

Action requise : Mise à jour de la connectivité pour la gestion des périphériques Xerox



13 juin 2024

CHANGEMENTS À VENIR :

Le 15 février 2025, Xerox mettra en œuvre un pare-feu d'application Web (WAF) pour améliorer la protection de ses applications sur le Web. Cette mesure fait partie de l'engagement de Xerox en matière de sécurité, car elle protège les données que vous nous confiez. Nous faisons de la sécurité notre priorité, et nos solutions et logiciels sont conçus selon ce principe. La mise en œuvre du WAF s'inscrit dans nos efforts continus pour vérifier systématiquement que chaque transaction est sécuritaire et autorisée avant son entrée dans notre espace numérique. Votre sécurité est notre priorité, et nous cherchons à maintenir et à améliorer nos défenses pour protéger vos données.

ACTION REQUISE :

Nous souhaitons vous informer de certaines conditions préalables à une communication fluide au moyen du nouveau pare-feu d'application Web (WAF) qui peuvent toucher votre connectivité avec Xerox Device Agent (XDA), Xerox Device Manager (XDM) ou Xerox Workplace Cloud Fleet Management Solution (CFM).

- Si vous ou vos clients avez suivi l'installation par défaut des outils ci-dessus en ce qui concerne la communication au moyen du nom de domaine totalement qualifié (FQDN, c'est-à-dire <https://office.services.xerox.com/>), vous n'avez aucun changement à apporter. Le passage vers les mesures de sécurité renforcées sera automatique.
- Toutefois, si vous ou vos clients configurez une **liste blanche de pare-feu** à l'aide de plages d'adresses IP pour nos centres de données (p. ex. 13.10.0.0/24), ce changement peut exiger une action de votre part au plus tard le jeudi 13 février pour prévenir les problèmes de connectivité.
 - Nous recommandons fortement d'utiliser le nom de domaine totalement qualifié pour éviter toute perturbation. Si des politiques de réseau vous empêchent de procéder, communiquez avec le **Software Support Group (xerox.com)** pour obtenir de l'aide (service en anglais).
 - En cas de problème, veuillez soumettre un ticket d'assistance auprès du **Software Support Group** (en anglais) ou communiquez avec votre service d'assistance locale.

Cette mise à jour est un moment charnière dans la progression de nos mesures de cybersécurité. Nous vous remercions de votre confiance et de votre coopération pour protéger vos données à leur entrée dans notre espace numérique.