Document technique Printanista Hub

Version 1.8

Table des matières

ECI fournira des services d'assistance exclusivement pour la dernière version commerciale disponible du logiciel, ainsi que pour la version immédiatement précédente du logiciel. Cette politique s'applique à tous les produits ECI Device Management.

Microsoft®, .NET Framework®, Windows® et Windows Server® sont des marques déposées ou des marques commerciales de Microsoft Corporation.

Présentation

La suite de produits Printanista offre une solution d'impression gérée de classe entreprise très facile à utiliser et à déployer. Elle est conçue et développée pour tirer parti des fonctionnalités avancées et des avantages de la plateforme Microsoft .NET. Ainsi, elle ne nécessite plus l'intervention de techniciens qualifiés pour installer le logiciel, configurer et entretenir le système. Les produits Printanista ne peuvent en aucun cas être configurés pour effectuer une tâche autre que celles pour lesquelles ils ont été conçus. La transmission de données depuis les produits vers des sources externes est strictement limitée. Les produits ne communiquent aucune autre information que celles relatives à l'équipement surveillé (c'est-à-dire le type d'équipement). Aucune information confidentielle n'est jamais transmise hors du réseau via les produits Printanista. La suite comprend les composants suivants :

Printanista Hub : un site web et un système backend hébergeant toutes les données reçues des outils de collecte de données Printanista. Il s'agit d'un référentiel qui vous permet de consulter les données à l'aide d'un navigateur, de générer des rapports, de configurer des workflows d'alerte et des notifications, et de synchroniser les données avec vos systèmes ERP pour la facturation ou l'approvisionnement.

ECI DCA : ce tout nouvel agent de collecte de données (DCA) offre des avantages majeurs par rapport à l'agent de collecte de données sur site (DCA) sans perdre aucune fonctionnalité, notamment la prise en charge native complète des plateformes Windows, macOS, Linux et Raspberry Pi, chacune avec des étapes d'installation, une documentation d'assistance et un personnel d'assistance formé spécifiques à ces plateformes. ECI DCA permet également la détection et l'analyse continues des appareils, une amélioration des capacités de collecte MIBWalk et Log, et la collecte d'un plus grand nombre de types de compteurs.

DCA sur site : un outil DCA traditionnel effectue automatiquement des évaluations d'impression et surveille les niveaux de consommables, l'état des imprimantes et les journaux d'erreurs. Cette application est installée sur le site du client et peut effectuer des évaluations d'impression automatiquement à intervalles réguliers sans intervention humaine. Les données capturées sont envoyées au site web Printanista Hub via HTTPS, HTTP ou, si le client le préfère, via un fichier crypté propriétaire.

L'objectif de ce document est de fournir une présentation technique de la gamme de produits Printanista Suite afin de faciliter les réponses aux questions les plus fréquentes que les équipes informatiques sont amenées à recevoir.

Comment fonctionne Printanista

Printanista Hub est conçu comme une application hébergée

Printanista Hub est hébergé par ECI Software Solutions dans des centres de données sécurisés et protégés situés dans différentes régions du monde. ECI Software Solutions comprend que la confidentialité, l'intégrité et la disponibilité des informations de nos clients sont essentielles à leurs activités commerciales et à notre propre succès. Nous utilisons une approche multicouche pour protéger ces informations clés, en surveillant et en améliorant constamment notre application, nos systèmes et nos processus, afin de répondre aux exigences et aux défis croissants en matière de sécurité.

Centres de données sécurisés ECI

Notre service est hébergé dans des espaces dédiés au sein de centres de données de premier ordre. Ces installations fournissent une assistance de niveau opérateur. Ce lien renvoie vers le document détaillé d'ECI relatif à la sécurité des centres de données.
Présentation de la sécurité du cloud ECI 2021 (ecisolutions.com)

Agent de collecte de données (DCA)

Le moteur central de l'agent de collecte de données, qui est au cœur de chaque produit Printanista, identifie et extrait correctement les données des imprimantes, photocopieurs et multifonctions en réseau en utilisant les protocoles pris en charge par les appareils.

Printanista prend actuellement en charge les protocoles SNMP (Simple Network Management Protocol) v1, v2c et v3. Le protocole SNMP v3 offre une protection accrue des paquets afin de garantir que les informations et les communications sont transmises via des sources fiables. Contrairement aux protocoles SNMPv1 ou v2, le protocole SNMP v3 est crypté pour une sécurité accrue et nécessite à la fois un nom d'utilisateur et un mot de passe. L'un des avantages du protocole SNMP v3 est que les administrateurs réseau peuvent déterminer la méthode de cryptage ainsi qu'un nom d'utilisateur et un mot de passe forts.

SNMP est un protocole réseau qui facilite l'échange d'informations entre les périphériques réseau en extrayant des données de la base d'informations de gestion (MIB) et d'autres emplacements au sein du périphérique d'impression. La base d'informations de gestion (MIB) est une base de données interne dont la plupart des périphériques connectés au réseau sont équipés. La base d'informations de gestion (MIB) contient des données telles que le nom du modèle, les niveaux de toner et l'état actuel de l'imprimante.

Configuration requise pour Printanista

s de l'application Printanista Hub Backend

Toutes les données collectées sont envoyées au serveur Printanista Hub où elles sont mises à disposition pour la création de rapports et l'envoi d'alertes.
ECI DCA se connecte à votre serveur Printanista Hub via HTTPS (port **443/TCP**). Veuillez contacter votre administrateur ECI Solutions pour obtenir des informations sur les noms de domaine et les adresses IP utilisés par votre serveur.

Cette connexion est protégée par le protocole **TLS** (Transport Layer Security) standard.
La version minimale requise est TLS 1.2.

Cette connexion reste ouverte pendant toute la durée d'exécution d'ECI DCA. Normalement, une connexion **WebSocket** est utilisée, mais dans certaines situations, ECI DCA peut revenir à l'utilisation **d'événements envoyés par le serveur** ou **de sondages HTTP longs**.

REMARQUE IMPORTANTE : plusieurs connexions sortantes HTTPS sécurisées sont requises depuis le serveur sur lequel Printanista Hub est installé :

- 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

Application Printanista Exigences

Agent de collecte de données (ECI DCA)

Les imprimantes, photocopieurs et imprimantes multifonctions doivent avoir le protocole SNMP (port 161) activé pour la détection et l'extraction d'informations. Le protocole SNMP est une partie standard de la couche application de la suite TCP/IP.

Configuration requise pour PC/serveur pour ECI DCA :

Configuration requise pour Microsoft Windows (x86/64) :

- Microsoft .NET Framework 4.7.2. ou version plus récente (recommandé : dernière version)
- Versions entièrement publiées et prises en charge par Microsoft de Windows Server (à l'exception des éditions Datacenter et Core) et Windows
  - ➢ *Microsoft qui ne sont plus prises en charge par Microsoft ne sont pas prises en charge par ECI DCA.*
- Les paramètres du réseau local et/ou du pare-feu permettent la connexion aux services ECI Updates Server et au serveur Printanista Hub.

Linux (x86/64 ou ARM) Configuration requise :

- Mono Framework 5.4 ou supérieur (recommandé : dernière version)
- Les paramètres du réseau local et/ou du pare-feu permettent la connexion aux services ECI Updates Server et au serveur Printanista Hub.
- Seuls Ubuntu LTS 20.04 et versions ultérieures sont officiellement pris en charge.

Configuration requise pour macOS (x64) :

- Mono Framework 5.4 ou supérieur (recommandé : dernière version)
- macOS® Sierra (10.12) jusqu'à Sequoia (15.4). Les versions plus récentes ne sont pas prises en charge.
- Les paramètres du réseau local et/ou du pare-feu permettent la connexion aux services du serveur ECI Updates et au serveur Printanista Hub.

Configuration requise pour Raspberry Pi :

- Raspberry Pi 3 modèle B ou Pi 4 Rev 1.5. Les versions plus récentes ne sont pas prises en charge.
- Carte microSD vierge de 8 Go ou plus
- PC capable d'écrire sur une carte microSD
- Les paramètres du réseau local et/ou du pare-feu permettent la connexion aux services ECI Updates Server et au serveur Printanista Hub.

Considérations relatives au pare-feu pour ECI DCA :

Connexions entrantes - Il n'y a pas de connexions entrantes depuis Internet vers ECI DCA.

Connexions sortantes

Service	Port	Connexion vers
Téléchargement de données	**443/TCP** (HTTPS)	Votre serveur Printanista Hub
Mises à jour logicielles	**443/TCP** (HTTPS)	Serveur de mises à jour ECI
Enregistrement (secours)	**53/UDP** (DNS)	Serveur DNS du réseau local (principal) Serveur de mises à jour ECI (secours)

Serveur de mises à jour ECI

Le serveur de mises à jour ECI est un service géré par ECI Device Management afin de faciliter l'enregistrement DCA, les mises à jour logicielles automatiques et les installations DCA (ce site). Il est nécessaire au fonctionnement de l'ECI DCA. Remarque : l'ECI DCA n'envoie aucune donnée collectée sur les appareils ou les configurations au serveur de mises à jour ECI.

Mises à jour logicielles

ECI DCA se met à jour automatiquement en téléchargeant les mises à jour publiées sur https://updates.printanista.net/ . Les connexions sont toujours établies sur le port HTTPS standard **443/tcp**.

Enregistrement

ECI DCA utilise des requêtes DNS vers `*.reg.pf-d.ca` pour s'enregistrer. Il essaie d'abord d'utiliser les serveurs DNS du réseau local, puis se rabat sur les adresses IP du serveur de mises à jour ECI (en utilisant le port **53/udp**). Le pare-feu doit uniquement autoriser cette connexion au serveur de mises à jour ECI si le ou les serveurs DNS locaux ne résolvent pas les requêtes d'enregistrement.

Région de service

ECI DCA est acheminé vers la région où la latence réseau est la plus faible et en fonction de la disponibilité du service. Dans certains endroits, la région utilisée peut changer au fil du temps, car l'activité sur l'infrastructure Internet mondiale peut affecter la latence.

Données collectées et cryptage de l'

Chiffrement des données

Tous les paquets de données provenant de l'ECI DCA et de l'ancien Onsite DCA sont cryptés et obscurcis. Printanista nécessite l'utilisation du protocole HTTPS pour la communication entre les DCA et le hub Printanista. ECI DCA nécessite HTTPS pour fonctionner. De plus, tous les paramètres et tâches sensibles entre ECI DCA et Printanista sont cryptés à l'aide de l'algorithme de cryptage symétrique standard AES256, à l'aide d'une clé partagée protégée. Cela garantit un cryptage de bout en bout, de sorte que les données sont protégées contre toute lecture si elles sont interceptées par un tiers, un concurrent ou une instance Printanista non autorisée.

Importance de l' s de sécurité

ECI DCA et l'ancienne version Onsite DCA communiquent avec Printanista Hub via le protocole HTTPS, en utilisant la norme industrielle **TLS 1.2** (Transport Layer Security). Les données confidentielles ne sont ni collectées, ni consultées, ni enregistrées par aucune application Printanista. Seules les données relatives à l'imprimante sont collectées et consultées. Aucune autre donnée réseau ne peut être identifiée ou collectée par ECI DCA ou l'ancienne version Onsite DCA, à l'exception de l'adresse IP, de l'adresse MAC et du nom d'hôte.

ECI DCA et l'ancienne version Onsite DCA ne collectent ni ne traitent aucune donnée personnelle. Le système ne collecte ce type d'informations que si vous ou vos clients saisissez les données dans Printanista dans un champ ou une étiquette tel que l'emplacement ou le nom du client. ECI DCA et l'ancienne version Onsite DCA vous permettent de surveiller les périphériques réseau à l'aide du protocole SNMP (Simple Network Management Protocol). L'application est déployée au sein du réseau du client et, à partir de là, elle communique avec les périphériques afin de recueillir des informations opérationnelles sur le périphérique, qui sont mises à disposition via le micrologiciel du périphérique et une base d'informations de gestion SNMP (MIB). Les données exposées par le périphérique varient selon le fabricant et le modèle. Elles sont toujours de nature technique ou opérationnelle et spécifiques au périphérique lui-même. Au niveau le plus élémentaire, les données exposées par la MIB d'une imprimante sont documentées dans la norme IETF RFC 3805 (https://tools.ietf.org/html/rfc3805). Des informations supplémentaires sur le périphérique peuvent être exposées par le fabricant via des extensions et des MIB (Management Information Base) privées, mais ces informations sont fondamentalement techniques et spécifiques au périphérique.

Printanista Hub stocke uniquement :

- Nom d'hôte
- Système d'exploitation
- Adresse IP distante
- Architecture du système

D'autres informations relatives au réseau/à l'environnement sont collectées et affichées pendant la connexion à des fins de dépannage, mais ne sont jamais stockées dans Printanista.

Types d'informations collectées par l'

ECI DCA et l'ancien Onsite DCA tentent de collecter les informations suivantes à partir des périphériques d'impression en réseau lors d'une analyse du réseau :

Attributs du périphérique

- Adresse IP (peut être masquée)
- Fabricant
- Numéro de série
- Numéro d'inventaire
- Adresse MAC
- Description de l'appareil
- Emplacement
- Divers (spécifique à la machine)

Service

- Lecture LCD
- État de l'appareil
- Codes d'erreur
- Micrologiciel

Consommables

- Numéro de série de la cartouche de toner
- Niveau de remplissage de la cartouche de toner
- Niveaux du tambour
- Niveaux du kit d'entretien
- Niveaux d'approvisionnement en produits autres que le toner
- Niveaux divers
- Détails de l'approvisionnement des imprimantes à étiquettes

Couverture et compteurs

- Lectures des compteurs
- Type de compteur
- Niveau de couverture
- Identification monochrome ou couleur

Détection du réseau et collecte de données

Pour améliorer l'efficacité du DCA, seules les données nouvelles ou modifiées provenant des appareils seront envoyées au serveur Printanista Hub. Cela permettra de réduire au minimum la charge réseau et d'éliminer la fréquence des retards dans la soumission des données des appareils. De plus, la découverte et l'analyse des appareils sont désormais indépendantes afin de garantir que seule l'adresse IP
(ou nom d'hôte) des appareils précédemment détectés sont analysés à intervalles réguliers, par opposition à une analyse complète du réseau (celle-ci est effectuée initialement, périodiquement ou lorsque l'administrateur le juge nécessaire).

Cela garantit que la vitesse de soumission des données des appareils est aussi à jour que possible. Cela permet aux utilisateurs d'être informés des appareils problématiques en quelques minutes, voire quelques secondes dans de nombreuses situations. ECI DCA sépare la détection des appareils des autres types d'analyse, ce qui vous permet de définir des intervalles d'analyse personnalisés pour récupérer les compteurs, les attributs des fournitures et les erreurs. Les valeurs par défaut, minimales et maximales pour les intervalles d'analyse sont les suivantes :

Fonction d'analyse	Par défaut	Minimum	Maximum
Détection	60 minutes	10 minutes	7 jours
Compteurs	24 heures	30 minutes	14 jours
Fournitures	4 heures	30 minutes	7 jours
Erreurs	60 minutes	30 minutes	7 jours
Attributs	24 heures	1 heure	14 jours

Veuillez noter que les intervalles d'analyse (compteurs, fournitures, erreurs et attributs) ne sont disponibles que si un périphérique dispose d'un fichier de définition de modèle (MDF). Si ce fichier n'est pas présent, une analyse complète sera effectuée sur le périphérique en question à l'aide d'un intervalle prédéfini.

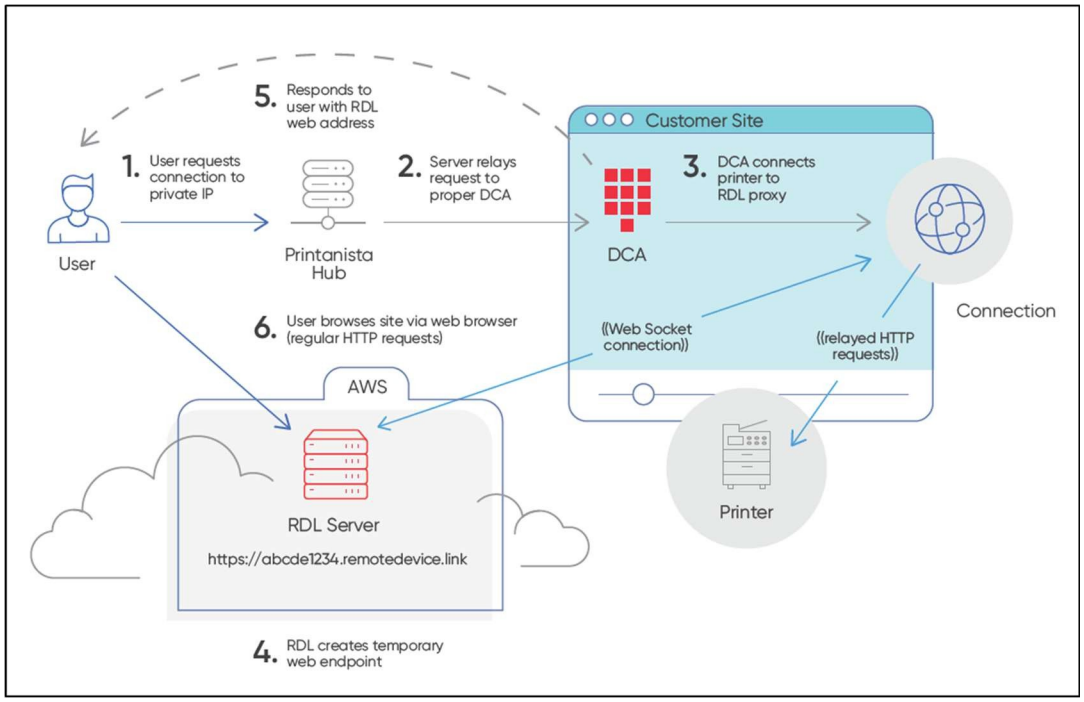
Les administrateurs Printanista Hub peuvent gérer à distance les ECI DCA qui ont été activés sur le serveur. Ils peuvent déclencher à distance l'ECI DCA pour exécuter des commandes prédéfinies telles que des tâches de collecte de données, fournir des journaux ECI DCA, exécuter des MIB Walks à distance ou mettre à jour les paramètres ECI DCA.

Remarque : l'ECI DCA initie toujours la communication avec le serveur Printanista, et non l'inverse.

Remarque : la communication n'a lieu que lorsque les informations relatives au compteur, à l'approvisionnement ou aux erreurs ont été mises à jour ou modifiées, ce qui réduit l'utilisation de la bande passante.

Remarque : HP JAMC ne fonctionne actuellement qu'avec l'ancien DCA sur site.

s sur la liaison à distance (RDL)



Présentation du système – s sur la liaison à distance (RDL)

Remote Device Link (RDL) est un service permettant à un **utilisateur final** distant d'accéder à un point de terminaison HTTP sur un réseau local privé. Il comprend 4 composants principaux :

1. **L'utilisateur final** qui accède au périphérique
2. Le **serveur Remote Device Link**, sur l'Internet public (via l'URL https://*.remotedevice.link)
3. Le **client RDL** (intégré au DCA), fonctionnant sur le réseau local privé
4. Le **point de terminaison HTTP** (imprimante) auquel on accède (fonctionnant sur le réseau local privé)

Sécurité : ports et SSL (Secure Sockets Layer)

Le chemin d'accès public pour RDL est toujours une URL https:// sur le port 443, quel que soit le port du point de terminaison et/ou le statut SSL.

Autorisations d'activation et d'

1. Option d'activation globale par instance de revendeur
2. Activation locale pour chaque compte client final
3. Des autorisations sont requises pour qu'un utilisateur puisse accéder à la fonctionnalité

Capacités d'audit d'

1. Audit local de Printanista Hub pour chaque détail de session
    a. Rapports d'administration Printanista Hub pour l'audit des liens vers des périphériques distants (RDL)
2. Remote Device Link (RDL) Journalisation dans le cloud AWS (Amazon Web Services) de tous les détails de session

Sécurité de l' Remote Device Link (RDL)

La sécurité de Remote Device Link (RDL) a été une préoccupation majeure lors du

développement de cet outil. Autorisation :

- L'utilisateur doit disposer d'une autorisation dans Printanista Hub pour accéder à la fonctionnalité Remote Device Link (RDL) sur le compte spécifique.
- L'agent de collecte de données (DCA) n'acceptera que les demandes de liaison à distance avec un périphérique (RDL) provenant du serveur Printanista Hub qui est mutuellement authentifié.
- L'agent de collecte de données (DCA) établit uniquement une connexion Remote Device Link (RDL) avec les périphériques d'impression connus et actuellement surveillés dans la ou les plages d'adresses IP de découverte des agents de collecte de données (DCA).
- Chaque requête Web individuelle doit être adressée à la même adresse IP. L'agent de collecte de données (DCA) ne suivra pas les redirections.

Sécurité de la connexion :

- Toutes les connexions vers et depuis les serveurs Remote Device Link (RDL) et Printanista Hub sont cryptées à l'aide de la version minimale standard TLS 1.2 (Transport Layer Security).
- Chaque connexion se voit attribuer un nom de domaine unique composé d'une combinaison aléatoire de 19 caractères alphanumériques (96 bits).
- Chaque requête nécessite un jeton de sécurité de 160 bits, stocké sous forme de cookie de navigateur, et uniquement défini au tout début de la session sécurisée par le cryptage TLS.
- L'agent de collecte de données (DCA) peut établir une connexion HTTP non cryptée avec le périphérique d'impression sur le réseau local, mais prend en charge la version minimale TLS 1.2 si le périphérique le permet.

Limites de durée de session :

- Chaque session Remote Device Link (RDL) expire après 20 minutes d'inactivité par défaut, avec un maximum absolu de 2 heures.

Implications

La connexion entre ECI DCA et Printanista Hub est protégée par des clés d'authentification spécifiques à l'installation DCA, et la connexion nécessite un certificat SSL valide et fiable pour être utilisée sur une connexion TLS.

Tout le trafic transitant entre le DCA et Internet est crypté. Cependant, l'ECI DCA peut communiquer avec l'appareil du réseau local via des connexions HTTP simples si l'appareil ne prend pas en charge les connexions sécurisées.

Application d' s Printanista Hub

Les fonctionnalités de Printanista Hub sont accessibles via une interface utilisateur Web. Gestion

des utilisateurs basée sur les autorisations

L'accès à l'interface Web Printanista Hub est contrôlé par une gestion des utilisateurs basée sur des autorisations. Les utilisateurs doivent se connecter à Printanista à l'aide d'un nom d'utilisateur et d'un mot de passe désignés. Les utilisateurs se voient attribuer un ou plusieurs rôles qui spécifient leurs autorisations et ont accès à un ou plusieurs groupes d'appareils. Les administrateurs disposant d'une autorisation complète peuvent spécifier exactement les écrans que chaque utilisateur peut afficher et/ou avec lesquels il peut interagir.

Accès HTTPS

Printanista exige que tous les sites utilisent le protocole HTTPS avec un certificat de sécurité SSL valide. Cela garantit le cryptage des données transférées sur Internet.

Printanista Side-By-Side

Printanista Hub utilise une base de données de métadonnées de modèles appelée Side-by-Side (SBS), qui contient divers attributs de modèles tels que : les vitesses d'impression, la date de mise sur le marché ou les compatibilités des numéros de pièces OEM, qui sont régulièrement mis à jour à mesure que les OEM lancent de nouveaux modèles et versions. Printanista Hub communique avec Side-by-Side pour vérifier les nouvelles mises à jour et récupérer les métadonnées des appareils afin de les mettre en cache localement sur chaque système Printanista Hub.

Hébergement de l'application Printanista Hub

Printanista Hub est hébergé par ECI Software Solutions dans des centres de données sécurisés et protégés situés dans différentes régions du monde. ECI Software Solutions comprend que la confidentialité, l'intégrité et la disponibilité des informations de nos clients sont essentielles à leurs activités commerciales et à notre propre succès. Nous utilisons une approche multicouche pour protéger ces informations clés, en surveillant et en améliorant constamment nos applications, nos systèmes et nos processus, afin de répondre aux exigences et aux défis croissants en matière de sécurité.

Centres de données sécurisés ECI

Notre service est hébergé dans des espaces dédiés au sein de centres de données de premier ordre. Ces installations fournissent une

assistance de niveau opérateur. Cliquez sur le lien suivant pour obtenir le document détaillé d'ECI relatif à la sécurité des centres de

données

[Présentation de la sécurité du cloud ECI 2021 (ecisolutions.com)]

Processus de test et de publication de la gestion des versions

Chaque version majeure et mineure du logiciel est soumise à un processus de contrôle qualité, au cours duquel plusieurs membres du personnel de Printanista effectuent des tests de régression sur les parties modifiées du système afin de s'assurer qu'il n'y a pas eu de dégradation de la sécurité ou des fonctionnalités du système, et de valider les nouvelles fonctionnalités. Les versions majeures sont soumises à un processus de version bêta au cours duquel certains clients sélectionnés exécutent les nouveaux et anciens systèmes en parallèle.

Sécurité du code source

Le code source de Printanista est conservé dans un système de contrôle de révision sécurisé, accessible uniquement aux personnes autorisées. Chaque modification apportée au code source doit être approuvée par deux développeurs autorisés avant d'être acceptée dans le référentiel de code de production, où chaque modification est suivie, y compris le nom du développeur qui a effectué la modification et la raison de celle-ci. Les produits sont cryptés et signés numériquement à l'aide d'un certificat de signature de code fiable avant leur expédition. Un dépôt fiduciaire peut être mis à disposition sur demande.

ECI fait appel à un tiers indépendant certifié CREST, SOC 2, NSA-CIRA et CSA-STAR, leader dans son secteur, pour effectuer des tests de pénétration au niveau des applications et corriger les résultats en fonction de ses exigences commerciales et de son cadre interne de gestion des risques. Les tests de pénétration sont effectués au moins une fois par an ou lorsque des modifications importantes sont apportées au système. La politique d'ECI consiste à déployer des efforts commercialement raisonnables pour remédier à toutes les conclusions critiques dans un délai de 30 jours ou dans un délai raisonnable avec une analyse de rentabilité fournie. ECI ne divulgue pas les détails concernant ses contrôles de sécurité ou les résultats des tests de pénétration, car ces informations sont exclusives et confidentielles et, entre de mauvaises mains, peuvent entraîner un risque accru.

Législation sur la confidentialité et l' des données

générale sur la protection des données (RGPD)

Depuis mai 2018, le Règlement général sur la protection des données (RGPD) de l'Union européenne est pleinement entré en vigueur. Le RGPD remplace la directive 95/46/CE sur la protection des données et vise à renforcer et à harmoniser les lois sur la confidentialité des données à travers l'Europe.

ECI a mis en place un programme structuré et complet de conformité au RGPD. Ce programme comprend, entre autres, la formation du personnel, l'audit et l'évaluation des risques dans l'ensemble de l'entreprise, les politiques et procédures, la gouvernance et les efforts continus en matière de conformité. Nous encourageons nos clients à prendre des mesures similaires afin de garantir la conformité de leur propre entreprise au RGPD pour les années à venir.

Les produits Printanista ne traitent, ne surveillent ni ne gèrent aucun dossier personnel ni aucune information spécifique à une personne ou à un groupe de personnes.

Les applications logicielles Printanista ne collectent, ne stockent ni ne transmettent aucune information concernant le contenu des travaux d'impression.

Printanista n'a aucun moyen d'accéder, de stocker ou de transmettre des informations à haut risque, même si ces informations sont imprimées ou envoyées à des périphériques d'impression surveillés par les applications logicielles Printanista.

Les applications logicielles Printanista ne stockent, ne traitent ni ne transmettent les données des titulaires de cartes ou les informations personnelles.

Les communications du moteur du produit sont contrôlées, avec un accès limité à des adresses IP et/ou plages d'adresses IP spécifiques.

Toutes les communications doivent provenir des produits Printanista, et il n'est pas possible de contacter et d'accéder aux produits depuis l'extérieur du réseau.

Les communications en dehors du réseau utilisent un flux de données compressé propriétaire qui est envoyé à l'aide du protocole SSL standard via HTTPS.

Pour plus d'informations sur la conformité à des lois et/ou réglementations spécifiques, veuillez contacter votre responsable de compte ECI.

Voici un lien vers la sécurité cloud ECI : [Présentation de la sécurité cloud ECI 2021 (ecisolutions.com)]

Foire aux questions (FAQ)

Les produits Printanista fonctionnent-ils avec les proxys Internet ?
Oui, ECI DCA fonctionne avec la plupart des proxys. La configuration des paramètres du proxy est requise sur le système où ECI DCA est installé et fonctionne.
Quelles sont les configurations minimales requises pour Printanista Hub, ECI DCA et Onsite ?
Veuillez vous reporter à la section Configuration requise pour l'application Printanista de ce document.

Les produits Printanista sont-ils compatibles avec les environnements Mac, Linux ou Raspberry Pi ?
Cette ECI DCA offre des avantages majeurs par rapport à la DCA sur site sans perdre aucune fonctionnalité, notamment la prise en charge native complète des plateformes Windows, macOS, Linux et Raspberry Pi. Chacune dispose de procédures d'installation uniques, d'une documentation d'assistance et d'un personnel d'assistance formé sur ces plateformes. Le processus d'installation a également été considérablement amélioré et est beaucoup plus intuitif pour tous les types d'utilisateurs.

ECI DCA nécessite-t-il Microsoft Internet Information Services (IIS) ?
Non. ECI DCA et Onsite DCA comprennent leur propre serveur pour héberger l'interface utilisateur (UI) basée sur le Web et sont configurés automatiquement lors de l'installation.

Pouvez-vous installer ECI DCA sur un ordinateur qui héberge déjà un autre site web IIS ?
Oui. Cependant, les ports répertoriés ci-dessous doivent être ajoutés à la liste blanche afin de garantir la connectivité de l'ECI DCA.

Service	Port	Connexion vers
Téléchargement de données	**443/TCP** (HTTPS)	Votre serveur Printanista Hub
Mises à jour logicielles	**443/TCP** (HTTPS)	Serveur de mises à jour ECI
Enregistrement (secours)	**53/UDP** (DNS)	Serveur DNS du réseau local (principal) Serveur de mises à jour ECI (secours)

ECI DCA utilise par défaut le port 31816 pour l'interface utilisateur Web DCA locale.

Quelle est la fréquence de maintenance requise pour ECI DCA ?
ECI DCA et Onsite DCA sont des services qui s'exécutent en arrière-plan et effectuent des audits et des exportations vers des destinations configurées selon des calendriers prédéfinis. Il est recommandé d'utiliser des sous-réseaux (plages d'adresses IP) plutôt que des adresses IP fixes. Lorsque de nouveaux appareils sont ajoutés au réseau, ils sont détectés et inclus dans les résultats de l'audit, ce qui limite les interventions manuelles.

Avec quelles marques d'équipements la surveillance Remote Device Link (RDL) est-elle compatible ? Quelles sont les conditions requises pour qu'elle fonctionne ?
Toutes les marques disposant d'une page Web intégrée sont détectées par ECI DCA. Les informations contenues dans les pages Web intégrées varient selon le fabricant et le modèle. Les appareils locaux n'affichent pas la page Web intégrée.

La fonction Remote Device Link (RDL) pose-t-elle des problèmes de sécurité supplémentaires ?
Un canal sécurisé est ouvert entre l'appareil sur le réseau local du client et un opérateur situé en dehors de ce réseau. RDL ne signalera que les appareils détectés et activement surveillés via ECI DCA. Un message s'affiche indiquant que la connexion de l'appareil n'est pas prise en charge via le DCA.

Le Remote Device Link (RDL) semble un peu lent, pourquoi ?
Cela est normal, car la connexion doit passer par nos services cloud. Cependant, le principal facteur qui influence la vitesse est la rapidité avec laquelle les appareils répondent aux requêtes de l'interface utilisateur Web (UI).
Nous avons constaté que les appareils répondaient en quelques dixièmes de seconde aux premières tentatives de connexion, mais qu'ils étaient influencés par l'utilisation actuelle ou les ressources disponibles pour l'interface utilisateur (UI).

Quelles sont les fonctionnalités disponibles avec Remote Device Link (RDL) ?
Toutes les options auxquelles le constructeur donne accès via la page Web intégrée sont accessibles via Remote Device Link (RDL).

La fonctionnalité Remote Device Link (RDL) peut-elle être désactivée ?
Oui, il est possible de désactiver cette fonctionnalité pour chaque compte.
Il est également possible de désactiver cette fonctionnalité par utilisateur, ce qui vous permet de bloquer l'accès d'un utilisateur à Remote Device Link (RDL).

Où puis-je obtenir des informations supplémentaires sur Printanista Hub, ECI DCA, l'ancienne version Onsite DCA, etc. ? Vous trouverez des informations supplémentaires sur le site Web Printanista de l'ECI : https://www.ecisolutions.com/products/printanista-hub/

Informations sur l'ancien Onsite DCA

Il est recommandé d'utiliser ECI DCA avec Printanista. Cependant, l'ancienne version Onsite DCA fonctionne actuellement avec Printanista.
Configuration requise pour PC/serveur pour Onsite DCA :

- 1 Go de RAM
- 400 Mo d'espace disque
- Microsoft .NET Framework 4.7.2 ou version plus récente
- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- La version 4.1.3 et les versions plus récentes prennent en charge Windows Server 2022.
- Internet Explorer 11.0 ou version ultérieure, Chrome, Firefox
- MDAC 2.8 ou version ultérieure (généralement inclus lors de l'installation de Windows)
- JET 4.0 ou version ultérieure (généralement inclus lors de l'installation de Windows)
- Installé sur un ordinateur fonctionnant 24 heures sur 24, 7 jours sur 7, ou au moins pendant toute la journée ouvrable
- Vous devez être connecté en tant qu'administrateur local (ou équivalent) pendant l'installation

Considérations relatives au pare-feu sortant (port 80 ou 443) :

Transmission de données :

- https://(company_Printanista_FQDN)/WebServices/Onsite2Service.asmx
- Application : fmaonsite.exe
- SOAP sur HTTP(s) doit être autorisé à passer le pare-feu

Exigences réseau :

Le trafic SNMP (port 161) doit être routable sur le réseau local ou le réseau étendu (WAN).

Veuillez utiliser ECI DCA si les systèmes d'exploitation macOS, Linux ou Raspberry Pi sont nécessaires. L'ancienne version Java Onsite sur les systèmes Linux et macOS n'est pas fonctionnelle.

Configuration requise pour le PC/l'imprimante afin d'utiliser l'agent local (installation facultative) :

- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- Microsoft .NET Framework 4.7.2 ou version plus récente
- Pilote actuel pour l'imprimante locale (UPD recommandé pour les périphériques HP)
- L'imprimante doit prendre en charge le langage PJL (Printer Job Language) ou PML (Printer Management Language).
- Supprimez tous les pilotes d'impression inutilisés.
- La prise en charge bidirectionnelle du pilote est activée.
- Modifications du pare-feu Windows — Port 161/33333 entrant/sortant pour TCP et UDP *Versions de Windows et Windows Server prises en charge par Microsoft. Les versions qui ne sont plus prises en charge par Microsoft ne sont pas prises en charge par ECI.*

Remarque : pour les versions récentes du système d'exploitation utilisant le modèle de pilote 4 (par exemple, Windows 10), seuls les OEM Kyocera et Ricoh, ainsi que leurs variantes, sont actuellement pris en charge.

Détection du réseau et collecte des compteurs et des fournitures (DCA sur site)

Les paramètres de détection automatique du réseau brevetés par Printanista utilisent une combinaison d'algorithmes pour identifier les plages réseau où les périphériques d'impression peuvent se trouver, puis détecter et communiquer avec les périphériques en ligne, en passant par plusieurs éléments du réseau tels que les postes de travail ou serveurs actifs, les routeurs, les concentrateurs, les commutateurs et d'autres matériels réseau.

Les administrateurs du hub Printanista peuvent gérer à distance les agents de collecte de données (DCA) activés sur le serveur et déclencher à distance l'exécution de commandes prédéfinies telles que des tâches de collecte de données, la fourniture de journaux sur site, l'exécution de MIBWalks à distance, l'installation de HP JAMC ou la mise à jour des paramètres sur site. Ces opérations sont expliquées plus en détail ci-dessous :

Fonction	**Emplacement**	**Description**
Tâches	Paramètres Onsite	Permet de configurer à distance des tâches à exécuter selon un calendrier prédéfini, mais permet également de sélectionner des tâches (cache, compteurs, fournitures, service) à exécuter immédiatement et de collecter les données des appareils sur commande.
MIB Walks	Paramètres sur site	Permet d'indiquer certains noms d'hôtes/IPv4/IPv6 d'appareils et de déclencher immédiatement la collecte des MIB Walks par Onsite.
Journaux (détaillés)	Paramètres sur site	Peut demander à Onsite de collecter les journaux (critiques, erreurs, avertissements, détails, débogage) à partir d'une certaine date.

Aucune de ces commandes n'entraîne la collecte de données au-delà des types d'informations collectées décrits ci-dessus. Les données échangées entre Onsite DCA et Printanista Hub sont cryptées à l'aide de protocoles de cryptage puissants conformes à la norme FIPS. Onsite reçoit des mises à jour logicielles sécurisées depuis les serveurs Printanista Updates.

L'ancien Onsite DCA communique avec Printanista à un intervalle prédéfini afin de déterminer s'il existe des actions en attente qui n'ont pas encore été exécutées. Cela garantit que les actions sont exécutées en temps opportun.

Remarque : Onsite DCA initie toujours cette communication avec le serveur Printanista, et non l'inverse.

Remarque : HP JAMC n'est pris en charge que lorsqu'il est utilisé conjointement avec l'ancien DCA sur site lors du lancement initial de Printanista.

Trafic réseau

Les audits effectués par le logiciel utilisent un système intelligent pour extraire un minimum d'informations pour chaque imprimante, photocopieur ou multifonction. Contrairement aux produits similaires qui envoient un ensemble fixe de requêtes (un sur-ensemble de toutes les requêtes possibles) à chaque périphérique en réseau, Onsite DCA n'envoie que les requêtes pertinentes en fonction des champs pris en charge par le périphérique cible, chaque requête ne dépassant pas quelques kilo-octets de données. Afin de réduire davantage la quantité de bande passante réseau utilisée, Onsite DCA communique avec un maximum de 20 appareils à la fois. Chaque adresse IP comprise dans les plages configurées sera interrogée et, si aucune réponse n'est reçue dans le délai de temporisation configuré, le système passera à l'adresse IP suivante. En règle générale, Printanista recueille des informations sur environ 65 000 appareils en un peu moins d'une heure.

Assistance du fabricant

Les produits Printanista sont indépendants des fabricants. Ils prennent en charge tous les principaux fabricants et toutes les familles de modèles. Certains appareils présentent des limitations qui empêchent l'extraction de certaines informations.

Problèmes liés aux virus

Les fichiers de l'application Printanista ont été signés numériquement afin d'empêcher leur exécution si leur intégrité est compromise. Cela garantit qu'aucun virus éventuellement présent ne sera activé et empêche la propagation du virus d'un réseau à un autre. Pour plus de sécurité, nous vous recommandons d'utiliser un logiciel antivirus sur votre réseau.

ECI fournira des services d'assistance exclusivement pour la dernière version commerciale disponible du logiciel, ainsi que pour la version immédiatement précédente du logiciel. Cette politique s'applique à tous les produits ECI Device Management.

