Add a trusted certificate to your ExtraHop appliance

Published: 2018-04-20

Your ExtraHop appliance 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. Only SMTP and LDAP connections are validated through these certificates.

Before you begin
You must log in as a user with full system 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. This can be achieved by either uploading the entire certificate chain for each trusted certificate or, preferably, by ensuring 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 SSL certificate validation on the LDAP Settings page or Email Settings page.

1. Log into the Admin UI on the ExtraHop appliance.
2. In the Network Settings section, click **Trusted Certificates**.
3. The ExtraHop appliance ships with a set of built-in certificates. Select **Trust System Certificates** if you want to trust these certificates, and then click **Save**.
4. To add your own certificate, click **Add Certificate** and then paste the contents of the PEM-encoded certificate chain into the Certificate field
5. Type a name into the Name field and click **Add**.

Next steps
Configure LDAP and SMTP settings to validate outbound connections with the trusted certificates.