

Create a trusted TLS certificate through the REST API

Published: 2024-09-03

By default, sensors and consoles include a self-signed TLS certificate. However, you can improve the security and performance of your system by adding a trusted certificate signed by a certificate authority (CA). You can create the certificate signing request to send to your CA through the ExtraHop REST API. After you receive the signed certificate, you can also add it to your sensor or console through the REST API.

Before you begin

- You must log in to the sensor or console with an account that has **system and access administration privileges** [↗](#) to generate an API key.
- You must have a valid API key to make changes through the REST API and complete the procedures below. (See **Generate an API key** [↗](#).)
- Familiarize yourself with the **ExtraHop REST API Guide** [↗](#) to learn how to navigate the ExtraHop REST API Explorer.



Note: You can also perform the procedures in this topic through the Administration settings. For more information, see the following topics:

- **Create a certificate signing request from your ExtraHop system** [↗](#)
- **TLS Certificate** [↗](#)

Create an TLS certificate signing request

To create a signed TLS certificate, you must send a certificate signing request to a trusted CA.

1. In a browser, navigate to the REST API Explorer.
The URL is the hostname or IP address of your sensor or console, followed by `/api/v1/explore/`. For example, if your hostname is `seattle-eda`, the URL is `https://seattle-eda/api/v1/explore/`.
2. Click **Enter API Key** and then paste or type your API key into the **API Key** field.
3. Click **Authorize** and then click **Close**.
4. Click **ExtraHop** and then click **POST/extrahop/sslcert/signingrequest**.
5. Click **Try it out**.
The JSON schema is automatically added to the SSL Certificate Signing Request Parameters parameter text box.
6. In the SSL Certificate Signing Request Parameters parameter text box, specify the certificate signing request fields.
 - a) In the `common_name` field, replace `string` with the fully qualified domain name of your sensor or console.
 - b) In the `subject_alternative_names` field, add one or more alternative domain names or IP addresses for your sensor or console.



Note: The `subject_alternative_names` field is required. If your system has only one domain name, duplicate the value from the `common_name` field. You must include at least one subject alternative name with the type set to `dns`, but additional alternative names can have the type set to `ip` or `dns`.

- c) Optional: In the `email_address` field, replace `string` with the email address of the certificate owner.
- d) Optional: In the `organization_name` field, replace `string` with the registered legal name of your organization.

- e) Optional: In the `country_code` field, replace `string` with the 2-character ISO country code of the country that your organization is located in.
- f) Optional: In the `state_or_province_name` field, replace `string` with the name of the state or that your organization is located in.
- g) Optional: In the `locality_name` field, replace `string` with the name of the city that your organization is located in.
- h) Optional: In the `organizational_unit_name` field, replace `string` with the name of your department within your organization.


The Value section should look similar to the following example:

```
{
  "subject": {
    "common_name": "example.com",
    "email_address": "admin@example.com",
    "organization_name": "Example",
    "country_code": "US"
  },
  "subject_alternative_names": [
    {
      "name": "www.example.com",
      "type": "dns"
    }
  ]
}
```

7. Click **Send Request** to create the signing request.
In the Server response section, the Response body displays the signing request in the `pem` field.

Next steps

Send the signing request to your CA to create your signed TLS certificate.

-  **Important:** The signing request contains escape sequences that represent line breaks (`\n`). Replace each instance of `\n` with a line break before sending the request to your CA. You can modify the PEM request manually in a text editor or automatically through a JSON parsing utility, as shown in the following example command:

```
echo '<json_output>' | python -c 'import sys, json; print json.load(sys.stdin)["pem"]'
```

Replace the `<json_output>` variable with the entire JSON string returned in the Response Body section.

Add a trusted TLS certificate to your sensor or console

You can add an TLS certificate signed by a trusted CA to your sensor or console through the REST API Explorer.

1. In a browser, navigate to the REST API Explorer.
The URL is the hostname or IP address of your sensor or console, followed by `/api/v1/explore/`. For example, if your hostname is `seattle-eda`, the URL is `https://seattle-eda/api/v1/explore/`.
2. Click **Enter API Key** and then paste or type your API key into the **API Key** field.
3. Click **Authorize** and then click **Close**.
4. Click **ExtraHop** and then click **PUT/extrahop/sslcert**.
5. Click **Try it out**.
6. In the **Certificate and Key** field, paste the TLS certificate.

The certificate should look similar to the following text:

```
-----BEGIN CERTIFICATE-----
a008zvV4MlDhWX4e0VyvGAJx+9d4AqQB4Czy/P7z36CmHe2Y7PPdVSeWHNCQoJ0g
CnO42u2V9YKNFYRQejiJv8CxGVJKsdfV0iP0WnCvpZXkaBOYIrDvE5xn010WPULs
6qe3mCXsUK87i++mYuVDA1U0A5YVXRO200WIWy7P+MCU/cR/op3Jpekng2cxN4qD
FqGbtRpLdCuJ/xGWL1FFRHBg76+Tb0+pxgZhiCtHYXfMKIaoPmDwsAqEtLbizzlW
mbMig9hs4QNcJ+aMNSnTZpkbeBR4a2nkGnQoYvnFOXV/nWzvfHmI4ydsH9g4I8qt
4ArqFepInvm70n07FYAKL6Mddli+7ieo9AqckltVzzKFzkakHm04214wtsYmle94
4HqIJ7p7NH5maXxttXMzHF1ArbnjHWC10gIv81Au+IvLj8aiGAb3zqveNz6ZAZ5j
PGAUsP+dVYV/8VjvqhkiP/1jWzUHwzpd1HbcD8qOkAF41fnbv+2EXqFJ096JSSiU
rqeJpgNuH3LbkT0KORaiLoGLMZKEKxF+3OpLVD7ox7NQh9pMdZ1B8tcTbTmsvD8T
3L2tMVZssqYOANcidtd17t72VW4hzQURT1me5tGWxpN6od/q6B+FivRq/7Vq0UE1
c2AG/om5UN/Vj3pUjXzq/B1IWUS9TicRcKdl5wrKEkPUGjK4w1R/87bj5Hsn8nyd
LMCcOpLTokHj0B5+801y1NhVXNPlj3eY0n60QOdClBqTDM0/4sB3XgeC/pjpleU3
3uot+wM/GoN/Dqb1LPt3BNpUQuCzSfmGSSOXiWELsEhz3ix/36a9eUWjfhmtPsW5
dne5Lf+G7cf+ebsRTb7R89GmgKzTpU11KazKINAebkT6WrWWljugpA0BcfANjs6o
mik4ZbY8d54UtA17evpr2+8UotIgvIrCbflG2DY8QOTCBYIFKJ3GZAedqRK9Sm
I2qdaB6QBczYNaVYSeCsBdHHw1+h7dBeqdUUwYKtmPW96/djj/6vJSXh9/UX/3c0
eqXG36w/lqJAYu8QtAydJsVC85IzqzikX0f0KE315Doginpg59yix9dHD2sxLb1
X39BRpLkZ9nvW6ke2YHU/VKBVIxqSslukGoTUIcUtpJrtMQOwCi/EQQXbPK9a2pW
K51938h6OuLjNbDTFuxfhe4zITWHTgyAs2MNVr9+uDUiVJclX+CIPjhZzjyPqmD6
6uh8Sr3zndOMabqDquo69rMQyvclF0xOUMVgUw1Rb8Y=
-----END CERTIFICATE-----
```



Note: If you want the certificate to be signed with your own private key, you can include your key after the TLS certificate, separated by a line break. However, we recommend that you do not specify your own key; by default, the sensor or console will sign the certificate with the private key on the system.

7. Click **Send Request** to add the certificate.