**Issue**

You may encounter the error described below when your WebAdmin CA cert is not trusted by Chrome

**Your connection is not private**

Attackers might be trying to steal your information from **XXX.XXX.XXX.XXX** (for example, passwords, messages, or credit cards). Learn more

NET::ERR\_CERT\_AUTHORITY\_INVALID

To get Chrome’s highest level of security, turn on enhanced protection

**XXX.XXX.XXX.XXX** normally uses encryption to protect your information. When Google Chrome tried to connect to **XXX.XXX.XXX.XXX** this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be **XXX.XXX.XXX.XXX**, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Google Chrome stopped the connection before any data was exchanged.

You cannot visit **XXX.XXX.XXX.XXX** right now because the website uses HSTS. Network errors and attacks are usually temporary, so this page will probably work later.

**Applies to the following Sophos product(s) and version(s)**
Sophos UTM

**Cause**

One possible cause of this error is using [SHA-1 certificates which is no longer supported by Chrome](https://www.chromium.org/Home/chromium-security/education/tls/sha-1). This is due to SHA-1 certificates being vulnerable to attacks.

 **Resolution**

Resolving this issue involves regenerating your WebAdmin CA and verifying the WebAdmin CA certificate in CLI to see the Signature and Valid date.

A- [Verify the WebAdmin CA certificate in CLI to see the Signature and Valid date](https://support.sophos.com/support/s/article/KB-000035452?language=en_US&name=KB-000035452#Verify)
B- [Regenerate the WebAdmin CA](https://support.sophos.com/support/s/article/KB-000035452?language=en_US&name=KB-000035452#RegenCA)

**A- Verify the WebAdmin CA certificate in CLI to see the Signature and Valid date**

The example below is showing the signature is SHA1 and was generated on **May 26 2012**

Run the command:

cc get\_object REF\_CaSigWebadminCa|head -14|tail -5

 Signature Algorithm: **sha1WithRSAEncryption**

 Issuer: C=CA, ST=ON, L=Ottawa, O=Sophos, CN=secureottawa.sophos.com/emailAddress= fakeuser@sophos.com

 **Validity**

 Not Before: May 31 14:37:07 2017 GMT

 Not After : Jan 1 00:00:00 2038 GMT

**B-Regenerate WebAdmin CA**

**Note:** It is not sufficient to only regenerate the certificate for the WebAdmin via the section Regenerate WebAdmin certificate in the WebAdmin. You first have to regenerate the CA via the CC.

To regenerate the CA proceed as follows:

1. Sign in to the shell of the UTM first as loginuser and then get root: **su -**
2. Now type in the following command to open the ConfdClient: cc
3. Within the ConfdClient type use the command: RAW
4. Now regenerate the CA with:

ca\_generate\_signing\_ca({name=>'webadmin ca', key\_size=>2048, country=>'CountryAcronym', state=>'StateName', city=>'CityName', organization=>'OrganizationName', common\_name=>'UTMhostname', email=>'mailaddress@maildomain.com'})
 **Note:** Adapt the *country, state, city, organization, common\_name* and *email* strings to your own UTM settings (country field **must be in caps - eg. CA, DE**)

The result should be result: **'REF\_CaSigWebadminCa2'**

**Sample data that adapted the data with a fetch info from step A:**

ca\_generate\_signing\_ca({name=>'webadmin ca', key\_size=>2048, country=>'CA', state=>'ON', city=>'Ottawa', organization=>'Sophos', common\_name=>'secureottawa.sophos.com', email=>'[fakeuser@sophos.com|mailto:fakeuser@sophos.com]'})

1. Switch to Main Mode: **MAIN**
2. Go to: **webadmin**
3. Now type in: ca$
4. The last step is to assign the new CA to the WebAdmin with: **=REF\_CaSigWebadminCa2**
**Note**: The result should be 1.

The next step is to regenerate the certificate for WebAdmin with the new CA, proceed as follows:

1. Go to **Management**> **WebAdmin Settings**> **HTTPS Certificate**.
2. In the area, **Regenerate WebAdmin certificate**click **Apply**.

The WebAdmin certificate will be regenerated. Your UTM will reload automatically and you will have to sign in again.