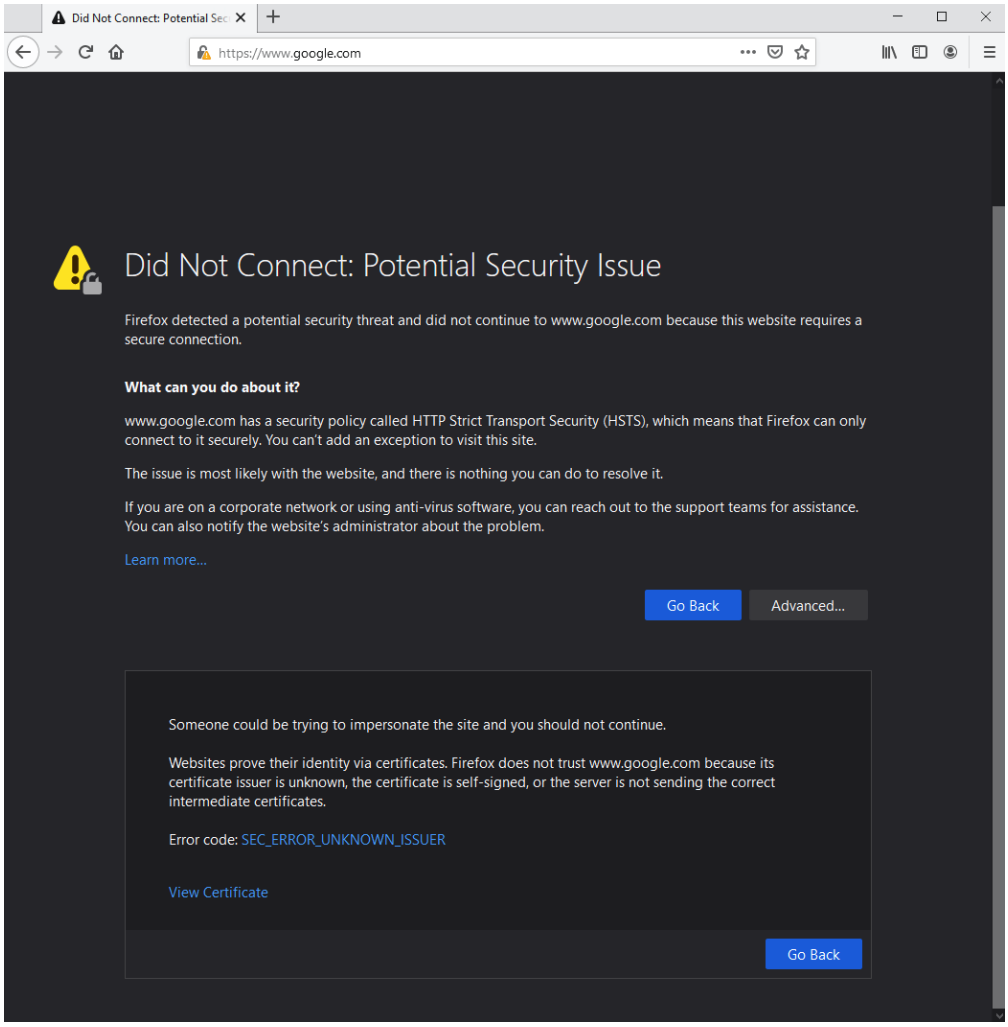
How to Clear the HSTS Cache or Disable HSTS for Firefox

https://campus.barracuda.com/doc/73699516/

HTTP Strict Transport Security is a security feature to warn users when the expected certificate for a secure website does not match the one that was returned. In order to perform Content Filtering, URL Logging, and *Scan and Deliver* threat detection on web traffic, the BCS agent will substitute its own trusted certificate in place of the one the web server is using. By default, Firefox will warn the user about this difference.



Resolution

Begin by ensuring that the endpoint is running the latest version of Firefox. Older versions used different security settings, which are no longer supported by the BCS agent.

If you still see this error after updating Firefox to the latest version, you will need to configure Firefox to recognize any enterprise root certificates that are installed in the system trust store.

1. In the address bar, type
   `about:config`
   This opens a settings panel with advanced configuration options.
2. In the search field, type `enterprise` to display the relevant configuration options.
3. Toggle the setting `security.enterprise_roots.enabled` to *True*.
4. Close the configuration tab and then reload any affected web pages.

After changing this setting in the profile, Firefox should not display an HSTS warning for any pages when the BCS agent is active.

Deploy enterprise trusted root certificates via GPO

If you use GPO or another tool to deploy the BCS software, you can also push this setting out to all of your users at once.

For GPO: Create a preference setting that enables trusted root certificates in an instance of Firefox. To enable trusted root certificates across your network, you can modify the security.enterprise_root setting and lock this setting. You can then distribute this preference setting with Windows Group Policy.

This procedure assumes that Firefox is installed in the default location on Windows. To modify the group policy, you must be a domain or enterprise administrator.

1. Create the configuration file that locks the preference setting to trust the certificates that are in the Windows certificate store:
   1. Create a text file with this content:
      `lockPref("security.enterprise_roots.enabled", true);`
   2. Save the file as `mozilla.cfg` and make sure it is ANSI encoded.
2. Create a JavaScript file that calls the new configuration file:
   1. Create a `local-setting.js` file with this content:

      ```
      pref("general.config.obscure_value", 0);

      pref("general.config.filename", "mozilla.cfg");
      ```

      Save the file as an ANSI encoded file.
3. Copy the `mozilla.cfg` and `local-settings.js` file to a network shared folder.
4. Distribute these files with GPO. In the Group Policy Management Editor, when you browse for the Computer Configuration / policies / Windows Settings files, for the source file(s), browse to the `mozilla.cfg` file in the network shared folder.

   For the Destination File, enter the default location where Firefox is installed. The path varies depending on Windows version:

On Windows 32-bit OS, specify `C:\Program Files\Mozilla Firefox\mozilla.cfg`

On Windows 64-bit OS, specify `C:\Program Files (x86)\Mozilla Firefox\mozilla.cfg`

For the Destination File, enter this location depending on Windows version:

On a Windows 32-bit OS, specify `C:\Program Files\Mozilla Firefox\defaults\pref\local-settings.js`

On a Windows 64-bit OS, specify `C:\Program Files (x86)\Mozilla Firefox\defaults\pref\local-settings.js`

Figures