How to configure automatic cleanup of suspicious certificates in Xcitium Client Security

Open CCS > Click 'Settings' > 'Advanced Protection' > 'Miscellaneous'

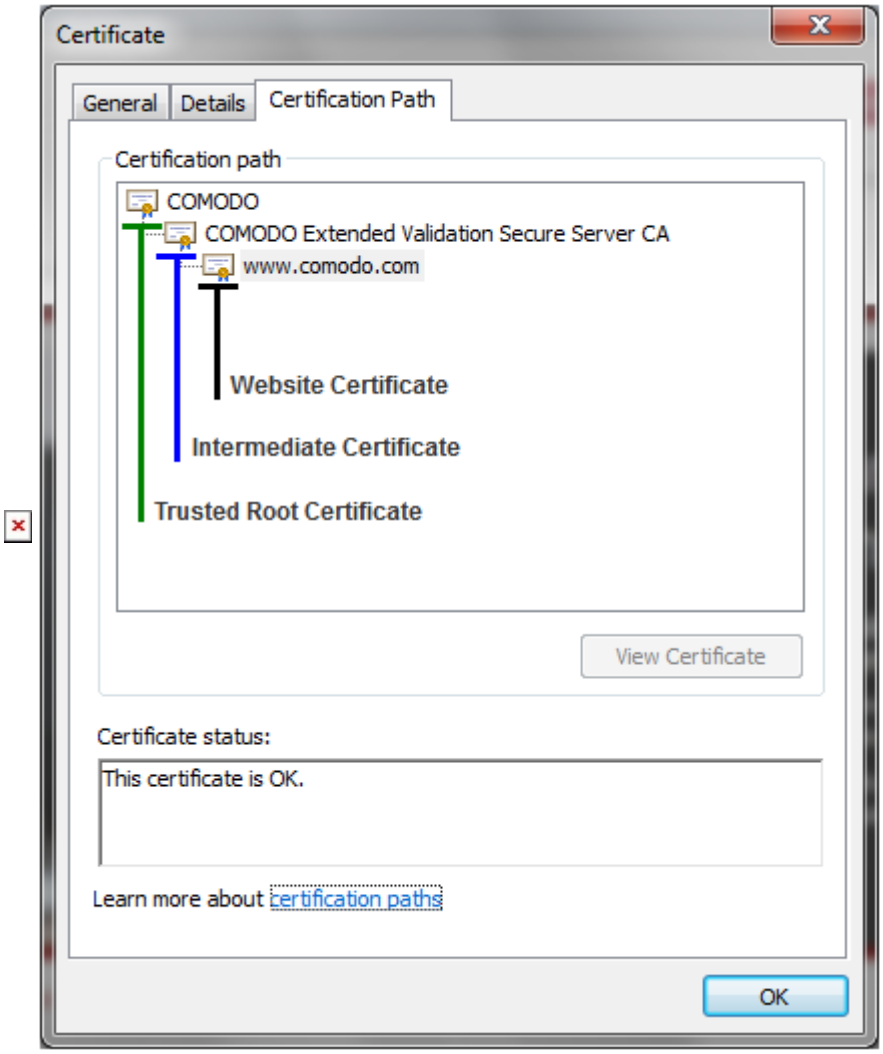
- CCS can identify and remove untrusted root certificates on the Endpoint during on-demand and scheduled scans.
- Untrusted/fake root certificates can be used to convince users to trust phishing and malware websites.
- This article explains how root certificates work and how to add certificate checks to malware scans.

What are SSL certificates and Root certificates?

Configure certificate checks in CCS

What are SSL certificates and Root certificates?

- SSL certificates are used by websites to encrypt the connection between your browser and their web-server.
- This ensures nobody can intercept the traffic sent between you and the site. All information sent from your browser to the site is private. This is especially important for sensitive transactions like online payments, where you send your credit card information over the internet.
- You can tell a site is using an SSL certificate by the padlock icon in the browser address bar.
- SSL certificates are issued to website owners by an organization known as a ‘Certificate Authority’ (CA). The CA checks that the applicant owns the website in question, and is a legitimate business.
- Once these checks have been passed, the CA will sign the applicant’s certificate with what is known as a ‘root certificate’. You should only trust websites whose certificates have been signed by the root certificate of a trusted CA.
- These trusted root certificates are embedded in your browser (Firefox, Chrome, Edge, etc). Your browser checks that the SSL certificate on a site is signed by a trusted root each and every time you visit the site.

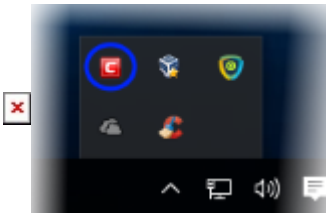


The image above shows the SSL certificate for www.Xcitium.com. The certification path shows the chain of trust that the browser uses to verify the certificate. The trusted root certificate has signed the Intermediate certificate which has in turn signed the Website certificate (the one for www xcitium.com).

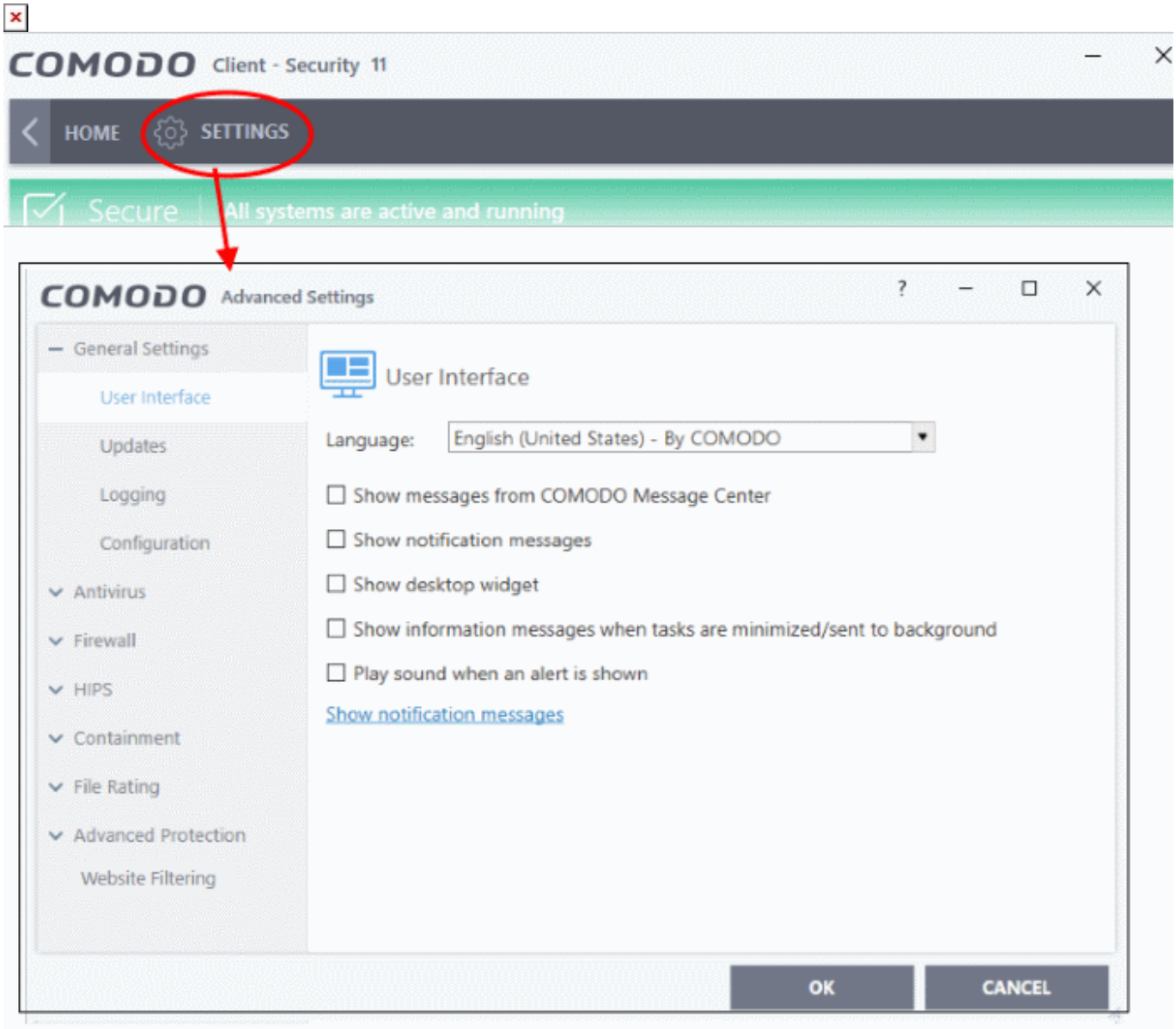
- A fake root certificate would, therefore, bypass this check of legitimacy. It could tell you to trust a website run by a hacker.
- CCS can detect and remove fake root certificates from the endpoint during on-demand and scheduled scans. Disable 'Do not automatically clean up suspicious certificates' to activate this feature.

Configure root certificate checks in CCS

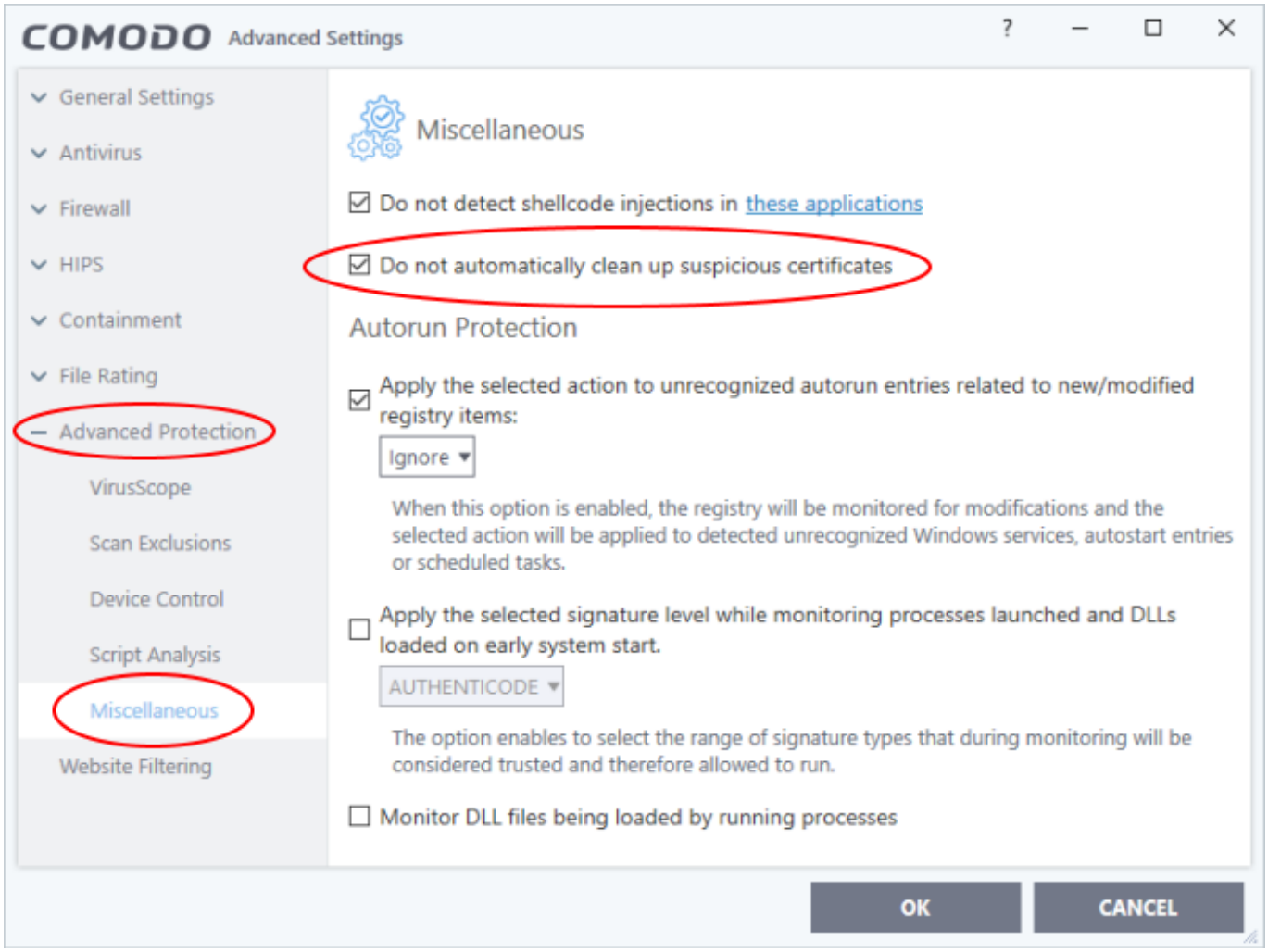
- Login to the endpoint and open CCS. You can open CCS by double-clicking the system tray icon:



- Click 'Settings' > Advanced Settings'



- Click 'Advanced Protection' > 'Miscellaneous' on the left
- Disable ‘Do not automatically clean up suspicious certificates’:



- **Do not automatically cleanup suspicious certificates**
    - **Enabled** – CCS ignores non-trusted root certificates found by a virus scan (Default)
    - **Disabled** – CCS deletes any root certificates that are not signed by a trusted CA
- Click 'OK' for your settings to take effect.