Xerox® Remote Services

Livre blanc sur la sécurité

Version 2.0

Services distants mondiaux

Xerox® Technology Information Management

Janvier 2017

BR19369

Le présent document est modifié périodiquement. Les modifications, les imprécisions techniques et les erreurs typographiques seront corrigées dans les prochaines éditions.

IS 614672/IS 514590

Version de document : 2.0 (Janvier 2017).

Table des matières

Objet général et public

Le présent document servira de guide au déploiement de Xerox® Remote Services sur les imprimantes Xerox et non Xerox dans l'environnement réseau du client. Il fournit des informations de sécurité et décrit l'ensemble des mécanismes de sécurité mis en œuvre par Xerox® Remote Services.

Le présent document est destiné aux fournisseurs de solutions techniques, aux responsables de réseau IT et aux professionnels de la sécurité IT intéressés par les fonctionnalités Remote Services et la mise en œuvre de la sécurité de ces fonctionnalités.

Nous recommandons la lecture de l'intégralité de ce document pour certifier l'utilisation de produits et services Xerox® dans l'environnement réseau du client.

Remote Services

Les informations sont l'atout majeur de toute organisation, et la sécurité des documents et des périphériques - notamment des imprimantes multifonctions - qui sont connectés au réseau est essentielle. Aujourd'hui, alors que le réseau est le centre névralgique de la quasi-totalité des activités, gérer un parc de multifonctions tout en maintenant un niveau acceptable de sécurité représente un enjeu unique que beaucoup d'entreprises ignorent. Xerox® comprend cette complexité et répond aux besoins de nos clients en matière de sécurité. Les offres de produits Xerox®, systèmes Xerox® et Xerox® Remote Services sont conçues pour s'intégrer au flux de travail de nos clients tout en mettant en œuvre les dernières technologies sécurisées.

Le livre blanc sur la sécurité Xerox® Remote Services est destiné à aider le client à comprendre et à déployer la solution sécurisée Remote Services appropriée compatible avec son infrastructure réseau. La structure du réseau du client détermine si des modifications doivent être apportées au pare-feu Internet, aux serveurs proxy Web ou à toute autre infrastructure réseau liée à la sécurité. Le choix de la solution Xerox® Remote Services, du périphérique et des contrôles dépend des politiques de sécurité des informations du client et déterminera le mode de fonctionnement utilisé.

La solution Xerox ® Remote Services est disponible pour certains modèles de périphériques. Elle permet l'assistance et la maintenance à distance des périphériques d'impression au moyen de leurs données d'attributs qui comprennent ***: l'identité du périphérique d'impression, les propriétés du périphérique impression, l'état, les niveaux de consommables, les données d'utilisation et les données de diagnostic détaillées.*** Depuis l'environnement réseau du client, ces données d'attributs sont transmises directement depuis le périphérique d'impression (Device Direct), via une application hébergée (application de gestion de périphériques) ou via une combinaison des deux méthodes au travers du canal de communication sécurisé Xerox® Remote Services. Les périphériques Xerox® comme les applications de gestion de périphériques Xerox® s'authentifient au moyen d'un certificat auprès des serveurs de communication Xerox® avant que les attributs d'impression puissent être transmis. Les transactions Remote Services Xerox® émanent toujours de l'environnement du client et sont toujours envoyées uniquement en fonction des autorisations définies par le client.

Les serveurs de communication Xerox® sont basés aux États-Unis et satisfont aux exigences strictes de l'infrastructure de gestion des informations interne de Xerox Corporation. Les centres de données Xerox® et l'application Xerox® Remote Services répondent aux normes SSAE 16 (Statement on Standards for Attestation), Sarbanes-Oxley Act (SOX) et sont certifiés ISO 27001:2013.

Par défaut, aucune donnée image provenant des travaux d'impression, de télécopie, de numérisation ou de copie ni aucune information confidentielle n'est transmise aux serveurs de communication Xerox®.

Contrôles client

Les applications de gestion de périphériques Xerox® permettent d'afficher les journaux exportés d'attributs de périphériques d'impression à des fins d'audit et de vérification avant le chiffrement et la transmission aux serveurs de communication Xerox® distants. Voir le guide de l'utilisateur de l'application de gestion de périphériques Xerox® concernée pour plus de détails.

Certains périphériques de bureau destinés aux PME sont dotés d'une fonctionnalité permettant de télécharger et de visualiser les données d'attributs avant leur chiffrement et leur transmission aux serveurs de communication Xerox® distants via Device Direct. Pour vérifier si un périphérique d'impression intègre cette fonctionnalité, rendez-vous sur la page CentreWare Internet Services, onglet État, lien Smart eSolutions (ou Services distants), puis onglet Maintenance Assistant.

La solution Xerox® Remote Services peut être adaptée en fonction des politiques de sécurité des informations du client qui limitent la transmission de certains types de données d'attributs de périphériques d'impression à l'extérieur du réseau (par exemple, les attributs liés aux adresses réseau). Les applications de gestion de périphériques Xerox® proposent des outils permettant de désactiver certains champs d'attributs de la transmission.

Les clients ont également la possibilité d'invoquer une *demande de dérogation* lors des négociations de contrat afin de **« se désinscrire »** de la solution Remote Services. Cela a pour effet d'empêcher toute communication et assistance à distance des périphériques d'impression de ce compte.

Afin de faciliter les activités d'assistance à distance et leur escalade, les clients peuvent, le cas échéant, activer l'accès distant. Ceci leur permet de recevoir les mises à jour logicielles des périphériques d'impression et les correctifs de sécurité. Ils peuvent en outre réaliser des diagnostics à distance et réparer et modifier les configurations des périphériques d'impression pour corriger les anomalies détectées. Lorsque l'accès distant est activé, Xerox® n'est pas autorisé à visualiser ou télécharger les documents, les données ou toute autre information du client résidant ou transitant sur le périphérique d'impression ou les systèmes d'information du client. Seule exception : lorsqu'un client travaille avec l'équipe d'assistance Xerox sur un problème difficile et que des informations supplémentaires sont requises pour résoudre le problème. Dans ce cas, le client peut décider d'autoriser Xerox à accéder aux journaux enregistrés localement sur le périphérique qui contiennent des données sensibles.

En conséquence, les équipes informatiques et les spécialistes de la sécurité de l'entreprise sont invités à lire l'intégralité de ce document afin de bien cerner les différentes fonctions et opérations de Xerox® Remote Services et comment les utiliser pour se conformer aux stratégies de sécurité des informations.

D'autres ressources de sécurité concernant les mécanismes de protection des données de sécurité des produits Xerox®, les partenariats et les certifications du secteur sont disponibles sur le site http://www.xerox.com/security.

Modèles de déploiement

Les modèles de déploiement de Xerox® Remote Services offrent tous le même niveau de sécurité. Les clients ont le choix entre les modèles suivants :

- **Modèle Device Direct** - Device Direct permet aux périphériques d'impression de communiquer directement avec les serveurs de communication Xerox® distants via Internet après avoir franchi le pare-feu du client.

- **Modèle Application de gestion de périphériques** - Une application de gestion de périphériques Xerox® (c'est-à-dire un gestionnaire de périphériques) peut être déployée sur le réseau du client pour collecter un sous-jeu de données d'attributs sur les périphériques d'impression. Les attributs de plusieurs périphériques d'impression sont collectés puis transmis de manière sécurisée aux serveurs de communication Xerox® distants.

- **Modèle mixte** – Déploiement des modèles Device Direct et Application de gestion de périphériques.

Tous les modèle de déploiement de Xerox® Remote Services mettent en œuvre les protocoles Web et les ports standard pour établir un canal sécurisé et chiffré en vue de transférer les attributs des périphériques d'impression vers l'extérieur aux serveurs de communication Xerox® situés dans des centres de données sécurisés redondants Xerox®.

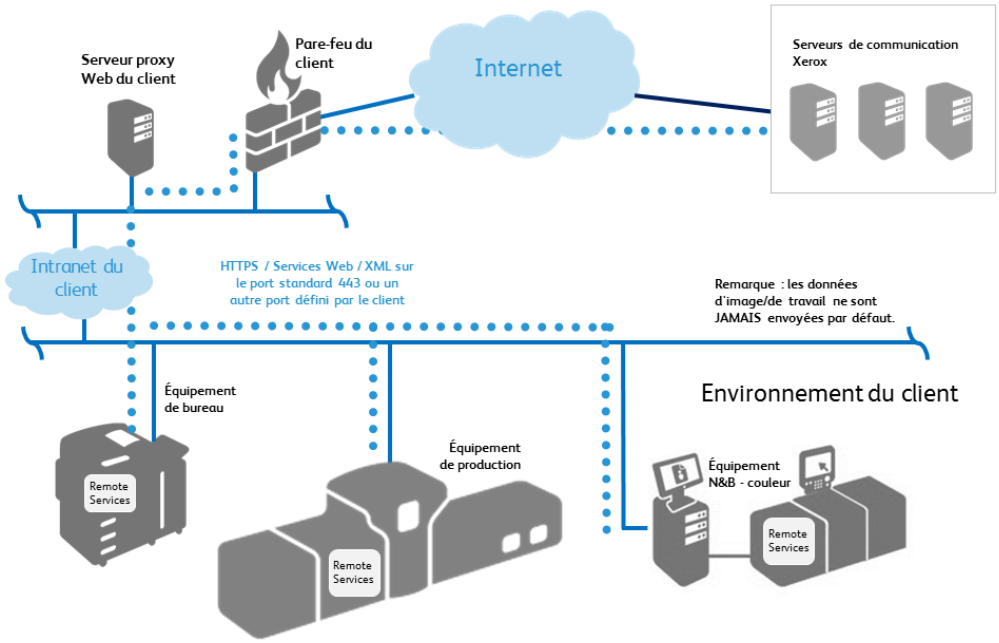
Le modèle de déploiement choisi dépend des politiques et des règles de nos clients en matière de sécurité des informations pour gérer la transmission des attributs des périphériques d'impression ainsi que de la solution de services d'impression et des périphériques achetés auprès de Xerox® (services d'impression de base ou services MPS).

Modèle de déploiement Device Direct

Le module de services distants intégré dans les périphériques Xerox® utilise une connexion TLS 1.2 sur un port standard 443 afin de communiquer avec les serveurs de communication Xerox® distants.

- Les périphériques d'impression dans l'environnement client communiquent directement avec les serveurs de communication Xerox® distants. Pour permettre les communications, des pare-feu standard doivent être configurés sur le site.
- Une URL valide doit être utilisée pour les serveurs de communication Xerox® distants.
- Les serveurs de communication Xerox® se trouvent derrière un pare-feu sécurisé et ne sont pas accessibles depuis Internet.

Figure 1



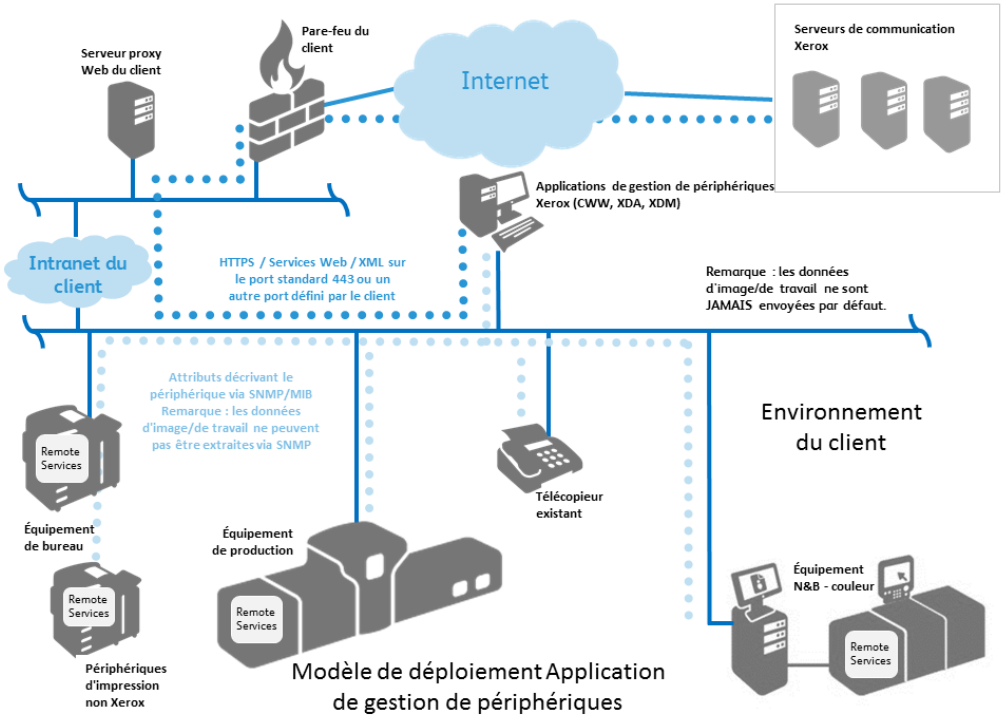
Modèle de déploiement Device Direct

Modèle de déploiement Application de gestion de périphériques

Les applications de gestion de périphériques (à savoir **Xerox® CentreWare® Web, Xerox® Device Agent, Xerox® Device Agent Partner Edition et Xerox® Device Manager)** utilisent également une connexion chiffrée sécurisée TLS 1.2 sur le port standard 443 pour communiquer avec les serveurs de communication distants Xerox®. D'autres fonctions sont employées pour améliorer la sécurité sur ce canal (qui est établi lors de l'installation initiale des applications de gestion de périphériques), notamment :

- L'application de gestion de périphériques dans l'environnement client lance toutes les communications avec les serveurs de communication Xerox® distants. Pour permettre les communications, des pare-feu standard doivent être configurés sur le site.
- Une URL valide doit être utilisée pour les serveurs de communication Xerox® distants.
- Les serveurs de communication Xerox® se trouvent derrière un pare-feu sécurisé et ne sont pas accessibles depuis Internet.
- Un ID de compte valide ou un identifiant de site et une clé d'enregistrement des serveurs de communication Xerox® doivent être utilisés pour accéder à certains services des serveurs de communication Xerox®.
- L'application de gestion de périphériques demande une inscription auprès des serveurs de communication distants Xerox® à l'aide des informations d'identification appropriées.
- Les serveurs de communication Xerox® distants valident les informations d'identification fournies, puis acceptent la demande.
- L'application de gestion de périphériques authentifie les serveurs de communication distants Xerox® et active le service.

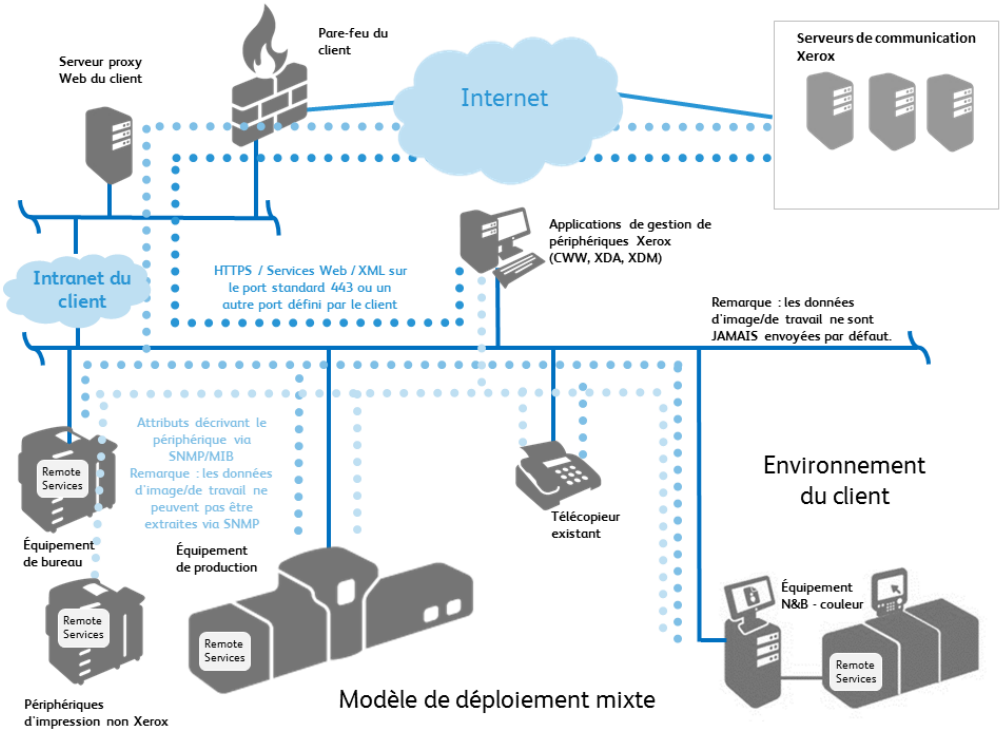
Figure 2



Modèle de déploiement mixte

Le déploiement mixte est possible lorsqu'un client achète plusieurs types de contrats de maintenance Xerox pour ses périphériques d'impression. Lors de l'installation initiale d'un périphérique d'impression Xerox® sur un réseau, le comportement par défaut de Xerox® Remote Services consiste à ce que le périphérique d'impression tente automatiquement d'établir une connexion directe avec les serveurs de communication Xerox®.

Figure 3



Transmission de données et charges utiles

Sources de données

Les données d'attributs des périphériques d'impression sont collectées pour Xerox® Remote Services depuis les sources suivantes :

- Imprimantes de bureau Xerox® en réseau
- Imprimantes réseau non Xerox®
- Imprimantes de production Xerox®
- Applications de gestion de périphériques Xerox®

Périphériques de bureau Xerox®

Les périphériques d'impression de bureau Xerox® transmettent les données d'attributs au format XML (eXtensible Markup Language) Xerox®, compressées dans un fichier .zip. Chaque fichier est ensuite transmis via un canal chiffré aux serveurs de communication Xerox® distants.

Le tableau 1 identifie les données d'attributs pouvant être transmises et leur description.

Données d'attributs	Description
Identité du périphérique d'impression	Inclut le modèle, la version du micrologiciel, les numéros de série des modules et la date d'installation.
Adresse réseau du périphérique d'impression	Inclut l'adresse MAC (Media Access Control) et l'adresse du sous-réseau.
Propriétés du périphérique d'impression	Inclut la configuration détaillée des composants matériels et des modules logiciels, les fonctionnalités/services pris en charge, les modes d'économie d'énergie, etc.
État du périphérique d'impression	Inclut l'état général, les alertes détaillées, l'historique des 40 dernières défaillances, les données de bourrage, etc.
Compteurs du périphérique d'impression	Inclut les compteurs de facturation, d'impressions, de copies, de télécopies, de travaux volumineux et de numérisations vers une destination, les statistiques relatives à l'utilisation, etc.
Consommables du périphérique d'impression	Inclut le nom, le type (p. ex. image, finition, type de papier), le niveau, la capacité, l'état, la taille du consommable, etc.

Données d'attributs	Description
Utilisation détaillée du périphérique d'impression	Inclut le détail des compteurs d'impressions, les états sous tension, le nombre de remplacements de CRU (unités remplaçables par le client), les données détaillées sur les défaillances de CRU et leur répartition, les données d'utilisation de la fonction de reconnaissance optique de caractères (ROC) intégrée, la répartition des longs tirages, la répartition de l'utilisation des magasins, les supports installés, la répartition des types de supports, des formats de supports, des longueurs de document, le nombre de jeux, les données HFSI, les données NVM, le nombre de pixels marqués, le taux de couverture moyen par couleur, les défaillances/incidents, le détail des compteurs de numérisations.
Ingénierie / Débogage	Inclut les données de débogage détaillées qui peuvent comprendre d'autres données que celles listées ci-dessus. Ces données peuvent inclure des informations d'identification personnelle telles que les noms d'utilisateur, les adresses électroniques et les données de travail. Elles sont transmises avec l'autorisation expresse du client et sont destinées exclusivement au support de niveau supérieur.

Remarque : le fichier et le contenu des données identifiées varient en fonction du modèle du produit.

Périphériques de production Xerox®

Les périphériques de production Xerox® transmettent les données d'attributs au format XML (eXtensible Markup Language) Xerox®, compressées dans un fichier .zip. Chaque fichier est ensuite transmis via un canal chiffré aux serveurs de communication Xerox® distants.

Le tableau 2 identifie les données d'attributs pouvant être transmises et leur description.

Données d'attributs	Description détaillée des données d'attributs
Identité du périphérique d'impression	Inclut le modèle, les versions des micrologiciels, les numéros de série et la date d'installation des modules, les coordonnées du client, les données de licence et l'emplacement, si ces informations sont disponibles.
Adresse réseau du périphérique d'impression	Inclut l'adresse MAC (Media Access Control) et l'adresse du sous-réseau.
Propriétés du périphérique d'impression	Inclut la configuration détaillée des composants matériels et des modules logiciels, les fonctionnalités/services pris en charge, etc.
État du périphérique d'impression	Inclut les états actifs, le décompte de l'historique des défaillances, le journal des événements DFE, l'historique des transmissions de données.
Compteurs du périphérique d'impression	Inclut les compteurs de facturation, d'impressions, de copies, de travaux volumineux, de production et de numérisations vers une destination sur les modèles de production d'entrée de gamme, etc.
Consommables du périphérique d'impression	Inclut le nom du fabricant, le modèle, le numéro de série, le nom, le type, le niveau, la capacité, les états, les compteurs sur toute la durée de vie, etc.
Utilisation détaillée du périphérique d'impression	Inclut les données HFSI, les données NVM, les remplacements de pièces, les journaux DFE, les données de diagnostic détaillées, la résolution des défaillances.
Ingénierie / Débogage	Inclut les données de débogage détaillées non structurées destinées exclusivement au support de troisième niveau.
En relation avec les travaux du client	Les périphériques de production Xerox® permettent de reproduire les données liées aux travaux d'impression via des commandes PostScript chiffrées afin de les transmettre aux équipes de support de deuxième et de troisième niveaux de Xerox. Le client peut choisir d'activer ou non cette fonction. S'il choisit de transmettre les données liées aux travaux d'impression (au format PostScript chiffré) à Xerox, celles-ci sont traitées conformément aux politiques et aux normes de sécurité des informations de Xerox.

Il existe des scénarios d'escalade dans lesquels les informations de débogage détaillées peuvent inclure des données d'attributs autres que celles identifiées dans les tableaux 1 à 3. Ces données sont transmises conformément aux politiques et aux normes de sécurité des informations de Xerox.

Remarque : le fichier et le contenu des données identifiées varient en fonction du modèle du produit.

Applications de gestion de périphériques Xerox®

Les applications de gestion de périphériques Xerox®, telles que Xerox® CentreWare® Web (**CWW**), Xerox® Device Agent (**XDA**), Xerox Device Agent Partner Edition (**XDA PE**) et Xerox® Device Manager (**XDM**) transmettent les données d'attributs des périphériques d'impression au format XML (eXtensible Markup Language), compressées dans un fichier .zip. Le fichier est ensuite chiffré et transmis via des canaux chiffrés aux serveurs de communication Xerox® distants.

Le tableau 3 identifie les données d'attributs pouvant être transmises via l'application de gestion de périphériques Xerox® et leur description.

Données d'attributs	Description détaillée des données d'attributs
Identité du périphérique d'impression	Inclut le nom du fabricant, le modèle, la description, la version du micrologiciel, le numéro de série, les étiquettes de l'équipement, le nom du système, le contact, l'emplacement, l'état de gestion, le nom de la file d'attente, le nom du poste de travail (bureau) et le numéro de téléphone/télécopie.
Adresse réseau du périphérique d'impression	Inclut l'adresse MAC, l'adresse IP, le nom DNS, le masque de sous-réseau, l'adresse IP de la passerelle par défaut, la dernière adresse IP connue, l'adresse IP modifiée, le fuseau horaire, l'adresse IPX, le numéro de réseau externe IPX et l'adresse IPX du serveur d'impression.
Propriétés du périphérique d'impression	Inclut les composants installés, la description des composants, les fonctionnalités et les services pris en charge, la vitesse d'impression, la prise en charge des couleurs, les options de finition, la prise en charge de l'impression recto verso, la technologie de marquage, les données de disque dur et de mémoire vive, les langues prises en charge, les propriétés définies par l'utilisateur.
État du périphérique d'impression	Inclut l'état général, les alertes détaillées, les messages de la console locale, l'état des composants, les données liées à l'extraction de l'état, la date de détection, la méthode et le type de détection, le temps de fonctionnement du périphérique, les pièges pris en charge/activés.
Compteurs du périphérique d'impression	Inclut les compteurs de facturation, d'impressions, de copies, de télécopies, de travaux volumineux et de numérisations, les statistiques relatives à l'utilisation et le volume cible.
Consommables du périphérique d'impression	Inclut le nom, le type (p. ex. image, finition, type de papier), le niveau, la capacité, l'état, la taille du consommable, etc.

Données d'attributs	Description détaillée des données d'attributs
Utilisation détaillée du périphérique d'impression	Données de suivi des tâches des utilisateurs incluant les caractéristiques des travaux (ID, nom du document, propriétaire, type de document, type de travail, couleur, recto verso, support requis, format, pages, jeux, erreurs), la destination (périphérique d'impression, modèle, nom DNS, adresse IP, adresse MAC, numéro de série), les résultats d'impression du travail (heure de la soumission, durée du travail d'impression, pages imprimées, pages couleur/noir et blanc imprimées, mode couleur utilisé, N en 1), les données de comptabilité (code de rétrofacturation, prix de rétrofacturation, source de comptabilité), la source du travail d'impression (poste de travail, nom/adresse MAC du serveur d'impression, nom de la file d'attente, port, nom d'utilisateur, ID utilisateur), les données de gestion Xerox (envoyées à Xerox® Services Manager).
Identité de l'application de gestion de périphériques	Inclut les informations relatives à l'ordinateur, par exemple le nom DNS, l'adresse IP, le nom du système d'exploitation, le type de système d'exploitation, le processeur, les tailles de RAM (libre et utilisée), les tailles de disque dur (libre et utilisé), le nom du site, la version de l'application, la date d'expiration de la licence de l'application, la version de l'infrastructure .NET, le fuseau horaire, la version du composant de détection, la taille de la base de données principale, la taille de la base de données de détection, le nombre d'imprimantes dans/hors champ d'application, les services critiques en cours d'exécution.
Mode de sécurité entreprise de l'application de gestion de périphériques	**Mode normal** = Xerox® Device Agent contacte Xerox® Services Manager quotidiennement. Les paramètres peuvent être modifiés à distance sans qu'aucune intervention sur site ne soit nécessaire, même lorsque les interrogations programmées sont désactivées. **Mode de verrouillage** = Outre la synchronisation des données relatives à l'imprimante, il n'y a aucune communication avec Xerox® Services Manager et les paramètres doivent être modifiés sur site. Les adresses IP du périphérique Xerox® Device Agent et de l'imprimante IP sont transmises à Xerox® Services Manager.
Politique de contrôle de l'impression de l'application de gestion de périphériques	Inclut le nom de l'ordinateur de l'utilisateur final, le serveur d'impression utilisé, la file d'impression utilisée, l'horodatage de la violation, le nom du document, le nom de l'utilisateur final, l'utilisation ou non du mode recto verso, l'utilisation ou non de l'impression couleur, le nombre total d'impressions du travail, le coût du travail, l'action effectuée, l'envoi ou non d'une notification à l'utilisateur final, l'affichage ou non d'un message, le nom de la politique d'impression, la règle de la politique d'impression.

Gestion à distance des périphériques d'impression

Le personnel de support de Xerox® peut traiter les actions suivantes par le biais de l'applications de gestion de périphériques Xerox®. Dans la mesure où elles sont autorisées, ces actions sont effectuées dans le cadre de la résolution d'anomalie et décrites dans le **Tableau 4** ci-dessous.

Données	Description
Actions à effectuer sur les périphériques d'impression	• **Obtenir l'état du périphérique** = extrait le dernier état à partir du périphérique d'impression • **Redémarrer le périphérique** = procède à l'arrêt/au redémarrage du périphérique d'impression • **Mettre à niveau le périphérique** = installe les nouveaux logiciels/micrologiciels sur le périphérique d'impression (.DLM via le port 9100) • **Dépanner le périphérique** = envoie une commande PING au périphérique + extrait le dernier état à partir du périphérique d'impression • **Imprimer une page de test** = soumet un travail test au périphérique d'impression pour valider le chemin d'impression (génère un rapport de configuration) • **Lancer la gestion du périphérique** = lance les transferts périodiques de données du périphérique d'impression vers les serveurs de communication Xerox® externes **Remarque :** chaque action peut être désactivée sur demande dans la section de configuration administrative des applications de gestion de périphériques Xerox® qui prennent en charge cette fonction.
Actions à effectuer sur les périphériques d'impression	• **Redémarrer le périphérique** = procède à l'arrêt/au redémarrage du périphérique d'impression • **Imprimer une page de test** = soumet un travail test au périphérique d'impression pour valider le chemin d'impression (génère un rapport de configuration)
Actions à exécuter sur les applications de gestion de périphériques	Les paramètres dans chaque application de gestion de périphériques qui peuvent être gérés comprennent la détection de périphériques, la fréquence d'exportation des données, les paramètres liés aux communications SNMP (nouvelle tentative, expiration du délai, noms des communautés), les profils d'alerte et la fréquence des mises à jour logicielles automatiques de l'application de gestion de périphériques.

Configuration système pour les applications de gestion de périphériques

La configuration requise minimale varie légèrement selon les offres. Reportez-vous au guide de l'utilisateur, au guide d'évaluation de la sécurité et/ou au guide de certification pour connaître les exigences de base propre à chaque application de gestion de périphériques. Des informations supplémentaires sont disponibles sur le site : http://www.support.xerox.com/support/enus.html

Lors de l'installation de l'application de gestion de périphériques, un fichier .readme ou .lisezmoi est également installé afin de vous donner plus de détails sur la configuration système requise pour cette application.

- Nous recommandons d'utiliser des ordinateurs hôtes exécutant un système d'exploitation Microsoft ® Corporation. Toutefois, les applications de gestion de périphériques Xerox® peuvent s'exécuter dans l'environnement d'exploitation Macintosh si vous utilisez le logiciel d'émulation Parallels Desktop. (Il est impossible pour le moment d'exécuter une application de gestion de périphériques Xerox® dans un environnement Macintosh natif.) Voir le guide de l'utilisateur de l'application de gestion de périphériques Xerox® concernée pour plus de détails.
- Nous vous recommandons de tenir à jour les ordinateurs hôtes avec les correctifs critiques et les service packs les plus récents disponibles auprès de Microsoft ® Corporation.
- Le protocole TCP/IP (Network Transmission Control Protocol/Internet Protocol) doit être chargé et opérationnel.
- Une connexion Internet est requise.
- Les droits administrateur sont requis pour installer l'application de gestion de périphériques sur la machine cliente.
- Requiert des périphériques SNMP et la possibilité d'acheminer des données SNMP sur le réseau. Il n'est pas nécessaire d'activer SNMP sur l'ordinateur sur lequel les applications de gestion de périphériques Xerox® seront installées ni sur aucun autre ordinateur réseau.
- Vous devez installer Microsoft®.NET Framework 4.6 (version intégrale) avant d'installer l'application.
- L'application ne doit pas être installée sur un ordinateur sur lequel sont installés d'autres applications SNMP ou d'autres outils de gestion de périphériques Xerox®, car cela risquerait de perturber leur fonctionnement respectif.

Configurations non prises en charge

- Installation de l'application sur un ordinateur sur lequel est déjà installée une autre application de gestion de périphériques Xerox®, telle que Xerox® Device Manager.
- Toute version des systèmes d'exploitation Unix® ou Linux®.
- Systèmes d'exploitation Microsoft® en fin de vie tels que Windows NT® 4.0, Windows® Media Center, Windows® XP et Windows® Server 2000 et 2003.
- Environnements virtuels autres que VMware® Lab Manager™/Workstation/vSphere Hypervisor™. Cette application peut fonctionner dans d'autres environnements virtuels ; toutefois, ces environnements n'ont pas été testés.

Processus métier et services Xerox®

Les données reçues par les serveurs de communication Xerox® provenant des périphériques d'impression de bureau Xerox®, des périphériques d'impression de production Xerox® et des applications de gestion de périphériques Xerox® sont utilisées par les processus métier Xerox suivants :

Nom du processus métier	Description
Relevés de compteurs automatiques	Une facture est générée automatiquement à partir des relevés de compteurs émanant des périphériques d'impression.
Réapprovisionnement automatique des consommables/pièces	Du toner est automatiquement envoyé aux clients quand un état de niveau de consommable faible est reçu en provenance des périphériques d'impression. Les composants remplaçables sont automatiquement expédiés aux clients lorsque cela est nécessaire sur leurs périphériques d'impression. Ces options sont uniquement accessibles aux clients qui optent pour les contrats d'approvisionnement avec relevés de compteurs.
Facilité d'entretien (Maintenance Assistant)	Le personnel de maintenance de Xerox a accès à des informations détaillées sur les défaillances, lorsque cela est nécessaire, pour accélérer la planification d'une visite sur site ou établir un diagnostic à distance après avoir reçu une demande d'intervention du client.
Support de troisième niveau (Ingénierie/Débogage)	Le personnel en charge du support produit peut résoudre les problèmes difficiles après avoir accédé aux journaux d'ingénierie et de débogage détaillés.

Les données de base des périphériques d'impression sont compressées, transmises, conservées et archivées dans un centre de données Xerox® certifié ISO-27001, conformément aux politiques de conservation des données d'entreprise de Xerox ®.

Les processus de travail et les pratiques qui prennent en charge et protègent les systèmes logiciels Xerox® Remote Services de back-office sont basés sur les meilleures pratiques définies par l'ITIL ainsi que sur les politiques relatives à la sécurité des informations de Xerox qui sont basées sur les normes ISO 27001. Les clients sont ainsi assurés que l'intégrité, la confidentialité et la protection des données seront gérées en conformité avec les normes les plus strictes en vigueur.

Détails de la technologie

Cette section décrit les détails techniques supplémentaires généralement nécessaires au personnel informatique et aux équipes en charge de la sécurité qui cherchent à gérer les risques en obtenant l'assurance de pratiques de développement sécurisées, ce qui permet la certification des périphériques d'impression et des applications de gestion de périphériques en vue de leur utilisation dans l'environnement réseau du client.

Conception des logiciels

La sécurité des produits Xerox® prime dès les premières phases de développement des produits et se traduit par la mise en œuvre de techniques de codage sécurisées et l'exécution de nombreux tests et analyses en vue d'éliminer les vulnérabilités. Xerox® met activement en application des pratiques de certification, telles que les Critères communs, et participe activement à l'élaboration de nouvelles normes, comme le P2600 Working Group et la méthodologie de développement sécurisée SDL (Security Development Lifecycle).

Utilisation

Xerox® Remote Services permet les types d'opérations suivants sur un réseau :

Méthode de déploiement	Application utilisée	Flux de données sur le réseau	Utilisation imposée sur un réseau
Device Direct	Aucune	Interne	Le périphérique d'impression Xerox® tente de détecter un serveur proxy Web (automatiquement ou acheminement vers une adresse spécifique).
		Interne	Le périphérique d'impression Xerox® génère des requêtes qu'il transmet à un serveur SMTP (Simple Mail Transport Protocol) pour envoyer une notification par courrier électronique à une liste de destinataires définie.
		Externe au réseau	Le périphérique d'impression Xerox® franchit le pare-feu de l'entreprise pour accéder à Internet (HTTPS sur le port 443).
		Externe au réseau	Le périphérique d'impression Xerox® s'authentifie au moyen de son certificat auprès des serveurs de communication Xerox avant la transmission des données d'attributs.
		Externe au réseau	Le périphérique d'impression Xerox® transmet automatiquement les données d'attributs via un canal chiffré (HTTPS sur le port 443) aux serveurs de communication Xerox® à une heure précise chaque jour ou à la demande du client.

Méthode de déploiement	Application utilisée	Flux de données sur le réseau	Utilisation imposée sur un réseau
		Externe au réseau	Le périphérique d'impression Xerox® interroge automatiquement les serveurs de communication Xerox® via un canal chiffré (HTTPS sur le port 443) à une heure précise chaque jour pour leur demander la liste des actions à effectuer (par exemple, envoi immédiat des données de facturation, ajout d'un service, etc.).
		Externe au réseau	Transmission sur demande unilatérale des données du journal d'ingénierie du périphérique d'impression Xerox® via un canal chiffré (HTTPS sur le port 443) au serveur de communication Xerox®
Applications de gestion de périphériques	CentreWare® Web	Interne	Chaque application détecte un serveur proxy Web (automatiquement ou acheminement vers une adresse spécifique).
		Interne	Chaque application extrait les fonctionnalités des périphériques d'impression dans le parc d'impression via SNMP.
		Interne	Chaque application extrait la configuration des périphériques d'impression dans le parc d'impression via SNMP.
		Interne	Chaque application extrait l'état des périphériques d'impression dans le parc d'impression via SNMP.
		Interne	Chaque application extrait les données relatives aux consommables des périphériques d'impression dans le parc d'impression via SNMP.
		Interne	Chaque application peut redémarrer un périphérique d'impression via SNMP ou via l'interface utilisateur Web du périphérique d'impression.
		Interne	Chaque application peut envoyer une page de test à un périphérique d'impression spécifique.
		Interne	Chaque application peut lancer la page Web d'un périphérique d'impression.
		Externe **(sortie uniquement)**	Chaque application franchit le pare-feu de l'entreprise pour accéder à Internet (HTTPS sur port 443).
		Externe **(sortie uniquement)**	Chaque application s'authentifie au moyen de son certificat auprès des serveurs de communication Xerox avant la transmission des données d'attributs.
		Externe **(sortie uniquement)**	Chaque application transmet automatiquement les données d'attributs des périphériques d'impression via un canal chiffré (HTTPS sur le port 443) aux serveurs de communication Xerox® à une heure précise chaque jour.

Méthode de déploiement	Application utilisée	Flux de données sur le réseau	Utilisation imposée sur un réseau
		Externe **(sortie uniquement)**	Chaque application interroge automatiquement les serveurs de communication Xerox® via un canal chiffré (HTTPS sur le port 443) à une heure précise chaque jour pour leur demander la liste des actions à effectuer.
Applications de gestion de périphériques	Xerox® Device Agent Partner Edition pour contrôler les périphériques d'impression connectés au réseau	Interne	Chaque application Xerox® Device Agent détecte un serveur proxy Web (automatiquement ou acheminement vers une adresse spécifique).
		Interne	Chaque application Xerox® Device Agent extrait les fonctionnalités des périphériques d'impression dans le parc d'impression via SNMP.
		Interne	Chaque application Xerox® Device Agent extrait la configuration des périphériques d'impression dans le parc d'impression via SNMP.
		Interne	Chaque application Xerox® Device Agent extrait l'état des périphériques d'impression dans le parc d'impression via SNMP.
		Interne	Chaque application Xerox® Device Agent extrait les données relatives aux consommables des périphériques d'impression dans le parc d'impression via SNMP.
		Interne	Chaque application Xerox® Device Agent peut demander l'impression d'un rapport de configuration sur le périphérique.
		Interne	Chaque application Xerox® Device Agent peut lancer la page Web d'un périphérique d'impression.
		Interne	Chaque application Xerox® Device Agent peut mettre à jour les logiciels des périphériques d'impression via la soumission d'un travail d'impression. (fichier .DLM sur le port 9100)
		Externe **(sortie uniquement)**	Chaque application Xerox® Device Agent franchit le pare-feu de l'entreprise pour accéder à Internet (HTTPS sur le port 443).
		Externe **(sortie uniquement)**	Chaque application s'authentifie au moyen de son certificat auprès des serveurs de communication Xerox avant la transmission des données d'attributs.
		Externe **(sortie uniquement)**	Chaque application Xerox® Device Agent transmet automatiquement les données d'attributs des périphériques d'impression via un canal chiffré (HTTPS sur le port 443) aux serveurs de communication Xerox® à une heure précise chaque jour.

Méthode de déploiement	Application utilisée	Flux de données sur le réseau	Utilisation imposée sur un réseau
		Externe **(sortie uniquement)**	Chaque application Xerox® Device Agent interroge automatiquement les serveurs de communication Xerox® via un canal chiffré (HTTPS sur le port 443) à une heure précise chaque jour pour leur demander la liste des actions à effectuer.
Applications de gestion de périphériques	Xerox®Device Manager pour contrôler les périphériques d'impression connectés au réseau	Interne	Chaque application Xerox® Device Manager / Xerox® Device Agent détecte un serveur proxy Web (automatiquement ou acheminement vers une adresse spécifique).
		Interne	Chaque application Xerox® Device Manager / Xerox® Device Agent extrait les fonctionnalités des périphériques d'impression dans le parc d'impression via SNMP.
		Interne	Chaque application Xerox® Device Manager / Xerox® Device Agent extrait la configuration des périphériques d'impression dans le parc d'impression via SNMP.
		Interne	Chaque application Xerox® Device Manager / Xerox® Device Agent extrait l'état des périphériques d'impression dans le parc d'impression via SNMP.
		Interne	Chaque application Xerox® Device Manager / Xerox® Device Agent extrait les données relatives aux consommables des périphériques d'impression dans le parc d'impression via SNMP.
		Interne	Chaque application Xerox® Device Manager / Xerox® Device Agent peut demander l'impression d'un rapport de configuration sur le périphérique.
		Interne	Chaque application Xerox® Device Manager / Xerox® Device Agent peut lancer la page Web d'un périphérique d'impression.
		Interne	Chaque application Xerox® Device Manager / Xerox® Device Agent peut mettre à jour les logiciels des périphériques d'impression via la soumission d'un travail d'impression.
		Interne	L'application Xerox® Device Manager prend en charge les communications SNMPv3 avec les périphériques d'impression.
		Interne	L'application ® Device Manager peut effectuer des changements dans la configuration des périphériques d'impression via SNMP et l'interface utilisateur Web.
		Interne	L'application Xerox® Device Manger extrait les données des journaux de comptabilité des travaux à partir de certaines imprimantes multifonctions Xerox®.

Méthode de déploiement	Application utilisée	Flux de données sur le réseau	Utilisation imposée sur un réseau
		Interne	L'application Xerox® Device Manager gère / met en œuvre les politiques de contrôle des impressions.
		Externe **(sortie uniquement)**	Les applications Xerox® Device Manager / Xerox® Device Agent franchissent le pare-feu de l'entreprise pour accéder à Internet (HTTPS sur le port 443).
		Externe **(sortie uniquement)**	Chaque application s'authentifie au moyen de son certificat auprès des serveurs de communication Xerox avant la transmission des données d'attributs.
		Externe **(sortie uniquement)**	Les applications Xerox® Device Manager / Xerox® Device Agent transmettent automatiquement les données d'attributs des périphériques d'impression aux serveurs de communication Xerox® via un canal chiffré (HTTPS sur le port 443) à une heure précise chaque jour.
		Externe **(sortie uniquement)**	Les applications Xerox® Device Manager / Xerox® Device Agent interrogent automatiquement les serveurs de communication Xerox® via un canal chiffré (HTTPS sur le port 443) à une heure précise chaque jour pour leur demander la liste des actions à effectuer.

Protocole SNMP (Simple Network Management Protocol)

Le protocole SNMP est l'outil de gestion de réseau le plus fréquemment utilisé pour les communications entre des systèmes de gestion de réseau et des imprimantes réseau. Les applications de gestion de périphériques utilisent le protocole SNMP durant les opérations de détection pour extraire les informations détaillées sur les périphériques d'impression installés sur le réseau. Les applications de gestion de périphériques Xerox® prennent en charge les protocoles SNMP v1/v2 et v3. Voir le guide de certification de l'application de gestion de périphériques Xerox® concernée pour plus de détails.

Le cadre SNMP v3 prend en charge plusieurs modèles de sécurité qui peuvent coexister au sein d'une même entité SNMP. SNMPv3 inclut des mécanismes de sécurité plus stricts que SNMPv2 en ajoutant des outils de chiffrement. De plus, SNMPv3 est rétrocompatible avec les versions précédentes et est largement utilisé sur les réseaux performants.

Les applications de gestion de périphériques Xerox® (CentreWare® Web / Xerox® Device Manager) peuvent communiquer avec les plateformes de périphériques conformes FIPS 140-2 dans leur mise en œuvre de SNMPv3.

Les applications de gestion de périphériques Xerox® n'utilisent pas le service SNMP de Windows, ni le service Windows SNMP Trap. Si ces services ont déjà été installés, ils **doivent** être désactivés sur tout ordinateur ou serveur sur lequel l'application de gestion de périphériques Xerox® est installée.

Les applications de gestion de périphériques Xerox® utilisent un agent SNMP développé par Xerox qui :

- comprend un mécanisme d'encodage/de décodage spécial ;
- est complètement géré par l'environnement .NET ;
- avec lequel l'exécutable .NET offre une sécurité accrue afin de prévenir les attaques ciblant les vulnérabilités logicielles, comme les manipulations de pointeurs non valides, les surcharges de la mémoire tampon et la vérification des limites.

Les applications de gestion de périphériques Xerox® utilisent les fonctions de sécurité disponibles dans le système d'exploitation Windows, notamment :

- Authentification et autorisation des utilisateurs
- Configuration et gestion des services
- Déploiement et gestion des stratégies de groupe

Pare-feu de Windows pour les connexions Internet comprenant des :

- Paramètres de journalisation de sécurité
- Paramètres ICMP

Applications de gestion de périphériques Xerox® : Xerox® Device Agent, Xerox® Device Agent Partner Edition ou Xerox® Device Manager utilisent l'application SQL CE Microsoft® SQL Server

Les applications de gestion de périphériques Xerox® peuvent être configurées pour tirer parti d'autres fonctions de sécurité de l'application MS SQL Server, notamment :

- Enregistrement des compte d'utilisateur
- Chiffrement DNS
- Restriction des droits d'accès à la base de données des comptes d'utilisateurs (c.-à-d. droits de propriété de la base de données)
- Mise en œuvre de numéros de port définis par l'utilisateur

Une clé d'enregistrement Xerox et un compte Xerox valide sont nécessaires pour transmettre des données aux serveurs de communication Xerox® distants.

Les communications externes des applications de gestion de périphériques Xerox® peuvent être affectées par le pare-feu de Windows pour les connexions Internet. (Nous recommandons que les clients placent l'URL Xerox sur liste blanche sur leur pare-feu et qu'ils spécifient l'adresse IP autorisé à accéder à l' URL.)

Les applications de gestion de périphériques Xerox® s'exécutent en arrière-plan à l'aide des identifiants de connexion du compte système local pour interroger automatiquement les périphériques d'impression réseau via SNMP et transmettre régulièrement les attributs des périphériques d'impression aux serveurs de communication Xerox®.

L’accès à l’interface utilisateur et aux fonctions de l’application Xerox® Device Manager (XDM) est contrôlé par des droits basés sur des rôles (p. ex., groupes Administrateurs CentreWare® Web, Utilisateurs avec privilèges CentreWare® Web, Utilisateurs SQ CentreWare® Web, Administrateurs client CentreWare® Web et Clients CentreWare® Web fournis).

Les noms d’utilisateur et les mots de passe ne franchissent pas les frontières du réseau ; des jetons d’accès sont utilisés à la place (du fait de la conception du système d’exploitation Windows®).

L'application Xerox® Device Manager (XDM) offre des fonctions de contrôle des soumissions d’impressions par la restriction des travaux selon la politique d’utilisation de la couleur, le type de document, les coûts d’impression, l’heure de la journée, le contrôle d’accès de groupes d’utilisateurs, la politique d’impression recto verso, les travaux d’impression autorisées et les quotas d’impression.

Remarques : l'utilisation de SNMP par une application Xerox® Remote Services ne devrait poser aucun risque pour la sécurité de l'environnement IT du client car l'intégralité du trafic SNMP généré et consommé par ces applications s'effectue dans l'intranet du client, derrière le pare-feu de l'entreprise. Par défaut, le service SNMP de Windows et le service Windows SNMP Trap ne sont pas activés sur les systèmes d'exploitation Windows.

Mode de sécurité entreprise

En plus des synchronisations programmées éventuellement effectuées par les applications de gestion de périphériques Xerox® avec Xerox® Services Manager, une synchronisation quotidienne est réalisée par défaut. Il existe deux modes de sécurité entreprise : le mode **normal** et le mode de **verrouillage.**

En mode **normal**, l'application de gestion de périphériques contacte Xerox® Services Manager chaque jour lorsque toutes les autres synchronisations programmées ont été désactivées ***(mode recommandé***).

En mode de **verrouillage**, outre la synchronisation des données relatives à l'imprimante, il n'y a aucune communication avec Xerox® Services Manager. Toute modification de ce mode doit s'effectuer sur site. (La ***synchronisation des données*** garantit que les informations sur les périphériques d'impression transmises depuis l'application de gestion de périphériques Xerox® sont identiques aux données capturés par Xerox® Services Manager.)

Par défaut, l'application de gestion de périphériques Xerox® contacte Xerox® Services Manager chaque jour et permet aux administrateurs de modifier les paramètres à distance, ce qui évite les interventions sur site. Nous recommandons de ne pas modifier ce paramètre. Si un client n'autorise pas le personnel Xerox à effectuer la maintenance des périphériques d'impression à distance, la communication des périphériques avec Xerox® Services Manager peut être verrouillée sauf pour la synchronisation des données d'imprimante. Dans ce mode, l'application ne transmet pas les adresses IP d'ordinateurs ou d'imprimantes ni les paramètres de sites à Xerox® Services Manager, et toute modification de paramètres nécessite une intervention sur site.

Remarque : l'absence de l'onglet Mode de sécurité entreprise dans Xerox® Device Agent indique que l'application fonctionne en mode normal.

Protocoles, ports et autres technologies connexes

Le tableau suivant identifie les protocoles, les ports et les technologies utilisés dans Xerox® Remote Services :

Numéro de port	Protocole	Description de l'utilisation	Flux de données sur le réseau
Selon les protocoles de la couche supérieure	**IP (Internet Protocol)**	**Transport sous-jacent de toutes les communications de données**	**Interne + Externe (sortie uniquement)**
S/O	ICMP (Internet Control Message Protocol)	Détection des périphériques d'impression + dépannage	Interne
25	SMTP (Simple Mail Transport Protocol)	Alertes de notification par courrier électronique des périphériques d'impression et des applications de gestion de périphériques	Interne
53	Services DNS (Domain Name Service)	Opérations de détection des périphériques d'impression DNS	Interne
80	HTTP (HyperText Transport Protocol)	Requêtes de pages Web des périphériques d'impression + requêtes de pages Web des applications de gestion de périphériques	Interne
135	Appel de procédure à distance (RPC, Remote Procedure Call)	Détection des périphériques d'impression	Interne
137, 139	NetBIOS	Détection des serveurs d'impression	Interne
161	SNMP (Simple Network Management Protocol) (SNMP v1 / v2C / v3)	Protocole standard servant à la détection des périphériques d'impression réseau + extrait l'état, les relevés de compteurs et les données relatives aux consommables + extrait et applique la configuration des périphériques d'impression Noms de communauté par défaut = « public » (GET), « private » (SET)	Interne
162	Pièges SNMP	Nom de communauté par défaut = « SNMP_trap »	Interne
389	LDAP (Lightweight Direct Access Protocol)	Détection des périphériques d'impression via l'énumération des partitions Microsoft Active Directory + Ensemble de configuration de services de numérisation + Importation client Active Directory + Configurations de groupe de clients	Interne

Numéro de port	Protocole	Description de l'utilisation	Flux de données sur le réseau
443	HTTPS (HyperText Transport Protocol Secure)	Requêtes de pages Web sécurisées des périphériques d'impression (si celles-ci sont configurées) + requêtes de pages Web sécurisées des applications de gestion de périphériques (si celles-ci sont configurées) + Transfert des données des périphériques d'impression aux serveurs de communication Xerox® + communications des contrôles d'impression à Xerox® Device Manager	Interne + Externe (sortie uniquement)
452	Netware SAP (Service Advertising Protocol)	Détection des périphériques d'impression à l'aide de requêtes Novell Server via IPX	Interne
515, 9100, 2000, 2105	Soumission de travaux d'impression TCP/IP LPR et Raw	Mise à jour logicielle des périphériques d'impression + Diagnostic de la page de test d'impression	Interne
631	IPP (Internet Printing Protocol)	Détection des périphériques d'impression	Interne

Meilleures pratiques en matière de sécurité

Veillez à toujours tenir à jour les périphériques d'impression en installant les dernières mises à jour des logiciels/micrologiciels. Pour effectuer ces mises à jour, utilisez l'interface utilisateur Web des périphériques d'impression ou l'application de gestion d'imprimantes fournie à l'achat de l'appareil par Xerox® et les autres fabricants.

Chaque fois que cela est possible, désactivez les ports et les protocoles non utilisés sur les périphériques d'impression. Cela peut généralement se faire dans l'interface utilisateur Web des périphériques d'impression de bureau ou dans l'interface utilisateur locale des périphériques d'impression de production.

Utilisez les fonctions de contrôle d'accès des utilisateurs sur les périphériques d'impression, si celles-ci sont disponibles. Cela peut généralement se faire dans l'interface utilisateur Web des périphériques d'impression de bureau ou dans l'interface utilisateur locale des périphériques d'impression de production.

Dans la mesure du possible, utilisez des protocoles sécurisés. Cela peut généralement se faire dans l'interface utilisateur Web des périphériques d'impression de bureau ou dans l'interface utilisateur locale des périphériques d'impression de production.

Activez les fonctions de sécurité intégrées au périphérique (par exemple, écrasement d'image, chiffrement du disque, impression sécurisée, etc.).

Assurez-vous que le pare-feu de l'entreprise peut acheminer les paquets HTTPS via le port 443 conformément aux politiques de sécurité de l'entreprise.