Documento técnico do Printanista Hub

Versão 1.8

Índice

A ECI fornecerá serviços de suporte exclusivamente para a versão mais recente do Software disponível comercialmente, bem como para a versão imediatamente anterior do Software. Esta política aplica-se a todos os produtos de gestão de dispositivos da ECI.

Microsoft®, .NET Framework®, Windows® e Windows Server® são marcas registadas ou marcas comerciais da Microsoft Corporation

Visão geral

O conjunto de produtos Printanista oferece uma solução de impressão gerida de classe empresarial que é bastante fácil de usar e implementar. Foi arquitetado e concebido para tirar partido das funcionalidades avançadas e dos benefícios da plataforma Microsoft .NET. Assim, já não são necessários técnicos especializados para instalar o software, configurar e manter o sistema. Os produtos Printanista não podem, de forma alguma, ser configurados para realizar tarefas além daquelas para as quais foram projetados. A transmissão de dados dos produtos para fontes externas é rigidamente restrita. Os produtos não relatam quaisquer outros detalhes, exceto informações sobre o equipamento que está a ser monitorizado (ou seja, tipo de equipamento). Nenhuma informação confidencial é transmitida para fora da rede através dos produtos Printanista. O conjunto é composto pelos seguintes componentes:

Printanista Hub: Um site e sistema backend que armazena todos os dados recebidos das ferramentas de recolha de dados da Printanista. É um repositório que permite visualizar dados usando um navegador, gerar relatórios, configurar fluxos de trabalho de alertas e notificações e sincronizar dados com os seus sistemas ERP para faturação ou cumprimento de fornecimentos.

ECI DCA: Este mais recente Agente de Recolha de Dados-DCA traz grandes vantagens em relação ao Agente de Recolha de Dados no Local-DCA, sem perder nenhuma funcionalidade, incluindo suporte nativo completo para várias plataformas, como Windows, macOS, Linux e Raspberry Pi, cada uma com etapas de instalação exclusivas, documentação de suporte e equipa de suporte treinada nessas plataformas. O ECI DCA também oferece descoberta e digitalização contínuas de dispositivos, capacidade aprimorada de recolha de MIBWalk e Log, e muitos mais tipos de medidores são recolhidos agora.

DCA no local: Uma ferramenta de agente de recolha de dados legada realiza automaticamente avaliações de impressão e monitora os níveis de consumíveis, o estado da impressora e os registos de erros. Esta aplicação é instalada nas instalações do cliente e pode realizar avaliações de impressão automaticamente de forma programada, sem intervenção humana. Os dados capturados são enviados para o site Printanista Hub usando HTTPS, HTTP ou, se o cliente preferir, um ficheiro criptografado proprietário.

O objetivo deste documento é fornecer uma visão geral da linha de produtos Printanista Suite de uma perspetiva técnica para ajudar a facilitar as respostas às perguntas mais frequentes que as equipas de Tecnologia da Informação recebem.

Como funciona o Printanista

Printanista Hub Concebido como uma aplicação hospedada

O Printanista Hub é hospedado pela ECI Software Solutions em centros de dados seguros e protegidos em diferentes regiões do mundo. A ECI Software Solutions compreende que a confidencialidade, integridade e disponibilidade das informações dos nossos clientes são vitais para as suas operações comerciais e para o nosso próprio sucesso. Utilizamos uma abordagem em várias camadas para proteger essas informações essenciais, monitorizando e melhorando constantemente a nossa aplicação, sistemas e processos, para atender às crescentes demandas e desafios de segurança.

Centros de dados seguros da ECI

O nosso serviço está localizado em espaços dedicados em centros de dados de primeira linha. Estas instalações fornecem suporte de nível de operadora. Este link leva ao documento detalhado da ECI relacionado à segurança dos centros de dados.
Visão geral da segurança na nuvem da ECI 2021 (ecisolutions.com)

Agente de recolha de dados (DCA)

O mecanismo central do agente de recolha de dados, que é o coração de todos os produtos Printanista, identifica e extrai corretamente os dados de impressoras, fotocopiadoras e multifuncionais em rede, utilizando os protocolos suportados pelos dispositivos.

Atualmente, a Printanista suporta os protocolos SNMP (Simple Network Management Protocol) v1, v2c e v3. O SNMP v3 oferece maior proteção de pacotes para garantir que as informações e comunicações sejam transmitidas por fontes confiáveis. Ao contrário do SNMPv1 ou v2, o SNMP v3 é criptografado para maior segurança e requer um nome de utilizador e uma palavra-passe. Uma vantagem de usar o SNMP v3 é que os administradores de rede podem determinar o método de criptografia, bem como um nome de utilizador e uma palavra-passe fortes.

O SNMP é um protocolo de rede que facilita a troca de informações entre dispositivos de rede, extraindo dados da Base de Informações de Gestão (MIB) e de outros locais dentro do dispositivo de impressão. A Base de Informações de Gestão (MIB) é uma base de dados interna que a maioria dos dispositivos conectados à rede possui como parte de sua anatomia. A Base de Informações de Gestão (MIB) contém dados como nome do modelo, níveis de toner e status atual da impressora.

Requisitos do Printanista

Backend do Printanista Hub Aplicação

Todos os dados recolhidos são enviados para o servidor Printanista Hub, onde ficam disponíveis para relatórios e alertas.
O ECI DCA liga-se ao servidor Printanista Hub utilizando HTTPS (porta **443/TCP**). Contacte o administrador da ECI Solutions para obter informações sobre nomes de domínio e endereços IP utilizados pelo servidor.

Esta ligação é protegida pelo padrão industrial **TLS** (Transport Layer Security).
É necessária a versão mínima TLS 1.2.

Esta ligação permanece aberta durante todo o tempo em que o ECI DCA estiver em execução. Normalmente, é utilizada uma ligação **WebSocket**, mas em algumas situações o ECI DCA pode recorrer ao uso de **eventos enviados pelo servidor** ou **HTTP long polling**.

NOTA IMPORTANTE: São necessárias várias ligações HTTPS seguras de saída a partir do servidor onde o Printanista Hub está instalado:

- 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 do aplicativo Printanista

Agente de recolha de dados (ECI DCA)

Impressoras, copiadoras e multifuncionais devem ter o protocolo SNMP (Porta 161) ativado para descoberta e extração de informações. O protocolo SNMP é uma parte padrão da Camada de Aplicação do conjunto TCP/IP.

Requisitos do PC/servidor para ECI DCA:

Requisitos do Microsoft Windows (x86/64):

- Microsoft .NET Framework 4.7.2. ou mais recente (recomendado: versão mais recente)
- Versões totalmente lançadas e suportadas pela Microsoft do Windows Server (excluindo as edições Datacenter e Core) e do Windows
  - ➢ *versões da Microsoft que já não são suportadas pela Microsoft não são suportadas pela ECI DCA.*
- As configurações da rede local e/ou do firewall permitem a ligação aos serviços do servidor ECI Updates e ao servidor Printanista Hub.

Requisitos do Linux (x86/64 ou ARM):

- Mono Framework 5.4 ou superior (recomendado: versão mais recente)
- As configurações da rede local e/ou firewall permitem a conexão com os serviços do ECI Updates Server e o servidor Printanista Hub.
- Apenas o Ubuntu LTS 20.04 e superior são oficialmente suportados.

Requisitos do macOS (x64):

- Mono Framework 5.4 ou superior (recomendado: versão mais recente)
- macOS® Sierra (10.12) até Sequoia (15.4). Versões mais recentes não são suportadas.
- As configurações da rede local e/ou firewall permitem a ligação aos serviços do servidor ECI Updates e ao servidor Printanista Hub.

Requisitos do Raspberry Pi:

- Raspberry Pi 3 Modelo B ou Pi 4 Rev 1.5. Versões mais recentes não são suportadas.
- Cartão microSD vazio de 8 GB ou superior
- PC capaz de gravar em cartão microSD
- As configurações da rede local e/ou firewall permitem a conexão com os serviços do servidor ECI Updates e o servidor Printanista Hub.

Considerações sobre firewall para ECI DCA:

Ligações de entrada - Não há ligações de entrada da Internet para o ECI DCA.

Ligações de saída

Serviço	Porta	Conexão para
Envio de dados	**443/TCP** (HTTPS)	O seu servidor Printanista Hub
Atualizações de software	**443/TCP** (HTTPS)	Servidor de atualizações ECI
Registo (fallback)	**53/UDP** (DNS)	Servidor DNS da rede local (primário) Servidor de atualizações ECI (fallback)

Servidor de atualizações ECI

O servidor de atualizações ECI é um serviço executado pelo ECI Device Management para facilitar o registo DCA, atualizações automáticas de software e instalações DCA (este site) e é necessário para o funcionamento do ECI DCA. Nota: O ECI DCA não envia quaisquer dados recolhidos do dispositivo ou de configuração para o servidor de atualizações ECI.

Atualizações de software

O ECI DCA atualiza-se automaticamente, descarregando as atualizações publicadas em https://updates.printanista.net/. As ligações são sempre feitas na porta HTTPS padrão **443/tcp**.

Registo

O ECI DCA utiliza pedidos DNS para `*.reg.pf-d.ca` para se registar. Primeiro, tentará fazer isso utilizando os servidores DNS da rede local e, em seguida, recorrerá diretamente aos endereços IP do servidor de atualizações ECI (utilizando a porta **53/udp**). A firewall só precisa permitir essa conexão com o servidor de atualizações ECI se os servidores DNS locais não resolverem os pedidos de registo.

Região de serviço

O ECI DCA é encaminhado para a região com a menor latência de rede e com base na disponibilidade do serviço. Em determinados locais, a região utilizada pode mudar ao longo do tempo, uma vez que a atividade na infraestrutura global da Internet pode afetar a latência.

Criptografia de dados coletados e e

Criptografia de dados

Todos os pacotes de dados do ECI DCA e do antigo Onsite DCA são codificados e ofuscados. O Printanista requer o uso de HTTPS para comunicação entre os DCAs e o Printanista Hub. O ECI DCA requer HTTPS para funcionar. Além disso, todas as configurações e tarefas confidenciais entre o ECI DCA e o Printanista são encriptadas usando o algoritmo de encriptação simétrica padrão AES256, usando uma chave partilhada protegida. Isso garante a encriptação de ponta a ponta, para que os dados fiquem protegidos contra leitura se forem interceptados por terceiros, uma instância concorrente ou não autorizada do Printanista.

Questões de segurança do e

O ECI DCA e o Onsite DCA legado comunicam com o Printanista Hub através do protocolo HTTPS, utilizando o padrão industrial **TLS 1.2** (Transport Layer Security). Os dados confidenciais não são recolhidos, visualizados ou guardados por qualquer aplicação Printanista. Apenas os dados relacionados com a impressora são recolhidos e visualizados. Nenhum outro dado de rede pode ser identificado ou recolhido pelo ECI DCA ou pelo Onsite DCA legado, exceto o endereço IP, o endereço MAC e o nome do host.

O ECI DCA e o Onsite DCA antigo não recolhem nem processam quaisquer dados pessoais. A única forma de o sistema recolher este tipo de informação é se você ou os seus clientes introduzirem os dados no Printanista num campo ou etiqueta, como a localização ou o nome do cliente. O ECI DCA e o Onsite DCA antigo permitem-lhe monitorizar dispositivos de rede usando o Protocolo Simples de Gestão de Rede (SNMP). A aplicação é implementada dentro da rede do cliente e, a partir daí, comunica com os dispositivos para recolher informações operacionais sobre o dispositivo que são disponibilizadas através do firmware do dispositivo e de uma Base de Informação de Gestão SNMP (MIB). Os dados expostos pelo dispositivo variam consoante o fabricante e o modelo. São sempre de natureza técnica ou operacional e específicos do próprio dispositivo. No nível mais básico, os dados expostos por uma MIB de impressora estão documentados na IETF RFC 3805 (https://tools.ietf.org/html/rfc3805). Informações adicionais sobre o dispositivo podem ser expostas pelo fabricante por meio de extensões e MIBs (Management Information Base) privadas, mas as informações são fundamentalmente técnicas e específicas do dispositivo.

O Printanista Hub armazena apenas:

- Nome do host
- Sistema operativo
- Endereço IP remoto
- Arquitetura do sistema

Outras informações de rede/ambiente são recolhidas e exibidas enquanto estiver conectado para fins de resolução de problemas, mas nunca armazenadas no Printanista.

Tipos de informações recolhidas pelo

O ECI DCA e o antigo Onsite DCA tentam recolher as seguintes informações de dispositivos de impressão em rede durante uma verificação da rede:

Atributos do dispositivo

- Endereço IP (pode ser mascarado)
- Fabricante
- Número de série
- Número do ativo
- Endereço MAC
- Descrição do dispositivo
- Local
- Diversos (específicos da máquina)

Serviço

- Leitura do LCD
- Estado do dispositivo
- Códigos de erro
- Firmware

Consumíveis

- Número de série do cartucho de toner
- Nível de tinta do cartucho
- Níveis do tambor
- Níveis do kit de manutenção
- Níveis de suprimento de não toner
- Níveis diversos
- Detalhes do abastecimento de impressoras baseadas em etiquetas

Cobertura e medidores

- Leituras do medidor
- Tipo de medidor
- Nível de cobertura
- Identificação monocromática ou a cores

Descoberta de rede e recolha de dados

Para aumentar a eficiência do DCA, somente quando houver dados novos ou alterados dos dispositivos é que essas informações serão enviadas para o servidor Printanista Hub. Isso garantirá uma carga mínima na rede e eliminará a frequência de atrasos no envio de dados dos dispositivos. Além disso, a descoberta e a digitalização de dispositivos agora são independentes para garantir apenas o endereço IP.
(ou nome do host) dos dispositivos anteriormente descobertos estão a ser verificados periodicamente, em vez de uma verificação completa da rede (isso é concluído inicialmente, periodicamente ou quando determinado por um utilizador administrador).

Isso garantirá que a velocidade de envio dos dados dos dispositivos seja a mais atualizada possível. Isso permite que os utilizadores sejam notificados sobre dispositivos problemáticos em questão de minutos ou até segundos em muitas situações. O ECI DCA separa a descoberta de dispositivos de outros tipos de verificação, permitindo que defina intervalos de verificação personalizados para recuperar medidores, atributos de suprimentos e erros. Os valores padrão, mínimo e máximo para os intervalos de verificação são:

Função de verificação	Padrão	Mínimo	Máximo
Descoberta	60 minutos	10 minutos	7 dias
Medidores	24 horas	30 minutos	14 dias
Suprimentos	4 horas	30 minutos	7 dias
Erros	60 minutos	30 minutos	7 dias
Atributos	24 horas	1 hora	14 dias

Observe que os intervalos de verificação (medidores, suprimentos, erros e atributos) só estão disponíveis se o dispositivo tiver um Ficheiro de Definição de Modelo (MDF). Se ele não estiver presente, será realizada uma verificação completa no dispositivo em questão usando um intervalo predefinido.

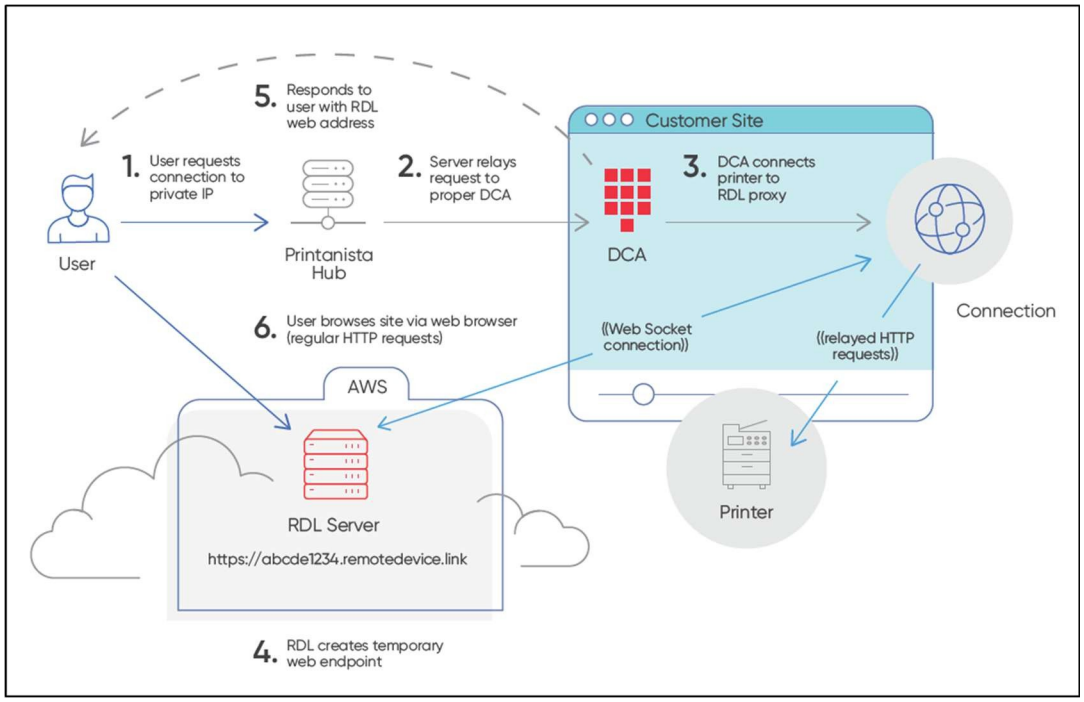
Os administradores do Printanista Hub podem gerir remotamente o ECI DCA que foi ativado no servidor. Podem acionar remotamente o ECI DCA para executar comandos predefinidos, tais como tarefas de recolha de dados, fornecimento de registos ECI DCA, execução remota de MIB Walks ou atualização das definições ECI DCA.

Nota: O ECI DCA inicia sempre a comunicação com o servidor Printanista, e não o contrário.

Nota: A comunicação só ocorre quando as informações do medidor, do fornecimento ou dos erros são atualizadas ou alteradas, reduzindo o uso da largura de banda.

Nota: O HP JAMC só funciona com o Onsite DCA antigo no momento.

o de Ligação Remota de Dispositivos (RDL)



Visão geral do sistema – Ligação remota a dispositivos (, RDL)

O Remote Device Link (RDL) é um serviço que permite que um **utilizador final** remoto aceda a um ponto final HTTP numa LAN privada. Existem quatro componentes principais:

1. O **utilizador final** que acede ao dispositivo
2. O **servidor Remote Device Link**, na Internet pública (através do URL https://*.remotedevice.link)
3. O **cliente RDL** (incorporado no DCA), em execução na LAN privada
4. O **ponto final HTTP** (impressora) que está a ser acedido (em execução na LAN privada)

Segurança: portas e SSL (Secure Sockets Layer)

O caminho público para RDL é sempre um URL https:// na porta 443, independentemente da porta do ponto final e/ou do estado SSL.

Permissões de ativação e

1. Opção de ativação global por instância do revendedor
2. Habilitação local para cada conta de cliente final
3. São necessárias permissões para que um utilizador possa aceder ao recurso

Capacidades de auditoria do

1. Auditoria local do Printanista Hub de cada detalhe da sessão
    a. Relatórios de administração do Printanista Hub para auditoria do Remote Device Link (RDL)
2. Remote Device Link (RDL) AWS (Amazon Web Services) registo na nuvem de todos os detalhes da sessão

Segurança do Remote Device Link (RDL)

A segurança do Remote Device Link (RDL) foi uma preocupação fundamental durante o

desenvolvimento desta ferramenta. Autorização:

- O utilizador deve ter permissão do Printanista Hub para aceder ao recurso Remote Device Link (RDL) na conta específica
- O Agente de Recolha de Dados (DCA) só aceitará pedidos de Ligação Remota a Dispositivos (RDL) do servidor Printanista Hub que seja mutuamente autenticado
- O Agente de Recolha de Dados (DCA) só estabelece a ligação Remote Device Link (RDL) a dispositivos de impressão conhecidos e atualmente monitorizados dentro do(s) intervalo(s) de IP de descoberta do Agente de Recolha de Dados (DCA).
- Cada solicitação individual da web deve ser para o mesmo IP – o Agente de Recolha de Dados (DCA) não seguirá redirecionamentos

Segurança da ligação:

- Todas as ligações de e para os servidores Remote Device Link (RDL) e Printanista Hub são encriptadas utilizando a versão mínima padrão TLS 1.2 (Transport Layer Security).
- Cada ligação recebe um nome de domínio único que utiliza uma combinação alfanumérica aleatória de 19 caracteres (96 bits).
- Cada pedido requer um token de segurança de 160 bits, armazenado como um cookie do navegador, e definido apenas no início da sessão protegida pela encriptação TLS
- O Data Collection Agent (DCA) pode estabelecer uma ligação HTTP não encriptada ao dispositivo de impressão através da rede local, mas suporta a versão mínima TLS 1.2 se o dispositivo também a suportar

Limites de tempo da sessão:

- Cada sessão individual do Remote Device Link (RDL) expira após 20 minutos de inatividade por predefinição, com um máximo absoluto de 2 horas.

Implicações

A ligação entre o ECI DCA e o Printanista Hub é protegida por chaves de autenticação específicas da instalação do DCA, e a ligação requer um certificado SSL válido e confiável para ser usada em uma ligação TLS.

Todo o tráfego que transita do DCA para a Internet é encriptado. No entanto, o ECI DCA pode comunicar com o dispositivo na rede local através de ligações HTTP simples, se o dispositivo não suportar ligações seguras.

Aplicação Printanista Hub

A funcionalidade do Printanista Hub é acessível através de uma interface de utilizador

baseada na web. Gestão de utilizadores baseada em permissões

O acesso ao front-end da web do Printanista Hub é controlado por uma gestão de utilizadores baseada em permissões. Os utilizadores devem iniciar sessão no Printanista utilizando um nome de utilizador e uma palavra-passe designados. São atribuídas aos utilizadores uma ou mais funções que especificam as permissões e é-lhes concedido acesso a um ou mais grupos de dispositivos. Os administradores com permissões totais podem especificar exatamente quais os ecrãs que cada utilizador pode visualizar e/ou com os quais pode interagir.

Acesso HTTPS

O Printanista exige que todos os sites utilizem HTTPS com um certificado de segurança SSL válido. Isso garante a criptografia dos dados transferidos pela Internet.

Printanista Side-By-Side

O Printanista Hub utiliza uma base de dados de metadados de modelos conhecida como Side-by-Side (SBS), que possui vários atributos de modelos, tais como: velocidades de impressão, data de lançamento no mercado ou compatibilidades de números de peças OEM, que são atualizados periodicamente à medida que novos modelos e versões são lançados pelos OEMs. O Printanista Hub comunicará com o Side-by-Side para verificar novas atualizações, bem como recuperar metadados de dispositivos para os armazenar localmente em cada sistema Printanista Hub.

Hospedagem do aplicativo Printanista Hub

O Printanista Hub é hospedado pela ECI Software Solutions em centros de dados seguros e protegidos em diferentes regiões do mundo. A ECI Software Solutions compreende que a confidencialidade, integridade e disponibilidade das informações dos nossos clientes são vitais para as suas operações comerciais e para o nosso próprio sucesso. Utilizamos uma abordagem em várias camadas para proteger essas informações essenciais, monitorizando e melhorando constantemente a nossa aplicação, sistemas e processos, para atender às crescentes demandas e desafios de segurança.

Centros de dados seguros da ECI

O nosso serviço está localizado em espaços dedicados em centros de dados de primeira linha. Estas instalações fornecem

suporte de nível de operadora. Clique na seguinte ligação para obter o documento detalhado da ECI relacionado com a

segurança dos centros de dados

Visão geral da segurança na nuvem da ECI 2021 (ecisolutions.com)

Processo de teste e lançamento de gerenciamento de versão

Cada lançamento principal e secundário do software passa por um processo de controlo de qualidade, no qual vários funcionários da Printanista realizam testes de regressão nas partes alteradas do sistema para garantir que não houve uma redução na segurança ou funcionalidade do sistema, bem como para validar os novos aspectos funcionais. Os lançamentos principais passam por um processo de lançamento beta, no qual clientes selecionados executam os sistemas novos e antigos em paralelo.

Segurança do código-fonte

O código-fonte da Printanista é mantido num sistema de controlo de revisão seguro, acessível apenas a pessoas autorizadas. Cada alteração no código-fonte requer a aprovação de dois programadores autorizados antes de ser aceite no repositório de código de produção, onde todas as alterações são rastreadas, incluindo quem fez a alteração e porquê. Os produtos são encriptados e assinados digitalmente com um certificado de assinatura de código confiável antes do envio. Um depósito em garantia pode ser disponibilizado mediante solicitação.

A ECI contrata uma empresa independente líder do setor, certificada pela CREST, SOC 2, NSA-CIRA e CSA-STAR, para realizar testes de penetração ao nível da aplicação e corrigir as conclusões com base nos seus requisitos comerciais e na estrutura interna de gestão de riscos. Os testes de penetração são realizados pelo menos uma vez por ano ou quando são feitas alterações significativas ao sistema. A política da ECI é envidar esforços comercialmente razoáveis para corrigir todas as conclusões críticas no prazo de 30 dias ou num prazo razoável com um caso de negócio fornecido. A ECI não divulga detalhes sobre os nossos controlos de segurança ou resultados de testes de penetração, uma vez que essas informações são proprietárias e confidenciais e, nas mãos erradas, podem levar a um aumento do risco.

Legislação sobre privacidade de dados e o Regulamento Geral sobre a Proteção de Dados ( )

Regulamento Geral sobre a Proteção de Dados (RGPD)

Em maio de 2018, o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia entrou em vigor. O RGPD substitui a Diretiva 95/46/CE sobre Proteção de Dados e foi concebido para reforçar e unificar as leis de privacidade de dados em toda a Europa.

A ECI implementou um programa estruturado e abrangente de conformidade com o RGPD. O programa consiste, entre outras coisas, em formação de pessoal, auditoria e avaliação de riscos em toda a empresa, políticas e procedimentos, governação e esforços contínuos de conformidade. Encorajamos os nossos clientes a tomarem medidas semelhantes para garantir que as suas próprias empresas cumprem o RGPD e nos anos vindouros.

Os produtos Printanista não processam, monitorizam ou gerem quaisquer registos pessoais ou quaisquer registos ou informações específicas de qualquer pessoa ou grupo de pessoas.

As aplicações de software da Printanista não recolhem, armazenam ou transmitem qualquer informação relativa ao conteúdo dos trabalhos de impressão.

A Printanista não tem como aceder, armazenar ou transmitir informações de alto risco, mesmo que essas informações sejam impressas ou enviadas para dispositivos de impressão monitorados pelos aplicativos de software da Printanista.

As aplicações de software da Printanista não armazenam, processam ou transmitem dados de titulares de cartões ou informações pessoais.

As comunicações do motor do produto são controladas, utilizando acesso limitado para contactar endereços IP específicos e/ou intervalos.

Todas as comunicações devem ter origem nos produtos Printanista, e não há como contactar e aceder aos produtos fora da rede.

A comunicação fora da rede utiliza um fluxo de dados comprimido proprietário que é enviado utilizando SSL padrão da indústria sobre HTTPS.

Para obter informações relacionadas com a conformidade com leis e/ou regulamentos específicos, contacte o seu gestor de conta ECI.

Segue-se um link para a ECI Cloud Security: [Visão geral da segurança na nuvem da ECI 2021 (ecisolutions.com)]

Perguntas frequentes (FAQs)

Os produtos Printanista funcionam com proxies de Internet?
Sim, o ECI DCA funciona com a maioria dos proxies. É necessário configurar as definições do proxy no sistema onde o ECI DCA está instalado e funciona.
Quais são os requisitos mínimos do Printanista Hub, ECI DCA e Onsite?
Consulte a secção Requisitos da aplicação Printanista neste documento.

Os produtos Printanista são compatíveis com os ambientes Mac, Linux ou Raspberry Pi?
Este ECI DCA traz grandes vantagens em relação ao Onsite DCA sem perder nenhum recurso, incluindo suporte nativo completo para várias plataformas, incluindo Windows, macOS, Linux e Raspberry Pi. Cada um com etapas de instalação exclusivas, documentação de suporte e equipe de suporte treinada nessas plataformas. O processo de instalação também melhorou muito e está muito mais intuitivo para todos os tipos de utilizadores.

O ECI DCA requer o Microsoft Internet Information Services (IIS)?
Não. O ECI DCA e o Onsite DCA incluem o seu próprio servidor para hospedar a interface de utilizador (UI) baseada na web e são configurados automaticamente durante a instalação.

É possível instalar o ECI DCA num computador que já hospeda outro site IIS?
Sim. No entanto, as portas listadas abaixo devem ser incluídas na lista de permissões para garantir a conectividade do ECI DCA.

Serviço	Porta	Conexão com
Upload de dados	**443/TCP** (HTTPS)	O seu servidor Printanista Hub
Atualizações de software	**443/TCP** (HTTPS)	Servidor de atualizações ECI
Registo (fallback)	**53/UDP** (DNS)	Servidor DNS da rede local (primário) Servidor de atualizações ECI (fallback)

O ECI DCA usa a porta 31816 por predefinição para a interface de utilizador baseada na Web do DCA local.

Quanta manutenção contínua o ECI DCA requer?
O ECI DCA e o Onsite DCA são serviços que funcionam em segundo plano e realizam auditorias e exportações para destinos configurados em horários predefinidos. Recomenda-se usar sub-redes (intervalos de IP) em vez de IPs fixos. Ao adicionar novos dispositivos à rede, eles serão descobertos e incluídos nos resultados da auditoria, limitando a intervenção manual.

Com quais marcas de equipamentos o monitoramento Remote Device Link (RDL) funciona? Quais são os requisitos para que ele funcione?
Todas as marcas com uma página web incorporada são detetadas pelo ECI DCA. As informações nas páginas web incorporadas variam de acordo com o fabricante e o modelo. Os dispositivos locais não mostram a página web incorporada.

Existem preocupações adicionais de segurança com o Remote Device Link (RDL)?
É aberto um canal seguro entre o dispositivo na rede local do cliente e um operador localizado fora dessa rede. O RDL só reportará os dispositivos descobertos e monitorizados ativamente através do ECI DCA. É apresentada uma mensagem a indicar que a ligação do dispositivo não é suportada através do DCA

O Remote Device Link (RDL) parece um pouco lento, por que isso acontece?
Isso é de se esperar, pois a ligação precisa ser tunelada através dos nossos serviços em nuvem. No entanto, o principal fator que influencia é a rapidez com que os dispositivos respondem às solicitações da interface do utilizador (UI) da Web.
Vimos dispositivos a responder em décimos de segundos às primeiras tentativas de ligação, sendo influenciados pela utilização atual ou pelos recursos disponíveis para a Interface do Utilizador (UI).

Quais funcionalidades estão disponíveis com o Remote Device Link (RDL)?
Todas as opções que o OEM disponibiliza através da página web incorporada estão acessíveis através do Remote Device Link (RDL).

O recurso Remote Device Link (RDL) pode ser desativado?
Sim, é possível desativar este recurso por conta.
Também é possível desativar este recurso por utilizador, permitindo bloquear o acesso de um utilizador ao Remote Device Link (RDL).

Onde posso obter informações adicionais sobre o Printanista Hub, ECI DCA, Onsite DCA antigo, etc.?
Informações adicionais podem ser encontradas no site da ECI Printanista:
https://www.ecisolutions.com/products/printanista-hub/

Informações sobre o antigo Onsite DCA

Recomenda-se a utilização do ECI DCA com o Printanista. No entanto, o Onsite DCA antigo funciona atualmente com o Printanista.
Requisitos de PC/servidor para o Onsite DCA:

- 1 GB de RAM
- 400 MB de espaço em disco
- Microsoft .NET Framework 4.7.2 ou mais recente
- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- A versão local 4.1.3 e mais recente suporta o Windows Server 2022
- Internet Explorer 11.0 ou mais recente, Chrome, Firefox
- MDAC 2.8 ou superior (normalmente incluído quando o Windows é instalado)
- JET 4.0 ou superior (normalmente incluído quando o Windows é instalado)
- Carregado numa máquina que esteja ligada 24 horas por dia, 7 dias por semana, ou pelo menos durante todo o dia útil
- É necessário estar conectado como Administrador Local (ou equivalente) durante a instalação

Considerações sobre firewall de saída (porta 80 ou 443):

Transmissão de dados:

- https://(company_Printanista_FQDN)/WebServices/Onsite2Service.asmx
- Aplicação: fmaonsite.exe
- SOAP sobre HTTP(s) deve ser permitido após o firewall

Requisitos de rede:

O tráfego SNMP (Porta 161) deve ser roteável através da LAN ou WAN (Wide Area Networks)

Utilize o ECI DCA se forem necessários sistemas operativos macOS, Linux ou Raspberry Pi O
Java Onsite legado em sistemas Linux e macOS não está funcional.

Requisitos de PC/impressora para utilizar o Agente Local (instalação opcional):

- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- Microsoft .NET Framework 4.7.2 ou mais recente
- Driver atual para a impressora local (recomenda-se UPD para dispositivos HP)
- A impressora deve suportar a linguagem PJL (Printer Job Language) ou PML (Printer Management Language)
- Remova todos os controladores de impressão não utilizados
- O suporte bidirecional do controlador está ativado
- Modificações na Firewall do Windows — Porta 161/33333 de entrada/saída para TCP e UDP *Versões do Windows e Windows Server suportadas pela Microsoft. As versões que já não são suportadas pela Microsoft não são suportadas pela ECI.*

Nota: Para versões recentes do sistema operativo que utilizam o modelo de controlador 4 (por exemplo, Windows 10), apenas os OEMs Kyocera e Ricoh, e suas variações, são suportados atualmente.

Descoberta de rede e recolha de medidores e suprimentos (DCA no local)

As configurações patenteadas de descoberta automática de rede da Printanista utilizam uma combinação de algoritmos para identificar os intervalos de rede onde os dispositivos de impressão podem estar localizados e, em seguida, descobrir e comunicar com os dispositivos que estão online, encaminhando através de vários elementos de rede, tais como estações de trabalho ou servidores ativos, routers, hubs, switches e hardware de rede adicional.

Os administradores do Printanista Hub podem gerir remotamente os DCAs (Agentes de Recolha de Dados) ativados no servidor, bem como acionar remotamente o Onsite para executar comandos predefinidos, tais como tarefas de recolha de dados, fornecimento de registos do Onsite, execução remota de MIBWalks, instalação do HP JAMC ou atualização das configurações do Onsite. Estes são explicados em mais detalhe abaixo:

Função	**Localização**	**Descrição**
Tarefas	Configurações do Onsite	É possível configurar remotamente tarefas para serem executadas em uma programação predefinida, mas é possível selecionar tarefas (cache, medidores, suprimentos, serviço) para serem executadas imediatamente e coletar dados do dispositivo sob comando.
MIB Walks	Configurações no local	É possível indicar determinados IPv4/IPv6/nomes de host de dispositivos e acionar o local para iniciar imediatamente a recolha dos MIB Walks.
Registos (detalhados)	Configurações no local	Pode instruir o Onsite a recolher os registos (críticos, erros, avisos, detalhes, depuração) a partir de uma determinada data.

Nenhum destes comandos leva à recolha de dados além dos tipos de informações recolhidas conforme descrito acima. Os dados trocados entre o Onsite DCA e o Printanista Hub são encriptados usando protocolos de encriptação fortes que são compatíveis com FIPS. O Onsite recebe atualizações de software seguras dos servidores Printanista Updates.

O Onsite DCA legado comunica com o Printanista em um intervalo predefinido para determinar se há alguma ação em fila que ainda não tenha sido executada. Isso garante que as ações sejam executadas em tempo hábil.

Nota: O Onsite DCA inicia sempre esta comunicação com o servidor Printanista, e não o contrário.

Nota: O HP JAMC só é suportado quando utilizado em conjunto com o Onsite DCA antigo no lançamento inicial do Printanista.

Tráfego de rede

As auditorias realizadas pelo software utilizam um sistema inteligente para extrair informações mínimas de cada impressora, copiadora ou MFP. Ao contrário de produtos semelhantes que enviam um conjunto fixo de consultas (um superconjunto de todas as consultas possíveis) para todos os dispositivos em rede, o Onsite DCA envia apenas as consultas relevantes de acordo com os campos suportados pelo dispositivo de destino, com cada consulta de dispositivo não excedendo alguns kilobytes de dados. Para reduzir ainda mais a quantidade de largura de banda de rede utilizada, o Onsite DCA comunica com no máximo 20 dispositivos ao mesmo tempo. Cada IP dentro dos intervalos configurados será consultado e, se nenhuma resposta for recebida dentro do período de tempo limite configurado, ele passará para o próximo endereço IP. Uma regra geral é que o Printanista reunirá informações sobre aproximadamente 65.000 dispositivos em menos de uma hora.

Suporte do fabricante

Os produtos Printanista são independentes do fabricante. Eles suportam todos os principais fabricantes e famílias de modelos. Alguns dispositivos têm limitações que impedem a extração de determinadas informações.

Preocupações com vírus

Os ficheiros da aplicação Printanista foram assinados digitalmente para impedir a execução caso a integridade do ficheiro seja comprometida. Isto garante que qualquer vírus presente não seja ativado e impede a propagação do vírus de uma rede para outra. Para maior segurança, recomendamos a utilização de software antivírus na sua rede.

A ECI fornecerá serviços de suporte exclusivamente para a versão mais recente do Software disponível comercialmente, bem como para a versão imediatamente anterior do Software. Esta política aplica-se a todos os produtos de gestão de dispositivos da ECI.

