



Livre blanc technique du Hub Printanista

Version 1.5



Table des matières

Vue d'ensemble.....	4
Comment fonctionne Printanista	5
Exigences de Printanista	6
Application backend du Hub Printanista	6
Conditions d'application de Printanista	7
Agent de collecte de données (ECI DCA)	7
Configuration PC/serveur requise pour l'ICE DCA	7
L'ICE met à jour son serveur	8
Mises à jour du logiciel.....	8
Enregistrement.....	8
Région de service	8
Données collectées et cryptage.....	9
Chiffrement des données	9
Questions de sécurité	9
Types d'informations collectées	9
Imprimeurs locaux	11
Flux de travail de Printanista	11
Liaison avec les dispositifs à distance (RDL)	13
Présentation du système - Remote Device Link (RDL)	13
Sécurité : Ports et SSL (Secure Sockets Layer)	13
Habilitation et permissions	13
Capacités d'audit	13
Sécurité des liaisons entre dispositifs à distance (RDL)	14
La sécurité de la liaison avec les appareils à distance (RDL) a été une préoccupation majeure lors de la mise au point de cet outil.	14
Application du Hub Printanista	15
Gestion des utilisateurs basée sur les permissions	15
Accès HTTPS	15
Printanista côte à côte	15
Hébergement de l'application Hub de Printanista.....	15
Centres de données sécurisés ECI.....	15
Gestion des versions	16
Processus de test et de mise à disposition	16
Sécurité du code source.....	16
Protection des données et législation	17

Règlement général sur la protection des données (RGPD)	17
Foire aux questions (FAQ).....	18
Informations sur l'ACD sur place de l'héritage.....	20
Exigences PC/Serveur pour l'ACD sur site.....	20
Considérations relatives au pare-feu sortant (port 80 ou 443).....	20
Exigences en matière de réseau.....	20
L'ancienne version de Java Onsite sur les systèmes Linux et macOS n'est pas fonctionnelle.....	20
Configuration PC/imprimante requise pour l'utilisation de l'agent local (installation facultative)	20
Découverte du réseau et collecte des compteurs et des fournitures (DCA sur site)	21
Trafic sur le réseau	21
Agent USB local (fonctionne UNIQUEMENT avec l'ACD sur site)	22
Soutien aux fabricants	22
Inquiétudes concernant les virus	22

Vue d'ensemble

La suite de produits Printanista offre une solution d'impression gérée de classe entreprise qui est 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, il n'est plus nécessaire de faire appel à des techniciens qualifiés pour installer le logiciel, configurer et maintenir 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 des données des produits à des sources extérieures est strictement limitée. Les produits ne communiquent aucun autre détail que les informations relatives à l'équipement surveillé (c'est-à-dire le type d'équipement). Aucune information confidentielle n'est jamais transmise hors du réseau par les produits Printanista. La suite se compose des éléments suivants :

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

ECI DCA : Ce nouvel agent de collecte de données apporte des avantages majeurs par rapport à l'agent de collecte de données sur site sans perdre aucune fonctionnalité, y compris un support natif multiplateforme complet de Windows, macOS, Linux et Raspberry Pi, chacun avec des étapes d'installation uniques, une documentation d'assistance et un personnel d'assistance formé sur ces plates-formes. ECI DCA apporte également une découverte et un balayage continus des appareils, une capacité améliorée de collecte de MIBWalk et de journaux, et de nombreux autres types de compteurs sont désormais collectés.

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

Outil d'évaluation WebAudit : Un outil de collecte de données qui fait partie de l'application Printanista Hub. Les évaluations de flotte sont effectuées directement à partir d'un navigateur sans installer de logiciel. Les données capturées sont envoyées directement à Printanista Hub.

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 les réponses aux questions les plus fréquentes que les équipes de technologie de l'information recevront.

Comment fonctionne Printanista

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

Printanista supporte actuellement le protocole SNMP v1, v2c et v3 (Simple Network Management Protocol). SNMP v3 offre une protection accrue des paquets afin de garantir que les informations et les communications sont transmises par des sources fiables. Contrairement à SNMPv1 ou v2, SNMP v3 est crypté pour une sécurité accrue et nécessite un nom d'utilisateur et un mot de passe. L'avantage d'utiliser SNMP v3 est que les administrateurs de 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 à l'intérieur du périphérique d'impression. La base d'informations de gestion (MIB) est une base de données interne que la plupart des périphériques connectés au réseau possèdent en tant que partie intégrante de leur anatomie. 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

Printanista Hub Backend Application

Printanista Hub Product Specifications

	Printanista Hub	ECI DCA	Onsite	Viewer	WebAudit	Agent	Microsoft	Notes
	5.0	1.5	4.1	3	on v4	4	Support	
Supported OSes¹								
Windows 7 SP1 (32/64)	No	Yes	Yes	Yes	Yes	Yes	April-2015 January 2020	
Windows 8 (32/64)	No	Yes	No	No	No	Partial ²	April-2018 January 2023	
Windows 8.1 (32/64)	No	Yes	Yes	Yes	No	Partial ²	April-2018 January 2023	
Windows 10 (32/64)	No	Yes	Yes	Yes	No	Partial ²	October-2020 October 2025	
Windows Server 2003 (32/64) Internet Information Services 6 ²	No	No	No	Yes	Yes	Yes	April-2010 April-2015	
Windows Server 2008 (32/64) Internet Information Services 7.0	No	No	No	Yes	Yes	Yes	April-2015 January 2020	
Windows Server 2008 R2 (32/64) Internet Information Services 7.5	No	Yes	Yes	Yes	Yes	Yes	April-2015 January 2020	
Windows Server 2012 Internet Information Services 8.0	No	Yes	Yes	Yes	Yes	Yes	October-2018 January 2023	
Windows Server 2012 R2 Internet Information Services 8.5	No	Yes	Yes	Yes	Yes	Yes	October-2018 October 2023	
Windows Server 2016 Internet Information Services 10	Yes	Yes	Yes	Yes	Yes	Yes	January 2022 January 2027	Recommended by ECI
Windows Server 2019 Internet Information Services 10	Yes	Yes	Yes	Yes	Yes	Yes	January 2024 January 2029	Recommended by ECI
Linux (x86/64 or ARM) Debian, Ubuntu and similar distributions	N/A	Yes	No	No	No	No	---	Mono 5.4 or higher required
macOS (x64) Sierra (10.12 or higher)	N/A	Yes	No	No	No	No	---	Mono 5.4 or higher required
Raspberry Pi 4B, 3B+, 3B, 2B	N/A	Yes	No	No	No	No	---	8GB or larger SD card required

Utilisez le lien suivant pour obtenir les spécifications complètes et actuelles des produits Printanista : [SysReq v3.0.html](https://www.eci.com/SysReq_v3.0.html)

Toutes les données collectées sont envoyées au serveur Printanista Hub où elles sont mises à disposition pour la création de rapports et d'alertes.

ECI DCA se connecte à votre serveur Printanista Hub en utilisant HTTPS (port **443/TCP**). Veuillez contacter l'administrateur de votre solution ECI pour obtenir des informations sur les noms de domaine et les adresses IP utilisées par votre serveur. Cette connexion est protégée par le standard industriel **TLS** (Transport Layer Security). **TLS 1.2 est recommandé**. TLS 1.0 et TLS 1.1 sont actuellement pris en charge mais ne sont pas recommandés à des fins de sécurité. La prise en charge de TLS 1.0 et TLS 1.1 sera supprimée à l'avenir.

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

NOTE IMPORTANTE : Plusieurs connexions HTTPS sécurisées sortantes sont nécessaires à partir du serveur sur lequel est installé Printanista Hub :

- <https://www.gttechonline.com>
- <https://modelmatch.printanista.net>
- <https://models.printanista.net>
- <https://updates.printanista.net>
- <https://api.printanista.net>
- <https://dcaregistry.printanista.net>
- <https://remotedevicelink.printanista.net>

Application Printanista Exigences

Agent de collecte de données (ECI DCA)

Les imprimantes, les copieurs et les appareils multifonctions doivent être dotés du protocole SNMP (port 161) pour la découverte et l'extraction d'informations. Le protocole SNMP est un élément standard de la couche application de la suite TCP/IP.

Configuration PC/serveur requise pour ECI

DCA : Microsoft Windows (x86/64)

Exigences :

- Windows 10 ou supérieur
- Windows Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, Server 2019 et Server 2022
- Microsoft .NET Framework 4.7.2. ou plus

récent Linux (x86/64 ou ARM)

Exigences :

- Ubuntu 14.04, 16.04 ou 18.04, Debian 9.5+, Raspbian Jessie ou Stretch, RedHat Enterprise 7.5+, CentOS 7.5+, Fedora 28+
- Mono 5.4 ou

supérieur macOS (x64)

Exigences :

- Sierra (10.12) ou supérieur
- Mono 5.4 ou supérieur

Raspberry Pi 2 Model B, Raspberry Pi 3 Model B, Raspberry Pi 3 Model B+, et Raspberry Pi 4 Model

Exigences :

- Carte microSD vierge de 8 Go ou plus
- PC capable d'écrire sur une carte microSD

Considérations relatives au pare-feu pour l'ECI DCA :

Connexions entrantes

Il n'y a pas de connexions entrantes depuis l'internet vers ECI DCA.

Connexions sortantes

Service	Port	Connexion à
Téléchargement des données	443/TCP (HTTPS)	Votre serveur Printanista Hub
Mises à jour du logiciel	443/TCP (HTTPS)	L'ICE met à jour le serveur



Printanista

Enregistrement (fallback)	53/UDP (DNS)	Réseau local Serveur DNS (primaire) Serveur de mise à jour ECI (fallback)
------------------------------	--------------	--

L'ICE met à jour le serveur

ECI Updates Server est un service géré par [ECI Device Management](#) pour faciliter l'enregistrement DCA, les mises à jour automatiques du logiciel et les installations DCA (ce site), et est nécessaire au fonctionnement de l'ECI DCA. Note : L'ECI DCA n'envoie aucune donnée de configuration ou d'appareil à l'ECI Updates Server.

Mises à jour du logiciel

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

Inscription

L'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 les adresses IP du serveur de mises à jour de l'ECI (en utilisant le port **53/udp**). Le pare-feu ne doit autoriser cette connexion au serveur de mises à jour de l'ICE que si le(s) serveur(s) DNS local(aux) ne résout(ent) pas les demandes d'enregistrement.

Région de service

L'ECI DCA est acheminé vers la région où le temps de latence du réseau est le 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

Cryptage des données

Tous les paquets de données provenant de l'ECI DCA et de l'ancienne DCA sur site sont encodés et obscurcis. Printanista exige l'utilisation de HTTPS pour la communication entre les ACD et le Hub de Printanista. L'ECI DCA a besoin de HTTPS pour fonctionner. En outre, tous les paramètres et travaux sensibles entre l'ECI DCA et Printanista sont cryptés à l'aide de l'algorithme de cryptage symétrique standard AES256, en utilisant une clé partagée protégée. Cela garantit un cryptage de bout en bout, de sorte que les données sont protégées contre la lecture si elles sont interceptées par une tierce partie, une instance Printanista concurrente ou non autorisée.

La sécurité est importante

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

L'ECI DCA et l'ancienne DCA sur site ne collectent ni ne traitent aucune donnée personnelle. Le seul moyen pour le système de collecter ce type d'informations est que vous ou vos clients saisissiez les données dans Printanista dans un champ ou une étiquette tels que l'emplacement ou le nom du client. L'ECI DCA et l'ancienne DCA sur site vous permettent de surveiller les périphériques du réseau à l'aide du protocole SNMP (Simple Network Management Protocol). L'application est déployée dans le réseau du client et, de là, elle communique avec les appareils pour recueillir des informations opérationnelles sur l'appareil qui sont disponibles via le micrologiciel de l'appareil et une base d'informations de gestion SNMP (MIB). Les données exposées par l'appareil varient selon le fabricant et le modèle. Elles sont toujours de nature technique ou opérationnelle et spécifiques à l'appareil lui-même. Au niveau le plus élémentaire, les données exposées par une MIB d'imprimante sont documentées dans la RFC 3805 de l'IETF (<https://tools.ietf.org/html/rfc3805>). Le fabricant peut fournir des informations supplémentaires sur l'appareil par le biais d'extensions et de MIB privées (Management Information Base), mais ces informations sont fondamentalement techniques et spécifiques à l'appareil.

Magasins Printanista Hub uniquement :

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

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

Types d'informations collectées

L'ECI DCA et l'ancienne DCA sur site tentent de collecter les informations suivantes auprès des périphériques d'impression en réseau au cours d'une analyse du réseau :

Attributs du dispositif

- Adresse IP (peut être masquée)
- Fabricant
- Numéro de série
- Numéro de l'actif
- Adresse MAC
- Description de l'appareil
- Localisation

Fournitures

- Numéro de série de la cartouche de toner
- Niveau d'alimentation de la cartouche de toner
- Niveaux de batterie
- Niveaux des kits d'entretien
- Niveaux d'approvisionnement en produits non-toner
- Niveaux divers
- Imprimantes à base d'étiquettes détails de l'offre

Service

- Divers (spécifique à la machine)
- Lecture de l'écran LCD
- État de l'appareil
- Codes d'erreur
- Firmware

Couverture et compteurs

- Relevés de compteurs
- Type de compteur
- Niveau de couverture
- Identification monochrome ou couleur

Découverte du réseau et collecte de données

Pour accroître l'efficacité de l'ACD, ce n'est que lorsqu'il y a des données nouvelles ou modifiées provenant des appareils que ces informations sont envoyées au serveur Hub de Printanista. Cela permet de minimiser la charge du réseau et d'éliminer la fréquence des retards dans les soumissions de données des appareils. En outre, la découverte et l'analyse des appareils sont désormais indépendantes, de sorte que seule l'adresse IP est prise en compte. (ou nom d'hôte) des dispositifs précédemment découverts sont analysés sur la base d'un réglage périodique par rapport à une analyse complète du réseau (cette analyse est effectuée initialement, périodiquement ou lorsqu'elle est déterminée par un utilisateur administrateur).

Cela permet de garantir que la vitesse de transmission des données relatives aux appareils est aussi actualisée que possible. Cela permet aux utilisateurs d'être informés des appareils défectueux en quelques minutes, voire en quelques secondes dans de nombreuses situations. L'ECI DCA sépare la découverte 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 des intervalles de balayage sont les suivantes :

Fonction de balayage	Défaut	Minimum	Maximum
Découverte	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 n'est pas le cas, une analyse complète sera effectuée sur l'appareil en question à l'aide d'un intervalle prédéfini.

Les administrateurs du Hub Printanista 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 de l'ECI DCA.

Note : 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 aux compteurs, à l'approvisionnement ou aux erreurs ont été mises à jour ou modifiées, ce qui réduit l'utilisation de la bande passante.

Remarque : pour l'instant, le HP JAMC ne fonctionne qu'avec l'ancienne ACD sur site.

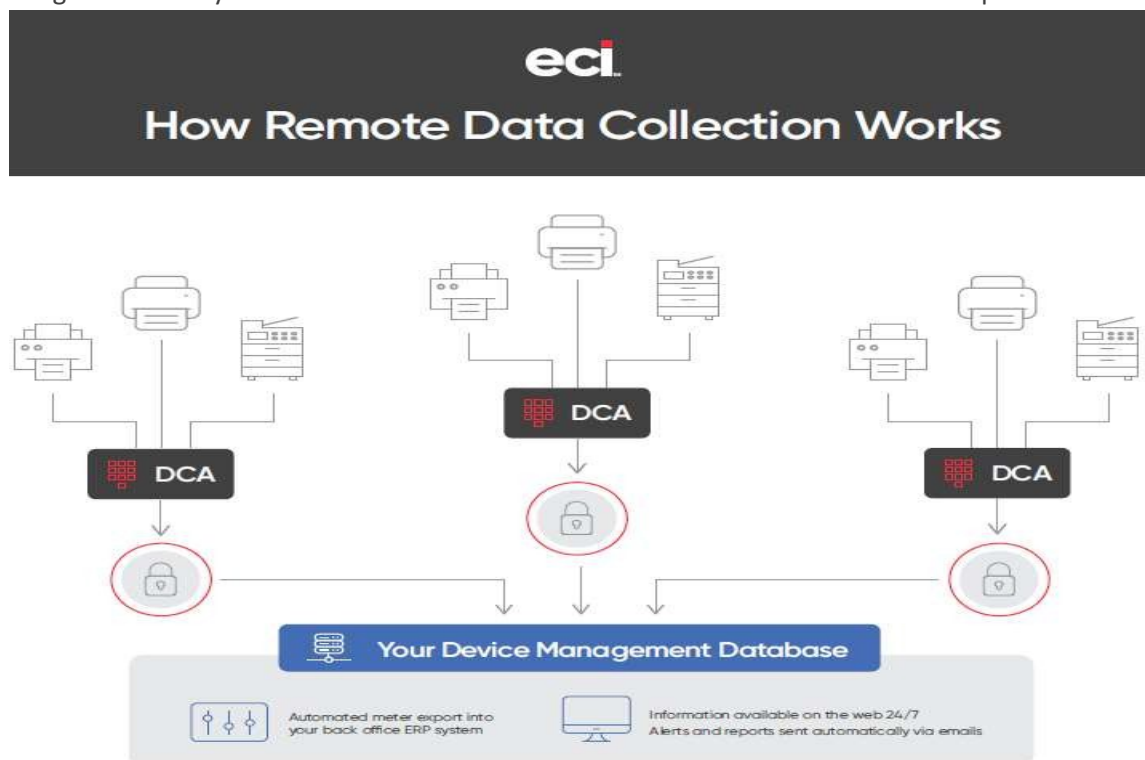
Imprimantes locales

Flux de travail de Printanista

Printanista Workflow est un outil de gestion d'impression robuste. Printanista Workflow peut aider vos clients à réduire le coût de production des documents, à augmenter leurs pratiques de sécurité des documents et à fournir des méthodes flexibles de recouvrement des coûts. Grâce à un processus d'installation simplifié, vos clients peuvent rapidement voir toutes leurs informations d'impression en un seul endroit. Ils peuvent ainsi réduire leurs coûts en comprenant chaque document qu'ils produisent.

Qu'est-ce que le Workflow Printanista ?

Printanista Workflow est la nouvelle génération de produits de gestion des utilisateurs utilisés pour suivre et gérer l'impression pour des centaines d'organisations et d'entreprises dans le monde entier. Si vous étiez familier avec l'application de gestion des utilisateurs dans le passé, vous serez heureux de constater que l'installation et la configuration de l'application sont toujours aussi intuitives que dans les versions précédentes. Les menus, les outils et l'administration générale du système ont été conservés. Si vous effectuez une mise à niveau à partir d'une version



antérieure, tout vous sera familier et la navigation sera transparente.

Fonctionnement du Workflow Printanista (par l'intermédiaire de l'ICE DCA, les données sont collectées à partir du Workflow)

Le Printanista Workflow étant la nouvelle génération de gestion des appareils, cette fonction ne fonctionne qu'avec l'ECI DCA. Le Printanista Workflow ne fonctionne pas avec la DCA sur site.

- Le client Workflow peut être installé sur les bureaux des systèmes d'exploitation MAC et Windows, ce qui permet de collecter des données à l'aide d'un dispositif USB connecté localement.
- Les paramètres sont déterminés à partir des données du spooler, de l'application et du pilote d'impression.
- Stocké dans la base de données Workflow
- ECI DCA demande les informations sur les compteurs au Workflow via un appel API (Application Programming Interface) au



Printanista

webservice.

-L'ECD fournit des données au centre Printanista pour

-La connexion entre le flux de travail et l'ECI DCA est cryptée (https).

Configuration requise pour Printanista Workflow

Serveur et outils d'administration

Vous pouvez installer les composants du serveur Printanista Workflow sur des ordinateurs qui fonctionnent :

- Microsoft Windows Server 2012 R2 ou version ultérieure
- Windows 8 Professional ou plus récent

(64bit) Une installation complète du serveur

nécessite :

- Un minimum de 5 gigaoctets d'espace libre pour supporter le logiciel de workflow.
- SQL Database et SQL Express 2012 sont nécessaires. SQL Express 2012 sera installé s'il est absent
- Internet Information Service (IIS) est nécessaire et sera installé s'il n'est pas présent.
- Microsoft .NET Framework 4.7.2 est requis et sera installé s'il n'est pas présent.
- Par défaut, tous les travaux d'impression et les journaux sont stockés sur ce serveur.

Important : les systèmes d'exploitation Microsoft Home et Microsoft Small Business Server ne sont pris en charge pour aucun des composants.

Configuration requise pour le client Windows et utilisation de la mémoire

Vous pouvez installer le logiciel Printanista Workflow Client Popup sur des ordinateurs fonctionnant sous Microsoft Windows 8 ou plus récent.

- Une installation complète du client nécessite environ 10 à 20 Mo d'espace

disque. Le client se compose de deux éléments : le Desktop Client et le Client Service.

- Le Desktop Client nécessite entre 5 et 20 mégaoctets, en fonction de l'activité.
- Aucun logiciel supplémentaire n'est nécessaire.

Configuration requise pour Workflow Client pour Mac

- Workflow Client for Mac® est supporté sur les systèmes d'exploitation Mac® suivant le modèle de support d'Apple.
- Le client Mac® ne prend en charge que la dernière version de Mac® OS et deux versions antérieures.
- Cliquez sur "À propos de ce Mac®" dans votre menu Apple, pour connaître la version de Mac® OS en cours d'exécution sur la station de travail.
- Workflow Client for Mac® nécessite également un (1) PC Windows pour héberger le serveur de workflow et la base de données.

Important : Printanista Workflow doit être installé sur un réseau avec au moins un ordinateur Windows.

Support du serveur web IIS

Le Workflow utilise Internet Information Services (IIS) pour communiquer avec les périphériques et en interne entre les composants du Workflow. L'installation nécessite la version complète d'IIS. Le programme d'installation détermine si vous disposez d'une installation IIS existante. Si ce n'est pas le cas, le programme d'installation créera un nouveau site et un pool d'applications à l'aide d'IIS.

Exigences en matière de mise en réseau

Printanista Workflow utilise par défaut la communication standard HTTP/SSL via les ports 80/443 pour les services web. Si ces ports ne sont pas disponibles, le Workflow utilisera 6320/6321. Cependant, vous pouvez changer les ports de communication s'il y a un conflit dans votre organisation.

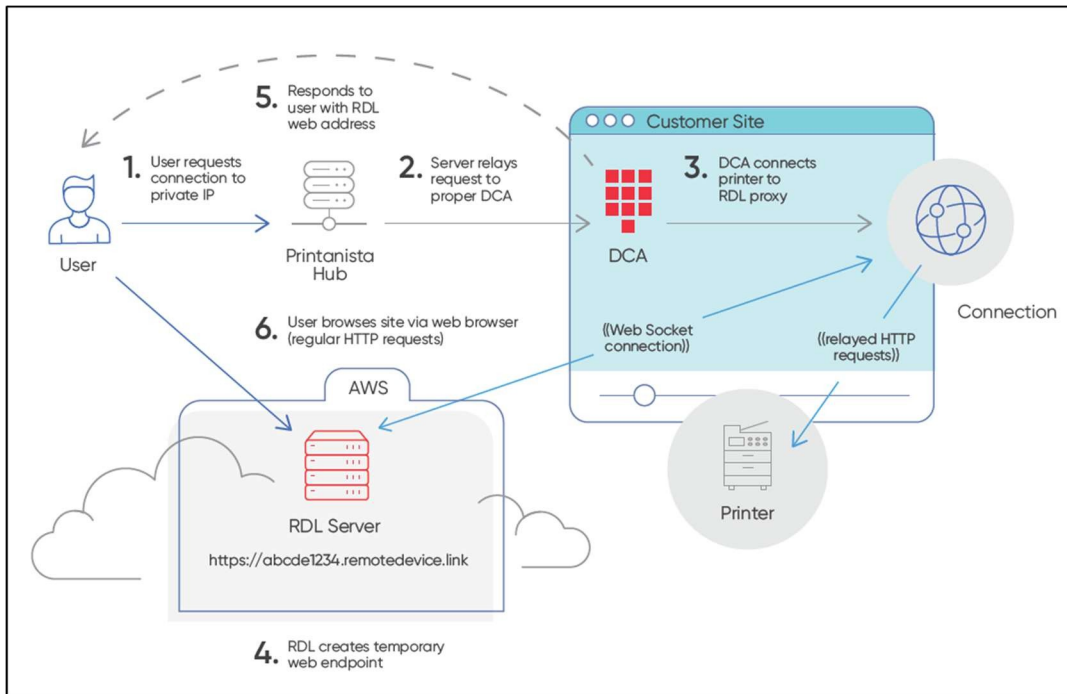
Données fournies à l'ICE DCA par le serveur de flux de travail :

Exemples d'informations d'identification des appareils : Fabricant, modèle, adresse IP, numéro de série/numéro d'actif, emplacement, pages couleur/monochrome, impressions couleur/monochrome, etc.

La documentation d'aide de Printanista Workflow est disponible ici :

[Aide sur le flux de travail de Printanista](#)

Remote Device Link (RDL)



Présentation du système - Remote Device Link (RDL)

Remote Device Link (RDL) est un service permettant à un **utilisateur final** distant d'accéder à un point d'accès HTTP sur un réseau local privé. Il se compose de quatre éléments principaux :

1. L'**utilisateur final** qui accède à l'appareil
2. Le **serveur Remote Device Link**, sur l'internet public (via l'URL `https://*.remotedevice.link`)
3. Le **client RDL** (intégré dans le DCA), fonctionnant sur le LAN privé
4. Le **point d'accès HTTP** (imprimante) auquel on accède (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 d'extrémité et/ou le statut SSL.

Permissions d'habilitation et

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

Audit Capacités

1. Audit local de Printanista Hub sur les détails de chaque session
 - a. Rapports d'administration du hub Printanista pour l'audit de la liaison de périphérique à distance (RDL)
2. Remote Device Link (RDL) Enregistrement de tous les détails de la session dans le nuage AWS (Amazon Web Services)

Remote Device Link (RDL) Sécurité

La sécurité de la liaison avec les appareils à distance (RDL) a été une préoccupation majeure lors de l'élaboration de cet outil. Autorisation :

- L'utilisateur doit avoir la permission d'accéder à la fonction Remote Device Link (RDL) sur le compte spécifique à partir de Printanista Hub.
- L'agent de collecte de données (DCA) n'acceptera que les demandes de liaison à distance (RDL) provenant du serveur Printanista Hub qui est mutuellement authentifié.
- L'agent de collecte des données (DCA) n'établit une connexion RDL (Remote Device Link) qu'avec les périphériques d'impression connus et actuellement surveillés qui se trouvent dans la ou les plages IP de découverte de l'agent de collecte des données (DCA).
- Chaque requête web doit être adressée à la même adresse IP - L'agent de collecte des données (DCA) ne suit 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 norme TLS 1.2 (Transport Layer Security).
- Chaque connexion reçoit un nom de domaine unique qui utilise une combinaison alpha/numérique aléatoire de 19 caractères (96 bits).
- Chaque demande nécessite un jeton de sécurité de 160 bits, stocké sous la forme d'un cookie du navigateur, qui n'est défini qu'au tout début de la session sécurisée par le cryptage TLS.
- L'agent de collecte des données (DCA) peut établir une connexion HTTP non cryptée avec le périphérique d'impression sur le réseau local, mais prend en charge TLS 1.2 si le périphérique n'a pas de connexion HTTP cryptée.

Limites de temps de la session :

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

Implications

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

Tout le trafic transitant du DCA vers l'internet est crypté. Cependant, le DCA ECI peut communiquer avec l'appareil dans le réseau local via des connexions HTTP ordinaires 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 basée sur le web. Gestion des utilisateurs basée sur les permissions

L'accès à l'interface web du Hub Printanista est contrôlé par une gestion des utilisateurs basée sur les permissions. Les utilisateurs doivent se connecter à Printanista en utilisant un nom d'utilisateur et un mot de passe désignés. Les utilisateurs se voient attribuer un ou plusieurs rôles qui spécifient les permissions et se voient accorder l'accès à un ou plusieurs groupes d'appareils. Les administrateurs disposant d'une autorisation complète peuvent spécifier exactement les écrans que chaque utilisateur peut visualiser 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 l'internet.

Printanista côte à côte

Printanista Hub utilise une base de données de métadonnées de modèle connue sous le nom de Side-by-Side (SBS), qui contient divers attributs de modèle tels que : les vitesses d'impression, la date d'introduction sur le marché ou les compatibilités des numéros de pièces OEM, qui est périodiquement mise à jour au fur et à mesure que les futurs modèles et versions sont mis sur le marché par les OEM. Le Hub Printanista communiquera avec Side-by-Side pour vérifier les nouvelles mises à jour ainsi que pour récupérer les métadonnées des appareils afin de les mettre en cache localement sur chaque système du Hub Printanista.

Hébergement d'applications du Hub Printanista

Printanista Hub est hébergé par ECI Software Solutions dans des centres de données sécurisés et protégés dans différentes régions du monde. ECI Software Solutions comprend que la confidentialité, l'intégrité et la disponibilité des informations de nos clients sont vitales pour leurs opérations commerciales et pour notre propre succès. Nous utilisons une approche à plusieurs niveaux 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

Nos services sont hébergés 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 de l'ECI relatif à la sécurité des centres de données.

[ECI Cloud Security Overview 2021 \(ecisolutions.com\)](https://www.ecisolutions.com/Cloud-Security-Overview-2021)

Gestion des versions

Processus de test et de mise
en production

Chaque version majeure ou mineure du logiciel est soumise à un processus de contrôle de la 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 de la fonctionnalité du système, et de valider les nouveaux aspects fonctionnels. Les versions majeures sont soumises à un processus de version bêta au cours duquel des clients sélectionnés utilisent le nouveau et l'ancien système en parallèle.

Sécurité du code source

Le code source de Printanista est conservé dans un système sécurisé de contrôle des révisions, accessible uniquement aux personnes autorisées. Chaque modification du code source doit être approuvée par deux développeurs autorisés avant d'être acceptée dans le dépôt de code de production, où chaque modification est suivie, avec indication du développeur qui l'a effectuée et de la raison de cette modification. Les produits sont cryptés et signés numériquement à l'aide d'un certificat de signature de code fiable avant d'être expédiés. Un dépôt fiduciaire peut être mis à disposition sur demande.

L'ECI fait appel à un tiers indépendant certifié CREST, SOC 2, NSA-CIRA, CSA-STAR pour effectuer des tests de pénétration au niveau des applications et remédier aux 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 changements importants sont apportés au système. La politique d'ECI consiste à déployer des efforts commercialement raisonnables pour remédier à toutes les constatations critiques dans les 30 jours ou dans un délai raisonnable sur la base d'une analyse de rentabilité. 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.

Confidentialité des données et législation

Règlement général sur la protection des données (GDPR)

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

ECI a mis en œuvre un programme structuré et complet de conformité au GDPR. 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 de mise en conformité. Nous encourageons nos clients à prendre des mesures similaires pour s'assurer que leurs propres entreprises sont conformes au GDPR et pour les années à venir.

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

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

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

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

Les communications du moteur du produit sont contrôlées, en utilisant un accès limité pour contacter une adresse IP spécifique et/ou une plage d'adresses.

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

La communication en dehors du réseau utilise un flux de données propriétaire et compressé qui est envoyé à l'aide de la norme industrielle SSL sur HTTPS.

Pour toute information relative au respect de lois et/ou de réglementations spécifiques, veuillez contacter votre gestionnaire de compte ECI.

Ce qui suit est un lien vers la sécurité de l'ECI Cloud : [ECI Cloud Security Overview 2021 \(ecisolutions.com\)](https://www.ecisolutions.com/eci-cloud-security-overview-2021)

Foire aux questions (FAQ)

Les produits Printanista fonctionnent-ils avec des proxys Internet ?

Oui, l'ECI DCA peut fonctionner avec la plupart des proxys. La configuration des paramètres du proxy est nécessaire sur le système où l'ECI DCA est installé et fonctionne.

Quelles sont les exigences minimales de Printanista Hub, ECI DCA, Onsite ?

Veillez vous référer à la section du présent document relative [aux exigences de la candidature Printanista](#).

Les produits Printanista sont-ils compatibles avec les environnements Mac, Linux ou Raspberry Pi ?

Cette ECI DCA présente des avantages majeurs par rapport à la DCA sur site, sans perdre aucune caractéristique, notamment la prise en charge native de Windows, macOS, Linux et Raspberry Pi. Chacune de ces plateformes est dotée d'étapes d'installation uniques, d'une documentation d'assistance et d'un personnel d'assistance formé. Le processus d'installation a également été grandement amélioré et est beaucoup plus intuitif pour tous les types d'utilisateurs.

L'ICE DCA nécessite-t-elle Microsoft Internet Information Services (IIS) ?

Non. L'ECI DCA et l'Onsite DCA comprennent leur propre serveur pour héberger l'interface utilisateur basée sur le web (UI) et sont configurés automatiquement pendant l'installation.

Pouvez-vous installer ECI DCA sur un ordinateur qui héberge déjà un autre site web IIS ?

Oui, mais les ports énumérés ci-dessous doivent être inscrits sur la liste blanche pour garantir la connectivité de l'ECI DCA.

Service	Port	Connexion à
Téléchargement des données	443/TCP (HTTPS)	Votre serveur Printanista Hub
Mises à jour du logiciel	443/TCP (HTTPS)	L'ICE met à jour le serveur
Enregistrement (fallback)	53/UDP (DNS)	Réseau local Serveur DNS (primaire) Serveur de mise à jour ECI (fallback)

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

Quel est le niveau d'entretien permanent de l'ECI DCA ?

ECI DCA et Onsite DCA est un service qui fonctionne en arrière-plan et effectue des audits et des exportations vers des destinations configurées selon des calendriers prédéfinis. Il est recommandé d'utiliser des sous-réseaux (plages d'IP) plutôt que des 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.

Comment fonctionne l'outil d'évaluation de WebAudit ?

Depuis Printanista Hub, le revendeur spécifie le cycle de facturation applicable à l'utilisateur final (vos clients). A ce moment-là, un e-mail est automatiquement généré et envoyé au contact approprié pour l'informer qu'il est temps de collecter ses compteurs. Les instructions comprennent une URL qui, lorsque l'utilisateur final clique sur le lien, lance automatiquement son navigateur web, prêt à effectuer l'action. L'utilisateur final clique ensuite sur "démarrer" et "enregistrer". C'est fait. Aucun logiciel n'est installé à aucun moment. Un lien vers la page WebAudit peut également être affiché sur le site web existant du concessionnaire, c'est-à-dire sur la page web de saisie des relevés de compteurs. Cela permet à l'utilisateur d'automatiser la collecte, plutôt que de passer manuellement d'un appareil à l'autre, d'imprimer la page de configuration et de transcrire les compteurs.

Avec quelles marques d'équipement la surveillance par liaison de dispositifs à distance (RDL) fonctionne-t-elle ? Quelles sont les conditions requises pour qu'il fonctionne ?

Toutes les marques ayant une page web intégrée sont découvertes par ECI DCA. Les informations contenues dans les pages web intégrées varient en fonction du fabricant et du modèle. Les appareils locaux n'afficheront pas la page web intégrée.

La liaison de dispositifs à distance (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 signale que les appareils découverts et activement surveillés par l'intermédiaire de l'ECI DCA. Un message s'affiche pour indiquer que la connexion du dispositif n'est pas prise en charge par la DCA.

Remote Device Link (RDL) semble un peu lent, pourquoi ?

On peut s'y attendre car la connexion doit passer par nos services en nuage. Cependant, le principal facteur d'influence est la rapidité avec laquelle les appareils répondent aux demandes de l'interface utilisateur Web.

Nous avons vu des appareils répondre en quelques dixièmes de secondes aux premières tentatives de connexion, ou être influencés par l'utilisation actuelle ou les ressources disponibles pour l'interface utilisateur (UI).

Quelles sont les fonctions disponibles avec Remote Device Link (RDL) ?

Toutes les options auxquelles l'équipementier donne accès via la page web intégrée sont accessibles via Remote Device Link (RDL).

La fonction "Remote Device Link" (RDL) peut-elle être désactivée ?

Oui, il est possible de désactiver cette fonction pour chaque compte.

Il est également possible de désactiver cette fonction pour chaque utilisateur, ce qui permet de bloquer l'accès d'un utilisateur à Remote Device Link (RDL).

Où puis-je obtenir des informations supplémentaires sur Printanista Hub, Printanista Workflow, ECI DCA, legacy Onsite DCA, etc. Des informations supplémentaires sont disponibles sur le site web Printanista de l'ECI : <https://www.ecisolutions.com/products/printanista-hub/>

Legacy Onsite DCA Information

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

- 1GB RAM
- 400 Mo d'espace disque
- Microsoft .NET Framework 4.7.2 ou plus récent
- Windows 7 SP1, 8.1, 10, 11, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022
- La version 4.1.3 d'Onsite et les versions plus récentes prennent en charge Windows Server 2022.
- Internet Explorer 11.0 ou plus récent, Chrome, Firefox
- MDAC 2.8 ou supérieur (normalement inclus lors de l'installation de Windows)
- JET 4.0 ou supérieur (normalement inclus lors de l'installation de Windows)
- Chargé sur une machine qui fonctionne 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](https://(company_Printanista_FQDN)/WebServices/Onsite2Service.asmx)
- Application : fmaonsite.exe
- SOAP over HTTP(s) doit être autorisé à franchir le pare-feu.

Exigences du réseau :

Le trafic SNMP (port 161) doit pouvoir être acheminé à travers le réseau local ou le réseau étendu (WAN).

Veillez utiliser ECI DCA si les systèmes d'exploitation macOS, Linux ou Raspberry Pi sont nécessaires. L'ancien système Java Onsite sur les systèmes Linux et macOS n'est pas fonctionnel.

Configuration PC/imprimante requise pour l'utilisation de 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 plus récent
- Pilote actuel de l'imprimante locale (UPD est recommandé pour les appareils HP)
- L'imprimante doit prendre en charge le langage des travaux d'impression (PJM) ou le langage de gestion d'imprimante (PML).
- Supprimer les pilotes d'impression inutilisés
- Le support bidirectionnel du conducteur est activé
- Modifications du pare-feu Windows - Port 161/33333 entrant/sortant pour TCP et UDP

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, et leurs variantes, sont actuellement pris en charge.

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

Les paramètres de découverte automatique du réseau brevetés de Printanista utilisent un mélange d'algorithmes pour identifier les plages de réseau où les périphériques d'impression peuvent être situés, puis découvrir et communiquer avec les périphériques qui sont en ligne, en passant par de multiples éléments de réseau tels que des postes de travail ou des serveurs actifs, des routeurs, des concentrateurs, des commutateurs et du matériel de réseau supplémentaire.

Les administrateurs du Hub Printanista peuvent gérer à distance les DCA (Data Collection Agent) activés sur le serveur et déclencher à distance l'exécution par l'Onsite de commandes prédéfinies 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 fonctions sont expliquées plus en détail ci-dessous :

Fonction	Localisation	Description
Tâches	Réglages sur place	Il est possible de configurer à distance des tâches à exécuter selon un calendrier prédéfini, mais aussi de sélectionner des tâches (cache, compteurs, fournitures, service) à exécuter immédiatement et de collecter des données sur l'appareil sur commande.
Marches MIB	Réglages sur place	Peut indiquer certains noms d'hôtes IPv4/IPv6 d'appareils et déclencher le lancement immédiat de la collecte des MIB Walks sur le site.
Journaux (détaillés)	Réglages sur place	Peut demander au site de collecter les journaux (critiques, erreurs, avertissements, détails, débogage) à partir d'une certaine date.

Aucune de ces commandes ne conduit à la collecte de données au-delà des types d'informations collectées tels que 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 des serveurs Printanista Updates.

L'ancienne ACD sur site communique avec Printanista à un intervalle prédéfini pour déterminer s'il y a des actions en file d'attente qui n'ont pas encore été exécutées. Cela permet de s'assurer que les actions sont exécutées en temps voulu.

Note : L'ACD sur site initie toujours cette communication avec le serveur Printanista, et non l'inverse.

Note : HP JAMC n'est supporté que lorsqu'il est utilisé en conjonction avec l'ancien DCA sur site lors du lancement initial de Printanista.

Trafic sur le réseau

Les audits réalisés par le logiciel utilisent un système intelligent pour extraire des informations minimales pour chaque imprimante, copieur ou MFP. Contrairement à des produits similaires qui envoient un ensemble fixe de requêtes (un surensemble de toutes les requêtes possibles) à chaque appareil en réseau, Onsite DCA n'envoie que les requêtes pertinentes en fonction des champs pris en charge par l'appareil cible, chaque requête ne représentant pas plus de quelques kilo-octets de données. Pour réduire encore la largeur de bande du réseau, Onsite DCA ne communique pas avec plus de 20 appareils à la fois. Chaque adresse IP dans les plages configurées sera interrogée et si aucune réponse n'est reçue dans le délai configuré, on 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.

Agent USB local (fonctionne UNIQUEMENT avec l'ACD sur site)

L'agent local USB est la solution utilisée pour extraire des informations d'une ou plusieurs imprimantes locales connectées à n'importe quel type de port Windows, tel que le port USB ou le port parallèle. L'agent USB local n'interrompt pas le flux du travail d'impression, il ne s'active que lorsqu'il est sollicité par l'un des outils d'application de collecte de Printanista - DCA sur site ou WebAudit - et se ferme ensuite. L'agent USB local collecte des informations spécifiques en fonction des niveaux d'intelligence du périphérique à partir du moteur et non du spooler d'impression. Les attributs les plus courants sont le modèle, le numéro de série, les compteurs de durée de vie, la couverture des consommables, le niveau des consommables et le service. Printanista Local USB Agent peut être déployé sur les postes de travail à l'aide d'une solution telle que Microsoft SMS. Une reconfiguration de l'antivirus ou des pare-feu logiciels peut être nécessaire si le port SNMP 161 ou le port de repli de l'agent 33333 sont bloqués.

Soutien du fabricant

Les produits Printanista sont neutres vis-à-vis des fabricants. Ils prennent en charge tous les principaux fabricants et familles de modèles. Certains appareils ont des limitations qui empêchent l'extraction de certaines informations.

Inquiétudes concernant les virus

Les fichiers de l'application Printanista ont été signés numériquement pour empêcher leur exécution si l'intégrité du fichier est compromise. Cela permet de s'assurer que tout virus éventuellement présent n'est pas activé et empêche la propagation du virus d'un réseau à l'autre. Pour plus d'assurance, nous vous recommandons d'utiliser un logiciel antivirus sur votre réseau.