

L'information est le capital essentiel de votre entreprise. Xerox vous aide à la conserver en toute sécurité.

Pour être tranquille, sécurisez vos documents.

La gamme de systèmes multifonctions Xerox présente une caractéristique essentielle : l'engagement pour la sécurité des informations. Nos systèmes, logiciels et services sont conformes aux normes reconnues du secteur et à la réglementation américaine la plus récente en matière de sécurité.

Certification

Les produits WorkCentre et WorkCentre Pro 232/238/245/255/265/275 ont reçu la certification Common Criteria délivrée par le NIAP (National Information Assurance Partnership)*.

Xerox est le seul fabricant à certifier des produits complets et non simplement des kits ou des sous-ensembles de fonctionnalités. Le champ d'application de la certification inclut les principaux éléments suivants :

- Le contrôleur réseau
- Le sous-pilote d'impression PostScript
- Le logiciel de télécopie
- L'interface de serveur Web
- Le système d'exploitation
- Le scanner
- L'interface utilisateur
- Le disque dur interne
- Le module de marquage



Principaux objectifs de sécurité



Confidentialité

Pas de divulgation non autorisée des données pendant leur traitement, transmission ou stockage



Non-répudiation

Une entité ne peut pas contester l'envoi ou la réception d'un message



Intégrité

Pas de modification non autorisée des données



Disponibilité

Pas de refus de service pour les utilisateurs autorisés



Comptabilisation

Les actions d'une entité peuvent faire l'objet d'un suivi adressé directement à cette entité

*Un nouveau processus de certification est en cours pour les améliorations produit décrites dans cette brochure.

Autres fonctions de sécurité



- **Authentification de l'utilisateur** Pour restreindre l'accès aux fonctions de numérisation, de courrier électronique et de télécopie réseau, cette fonction commence par valider les noms d'utilisateur et les mots de passe.
 - **Authentification réseau** Lorsqu'elle est utilisée avec l'option de numérisation vers courrier électronique, cette fonction permet de renseigner automatiquement l'adresse de l'expéditeur avec le nom de l'utilisateur connecté. Une fois l'utilisateur validé, ce champ ne peut plus être modifié.
 - **La comptabilisation standard Xerox sur WorkCentre / WorkCentre Pro*** permet de gérer l'accès aux fonctions de copie/impression/télécopie/numérisation par l'utilisateur ou un groupe, et leur utilisation.
 - **L'authentification de l'administrateur système avec protection de l'accès au périphérique par mot de passe** permet d'imposer la saisie d'un code personnel pour pouvoir consulter les écrans d'administration et de configuration et les paramètres de réseau distant.
- **Liste de contrôle** Interne au périphérique. Permet de savoir qui a fait quoi (impression, numérisation, télécopie réseau) et quand (date et horodatage).
- **Administration réseau/gestion des périphériques**
 - **Sécurité basée sur les certificats via le protocole HTTPS (SSL)** Le SSL offre une liaison sécurisée vers l'interface utilisateur Web (CentreWare Internet Services).
 - **SNMP V3** fournit des communications chiffrées d'administration réseau avec le périphérique. Pris en charge par CentreWare Web et d'autres outils d'administration réputés.
- **Numérisation sécurisée**
 - **Canal sécurisé pour la transmission des fichiers numérisés à l'aide de HTTPS (SSL).**
 - **Sécurité basée sur les certificats via le protocole HTTPS (SSL).**
- **Chiffrement du canal d'impression** Canal sécurisé pour l'envoi des travaux d'impression via IPSec.
- **Pare-feu intégré** Il contrôle les communications avec des clients réseau spécifiques grâce à des règles de filtrage basées sur l'adresse IP et/ou le numéro de port.
- **Impression sécurisée** Pour empêcher la consultation non autorisée des sorties papier, les travaux d'impression sont retenus dans une file d'attente jusqu'à la saisie d'un code personnel.

Séparation de la télécopie et du réseau

Alors que les pare-feu empêchent l'accès non autorisé à un système via la connexion réseau, les connexions de télécopie non protégées des systèmes multifonctions peuvent constituer une porte d'accès au réseau. Xerox est le premier fabricant à obtenir l'assurance d'un tiers, par l'intermédiaire de la certification Common Criteria, que les lignes de télécopie et du réseau sont séparées. Nous avons ainsi la garantie d'obtenir une séparation complète de la ligne téléphonique du télécopieur et de la connexion réseau.



*Remarque : Pour Copy Centre, cela permet à la fonction Auditron interne de gérer l'accès et l'utilisation de la copie.

Nouveautés des systèmes WorkCentre/WorkCentre Pro

Xerox fabrique les produits les plus sécurisés du marché et actuellement, les systèmes multifonctions WorkCentre / WorkCentre Pro sont plus sûrs que jamais grâce à ces améliorations* :

- Le **protocole IEEE 802,1x** offre une méthode plus efficace de contrôle de l'ensemble du trafic réseau et veille à la sécurité des connexions filaires et sans fil.
- Utilisez une **clé maîtresse** pour initier un processus de cryptage des données appelé **Temporal Key Integrity Protocol (TKIP)**. Le processus TKIP résout les faiblesses du WEP (802.11b) en déduisant de nouvelles clés de cryptage de la clé maîtresse, puis en les faisant varier. Une même clé de cryptage n'est jamais utilisée deux fois.
- **Authentification LDAP/LDAP sécurisé via SSL**. Connexion LDAP sécurisée à l'aide des informations d'authentification de l'utilisateur sur un canal SSL crypté.
- Amélioration de la **protection par écrasement de l'image** en option (voir ci-dessous). Les utilisateurs peuvent à présent programmer l'écrasement au moment de la journée voulu.
- **Cryptage simple du disque** (WorkCentre Pro uniquement) : le disque dur est partitionné et crypté afin de prendre en charge le stockage sécurisé des données pour les fonctionnalités de numérisation vers la boîte aux lettres et de stockage des impressions/réimpressions.
- **Xerox Secure Access Unified ID System™** : nouvel outil, très pratique, conçu pour améliorer la sécurité des périphériques et des documents et proposer au service informatique une méthode de contrôle de l'activité pour l'ensemble des fonctionnalités des périphériques (voir page suivante).



Option de protection par écrasement de l'image

Cette fonctionnalité « broie » électroniquement les données stockées sur le disque dur de la machine durant les opérations habituelles d'impression, de numérisation, de photocopie ou de télécopie. La suppression électronique des données peut s'effectuer automatiquement après chaque tâche ou à la demande. Les données sont écrasées à l'aide d'un algorithme en 3 passes conforme à la directive du Ministère américain de la défense (DOD) 5200.28-M. Xerox est le seul fabricant à respecter cette méthode standard de suppression des données.

*Ces améliorations n'ont pas reçu la certification Critères communs (Common Criteria).

Présentation de Xerox Secure Access Unified ID System™

Actuellement, dans un environnement porté sur la réglementation, les entreprises ont besoin de moyens sophistiqués pour sauvegarder leurs données et les suivre. En outre, la plupart des entreprises considèrent la sécurité des réseaux comme leur principal défi informatique. Les responsables informatiques sont sans cesse à la recherche de moyens pour protéger l'ensemble des ressources sur leur réseau. Les systèmes multifonctions sont logiquement impliqués dans la sécurisation des réseaux, l'amélioration de la sécurité des documents et la génération de journaux d'activité.

Pour répondre à ces besoins, Xerox a développé la fonctionnalité d'authentification réseau. Pour utiliser cette fonctionnalité, les utilisateurs se connectent au système multifonction à l'aide de leurs informations d'authentification réseau. Bien qu'il s'agisse là d'une solution satisfaisante et sécurisée, certains environnements exigent une méthode plus pratique et plus rationnelle pour accéder à l'ensemble des fonctionnalités du périphérique. C'est la raison pour laquelle Xerox a franchi un nouveau cap en créant Xerox Secure Access. Cet outil dote les entreprises possédant déjà une infrastructure d'identification par carte d'une méthode simple et rapide d'identification des utilisateurs directement sur le système multifonction. Les utilisateurs accèdent ainsi au périphérique en insérant leur badge d'identification dans le lecteur approprié. Pour plus de sécurité, un code confidentiel ou un mot de passe peuvent être exigés. Ils sont saisis au niveau du périphérique.

Mode de fonctionnement

La solution d'identification Secure Access se compose de deux parties simples :

- Le logiciel d'administration Secure Access, chargé sur le serveur de l'entreprise, gère la configuration du périphérique et de l'utilisateur et est responsable de l'authentification des utilisateurs au sein du réseau.
- Un ensemble contrôleur-carte associé à un système WorkCentre / WorkCentre Pro 232/238/245/255/265/275.

La solution Secure Access reprend ainsi l'infrastructure existante d'une société, sans intervenir sur les systèmes déjà en place. Une fois la solution Secure Access installée, une étape d'identification unique permet à l'utilisateur de se connecter au périphérique pour accéder à l'ensemble des fonctionnalités disponibles. Toutes les communications à destination et en provenance du système multifonction, du lecteur de cartes et du serveur d'authentification sont sécurisées grâce à des mécanismes de cryptage standard.

Avantages supplémentaires

Gagnez en flexibilité avec les impressions « à la trace »

Une fois la solution Secure Access installée, les utilisateurs peuvent libérer leurs impressions en toute sécurité dans leur environnement d'impression en glissant leur carte d'identification dans le lecteur, quel que soit le périphérique utilisé. Nous appelons cela les impressions « à la trace ». Les utilisateurs ont la possibilité d'envoyer leurs tâches d'impression dans une file d'attente sécurisée, puis de les imprimer sur le périphérique de leur choix. Ce système réduit les coûts d'impression des documents, ainsi que le gaspillage, dans la mesure où les utilisateurs impriment uniquement ce qu'ils souhaitent et récupèrent l'intégralité de ce qu'ils impriment.

L'utilisateur gagne du temps

Secure Access passe outre certaines étapes en permettant au système multifonction de préremplir certains champs de données en fonction des informations d'authentification de l'utilisateur fournies dès l'ouverture de session. Par exemple, le périphérique remplit automatiquement les champs "A" et "De" dans les cas d'une numérisation vers e-mail.

Le département informatique gagne du temps

La solution Secure Access est facile à gérer grâce à la console de gestion des tâches. Elle s'intègre en toute transparence à l'infrastructure réseau existante d'identification par carte.

La sécurité à l'œuvre : respect de la vie privée dans le secteur de la santé

Xerox Secure Access peut aider les grandes entreprises à protéger leurs enregistrements confidentiels. Le secteur de la santé, par exemple, doit se conformer à des réglementations très strictes en matière de respect de la vie privée. Les entreprises du secteur de la santé doivent respecter les normes visant à protéger les informations confidentielles contenues dans les dossiers des patients.

Les systèmes multifonctions sont étroitement intégrés aux processus des entreprises de ce secteur et gèrent des volumes croissants de documents confidentiels. Les entreprises du secteur de la santé peuvent protéger leurs impressions grâce à Xerox Secure Access, qui sécurise les documents très simplement grâce à sa fonctionnalité de libération sécurisée des impressions par carte d'identification.