Remote Desktop Manager est désormais conforme aux fonctions de chiffrement approuvées par la norme FIPS 140-2 Annexe A

FIPS 140-2 EST UNE NORME DU NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

C'est avec plaisir qu'on vous annonce que la dernière édition de Remote Desktop Manager 2022.1 est enfin conforme aux fonctions de chiffrement approuvées par la norme FIPS 140-2 Annexe A.

Qu'est-ce que la norme FIPS 140-2 Annexe A?

FIPS 140-2 est une norme du National Institute of Standards and Technology (NIST) qui établit les exigences de sécurité pour les modules cryptographiques des agences gouvernementales. L'annexe A « Fonctions de sécurité approuvées pour FIPS PUB 140-2 » décrit la liste des fonctions approuvées qui sont sécuritaires pour les environnements hautement sensibles. Pour garantir que Remote Desktop Manager respecte les restrictions de ces environnements, nous l'avons aligné sur les fonctions de sécurité approuvées par la norme pour le chiffrement au repos et en transit.

Comment activer le mode FIPS-Only

Remote Desktop Manager passe automatiquement en mode FIPS sur les systèmes d'exploitation qui fonctionnent sous Windows avec une configuration d'algorithmes FIPS-Only et lorsque le mode d'authentification de Remote Desktop Manager est sur Mots de passe d'application. L'utilisation d'entrées qui ne prennent pas nativement en charge les fonctions de sécurité approuvées FIPS-Only sera toujours possible. RDM est une solution de connexion à distance complète et polyvalente. On doit donc s'assurer de continuer à prendre en charge les connexions non sécurisées (Telnet par exemple). Toutefois, pour maintenir la conformité FIPS, les utilisateurs doivent limiter l'utilisation des algorithmes côté serveur aux fonctionalités de sécurité FIPS 140-2 Annexe A. Les fonctions de sécurité utilisées pour le chiffrage en mode FIPS-Only sont détaillées dans notre document officiel « Modèle de sécurité et chiffrement », qui est disponible sur notre site web.

Entrées prises en charge et source de données

Le mode FIPS-Only prend en charge les protocoles RDP et SSH. Pour utiliser le protocole SSH, il faut le configurer manuellement afin d'autoriser les fonctions de sécurité approuvées. Consultez notre tutoriel.

Les sources de données prises en charge incluent MSSQL Server et DVLS, tous deux par TLS. Ce protocole est géré nativement par le système d'exploitation pour utiliser les fonctions de sécurité approuvées lorsqu'il est configuré en mode FIPS-Only.

Que faire si je n'utilise pas le mode FIPS-Only?

Vous n'êtes pas obligés de vous conformer à la norme FIPS 140-2. Remote Desktop Manager est hautement sécurisé et utilise un chiffrage solide approuvé par l'industrie pour fournir un niveau de confidentialité et d'intégrité élevé pour les données en transit et au repos. Pour en savoir plus sur nos normes de chiffrement, consultez notre document officiel « Modèle de sécurité et chiffrement » disponible sur notre site Web.