Create a certificate signing request from your ExtraHop system

Published: 2025-01-04

A certificate signing request (CSR) is a block of encoded text that is given to your Certificate Authority (CA) when you apply for an TLS certificate. The CSR is generated on the ExtraHop system where the TLS certificate will be installed and contains information that will be included in the certificate such as the common name (domain name), organization, locality, and country. The CSR also contains the public key that will be included in the certificate. The CSR is created with the private key from the ExtraHop system, making a key pair.

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 **TLS Certificate**.
3. Click **Manage certificates** and then click **Export a Certificate Signing Request (CSR)**.
4. In the Subject Alternative Names section, type the DNS name of the ExtraHop system.
   You can add multiple DNS names and IP addresses to be protected by a single TLS Certificate.
5. In the Subject section, complete the following fields.
   Only the **Common Name** field is required.

Field	Description	Examples
Common Name	The fully qualified domain name (FQDN) of the ExtraHop system. The FQDN must match one of the Subject Alternative Names.	*.example.com discover.example.com
E-mail Address	The email address of the primary contact for your organization.	webmaster@example.com
Organizational Unit	The division of your organization handling the certificate.	IT Department
Organization	The legal name of your organization. This entry should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.	Example, Inc.
Locality/City	The city where your organization is located.	Seattle
State/Province	The state or province where your organization is located. This entry should not be abbreviated.	Washington
Country Code	The two-letter ISO code for the country where your organization is located.	US

6. Click **Export**.
   The CSR file is automatically downloaded to your computer.

Next steps

Send the CSR file to your certificate authority (CA) to have the CSR signed. When you receive the TLS certificate from the CA, return to the TLS Certificate page in the Administration settings and upload the certificate to the ExtraHop system.

Tip: If your organization requires that the CSR contains a new public key, generate a self-signed certificate to create new key pairs before creating the CSR.