Add a trusted certificate to your ExtraHop system

Published: 2024-11-13

Your ExtraHop system only trusts peers who present a Transport Layer Security (TLS) certificate that is signed by one of the built-in system certificates and any certificates that you upload. SMTP, LDAP, HTTPS ODS and MongoDB ODS targets, as well as Splunk recordstore connections can be validated through these certificates.

Before you begin
You must log in as a user with setup or system and access administration privileges to add or remove trusted certificates.

When uploading a custom trusted certificate, a valid trust path must exist from the uploaded certificate to a trusted self-signed root in order for the certificate to be fully trusted. Either upload the entire certificate chain for each trusted certificate or (preferably) ensure that each certificate in the chain has been uploaded to the trusted certificates system.

> ⚠️ **Important:** To trust the built-in system certificates and any uploaded certificates, you must also enable TLS or STARTTLS encryption and certificate validation when configuring the settings for the external server.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **Trusted Certificates**.
3. Optional: If you want to trust the built-in certificates included in the ExtraHop system, select **Trust System Certificates**, click **Save**, and then save the running configuration file ↗.
4. To add your own certificate, click **Add Certificate** and then in the Certificate field, paste the contents of the PEM-encoded certificate chain.
5. In the Name field, type a name.
6. Click **Add**.