Livre blanc technique sur Printanista Hub

Version 1.10

Table des matières

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

Présentation

La suite de produits Printanista offre une solution d'impression gérée de classe entreprise, très facile à utiliser et à déployer. Elle est architecturée et conçue pour tirer parti des fonctionnalités avancées et des avantages de la plateforme Microsoft .NET. Ainsi, elle ne nécessite plus 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 concernant 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 à des fins de facturation ou d'approvisionnement.

ECI DCA : Ce tout dernier agent de collecte de données (DCA) offre des avantages majeurs par rapport à l'agent de collecte de données sur site (DCA) sans rien perdre de ses fonctionnalités, notamment une prise en charge native complète et multiplateforme de Windows, macOS, Linux et Raspberry Pi, chacune avec des procédures d'installation spécifiques, une documentation d'assistance et une équipe d'assistance formée à ces plateformes. ECI DCA permet également la détection et l'analyse continues des périphériques, offre des capacités améliorées de collecte de données MIBWalk et de journaux, et prend désormais en charge un nombre bien plus important de types de compteurs.

DCA sur site : Cet outil d'agent de collecte de données 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 selon un calendrier défini, sans intervention humaine. Les données capturées sont envoyées au site web Printanista Hub via HTTPS, HTTP ou, si le client le préfère, sous forme de fichier crypté propriétaire.

L'objectif de ce document est de fournir une vue d'ensemble de la gamme de produits Printanista d'un point de vue technique afin de faciliter la réponse aux questions les plus fréquentes que les équipes informatiques sont amenées à recevoir.

Comment fonctionne Printanista

Printanista Hub : une application hébergée

Printanista Hub est hébergé par ECI Software Solutions au sein de centres de données sécurisés et protégés situés dans différentes régions du monde. ECI Software Solutions est conscient que la confidentialité, l'intégrité et la disponibilité des informations de nos clients sont essentielles à leurs opérations 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 plan. Ces installations offrent un support 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

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 imprimantes multifonctions en réseau en utilisant les protocoles pris en charge par ces appareils.

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

SNMP est un protocole réseau facilitant 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 disposent dans leur architecture. 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

Application backend du hub Printanista

Toutes les données collectées sont transmises au serveur Printanista Hub, où elles sont mises à disposition pour la génération de rapports et les 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 utilisées par votre serveur.

Cette connexion est protégée par **le protocole TLS** (Transport Layer Security), norme industrielle.
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 se rabattre sur l'utilisation **d'événements envoyés par le serveur** ou **du long polling HTTP**.

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

Configuration système requise pour Printanista Hub

Cliquez sur le lien suivant pour consulter les spécifications système complètes et à jour du produit

Printanista : Configuration système requise pour Printanista Hub v4.0

Configuration requise pour l'application Printanista

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 fait partie intégrante de la couche application de la suite TCP/IP.

Configuration requise pour le PC/serveur ECI DCA :

Configuration requise pour Microsoft Windows (x86/64) :

- Microsoft .NET Framework 4.7.2 ou version plus récente (recommandé : dernière version)
- Les versions de Windows Server (à l'exception des éditions Datacenter et Core) et de Windows
  - ➢ *Les versions de 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 du serveur ECI Updates et au serveur Printanista
  .

Configuration requise pour Linux (x86/64 ou ARM) :

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

Configuration requise pour macOS (x64) :

- Mono Framework 5.4 ou supérieur (recommandé : dernière version)
- macOS® Sierra (10.12) à Sequoia (15.4). Les versions plus récentes ne sont pas prises en charge.
- Les paramètres du réseau local et/ou du pare-feu doivent permettre la connexion aux services du serveur ECI Updates Server 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 du serveur 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 (solution de secours)	**53/UDP** (DNS)	Serveur DNS du réseau local (principal) Serveur de mises à jour ECI (de secours)

Serveur de mises à jour ECI

ECI Updates Server est un service géré par ECI Device Management destiné à faciliter l'enregistrement des DCA, les mises à jour logicielles automatiques et les installations de DCA (ce site) ; il est indispensable au fonctionnement des DCA ECI. Remarque : les DCA ECI n'envoient aucune donnée relative aux appareils ou à la configuration collectée au serveur ECI Updates Server.

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 s'effectuent toujours sur le port HTTPS standard **443/tcp**.

Enregistrement

ECI DCA utilise des requêtes DNS vers `*.reg.pf-d.ca` pour s'enregistrer. Il essaiera d'abord de le faire en utilisant les serveurs DNS du réseau local, puis se rabattra sur une communication directe avec les adresses IP du serveur de mises à jour ECI (en utilisant le port **53/udp**). Le pare-feu n'a besoin d'autoriser cette connexion au serveur de mises à jour ECI que si le ou les serveurs DNS locaux ne parviennent pas à résoudre les requêtes d'enregistrement.

Région de service

Le trafic ECI DCA est acheminé vers la région présentant la latence réseau la plus faible, en fonction de la disponibilité du service. Dans certaines zones, la région utilisée peut changer au fil du temps, car l'activité sur l'infrastructure Internet mondiale peut avoir une incidence sur la latence.

Données collectées et chiffrement

Chiffrement des données

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

Questions de sécurité

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

ECI DCA et l'ancienne version d'Onsite DCA ne collectent ni ne traitent aucune donnée à caractère personnel. Le système ne recueille ce type d'informations que si vous ou vos clients saisissez ces données dans Printanista, dans un champ ou une étiquette, par exemple pour l'emplacement ou le nom du client. ECI DCA et l'ancienne version d'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 pour recueillir des informations opérationnelles sur le périphérique, 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 ne stocke que :

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

D'autres informations relatives au réseau et 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

ECI DCA et l'ancienne version de DCA sur site tentent de collecter les informations suivantes auprès 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 de l'écran 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 de maintenance
- Niveaux des consommables autres que le toner
- Niveaux divers
- Détails des consommables pour imprimantes à étiquettes

Couverture et compteurs

- Relevés de compteurs
- Type de compteur
- Niveau de couverture
- Identification en noir et blanc ou en couleur

Détection du réseau et collecte des données

Pour améliorer l'efficacité du DCA, seules les données nouvelles ou modifiées provenant des périphériques sont envoyées au serveur Printanista Hub. Cela permet de réduire au minimum la charge réseau et d'éliminer les retards dans la transmission des données des périphériques. De plus, la découverte et l'analyse des périphériques sont désormais indépendantes afin de garantir que seules les adresses IP
(ou le nom d'hôte) des périphériques précédemment détectés soient analysées selon une fréquence définie périodiquement, plutôt que de procéder à une analyse complète du réseau (celle-ci est effectuée initialement, périodiquement ou lorsque l'administrateur le décide).

Cela garantit que les données des appareils sont transmises aussi rapidement que possible. Les utilisateurs peuvent ainsi être informés des appareils défaillants en quelques minutes, voire quelques secondes, dans de nombreux cas. 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 consommables et les erreurs. Les valeurs par défaut, minimales et maximales pour les intervalles d'analyse sont :

Fonction d'analyse	Par défaut	Minimum	Max
Détection	60 minutes	10 minutes	7 jours
Mètres	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 appareil dispose d'un fichier de définition de modèle (MDF). Si ce fichier n'est pas présent, une analyse complète sera effectuée sur l'appareil en question à l'aide d'un intervalle prédéfini.

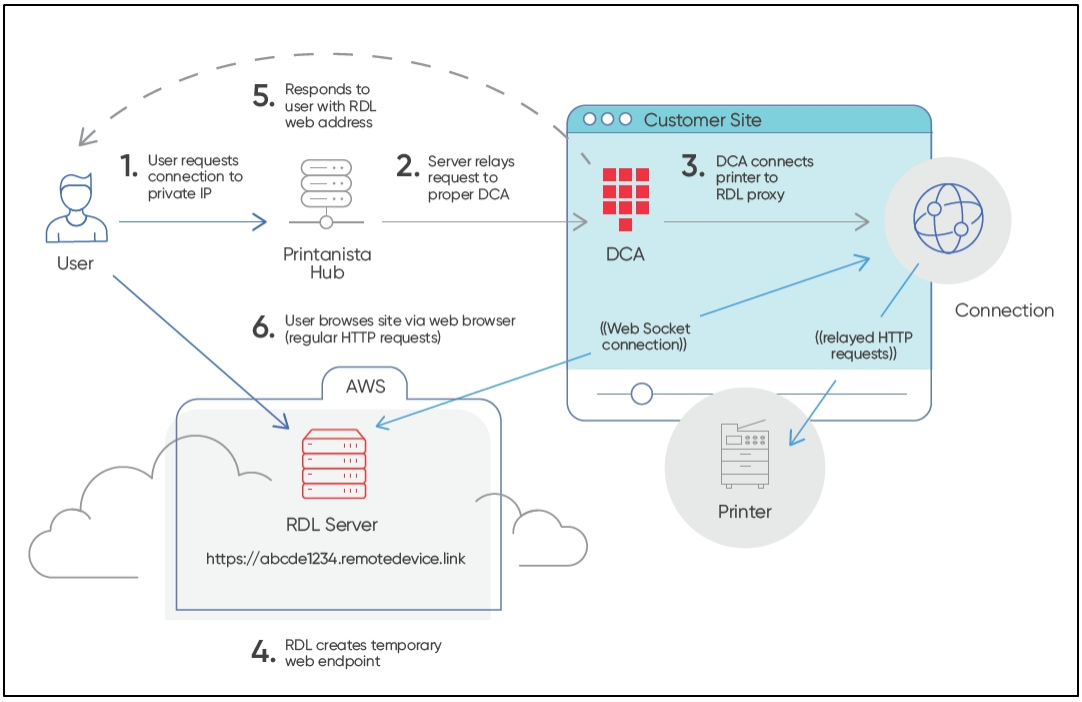
Les administrateurs du Printanista Hub peuvent gérer à distance les ECI DCA qui ont été activés sur le serveur. Ils peuvent déclencher à distance l'ECI DCA pour exécuter des commandes prédéfinies telles que des tâches de collecte de données, la fourniture de journaux ECI DCA, l'exécution de MIB Walks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

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

Remarque : la communication n'a lieu que lorsque les informations relatives au compteur, aux consommables 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'ancienne version d'Onsite DCA.

Liaison à distance avec les périphériques (RDL)



Présentation du système – Liaison à distance avec les périphériques (RDL)

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

1. L'**utilisateur final** accédant à l'appareil
2. **Le serveur Remote Device Link**, accessible via 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)

L'adresse publique de RDL est toujours une URL de type https:// sur le port 443, quels que soient le port du point de terminaison et/ou l'état du protocole SSL.

Activation et autorisations

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

Fonctionnalités d'audit

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

Sécurité de 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 au sein de Printanista Hub pour accéder à la fonctionnalité Remote Device Link (RDL) sur le compte concerné
- L'agent de collecte de données (DCA) n'acceptera que les requêtes Remote Device Link (RDL) provenant du serveur Printanista Hub, qui fait l'objet d'une authentification mutuelle
- L'agent de collecte de données (DCA) établit uniquement une connexion RDL (Remote Device Link) avec les périphériques d'impression connus et actuellement surveillés qui se trouvent dans la ou les plages d'adresses IP de découverte de l'agent de collecte de données (DCA).
- Chaque requête Web doit être adressée à la même adresse IP – L'agent de collecte de données (DCA) ne suit pas les redirections

Sécurité des connexions :

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

Limites de durée de session :

- Chaque session RDL (Remote Device Link) expire par défaut après 20 minutes d'inactivité, avec une durée maximale absolue de 2 heures.

Implications

La connexion entre ECI DCA et Printanista Hub est protégée par des clés d'authentification propres à chaque installation de DCA, et elle nécessite un certificat SSL valide et de confiance pour fonctionner via une connexion TLS.

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

Application 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 du 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 spécifiques. Un ou plusieurs rôles, qui définissent les autorisations, sont attribués aux utilisateurs, et ceux-ci se voient accorder l'accès à un ou plusieurs groupes d'appareils. Les administrateurs disposant de tous les droits peuvent définir précisément les écrans que chaque utilisateur est autorisé à consulter 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 chiffrement 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 la compatibilité des références OEM. Cette base de données est mise à jour périodiquement à mesure que de nouveaux modèles et versions sont lancés par les fabricants OEM. 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 au sein de centres de données sécurisés et protégés situés dans différentes régions du monde. ECI Software Solutions est conscient que la confidentialité, l'intégrité et la disponibilité des informations de nos clients sont essentielles à leurs activités commerciales et à notre propre réussite. Nous adoptons une approche multicouche pour protéger ces informations cruciales, en surveillant et en améliorant en permanence 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 plan. Ces installations offrent un support

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

Processus de gestion des versions, de test et de mise en production d'

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 nouveaux aspects fonctionnels. Les versions majeures passent par 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 version sécurisé, accessible uniquement aux personnes autorisées. Toute modification du 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 l'identité du développeur qui l'a effectuée et la raison de cette modification. Les produits sont chiffrés et signés numériquement à l'aide d'un certificat de signature de code de confiance avant leur livraison. Un dépôt fiduciaire peut être mis à disposition sur demande.

ECI fait appel à un organisme tiers indépendant de premier plan, certifié CREST, SOC 2, NSA-CIRA et CSA-STAR, pour réaliser des tests d'intrusion au niveau des applications et corriger les failles identifiées en fonction de ses exigences métier et de son cadre interne de gestion des risques. Les tests d'intrusion sont effectués au moins une fois par an ou lorsque des modifications majeures sont apportées au système. La politique d'ECI consiste à déployer tous les efforts commercialement raisonnables pour remédier à toutes les failles critiques dans un délai de 30 jours ou dans un délai raisonnable, sur la base d'une analyse de rentabilité fournie. ECI ne divulgue pas de détails concernant ses contrôles de sécurité ou les résultats des tests d'intrusion, car ces informations sont exclusives et confidentielles et, si elles tombaient entre de mauvaises mains, pourraient entraîner une augmentation des risques.

Confidentialité des données et législation

Règlement général sur la protection des données (RGPD)

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

ECI a mis en place un programme structuré et complet de mise en conformité avec le RGPD. Ce programme comprend, entre autres, la formation du personnel, des audits et des évaluations des risques à l'échelle de l'entreprise, des politiques et des procédures, la gouvernance, ainsi que des efforts continus en matière de conformité. Nous encourageons nos clients à prendre des mesures similaires pour garantir la conformité de leurs propres entreprises avec le RGPD, aujourd'hui et pour les années à venir.

Les produits Printanista ne traitent, ne surveillent ni ne gèrent aucune donnée à caractère personnel, ni aucune donnée ou 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 à des informations à haut risque, de les stocker ou de les transmettre, même si ces informations sont imprimées ou envoyées d'une autre manière vers des périphériques d'impression surveillés par les applications logicielles Printanista.

Les applications logicielles Printanista ne stockent, ne traitent ni ne transmettent aucune donnée relative aux titulaires de cartes ou aucune information personnelle.

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

Toutes les communications doivent provenir des produits Printanista, et il n'existe aucun moyen de contacter ou d'accéder aux produits depuis l'extérieur du réseau.

Les communications en dehors du réseau utilisent un flux de données compressé propriétaire, envoyé via HTTPS avec le protocole SSL standard.

Pour toute information relative à la conformité à des lois et/ou réglementations spécifiques, veuillez contacter votre responsable de compte ECI.

Voici un lien vers la page « Sécurité du cloud ECI » : Présentation de la sécurité cloud ECI

Foire aux questions (FAQ)

Les produits Printanista fonctionnent-ils avec des proxys Internet ?
Oui, ECI DCA est compatible 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 solution ECI DCA offre des avantages majeurs par rapport à la solution DCA sur site sans perdre aucune fonctionnalité, notamment une prise en charge native complète et multiplateforme de Windows, macOS, Linux et Raspberry Pi. Chacune dispose de procédures d'installation spécifiques, d'une documentation d'assistance et d'une équipe d'assistance formée sur ces plateformes. Le processus d'installation a également été considérablement amélioré et est désormais 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 intègrent leur propre serveur pour héberger l'interface utilisateur (UI) web et sont configurés automatiquement lors de l'installation.

Peut-on installer ECI DCA sur un ordinateur qui héberge déjà un autre site web IIS ?
Oui. Cependant, les ports indiqués ci-dessous doivent être ajoutés à la liste blanche pour 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 (solution de secours)	**53/UDP** (DNS)	Serveur DNS du réseau local (principal) Serveur de mises à jour ECI (de secours)

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

Quelle est la charge de maintenance requise pour ECI DCA ?
ECI DCA et Onsite DCA sont des services qui s'exécutent en arrière-plan et effectuent des audits ainsi que des exportations vers les 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 d'audit, ce qui limite les interventions manuelles.

Avec quelles marques d'équipements la surveillance Remote Device Link (RDL) fonctionne-t-elle ? 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 figurant sur les pages Web intégrées varient selon le fabricant et le modèle. Les appareils locaux n'afficheront pas la page Web intégrée.

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

Remote Device Link (RDL) semble un peu lent, pourquoi ?
Ceci est normal, car la connexion doit passer par nos services cloud. Cependant, le principal facteur déterminant 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 que ce temps pouvait varier en fonction de l'utilisation actuelle ou des ressources disponibles pour l'interface utilisateur (UI).

Quelles sont les fonctionnalités disponibles avec Remote Device Link (RDL) ?
Toutes les options auxquelles l'OEM 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 la désactiver pour chaque utilisateur, ce qui vous permet de bloquer l'accès d'un utilisateur à Remote Device Link (RDL).

Où puis-je trouver des informations supplémentaires sur Printanista Hub, ECI DCA, l'ancienne version d'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'ancienne version d'Onsite DCA

Il est recommandé d'utiliser ECI DCA avec Printanista. Cependant, l'ancienne version d'Onsite DCA fonctionne actuellement avec Printanista.
Configuration PC/serveur requise 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 ultérieures d'Onsite 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 une machine fonctionnant 24 h/24, 7 j/7 ou au moins pendant toute la journée de travail
- 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
- Le protocole SOAP sur HTTP(s) doit être autorisé à passer le pare-feu

Configuration réseau requise :

Le trafic SNMP (port 161) doit pouvoir transiter sur le réseau local (LAN) ou le réseau étendu (WAN)

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

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 ultérieure
- Pilote à jour pour l'imprimante locale (une mise à jour est recommandée pour les périphériques HP)
- L'imprimante doit prendre en charge le langage PJL (Printer Job Language) ou le langage 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 — Ports 161/33333 entrants/sortants 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 fabricants d'origine Kyocera et Ricoh, ainsi que leurs variantes, sont actuellement pris en charge.

Détection du réseau et collecte des données de comptage et des stocks (DCA sur site)

Les paramètres de découverte automatique du réseau brevetés par Printanista utilisent une combinaison d'algorithmes pour identifier les plages de réseau où les périphériques d'impression sont susceptibles de se trouver, puis pour détecter et communiquer avec les périphériques en ligne, en acheminant le trafic via plusieurs éléments du réseau tels que des postes de travail ou des serveurs actifs, des routeurs, des concentrateurs, des commutateurs et d'autres équipements réseau.

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

Fonction	**Emplacement**	**Description**
Tâches	Paramètres Onsite	Il est possible de configurer à distance l'exécution de tâches selon un calendrier prédéfini, mais aussi de sélectionner certaines tâches (Cache, Compteurs, Consommables, Maintenance) pour qu'elles s'exécutent immédiatement et de collecter les données des appareils sur simple commande.
MIB Walks	Paramètres sur site	Possibilité d'indiquer certaines adresses IPv4/IPv6 ou certains noms d'hôte des appareils et de déclencher la collecte immédiate des MIB Walks sur site.
Journaux (détaillés)	Paramètres Onsite	Permet de demander à Onsite de collecter les journaux (critiques, erreurs, avertissements, détails, débogage) à partir d'une date donnée.

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

L'ancienne version d'Onsite DCA communique avec Printanista à un intervalle prédéfini afin de vérifier 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 : c'est toujours Onsite DCA qui initie 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 Onsite DCA lors du lancement initial de Printanista.

Trafic réseau

Les audits réalisés par le logiciel s'appuient sur un système intelligent pour extraire un minimum d'informations pour chaque imprimante, photocopieur ou multifonction. Contrairement à des 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 bande passante réseau utilisée, Onsite DCA communique avec un maximum de 20 périphériques à la fois. Chaque adresse IP comprise dans les plages configurées est interrogée et, si aucune réponse n'est reçue dans le délai d'attente défini, le programme passe à l'adresse IP suivante. En règle générale, Printanista recueille des informations sur environ 65 000 périphériques en un peu moins d'une heure.

Prise en charge des fabricants

Les produits Printanista sont indépendants des fabricants. Ils prennent en charge tous les principaux fabricants et gammes de modèles. Certains appareils présentent des limitations empêchant 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 venait à être compromise. Cela garantit qu'aucun virus éventuellement présent ne sera activé et empêche sa propagation d'un réseau à l'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 du logiciel disponible dans le commerce, ainsi que pour la version immédiatement précédente du logiciel. Cette politique s'applique à tous les produits ECI Device Management.

