# How to configure automatic cleanup of suspicious certificates in Comodo 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 webserver.
- 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.

Certificate General Details Certification Path Certification path Certification path ComoDO ComoDO Extended Validation Secure Server CA Website Certificate Intermediate Certificate Trusted Root Certificate					
Certificate status: This certificate is OK. Learn more about certific	View Certificate				

The image above shows the SSL certificate for www.comodo.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.comodo.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'

OMODO Client - Security 11					
HOME 🔅 SETTING	s				
	stems are active and running	?			×
<ul> <li>General Settings</li> <li>User Interface</li> </ul>	User Interface				
Updates	Language: English (United States) - By COMODO	•			
Logging	□ Show messages from COMODO Message Center				
Configuration	Show notification messages				
<ul> <li>Antivirus</li> </ul>	Show desktop widget				
<ul> <li>Firewall</li> </ul>	Show information messages when tasks are minimized/se	nt to back	ground		
✓ HIPS	Play sound when an alert is shown				
<ul> <li>Containment</li> </ul>	Show notification messages				
<ul> <li>File Rating</li> </ul>					
<ul> <li>Advanced Protection</li> </ul>					
Website Filtering					
		_			

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

COMODO Advanced Settings		?	-		×
<ul><li>General Settings</li><li>Antivirus</li></ul>	Miscellaneous				
✓ Firewall	☑ Do not detect shellcode injections in <u>these applications</u>				
✓ HIPS	Do not automatically clean up suspicious certificates				
✓ Containment	Autorun Protection				
<ul> <li>File Rating</li> <li>Advanced Protection</li> <li>VirusScope</li> <li>Scan Exclusions</li> </ul>	Apply the selected action to unrecognized autorun entries represented action to unrecognized autorun entries represented registry items:           Ignore           When this option is enabled, the registry will be monitored for m selected action will be applied to detected unrecognized Window or scheduled tasks.	lated to nodifica ws servi	o new/m tions and	nodified d the ostart en	tries
Device Control Script Analysis Miscellaneous Website Filtering	Apply the selected signature level while monitoring processes loaded on early system start. AUTHENTICODE T The option enables to select the range of signature types that due considered trusted and therefore allowed to run.	s launc	hed and	J DLLs g will be	
	☐ Monitor DLL files being loaded by running processes				
	ок		C/	ANCEL	

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