alguna 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 cualquier otra forma 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 están controladas, mediante un acceso restringido a direcciones IP y/o rangos específicos.

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

La comunicación fuera de la red utiliza un flujo de datos comprimido y patentado que se envía mediante el protocolo SSL estándar del sector 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.

A continuación se incluye un enlace a la seguridad en la nube de ECI: Descripción general de ECI Cloud Security

Preguntas frecuentes (FAQ)

¿Funcionan los productos de Printanista con proxies de Internet?
Sí, ECI DCA es compatible con la mayoría de los proxies. Es necesario configurar los ajustes del proxy en el sistema donde 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.

¿Son los productos Printanista compatibles con entornos Mac, Linux o Raspberry Pi?
Este ECI DCA ofrece importantes ventajas con respecto al DCA local sin perder ninguna funcionalidad, incluida la compatibilidad nativa multiplataforma completa con Windows, macOS, Linux y Raspberry Pi. Cada una de ellas cuenta con pasos de instalación específicos, documentación de soporte y personal de asistencia cualificado para estas plataformas. El proceso de instalación también ha mejorado considerablemente y resulta mucho más intuitivo para todo tipo de usuarios.

¿Requiere ECI DCA 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 indican a continuación deben incluirse en la lista de permitidos para garantizar la conectividad de ECI DCA.

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

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

¿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 direcciones IP fijas. Al añadir nuevos dispositivos a la red, estos serán detectados e incluidos 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 que cuentan 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, ¿a qué se debe?
Esto es de esperar, ya que la conexión debe tunelizarse a través de 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, aunque esto puede verse influido por el uso actual o 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) da acceso a través de la página web integrada son accesibles mediante 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 más información sobre Printanista Hub, ECI DCA, Onsite DCA heredado, etc.?
Puede encontrar más información en el sitio web de Printanista de ECI:
https://www.ecisolutions.com/products/printanista-hub/

Información sobre el Onsite DCA heredado

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

- 1 GB de RAM
- 400 MB de espacio en disco
- Microsoft .NET Framework 4.7.2 o posterior
- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- La versión 4.1.3 y posteriores de la versión local 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)
- Instalado 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 cortafuegos de salida (puerto 80 o 443):

Transmisión de datos:

- https://(company_Printanista_FQDN)/WebServices/Onsite2Service.asmx
- Aplicación: fmaonsite.exe
- Se debe permitir el paso de SOAP sobre HTTP(s) a través del cortafuegos

Requisitos de red:

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

Utilice ECI DCA si necesita sistemas operativos macOS, Linux o Raspberry Pi La versión heredada de Java Onsite 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 4.7.2 o una versión posterior
- Controlador actualizado para la impresora local (se recomienda la actualización para dispositivos HP)
- La impresora debe ser compatible con Printer Job Language (PJL) o Printer Management Language (PML)
- Elimine cualquier controlador de impresión que no utilice
- La compatibilidad bidireccional del controlador está habilitada
- Modificaciones del Firewall de Windows: puertos 161/33333 de entrada/salida 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: En el caso de 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 (OEM) Kyocera y Ricoh, así como sus variantes.

Detección de red y recopilación de datos de contadores y consumibles (DCA in situ)

La configuración de detección automática de redes patentada por 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, routers, concentradores, conmutadores y hardware de red adicional.

Los administradores de Printanista Hub pueden gestionar de forma remota los DCA (agentes de recopilación de datos) Onsite 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 explican con más detalle:

Función	**Ubicación**	**Descripción**
Tareas	Configuración de Onsite	Permite configurar de forma remota tareas para que se ejecuten según un calendario preestablecido, pero también permite seleccionar tareas (Caché, Contadores, Suministros, Servicio) para que se ejecuten de inmediato y recopilar datos de los dispositivos cuando se le ordene.
Recorridos MIB	Configuración in situ	Se pueden indicar determinadas direcciones IPv4/IPv6 o nombres de host de los dispositivos y hacer que el dispositivo in situ inicie inmediatamente la recopilación de los recorridos MIB.
Registros (detallados)	Configuración de Onsite	Puede indicar a Onsite que recopile los registros (críticos, de error, de advertencia, de detalles y de depuración) a partir de una fecha determinada.

Ninguno de estos comandos da lugar a una 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 utilizando protocolos de cifrado robustos que cumplen con la norma FIPS. Onsite recibe actualizaciones de software seguras desde los servidores de actualizaciones de Printanista.

El sistema Onsite DCA heredado 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 a tiempo.

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 Onsite DCA 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, fotocopiadora o dispositivo multifunción. A diferencia de 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 pertinentes en función de los campos que admite el dispositivo de destino, y cada consulta no supera los pocos kilobytes de datos. Para reducir aún más el ancho de banda de red utilizado, Onsite DCA se comunica con un máximo de 20 dispositivos a la vez. Se consultará cada IP dentro de los rangos configurados y, si no se recibe respuesta dentro del periodo de tiempo de espera configurado, pasará a la siguiente dirección IP. Como regla general, Printanista recopilará información de aproximadamente 65 000 dispositivos en poco menos de una hora.

Compatibilidad con fabricantes

Los productos de 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 en caso de que la integridad del archivo se vea comprometida. Esto garantiza que, si hubiera algún virus presente, no se active y evita que el virus se propague de una red a otra. Para mayor seguridad, recomendamos utilizar un programa antivirus en su red.

ECI prestará 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.

