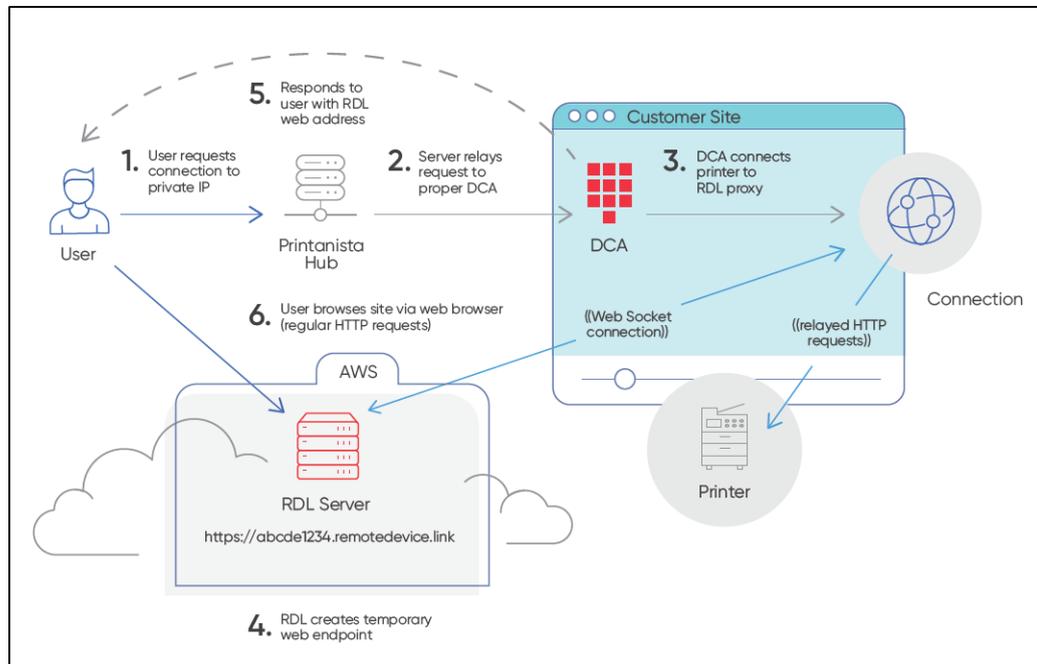


## Remote Device Link - RDL



### 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](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

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.

### Capacités d'Audit

1. Audit local de KDFM Printanista 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)

### Sécurité du Remote Device Link (RDL)

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 KDFM 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.

Tray	Size	Type	Capacity	Level
MP Tray	Legal	Plan	200	Empty
Cassette 1	Letter-R	Plan	500	30%
Cassette 2	Letter	Plan	500	30%

## FAQs

*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).