PRINT AUDIT
INFINITE DEVICE MANAGEMENT

La Sécurité dans Infinite Device Management

Scans

- Les scans SNMP ne sont fait que dans le réseau interne, via le port standard SNMP (port UDP 161).
- Le Moteur de Collecte d'Informations (Information Collection Engine ou ICE) utilise une transmission unicast pour communiquer avec chaque adresse IP faisant partie de la plage d'adresses. Il n'y a pas de paquets broadcast envoyés.
- Une chaîne de communauté SNMP peut être spécifiée dans la configuration du ICE si besoin.

Stockage des données

- Le serveur de Print Audit est situé dans un environnement sécurisé.
- Le serveur de Print Audit est placé derrière un pare-feu matériel qui bloque les accès extérieurs exceptés ceux autorisés par Infinite Device Management.
- Ce serveur est mis à jour avec les dernières versions et corrections de système d'exploitation et d'antivirus
- L'administration du serveur est limitée à nombre très restreint de personnes pour des besoins de maintenance et de sauvegarde.
- Infinite Device Management est la seule application du serveur et ne pose pas de problème de conflit avec d'autres applications.

Data Collection

Aucune information nominative n'est collectée par le ICE. Les seules informations collectées et transmises au serveur sécurisé Print Audit sont les suivantes :

- Nom de l'imprimante, marque et modèle
- Localisation, Numéro de Série
- Adresse IP, Adresse MAC
- Compteurs de Pages
- Niveaux de Toner
- Statut et messages (bourrage, toner vide…)

Transmission des données

- Le ICE se connecte au serveur de Print Audit via une connexion sortante uniquement. Il n'y a pas de connexion du serveur Print Audit vers le ICE.
- La méthode d'envoi configurée dans le ICE est le HTTPS. Les données sont ainsi cryptées avant leur envoi (128 bit SSL on TCP port 443). Si le HTTPS n'est pas disponible, le ICE utilisera le HTTP (port 80).
- Le HTTPS (128-bit SSL) a le même niveau de sécurité que les transactions bancaires ou les achats en ligne sur des sites comme Amazon.
- Le serveur envoie juste un accusé de réception des données reçues, aucune autre information n'est transmise. Cette réponse également cryptée de la même manière que l'envoi.

Interface Web

- Tous les accès se font via une connexion sécurisée (utilisateur et mot de passe) et uniquement à partir du portail https://idm.printaudit.com
- Les logins Infinite Device Management peuvent être restreints à un groupe de client pour un même revendeur (pour un comte de niveau "revendeur") ou à un seul client (pour un compte de niveau "client"). Des privilèges avancés peuvent être accordés aux utilisateurs.
- L'accès sécurisé à l'application fait à https://idm.printaudit.com via un encryptage SSL 128-bit.