



Documento técnico do Printanista Hub

Versão 1.10



Índice

| | |
|--|----|
| Visão geral | 4 |
| Printanista Hub Concebido como uma aplicação alojada | 5 |
| Centros de dados seguros da ECI | 5 |
| Agente de recolha de dados (DCA)..... | 5 |
| Aplicação de backend do Printanista Hub | 6 |
| Requisitos da aplicação Printanista | 7 |
| Agente de recolha de dados (ECI DCA) | 7 |
| Requisitos de PC/servidor para o ECI DCA..... | 7 |
| Servidor de atualizações ECI | 8 |
| Atualizações de software..... | 8 |
| Registo | 8 |
| Área de cobertura | 8 |
| Dados recolhidos e encriptação | 9 |
| Criptografia de dados | 9 |
| Questões de segurança | 9 |
| Tipos de informações recolhidas | 9 |
| Ligação de Dispositivos Remotos (RDL)..... | 11 |
| Visão geral do sistema – Remote Device Link (RDL) | 11 |
| Segurança: Portas e SSL (Secure Sockets Layer) | 11 |
| Ativação e permissões | 11 |
| Funcionalidades de auditoria | 11 |
| Segurança da Ligação de Dispositivos Remotos (RDL) | 12 |
| A segurança da Ligação de Dispositivos Remotos (RDL) foi uma preocupação fundamental durante o desenvolvimento desta ferramenta..... | 12 |
| Aplicação Printanista Hub | 13 |
| Gestão de utilizadores baseada em permissões | 13 |
| Acesso HTTPS | 13 |
| Printanista lado a lado..... | 13 |
| Hospedagem de aplicações Printanista Hub | 13 |
| Centros de dados seguros da ECI | 13 |
| Gestão de versões | 14 |
| Processo de teste e lançamento..... | 14 |
| Segurança do código-fonte..... | 14 |
| Privacidade de dados e legislação | 15 |
| Regulamento Geral sobre a Proteção de Dados (RGPD) | 15 |
| Perguntas frequentes (FAQs) | 16 |
| Informações sobre o DCA no local | 18 |

| | |
|---|----|
| Requisitos de PC/servidor para o DCA no local: | 18 |
| Considerações sobre a firewall de saída (Porta 80 ou 443)..... | 18 |
| Requisitos de rede | 18 |
| O Java Onsite legado em sistemas Linux e macOS não está funcional | 18 |
| Requisitos de PC/impressora para utilizar o Agente Local (instalação opcional) | 18 |
| Detecção de rede e recolha de dados de contadores e fornecimento (DCA no local) | 19 |
| Tráfego de rede | 19 |
| Suporte do fabricante | 20 |
| Preocupações com vírus | 20 |

A ECI prestará serviços de suporte exclusivamente para a versão mais recente do Software disponível no mercado, 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

A suite de produtos Printanista oferece uma solução de gestão de impressão de classe empresarial que é bastante fácil de utilizar e implementar. Foi arquitetada e concebida 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 executar tarefas além daquelas para as quais foram concebidos. A transmissão de dados dos produtos para fontes externas é estritamente restringida. Os produtos não comunicam quaisquer outros detalhes, exceto informações sobre o equipamento que está a ser monitorizado (ou seja, o tipo de equipamento). Nunca é transmitida qualquer informação confidencial para fora da rede através dos produtos Printanista. A suite é composta pelos seguintes componentes:

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

ECI DCA: Este mais recente Agente de Recolha de Dados (DCA) oferece vantagens significativas em relação ao Agente de Recolha de Dados no Local (DCA), sem perder nenhuma funcionalidade, incluindo suporte nativo completo para várias plataformas: Windows, macOS, Linux e Raspberry Pi, cada uma com passos de instalação específicos, documentação de suporte e pessoal de assistência técnico com formação específica para essas plataformas. O ECI DCA também permite a deteção e análise contínuas de dispositivos, capacidade melhorada de MIBWalk e recolha de registos, e agora recolhe muitos mais tipos de medidores.

DCA no Local: Uma ferramenta de agente de recolha de dados tradicional realiza automaticamente avaliações de impressão e monitoriza os níveis de consumíveis, o estado das impressoras 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 website do Printanista Hub utilizando HTTPS, HTTP ou, se o cliente preferir, um ficheiro encriptado 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 Tecnologias da Informação receberão.

Como funciona o Printanista

Printanista Hub concebido como uma aplicação alojada

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 responder às crescentes exigências e desafios de segurança.

Centros de Dados Seguros da ECI

O nosso serviço está alojado em espaços dedicados em centros de dados de primeira linha. Estas instalações oferecem suporte ao nível das operadoras. Esta ligação remete para o documento detalhado da ECI relativo à segurança dos centros de dados.

[Visão Geral da Segurança na Nuvem da ECI](#)

Agente de Recolha de Dados (DCA)

O motor central do agente de recolha de dados, que constitui o coração de todos os produtos Printanista, identifica e extrai corretamente os dados de impressoras, fotocopiadoras e multifuncionais ligadas 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 a comunicação sejam transmitidas através de fontes fiáveis. Ao contrário do SNMP v1 ou v2, o SNMP v3 é encriptado para maior segurança e requer tanto um nome de utilizador como uma palavra-passe. Uma vantagem de utilizar o SNMP v3 é que os administradores de rede podem determinar o método de encriptação, 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 ligados à rede possui como parte da sua estrutura. A Base de Informações de Gestão (MIB) contém dados como o nome do modelo, os níveis de toner e o estado atual da impressora.

Requisitos do Printanista

Aplicação de backend do Printanista Hub

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

Esta ligação é protegida pelo padrão da indústria **TLS** (Transport Layer Security).

É necessária, no mínimo, a versão 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 à utilização **de eventos enviados pelo servidor** ou **de long polling HTTP**.

NOTA IMPORTANTE: São necessárias várias ligações de saída HTTPS seguras 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 sistema do Printanista Hub

Utilize a seguinte ligação para consultar as especificações completas e atualizadas do sistema do

produto Printanista: [Requisitos do sistema do Printanista Hub v4.0](#)

Requisitos da aplicação Printanista

Agente de Recolha de Dados (ECI DCA)

As impressoras, fotocopiadoras e multifuncionais devem ter o protocolo SNMP (Porta 161) ativado para a deteção e extração de informações. O protocolo SNMP é uma parte padrão da Camada de Aplicação do conjunto TCP/IP.

Requisitos de PC/servidor para o ECI DCA:

Requisitos do Microsoft Windows

(x86/64):

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

Requisitos do Linux (x86/64 ou ARM):

- Mono Framework 5.4 ou superior (recomendado: versão mais recente)
- As configurações da rede local e/ou da firewall permitem [a ligação aos serviços do ECI Updates Server e ao servidor Printanista Hub.](#)
- Apenas o Ubuntu LTS 20.04 e versões posteriores são oficialmente suportadas.

Requisitos para 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 da firewall permitem [a ligação aos serviços do ECI Updates Server 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 no cartão microSD
- As configurações da rede local e/ou do firewall permitem [a ligação aos serviços do Servidor de Atualizações ECI e ao servidor Printanista Hub.](#)

Considerações sobre a firewall para o ECI DCA:

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

Conexões de saída

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

Servidor de atualizações ECI

O ECI Updates Server é um serviço gerido pelo [ECI Device Management](#) para facilitar o registo do DCA, as atualizações automáticas de software e as instalações do DCA (este site), sendo necessário para o funcionamento do ECI DCA. Nota: O ECI DCA não envia quaisquer dados recolhidos sobre dispositivos ou configurações para o ECI Updates Server.

Atualizações de software

O ECI DCA atualiza-se automaticamente através do download de atualizações publicadas em <https://updates.printanista.net/>. As ligações são sempre estabelecidas na porta HTTPS padrão **443/tcp**.

Registo

O ECI DCA utiliza pedidos DNS para `*.reg.pf-d.ca` para se registar. Primeiro, tentará fazê-lo utilizando os servidores DNS da rede local e, em seguida, recorrerá à comunicação direta com os endereços IP do Servidor de Atualizações da ECI (utilizando a porta **53/udp**). A firewall só precisa de permitir esta ligação ao Servidor de Atualizações da ECI se o(s) servidor(es) DNS local(is) não resolver(em) 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.

Dados recolhidos e encriptação

Encriptação de dados

Todos os pacotes de dados do ECI DCA e do Onsite DCA antigo são codificados e ofuscados. O Printanista requer a utilização de HTTPS para a comunicação entre os DCA e o Printanista Hub. O ECI DCA requer HTTPS para funcionar. Além disso, todas as configurações e trabalhos sensíveis entre o ECI DCA e o Printanista são encriptados utilizando o algoritmo de encriptação simétrica padrão AES256, com uma chave partilhada protegida. Isto garante uma encriptação de ponta a ponta, de modo que os dados ficam protegidos contra a leitura caso sejam interceptados por terceiros, por uma instância concorrente ou por qualquer outra instância não autorizada do Printanista.

Questões de segurança

O ECI DCA e o Onsite DCA legado comunicam com o Printanista Hub através do protocolo HTTPS, utilizando o padrão da indústria **TLS 1.2** (Transport Layer Security). Os dados confidenciais não são recolhidos, visualizados ou guardados por nenhuma aplicação Printanista. Apenas são recolhidos e visualizados dados relacionados com a impressora. 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 anfitrião.

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 o utilizador 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 legado permitem-lhe monitorizar dispositivos de rede utilizando 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, 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 (Base de Informações de Gestão) privadas, mas as informações são fundamentalmente técnicas e específicas do dispositivo.

O Printanista Hub armazena apenas:

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

Outras informações de rede/ambiente são recolhidas e apresentadas enquanto se está ligado para fins de resolução de problemas, mas nunca são armazenadas no Printanista.

Tipos de informações recolhidas

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

Atributos do dispositivo

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

Assistência

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

Consumíveis

- Número de série do cartucho de toner
- Nível de toner do cartucho
- Níveis do tambor
- Níveis do kit de manutenção
- Níveis de consumíveis não relacionados com o toner
- Níveis diversos
- Detalhes de consumíveis para impressoras com etiquetas

Cobertura e contadores

- Leituras do contador
- Tipo de contador
- Nível de cobertura
- Identificação a preto e branco ou a cores

Detecção de rede e recolha de dados

Para aumentar a eficiência do DCA, apenas quando houver dados novos ou alterados dos dispositivos é que esta informação será enviada para o servidor Printanista Hub. Isto garantirá uma carga mínima na rede e eliminará a frequência de eventuais atrasos no envio de dados dos dispositivos. Além disso, a detecção e a verificação dos dispositivos são agora independentes, para garantir que apenas o endereço IP

(ou nome de host) dos dispositivos previamente detetados que são verificados numa base periódica, em vez de uma verificação completa da rede (esta é concluída inicialmente, periodicamente ou quando determinado por um utilizador administrador).

Isto garantirá que a velocidade de envio de dados dos dispositivos seja o mais atualizada possível. Isto permite que os utilizadores sejam notificados sobre dispositivos problemáticos em poucos minutos ou mesmo segundos em muitas situações. O ECI DCA separa a descoberta de dispositivos de outros tipos de verificação, permitindo-lhe definir intervalos de verificação personalizados para recuperar contadores, atributos de consumíveis e erros. Os valores padrão, mínimo e máximo para os intervalos de verificação são:

| Função de verificação | Padrão | Mínimo | Máximo |
|-----------------------|------------|------------|---------|
| Detecção | 60 minutos | 10 minutos | 7 dias |
| Metros | 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 |

Tenha em atenção que os intervalos de verificação (medidores, consumíveis, erros e atributos) só estão disponíveis se um dispositivo tiver um Ficheiro de Definição de Modelo (MDF). Se este não estiver presente, será realizada uma verificação completa no dispositivo em questão utilizando um intervalo predefinido.

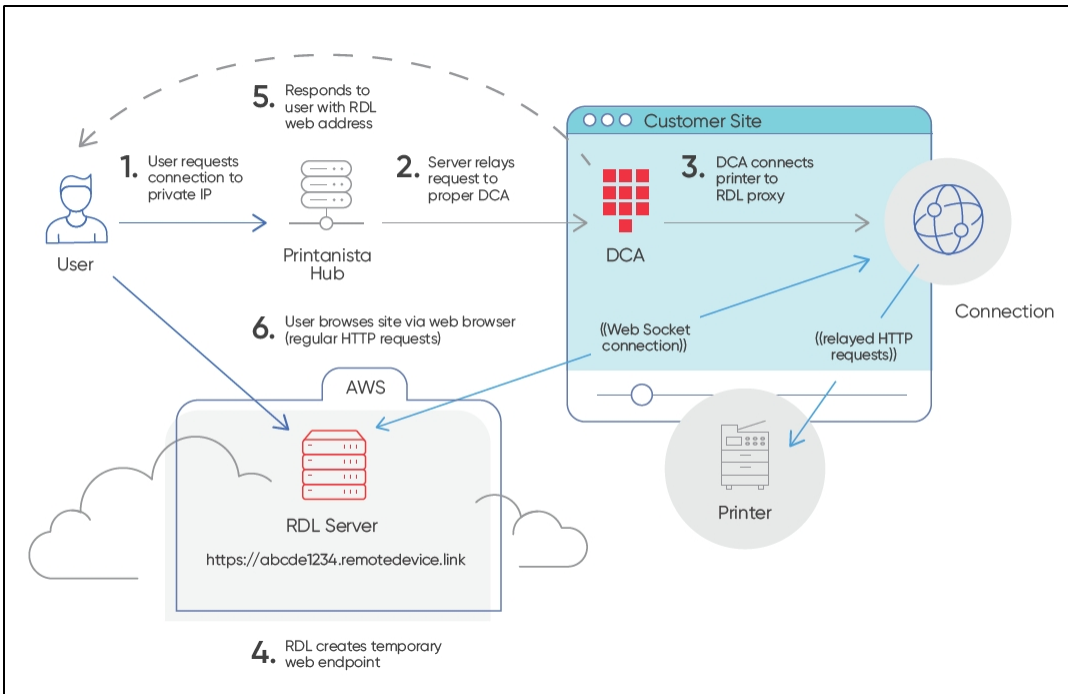
Os administradores do Printanista Hub podem gerir remotamente os ECI DCA que tenham sido ativados no servidor. Podem acionar remotamente o ECI DCA para executar comandos predefinidos, tais como tarefas de recolha de dados, fornecimento de registos do ECI DCA, execução de MIB Walks remotos ou atualização das definições do 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 relativas ao contador, aos consumíveis ou aos erros são atualizadas ou alteradas, reduzindo assim a utilização da largura de banda.

Nota: O HP JAMC só funciona com o Onsite DCA antigo neste momento.

Ligação de Dispositivos Remotos (RDL)



Visão geral do sistema – Ligação de dispositivo remoto (RDL)

O Remote Device Link (RDL) é um serviço que permite a um **utilizador final** remoto aceder a um ponto de extremidade HTTP numa LAN privada. Compõe-se de 4 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 de extremidade HTTP** (impressora) a ser acedido (em execução na LAN privada)

Segurança: Portas e SSL (Secure Sockets Layer)

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

Ativação e permissões

1. Opção de ativação global por instância de revendedor
2. Ativação local para cada conta de cliente final
3. São necessárias permissões para que um utilizador possa aceder à funcionalidade

Capacidades de auditoria

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

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 no Printanista Hub para aceder à funcionalidade Remote Device Link (RDL) na conta específica
- O Data Collection Agent (DCA) só aceitará pedidos do Remote Device Link (RDL) provenientes do servidor do Printanista Hub, que é autenticado mutuamente
- O Agente de Recolha de Dados (DCA) apenas estabelece uma ligação Remote Device Link (RDL) com dispositivos de impressão conhecidos e atualmente monitorizados dentro do(s) intervalo(s) de IP de deteção do Agente de Recolha de Dados (DCA).
- Cada pedido web individual deve ser direcionado 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)
- A cada ligação é atribuído um nome de domínio único que utiliza uma combinação aleatória alfanumérica 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 por encriptação TLS
- O Agente de Recolha de Dados (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 o fizer

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 de confiança para ser utilizada através de 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, caso o dispositivo não suporte 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 web do Printanista Hub é controlado através de uma gestão de utilizadores baseada em permissões. Os utilizadores devem iniciar sessão no Printanista utilizando um nome de utilizador e uma palavra-passe específicos. Aos utilizadores são atribuídas uma ou mais funções que especificam as permissões, sendo-lhes concedido acesso a um ou mais grupos de dispositivos. Os administradores com permissões totais podem especificar exatamente quais as páginas que cada utilizador pode visualizar e/ou com as quais pode interagir.

Acesso HTTPS

O Printanista exige que todos os sites utilizem HTTPS com um certificado de segurança SSL válido. Isto garante a encriptação dos dados transferidos através da Internet.

Printanista Side-By-Side

O Printanista Hub utiliza uma base de dados de metadados de modelos conhecida como Side-by-Side (SBS), que contém vários atributos de modelos, tais como: velocidades de impressão, data de lançamento no mercado ou compatibilidades de números de peça OEM, sendo atualizada periodicamente à medida que novos modelos e versões são lançados pelos OEMs. O Printanista Hub comunica com o Side-by-Side para verificar se existem novas atualizações, bem como para recuperar metadados de dispositivos e armazená-los em cache localmente em cada sistema Printanista Hub.

Alojamento da aplicação Printanista Hub

O Printanista Hub é alojado pela ECI Software Solutions em centros de dados seguros e protegidos em diferentes regiões do mundo. A ECI Software Solutions compreende que a confidencialidade, a integridade e a 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, os nossos sistemas e os nossos processos, de modo a responder às crescentes exigências e desafios em matéria de segurança.

Centros de Dados Seguros da ECI

O nosso serviço está alojado em espaços dedicados em centros de dados de primeira linha. Estas instalações oferecem suporte ao nível das operadoras. Clique na ligação seguinte para obter o documento detalhado da ECI relativo à segurança dos centros de dados

[Visão geral da segurança na nuvem da ECI](#)

Gestão de Versões Processo de

Teste e Lançamento d

Cada lançamento principal e secundário do software passa por um processo de controlo de qualidade, no qual vários membros da equipa da Printanista realizam testes de regressão nas partes alteradas do sistema para garantir que não houve uma redução na segurança ou na funcionalidade do sistema, bem como para validar os novos aspetos 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 revisões seguro, acessível apenas a pessoas autorizadas. Cada alteração ao 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 as efetuou e o motivo. Os produtos são encriptados e assinados digitalmente com um certificado de assinatura de código fiável antes do envio. Pode ser disponibilizado um depósito em garantia, mediante solicitação.

A ECI contrata uma entidade terceira independente líder no setor, certificada pela CREST, SOC 2, NSA-CIRA e CSA-STAR, para realizar testes de penetração ao nível da aplicação e corrigir as falhas detetadas com base nos seus requisitos de negócio 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 consiste em envidar esforços comercialmente razoáveis para corrigir todas as falhas críticas no prazo de 30 dias ou num prazo razoável, com um caso de negócio apresentado. A ECI não divulga detalhes relativos aos nossos controlos de segurança ou aos resultados dos testes de penetração, uma vez que essa informação é proprietária e confidencial e, nas mãos erradas, pode conduzir a um aumento do risco.

Privacidade de dados e legislação

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 na íntegra. O RGPD substituiu a Diretiva 95/46/CE relativa à proteção de dados e visa reforçar e unificar as leis de privacidade de dados em toda a Europa.

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

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

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

A Printanista não tem qualquer forma de aceder, armazenar ou transmitir informações de alto risco, mesmo que essas informações sejam impressas ou enviadas de outra forma para dispositivos de impressão monitorizados pelas aplicações 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, através de acesso limitado a endereços IP e/ou intervalos de endereços específicos.

Todas as comunicações devem ter origem nos produtos Printanista, e não há forma de contactar e aceder aos produtos a partir do exterior da rede.

A comunicação fora da rede utiliza um fluxo de dados comprimido e proprietário, enviado através de 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 da ECI.

Segue-se um link para a ECI Cloud Security:

[Visão geral da ECI Cloud Security](#)

Perguntas frequentes (FAQs)

Os produtos Printanista funcionam com proxies de Internet?

Sim, o ECI DCA é compatível com a maioria dos proxies. É necessário configurar as definições do proxy no sistema onde o ECI DCA está instalado e em funcionamento.

Quais são os requisitos mínimos para o Printanista Hub, o ECI DCA e o Onsite?

Consulte a secção [Requisitos da aplicação Printanista](#) neste documento.

Os produtos Printanista são compatíveis com ambientes Mac, Linux ou Raspberry Pi?

Este ECI DCA oferece grandes vantagens em relação ao Onsite DCA sem perder nenhuma funcionalidade, incluindo suporte nativo completo para várias plataformas, como Windows, macOS, Linux e Raspberry Pi. Cada uma com passos de instalação exclusivos, documentação de suporte e equipa de suporte qualificada para estas plataformas. O processo de instalação também foi significativamente melhorado e é 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 alojar 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 abaixo indicadas devem ser incluídas na lista de permissões para garantir a conectividade do ECI DCA.

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

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

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, de acordo com horários predefinidos. Recomenda-se a utilização de sub-redes (intervalos de IP) em vez de IPs fixos. Ao adicionar novos dispositivos à rede, estes serão detetados e incluídos nos resultados da auditoria, limitando a intervenção manual.

Com que marcas de equipamento funciona a monitorização Remote Device Link (RDL)?

Quais são os requisitos para que funcione?

Todas as marcas com uma página web incorporada são detetadas pelo ECI DCA. As informações nas páginas web incorporadas variam consoante o fabricante e o modelo. Os dispositivos locais não apresentam a página web incorporada.

Existem preocupações de segurança adicionais com o Remote Device Link (RDL)?

É estabelecido um canal seguro entre o dispositivo na rede local do cliente e um operador localizado fora dessa rede. O RDL apenas reportará os dispositivos detetados 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, porquê?

Isto é de esperar, uma vez que a ligação tem de ser encaminhada através dos nossos serviços na nuvem. No entanto, o principal fator determinante é a rapidez com que os dispositivos respondem aos pedidos da Interface de Utilizador (UI) Web.

Temos observado dispositivos a responder em décimos de segundo às primeiras tentativas de ligação, sendo que o tempo de resposta é influenciado pela utilização atual ou pelos recursos disponíveis para a Interface do Utilizador (UI).

Que funcionalidades estão disponíveis com o Remote Device Link (RDL)?

Todas as opções às quais o OEM dá acesso através da página web incorporada estão acessíveis através do Remote Device Link (RDL).

É possível desativar a funcionalidade Remote Device Link (RDL)?

Sim, é possível desativar esta funcionalidade por conta.

Também é possível desativar esta funcionalidade por utilizador, permitindo-lhe bloquear o acesso de um utilizador ao Remote Device Link (RDL).

Onde posso obter informações adicionais sobre o Printanista Hub, o ECI DCA, o Onsite DCA antigo, etc.? É possível encontrar informações adicionais no site Printanista da ECI:

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

Informações sobre o Onsite DCA antigo

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 4.1.3 e versões posteriores do Onsite são compatíveis com o Windows Server 2022
- Internet Explorer 11.0 ou mais recente, Chrome, Firefox
- MDAC 2.8 ou superior (normalmente incluído na instalação do Windows)
- JET 4.0 ou superior (normalmente incluído na instalação do Windows)
- Instalado num computador que esteja ligado 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 relativas à firewall de saída (Porta 80 ou 443):

Transmissão de dados:

- [https://\(company_Printanista_FQDN\)/WebServices/Onsite2Service.asmx](https://(company_Printanista_FQDN)/WebServices/Onsite2Service.asmx)
- Aplicação: fmaonsite.exe
- O SOAP sobre HTTP(s) deve ser permitido através do firewall

Requisitos de rede:

O tráfego SNMP (Porta 161) deve ser roteável através da LAN ou WAN (Redes de Área Alargada)

Utilize o ECI DCA se forem necessários os sistemas operativos macOS, Linux ou Raspberry Pi
O Java Onsite antigo 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 a atualização para dispositivos HP)
- A impressora deve suportar a Printer Job Language (PJM) ou a Printer Management Language (PML)
- Remova quaisquer controladores de impressão não utilizados
- O suporte bidirecional do controlador está ativado
- Alterações na Firewall do Windows — Portas 161/33333 de entrada/saída para TCP e UDP

Versões do Windows e do Windows Server suportadas pela Microsoft. As versões que já não são suportadas pela Microsoft não são suportadas pela ECI.

Nota: No caso das versões recentes do sistema operativo que utilizam o modelo de controlador 4 (por exemplo, Windows 10), atualmente só são suportados os fabricantes de equipamento original (OEM) Kyocera e Ricoh, bem como as suas variantes.

Detecção de rede e recolha de dados de contadores e consumíveis (DCA no local)

As configurações de detecção automática de rede patenteadas pela Printanista utilizam uma combinação de algoritmos para identificar os intervalos de rede onde os dispositivos de impressão podem estar localizados e, em seguida, detetar 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 Onsite 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 de MIBWalks remotos, instalação do HP JAMC ou atualização das definições do Onsite. Estes são explicados em mais pormenor abaixo:

| Função | Local | Descrição |
|-----------------------|-------------------------|--|
| Tarefas | Configurações do Onsite | É possível configurar remotamente tarefas para serem executadas de acordo com um horário pré-definido, mas também selecionar tarefas (Cache, Contadores, Consumíveis, Assistência) para serem executadas imediatamente e recolher dados do dispositivo mediante comando. |
| MIB Walks | Configurações no local | É possível indicar determinados endereços IPv4/IPv6/nomes de host dos dispositivos e acionar o Onsite para iniciar imediatamente a recolha das MIB Walks. |
| Registos (Detalhados) | Configurações do Onsite | Pode instruir o Onsite a recolher os registos (Críticos, Erro, Aviso, Detalhes, Depuração) a partir de uma determinada data. |

Nenhum destes comandos leva à recolha de dados para além dos tipos de informação recolhidos conforme descrito acima. Os dados trocados entre o Onsite DCA e o Printanista Hub são encriptados utilizando protocolos de encriptação robustos que estão em conformidade com a norma FIPS. O Onsite recebe atualizações de software seguras a partir dos servidores de atualizações da Printanista.

O Onsite DCA antigo comunica com o Printanista a intervalos predefinidos para determinar se existem ações em fila que ainda não tenham sido executadas. Isto garante que as ações sejam executadas atempadamente.

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 legado no lançamento inicial do Printanista.

Tráfego de rede

As auditorias realizadas pelo software utilizam um sistema inteligente para extrair o mínimo de informação de cada impressora, fotocopiadora ou multifuncional. Ao contrário de produtos semelhantes que enviam um conjunto fixo de consultas (um superconjunto de todas as consultas possíveis) a todos os dispositivos em rede, o Onsite DCA envia apenas as consultas relevantes de acordo com os campos que o dispositivo de destino suporta, sendo que cada consulta a um dispositivo não ultrapassa alguns kilobytes de dados. Para reduzir ainda mais a largura de banda de rede utilizada, o Onsite DCA comunica com um máximo de 20 dispositivos de cada vez. Cada IP dentro dos intervalos configurados será consultado e, se não for recebida qualquer resposta dentro do período de tempo limite configurado, passará para o endereço IP seguinte. Como regra geral, o Printanista recolherá informações sobre aproximadamente 65 000 dispositivos em pouco menos de uma hora.

Suporte aos fabricantes

Os produtos Printanista são independentes do fabricante. 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 sua execução caso a integridade do ficheiro seja comprometida. Isto garante que, caso exista algum vírus, este 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 prestará serviços de suporte exclusivamente para a versão mais recente do Software disponível no mercado, 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.