

Sécurité des documents

Les informations constituent l'atout le plus important de votre société. Xerox peut vous aider à garantir leur sécurité.



La sécurité des documents est synonyme de tranquillité d'esprit. L'une des caractéristiques des systèmes multifonctions Xerox est leur engagement pour la sécurité des informations. Nos systèmes, logiciels et services se conforment et englobent les normes reconnues du secteur et aux dernières réglementations officielles de sécurité en date.

Sécurité certifiée

La Certification Common Criteria offre une validation indépendante et objective de la fiabilité et de la qualité des produits informatiques. Il s'agit d'une norme à laquelle les clients peuvent se fier pour prendre leurs décisions en toute connaissance de cause en ce qui concerne les achats informatiques. Cette certification définit des objectifs spécifiques de garantie relative aux informations, notamment des niveaux stricts d'intégrité, de confidentialité et de disponibilité pour les systèmes et les données, la comptabilisation au niveau individuel et la garantie du respect de tous ces objectifs.

Appareils certifiés Common Criteria

WorkCentre™ 4250/4260
WorkCentre 5325/5330/5335
WorkCentre 5735/5740/5745/5755
WorkCentre 5765/5775/5790
WorkCentre 7120/7125
WorkCentre 7525/7530/7535/7545/7556*
ColorQube® 9301/9302/9303*
Xerox Colour 550/560 Printer

* Certification en attente

Principaux objectifs de sécurité

Confidentialité

Aucune donnée n'est divulguée sans autorisation pendant le traitement, la transmission ou le stockage.

Intégrité

Aucune donnée n'est altérée sans autorisation.

Disponibilité

Aucun refus de service pour les utilisateurs autorisés.

Comptabilisation

Les actions d'une entité peuvent être tracées directement jusqu'à celle-ci.

Rejet impossible

Il est impossible pour une entité de nier l'envoi ou la réception d'un message.

Sécurité des systèmes multifonctions Xerox

Protection de vos informations stratégiques

Fonctionnalités de sécurité disponibles sur les appareils Xerox

Authentification réseau avec autorisation par utilisateur pour les services individuels. L'accès personnalisé aux services individuels tels que "Scan to email" peut être configuré pour exiger une authentification de l'utilisateur au niveau du périphérique. L'authentification peut exiger un mot de passe de périphérique ou être intégrée de manière transparente dans un environnement informatique via MS Active Directory et d'autres outils.

Interface Extensible Xerox®. S'interface avec les fonctionnalités d'authentification des solutions EIP pour garantir la sécurité des accès.

Comptabilisation standard Xerox (XSA). Gère les accès et l'utilisation des fonctions de copie/d'impression/de télécopie/de numérisation par utilisateur ou par groupe.

Authentification des administrateurs système avec protection par mot de passe de l'accès au périphérique. Nécessite préalablement la saisie d'un nom d'utilisateur et d'un mot de passe pour l'affichage ou la modification des écrans de configuration administrative et des paramètres de réseau distant.

Liste de contrôle. Enregistre les activités liées aux travaux et permet une exportation dans un fichier journal via HTTPS.

Sécurité basée sur les certificats à l'aide du protocole HTTPS (SSL). Offre un lien sécurisé vers l'interface utilisateur Web (CentreWare® Internet Services).

SNMP V3. Crypte les communications de gestion réseau avec le périphérique. Pris en charge par CentreWare Web et d'autres outils de gestion courants.

802.1X. Garantit que les périphériques connectés au réseau sont correctement authentifiés.

Ecrasement d'image. Effectue un recouvrement en trois passages d'un schéma prédéfini de 1 et de 0 qui écrase les images du disque dur. Cet écrasement peut être effectué après chaque travail, à la demande ou à une heure précise dans le cadre d'une planification.

Filtre IP. Permet à un administrateur système de restreindre l'accès par adresse IP ou par plage d'adresses IP.

IPv6. Les périphériques disposent d'une prise en charge intégrée pour les réseaux utilisant la norme IPv6.

IPSec. La prise en charge IPv6 comprend l'activation totale du nouveau standard IPSec qui fait partie des standards de sécurité les plus forts et les plus adaptables à ce jour.

Fichiers PDF protégés par mot de passe¹.

Lors de la création d'un fichier PDF depuis un document numérisé, un utilisateur peut créer un mot de passe unique qui sera exigé pour ouvrir le fichier.

Fichiers PDF cryptés². Les fichiers PDF sont cryptés à l'aide des normes de cryptage AES 128 bits ou RC4.

Courriers électroniques cryptés³. Les courriers électroniques envoyés depuis le périphérique WorkCentre vers le serveur de messagerie sont cryptés à l'aide de clés numériques et du protocole S/MIME.

Impressions cryptées. Les travaux d'impression sont envoyés par le biais d'une communication SSL (Secure Socket Layer) ou TLS.

Disque dur crypté. Les données stockées sur le disque dur bénéficient d'un cryptage allant jusqu'à 256 bits.

Impression sécurisée. Permet à un travail d'impression disposant d'un code PIN unique d'être envoyé vers le périphérique WorkCentre où il est imprimé dès que l'utilisateur saisit ce même code PIN au niveau de l'interface du panneau avant du périphérique.

Isolation de la télécopie et du réseau. La séparation entre la carte de télécopie et le contrôleur réseau supprime les risques de sécurité liés au piratage d'un réseau de bureau par le biais de la ligne de télécopie.

Secure Access

"Secure Access" de Xerox s'intègre à la solution client existante de badges d'identification pour les employés/étudiants. Système d'authentification souple et pratique, "Secure Access" permet aux utilisateurs de se connecter à un périphérique WorkCentre à l'aide d'une carte d'identification magnétique ou de proximité. Ainsi, les utilisateurs disposent d'un accès rapide, simple et sécurisé aux fonctions du périphérique dont il est nécessaire d'assurer un suivi dans le cadre d'exigences réglementaires ou de comptabilisation.

Plus de flexibilité avec l'impression

Follow-You Print™. Avec la mise en place de "Secure Access", les utilisateurs peuvent effectuer des travaux d'impression en toute sécurité depuis n'importe quel périphérique de leur environnement grâce à leur carte d'identification. Les utilisateurs ont la possibilité d'envoyer les travaux d'impression vers une file d'attente sécurisée, puis de les imprimer sur le périphérique de leur choix. Ce système réduit les coûts d'impression des documents et les déchets sous forme de papier car les utilisateurs impriment uniquement ce qu'ils souhaitent et récupèrent tout ce qu'ils impriment.

Gain de temps pour l'utilisateur.

"Secure Access" réduit le nombre d'étapes nécessaires en dotant le système multifonction de la capacité de préremplir certains champs de données en fonction des références fournies par l'utilisateur au moment de la connexion. Par exemple, le périphérique remplit automatiquement les champs « A » et « De » lorsque la fonction "Scan to email" est utilisée.

Gain de temps pour le service

informatique. L'administration de "Secure Access" est très simple grâce à une console de gestion basée sur des tâches qui s'intègre parfaitement à l'infrastructure existante de cartes d'identification réseau du client.

Remarque : Vérifiez les caractéristiques techniques de chaque produit pour connaître la disponibilité des fonctionnalités de sécurité. Sur certains produits, un kit de sécurité disponible en option peut être nécessaire pour activer certaines des fonctionnalités mentionnées.

¹ Non disponible sur les modèles WorkCentre 5735/5740/5745/5755/5765/5775/5790

² Non disponible sur les modèles WorkCentre 4250/4260, WorkCentre 5735/5740/5745/5755/5765/5775/5790 et ColorQube 9301/9302/9303

³ Non disponible sur les modèles WorkCentre 7525/7530/7535/7545/7556 et ColorQube 9301/9302/9303

Appelez dès aujourd'hui. Pour plus d'informations, rendez-vous sur le site www.xerox.com/office.

