

Ajouter un certificat de confiance à votre système ExtraHop


Publié: 2023-09-19

Votre système ExtraHop ne fait confiance qu'aux pairs qui présentent un certificat TLS (Transport Layer Security) signé par l'un des certificats système intégrés et par tout certificat que vous téléchargez. Les cibles SMTP, LDAP, HTTPS ODS et MongoDB ODS, ainsi que les connexions Splunk recordstore peuvent être validées par le biais de ces certificats.

Avant de commencer

Vous devez vous connecter en tant qu'utilisateur avec des privilèges de configuration ou d'administration du système et des accès pour ajouter ou supprimer des certificats de confiance.

Lors du téléchargement d'un certificat de confiance personnalisé, un chemin de confiance valide doit exister entre le certificat téléchargé et une racine auto-signée de confiance pour que le certificat soit totalement fiable. Téléchargez toute la chaîne de certificats pour chaque certificat de confiance ou (de préférence) assurez-vous que chaque certificat de la chaîne a été téléchargé dans le système de certificats de confiance.

 **Important:** Pour faire confiance aux certificats du système intégré et à tous les certificats téléchargés, vous devez également activer le cryptage SSL/TLS ou STARTTLS et la validation des certificats lors de la configuration des paramètres du serveur externe

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Paramètres réseau, cliquez sur **Certificats de confiance**.
3. Optionnel : Le système ExtraHop est livré avec un ensemble de certificats intégrés. Sélectionnez **Trust System Certificates** si vous souhaitez faire confiance à ces certificats, puis cliquez sur **Save (Enregistrer)**.
4. Pour ajouter votre propre certificat, cliquez sur **Ajouter un certificat**, puis collez le contenu de la chaîne de certificats codée en PEM dans le champ Certificat
5. Saisissez un nom dans le champ Nom et cliquez sur **Ajouter**.