COMODO
Creating Trust Online®

Comodo
Internet Security Essentials

Software Version 1.3

User Guide

Guide Version 1.3.120318

Comodo Security Solutions
1255 Broad Street
Clifton, NJ, 07013
United States

Table of Contents

Comodo Internet Security Essentials

What is Comodo Internet Security Essentials?

Comodo Internet Security Essentials (CISE) protects you from man-in-the-middle attacks during online banking and shopping sessions by verifying that sites you connect to are using a trusted SSL certificate.

CISE runs as a background process and will alert you if a site uses a potentially malicious certificate. You will have the option to discontinue the connection (recommended) or to continue.

CISE blocks man-in-the-middle attacks attempts by verifying certificates against Comodo's trusted root certificate list. This functionality is especially important if you are accessing sensitive websites while on a public Wi-Fi such as

those found in an cafe, park or airport.

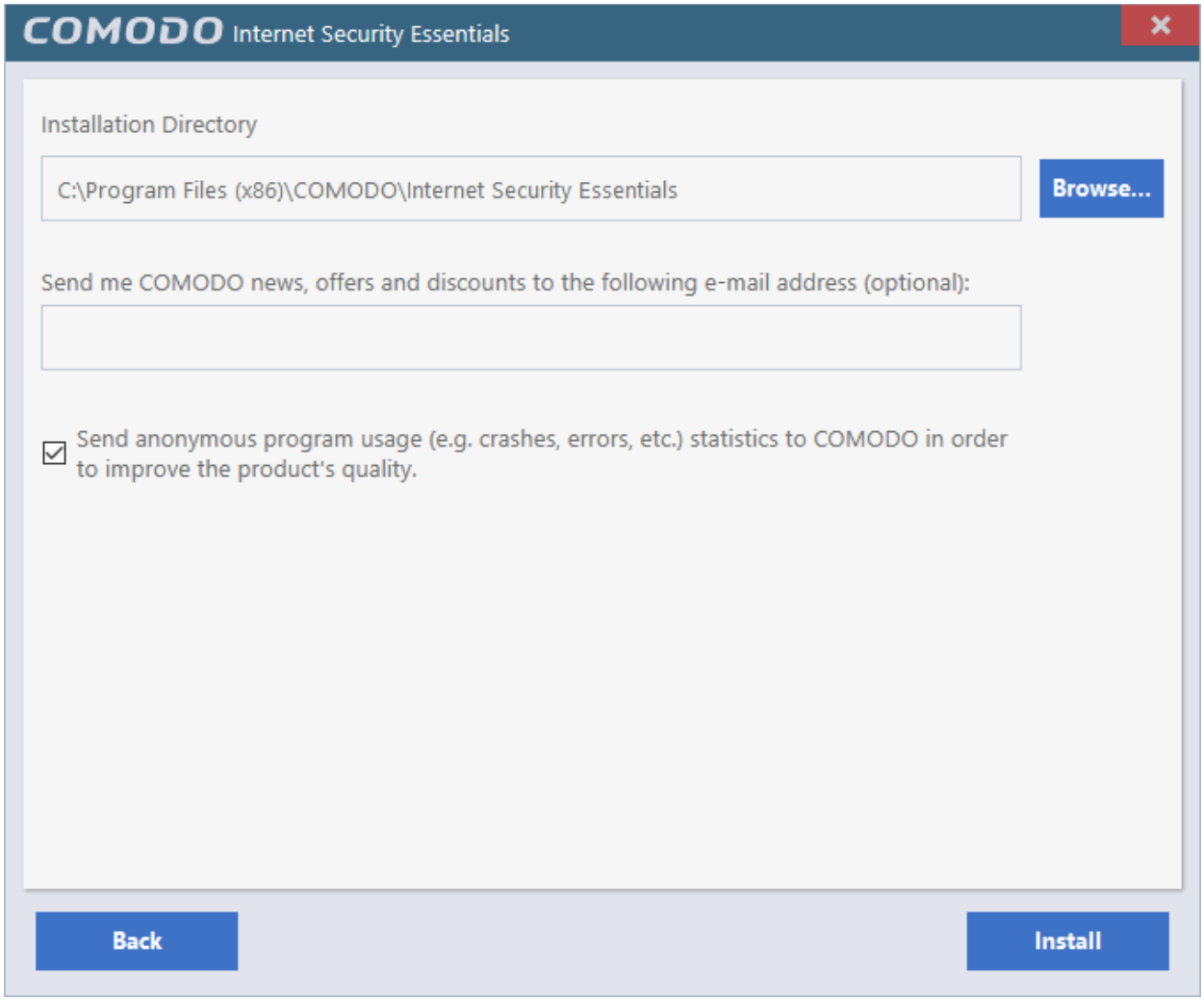
Please note, Internet Explorer is currently the only supported browser.

Back to top

How do I install Comodo Internet Security Essentials?

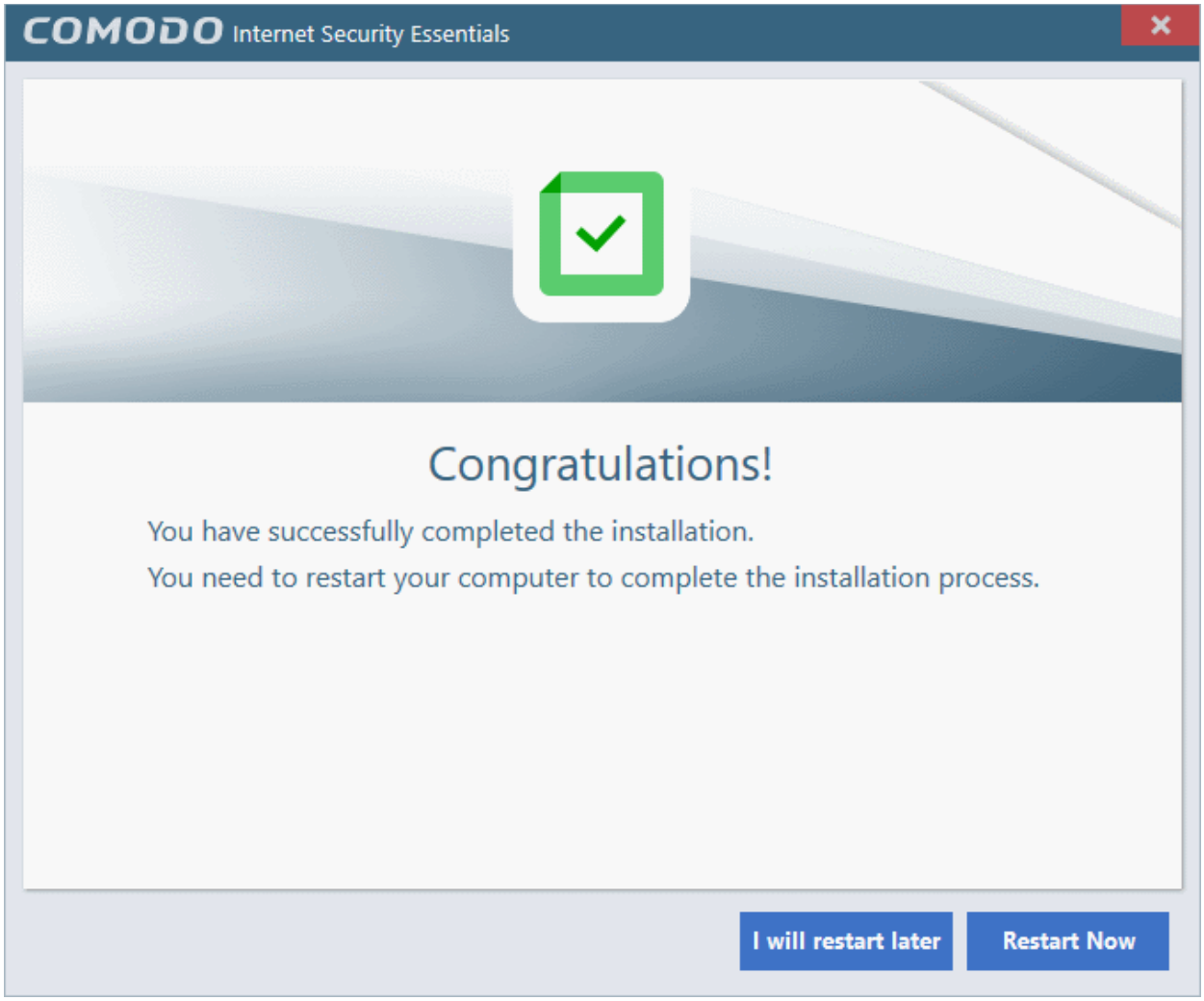
- Download the setup file from **https://www.comodo.com/home/internet-security/internet-security-essentials.php** and save to your local drive.
- Double-click on ise_installer.exe to launch the installation wizard

- First, select the language in which you want to install CISE from the drop-down menu
- Next, view and agree to the terms and conditions by clicking 'I agree' at the bottom of the interface.



- The default installation location is C:/Program Files/COMODO/Comodo Internet Security Essentials. Click the 'Browse...' button if you want to install to a different location.
- Enter your email address in the second field if you would like to subscribe to Comodo news and get offers and discounts from Comodo
- 'Send anonymous program usage (e.g. crashes, errors etc.) statistics to Comodo...' – Help us to improve Comodo Internet Security Essentials by automatically submitting crash and error reports. All data is submitted anonymously over an encrypted channel.

- Click 'Install' to start the installation process. A success message will be shown when the process is complete:



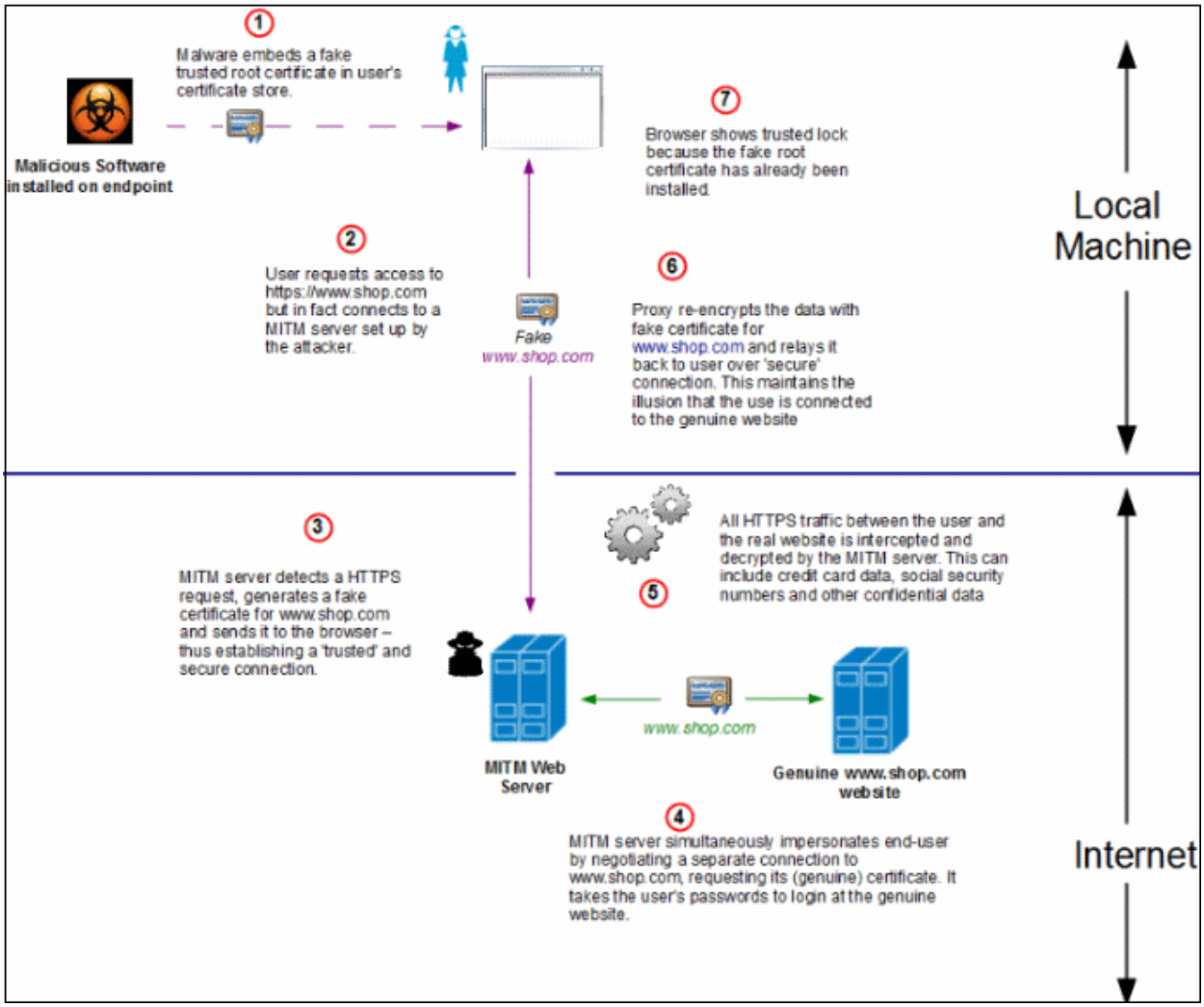
- You need to restart your system to the complete the installation process. Click 'Restart Now' or 'I will restart later'.

Back to top

What is a man-in-the-middle attack?

Man-in-the-middle attacks occur when an attacker forces a client to connect to a server other than the one that the client intended to connect.

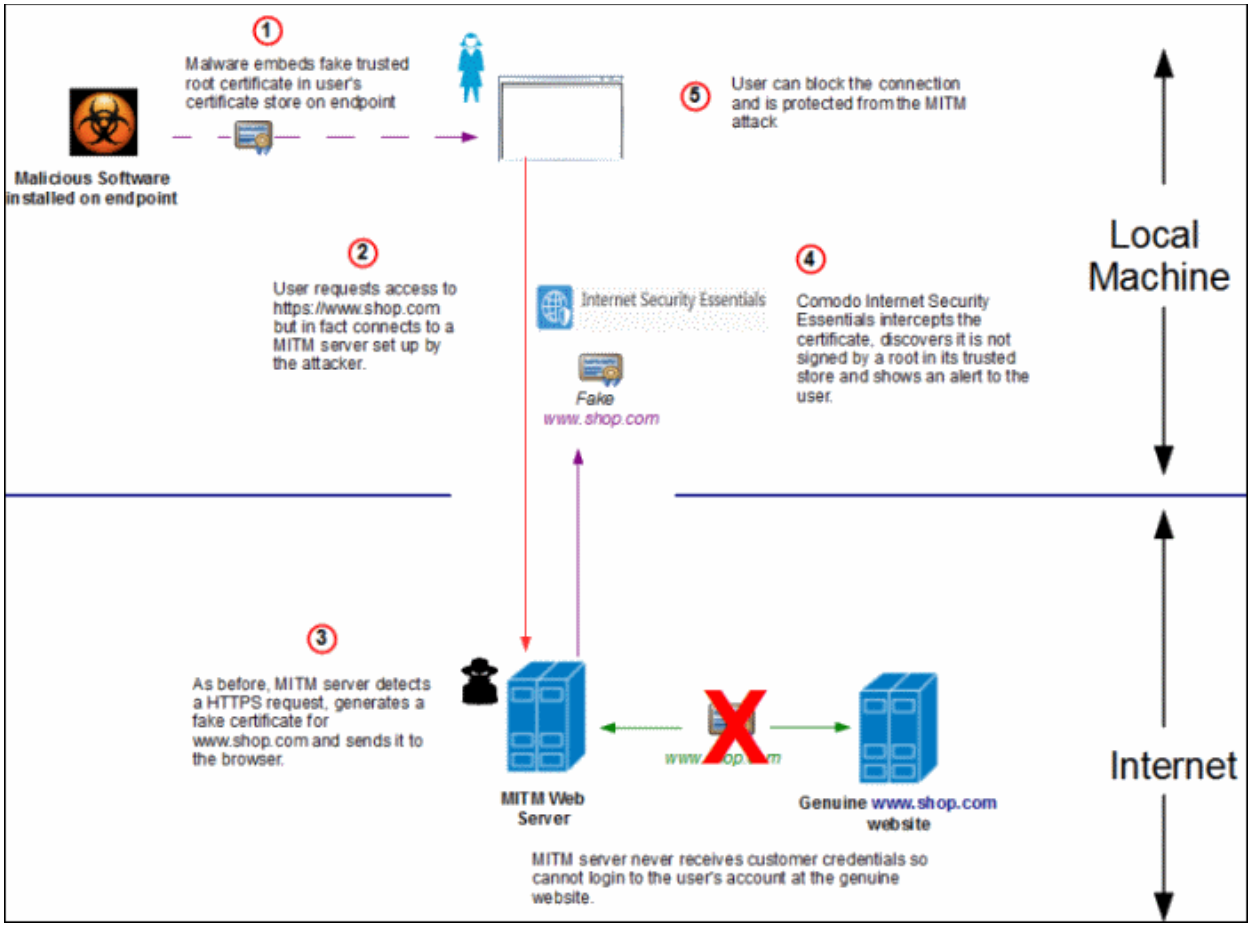
By injecting a fake root certificate into the Windows certificate store, malicious actors can often fool browsers into trusting a connection to a server operated by an attacker. This is known as certificate root poisoning and is the most commonly used technique for launching man-in-the-middle attacks. If successful, all data sent from your browser would be routed through the attacker's server. The following diagram shows a typical man-in-the-middle attack:



Back to top

How does Comodo Internet Security Essentials protect me from a man-in-the-middle attack?

Comodo Internet Security Essentials blocks these attacks by independently verifying all certificates used for secure connections against an internal, verified list of trusted root certificates. The following diagram shows hows CISE will thwart a man-in-the-middle attack:



Back to top

What is the install location of Comodo Internet Security Essentials?

By default, Comodo Internet Security Essentials is installed at:

C:\Program Files (x86)\Comodo\Internet Security Essentials

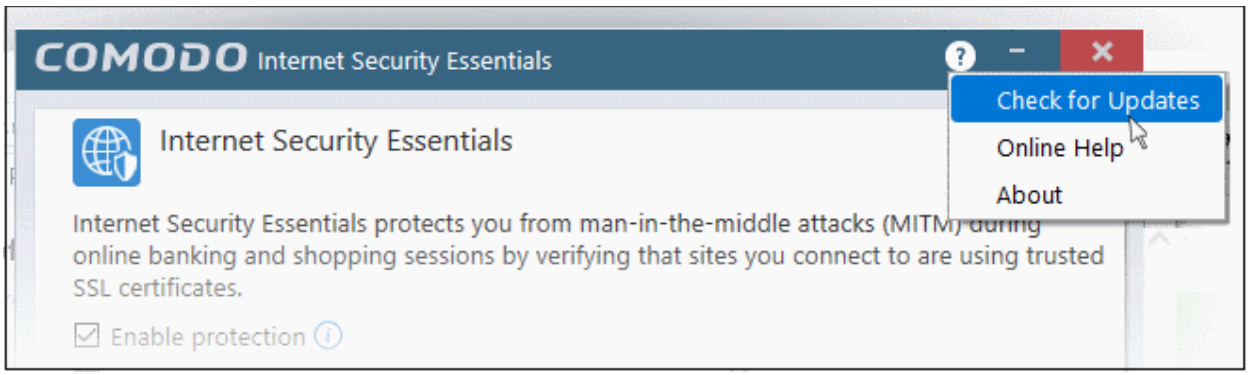
Back to top

How do I update CISE?

You can update manually or configure automatic updates.

To check and update manually

- Open Comodo Internet Security Essentials
- Click the help icon at the top right
- Select 'Check for Updates' from the options:

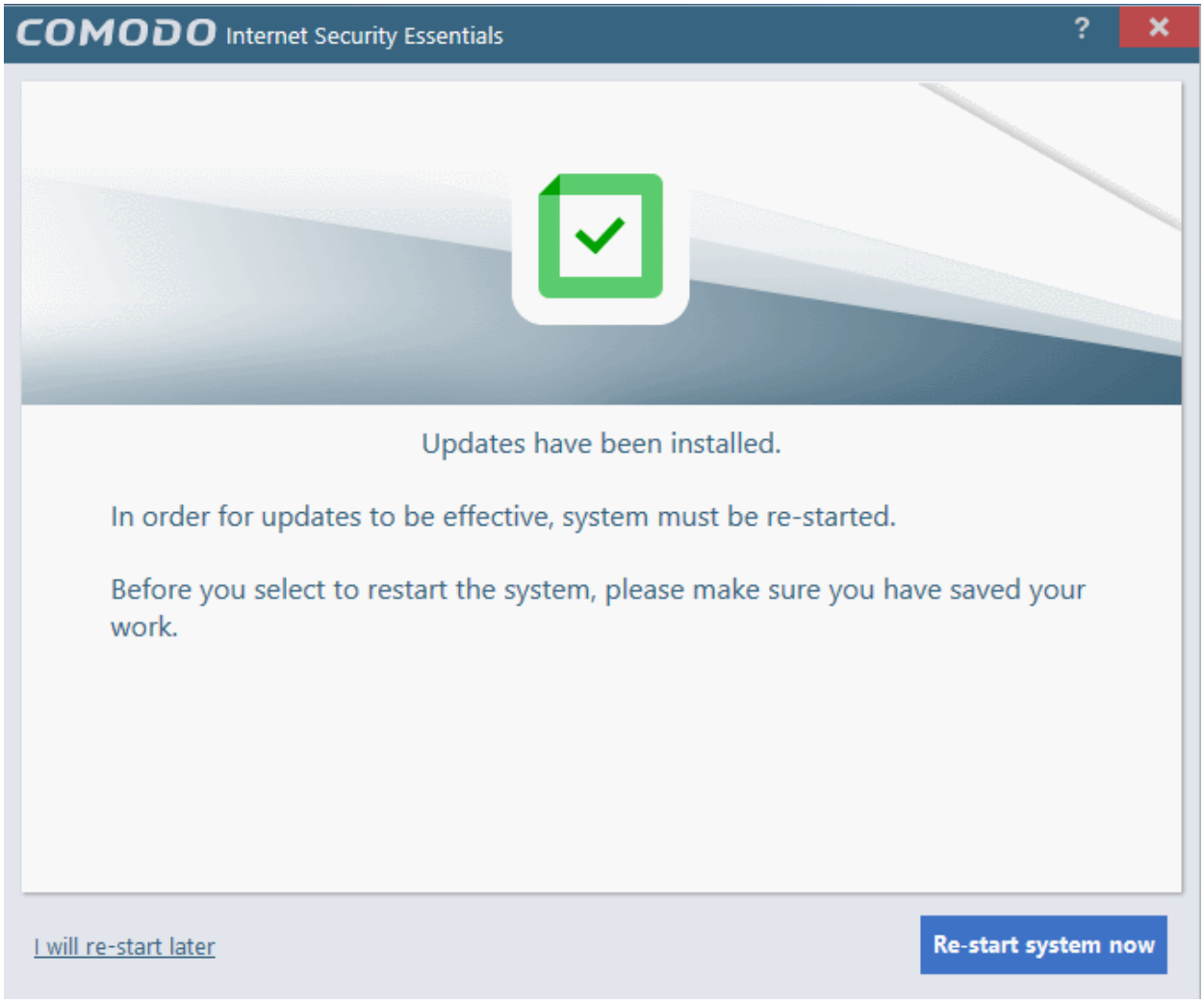


- CISE will check Comodo servers for any updates. Please make sure your internet connection is active.

- Click 'Apply'

Updates will be automatically installed if available:

Click the 'Finish' button to finalize the installation.



- Click 'Re-start system now' to apply the updates.

To configure automatic updates

Open the CISE configuration screen

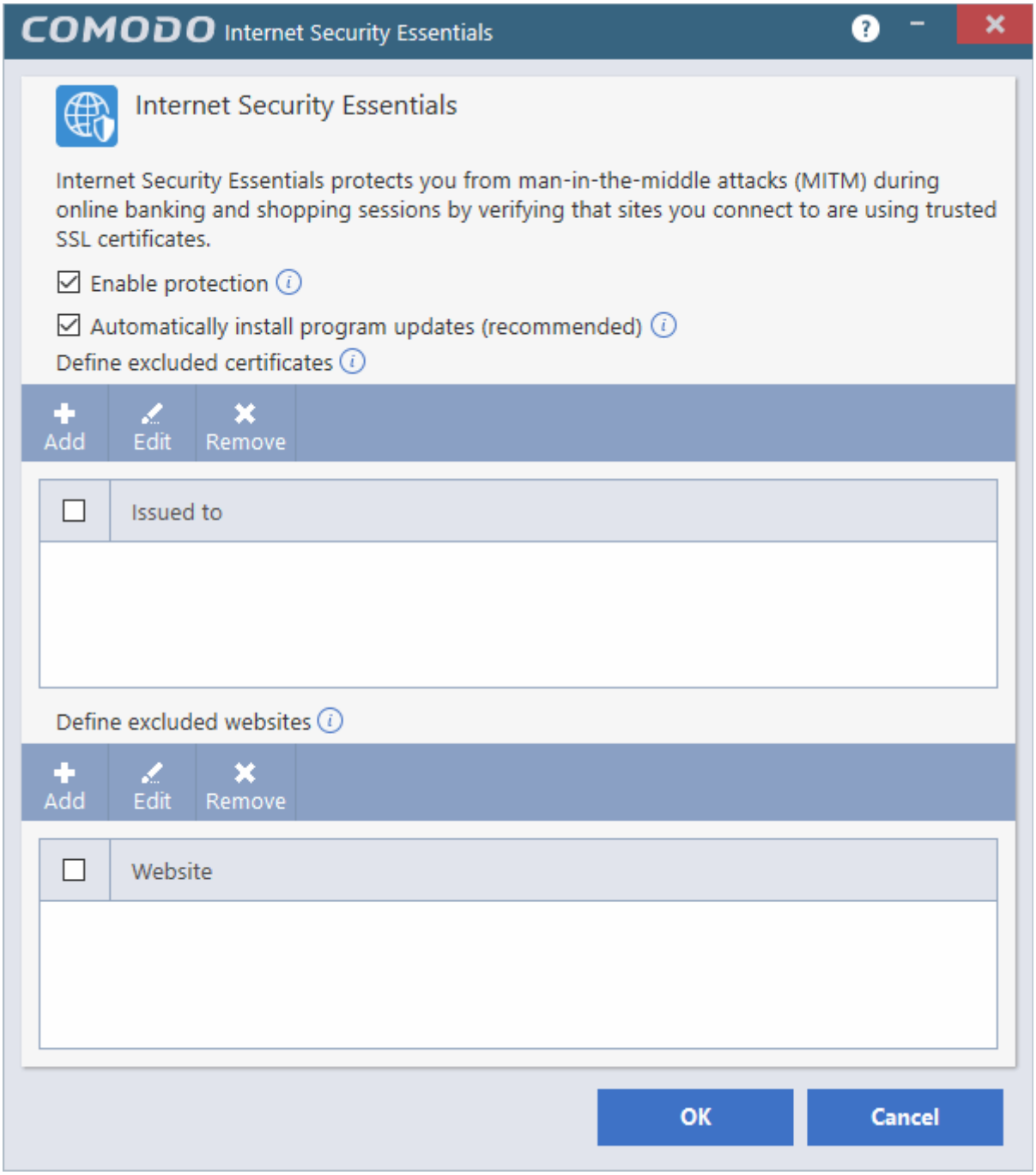
- via the Windows Start Menu:

  Click Start and select All Programs > Comodo > Internet Security Essentials

  OR

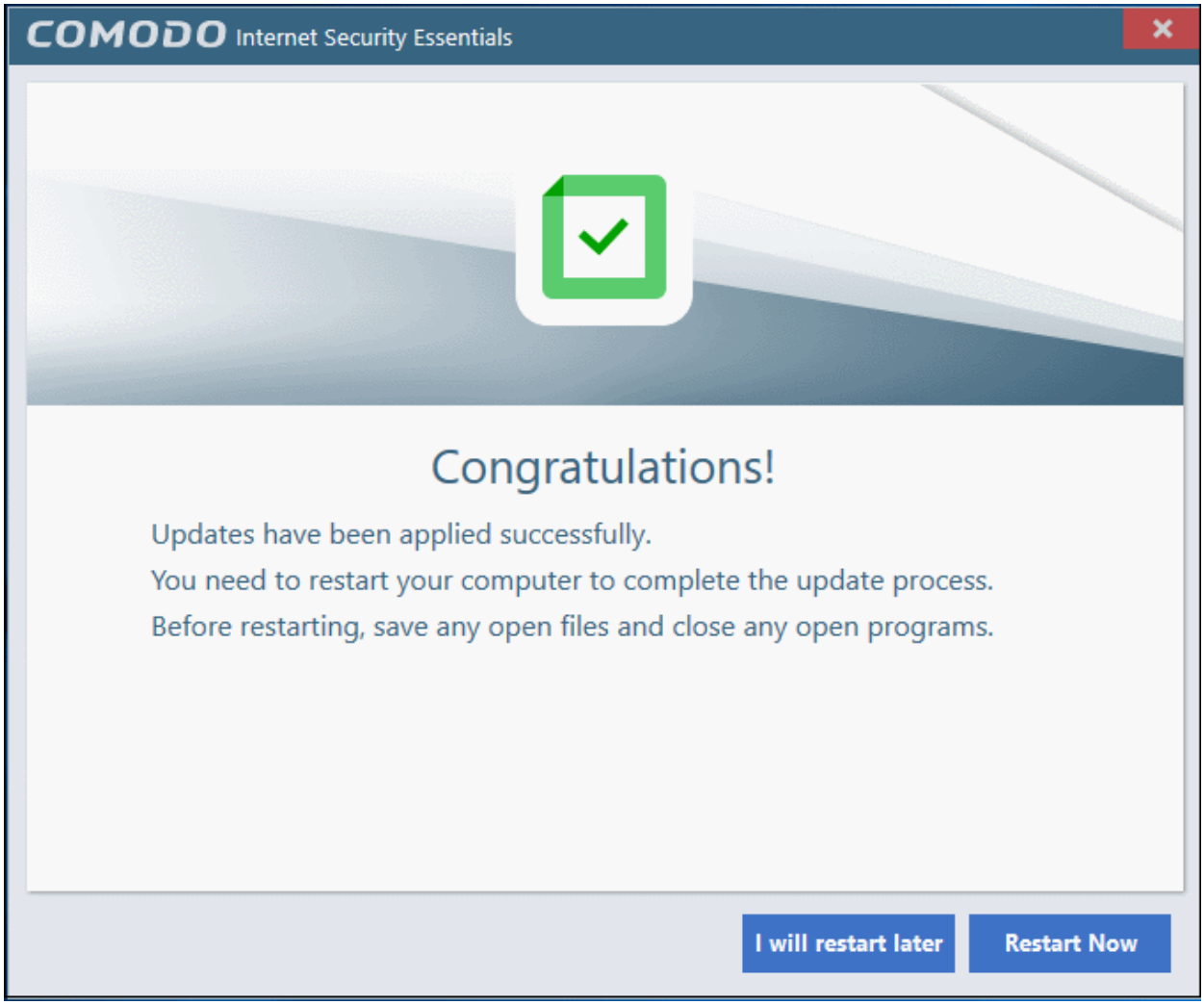
- by clicking the cog icon in the alert:

This will open the CISE configuration screen:



- Enable 'Automatically install program updates (recommended)'
- CISE will check Comodo servers every day for updates
- You will be alerted if an update is available:

- Click 'Update Now' to apply the update immediately.
- To apply the update later, select when you would like to be reminded from the drop-down and click 'Postpone'.
- You will see the following confirmation when the updates have been successfully installed:



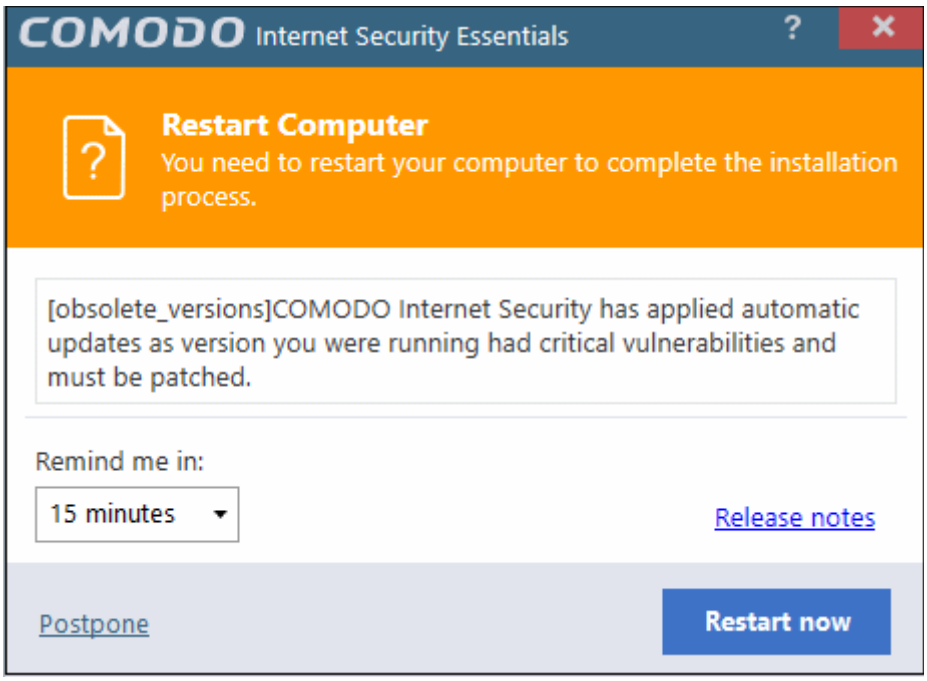
- Click 'Restart Now' to reboot your computer and finalize the update
- Click 'I will restart later' to restart at later time

Note: CISE will automatically install updates if:

1. The application has not been updated for a long time and has become obsolete.
2. There are compatibility issues with the existing build or a serious vulnerability has emerged.

These kind of updates will be applied even if automatic updates are disabled.

The following dialog will be shown after a forced update:

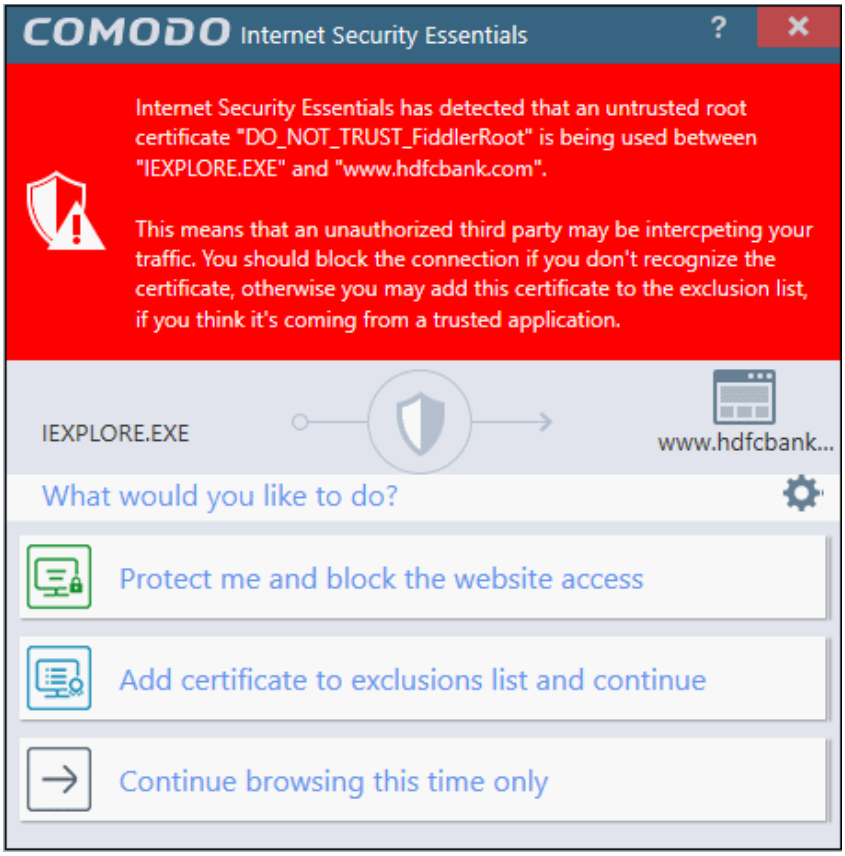


- Click 'Restart Now' to restart the system immediately.
- To apply the update later, select when you would like to be reminded from the drop-down and click 'Postpone'.

Back to top

Understanding alerts and configuring exceptions

If CISE detects that a website is potentially using a fraudulent certificate it will present you with an alert similar to the following:



The alert means that the website you are visiting may be fraudulent as it is using a certificate signed by a root that is not in CISE's internal store of trusted root certificates.

- Protect me and block website access - Closes your connection to the website (recommended)
- Add certificate to exception list and continue – Adds the certificate to the whitelist and allows the connection to proceed. The root certiicate will not be flagged if CISE detects it in future on any sites. Only choose this option if you are sure the website can be trusted or is using, for example, a self-signed certificate that you have already been made aware of. Do not choose this option if this is one of your regular shopping or banking websites.
- Continue browsing this time only – Accept the connection only for the current session. CISE will warn you again if it detects this certificate next time.

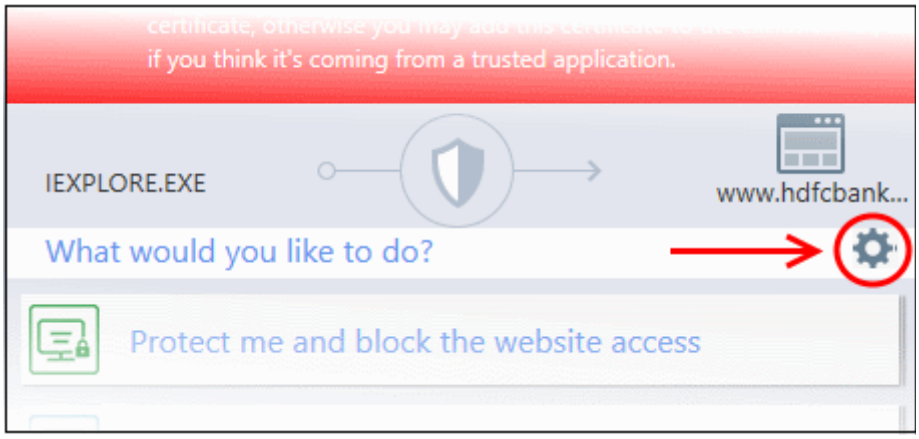
You can whitelist certificates and websites in two ways:

- via the Windows Start Menu:

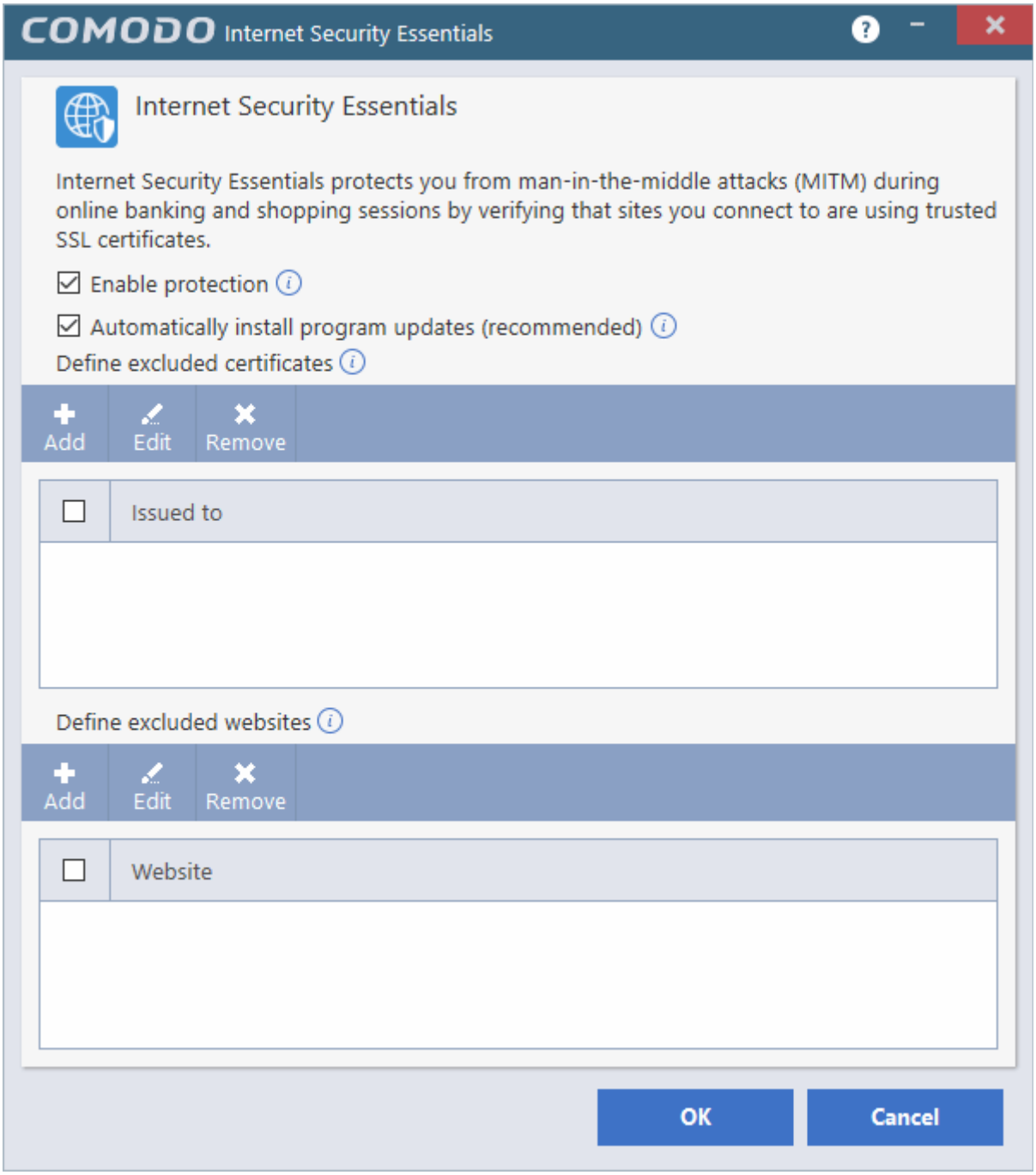
  Click Start and select All Programs > Comodo > Internet Security Essentials

  OR

- by clicking the cog icon in the alert:



This will open the CISE configuration screen:



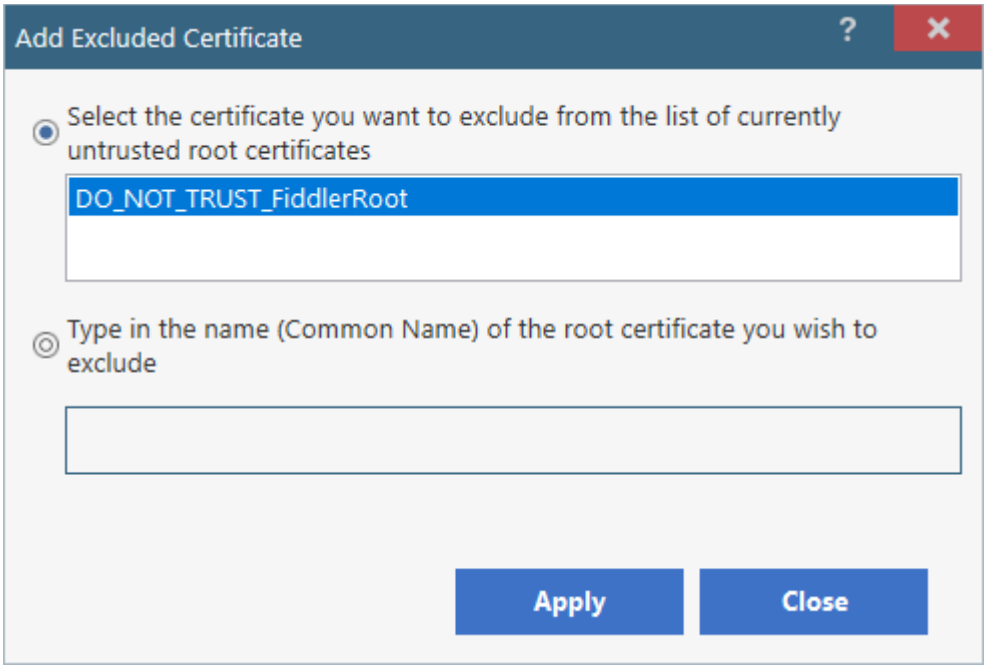
- Enable protection - CISE will monitor the SSL certificates used on the sites you visit and will warn you if a potentially fraudulent certificate is used.
- Automatically install program updates (recommended) - CISE will check with Comodo servers every day for any updates.

You can add certificates and/or website(s) to the list of exceptions:

- Certificate exception – Certificates added to this list will not be flagged by CISE in future.
- Website exception – CISE will not flag any certificates on the domains you add here.

Add a certificate to exceptions

- Click 'Add' under 'Define excluded certificates' to open the certificate configuration dialog:



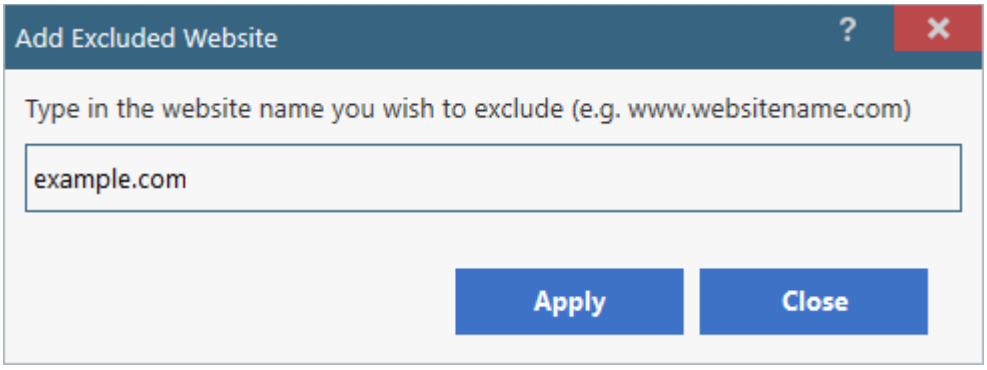
  - Select the certificate you wish to whitelist from the list of untrusted certificates that CISE has encountered since installation.

  OR

  - Manually type the name (Common Name) of the root certificate you wish to exclude.
  - Click 'Apply' for your settings to take effect.
  - The certificate(s) will be added to the list of exceptions.
- Repeat the process to add more certificates.

Add a website to the exclusion list

- Click 'Add' under 'Define excluded websites' to open the website whitelist configuration dialog:



- Enter the URL of the web site you wish to exclude in the field provided then click 'Apply'.
- CISE will no longer flag potentially fraudulent certificates found on whitelisted domains.
- Click 'OK'. Repeat the process to add more websites.

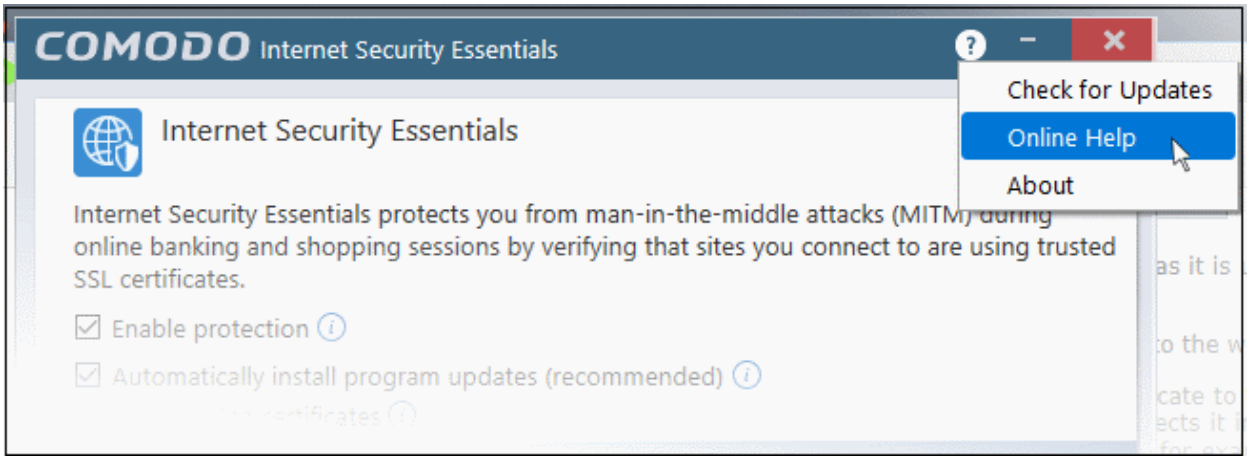
Edit / remove a certificate / website

- To edit a website name or a certificate, select it and click 'Edit'.
- To remove a website or a certificate, select it and click 'Remove'.
- Click 'OK' for your settings to take effect

Back to top

How do I view CISE help?

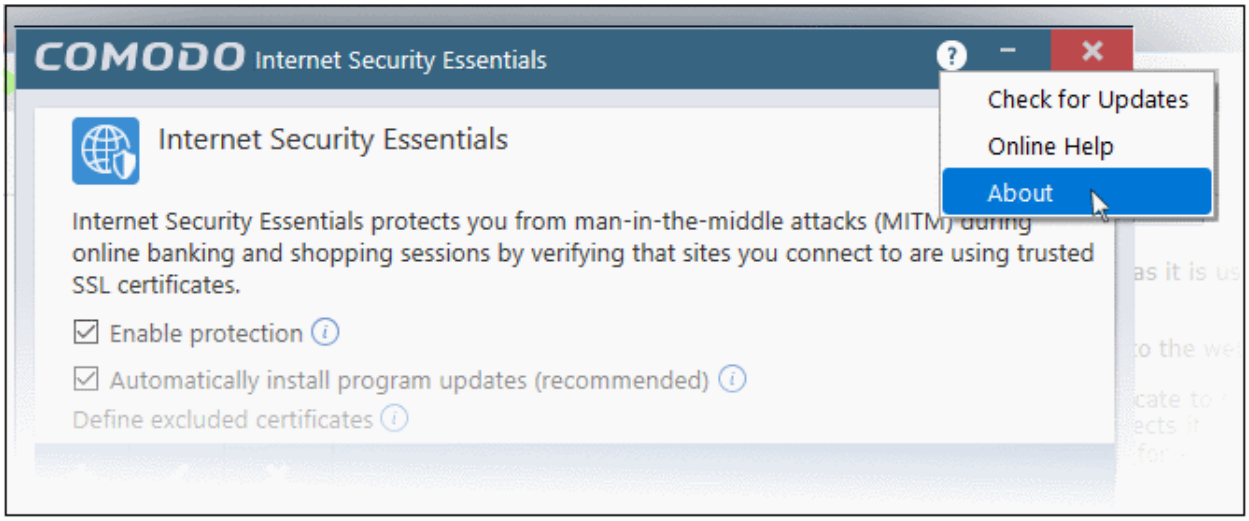
- Click the help icon at the top right of the application or an alert
- Select 'Online Help' to view the product help guide at **https://help.comodo.com/topic-435-1-841-10768-Introduction-to-Comodo-Internet-Security-Essentials.html**



Back to top

How do I view the version number and release notes?

- Click the help icon at the top right of the application or an alert
- Select 'About':



The 'About' screen contains:

- Version details including copyright information.
- A link to the latest release notes where you can find out about new features and bug fixes.

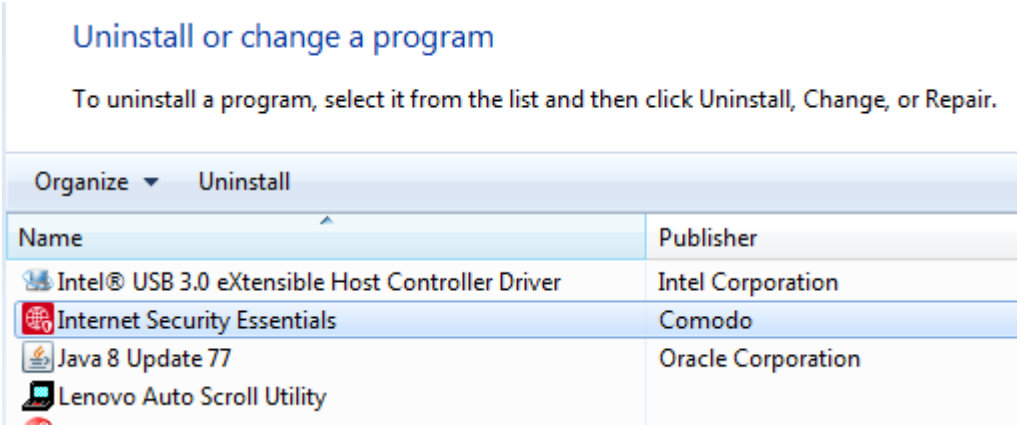
Back to top

How do I remove Comodo Internet Security Essentials?

Comodo Internet Security Essentials installs as a standalone program and must be removed separately. Uninstalling the application that CISE was bundled with will not remove nor deactivate the program.

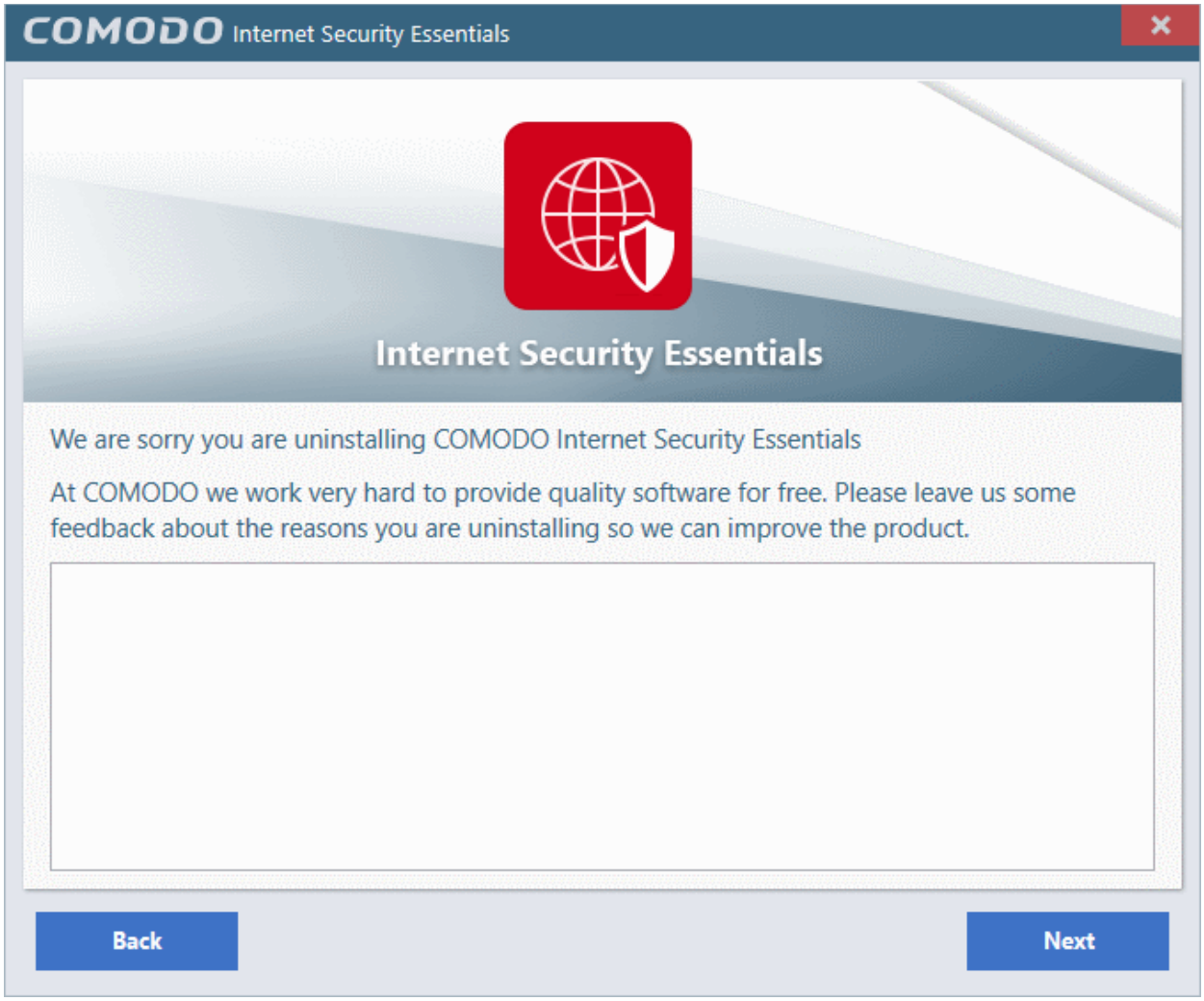
To remove Comodo Internet Security Essentials:

- Open the Windows control panel then open 'Programs and Features' (or 'Add/Remove Programs' on older versions of Windows)
- Select 'Internet Security Essentials' in the list of programs
- Click 'Uninstall'

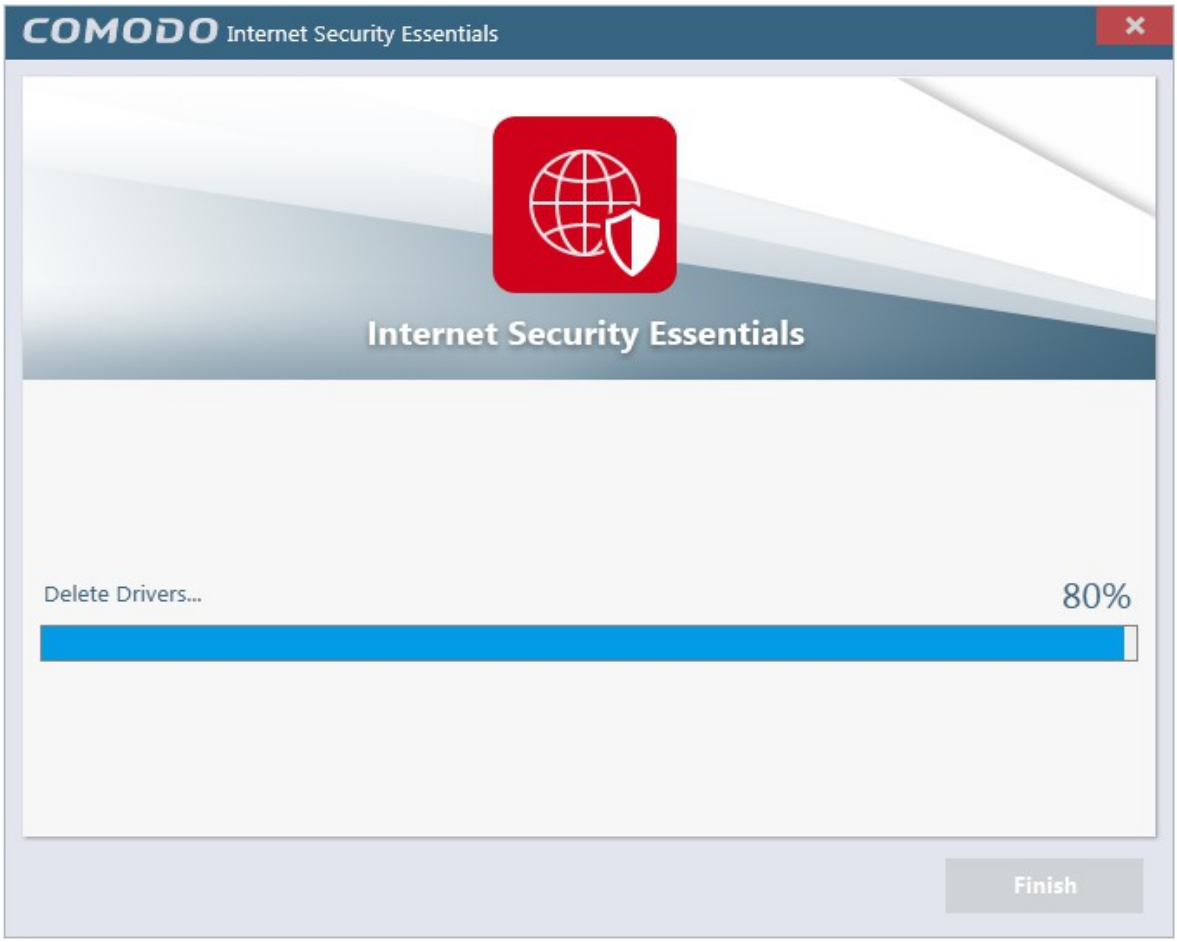


- The uninstallation wizard will start. Click 'Uninstall' to remove the program:

- Please provide us with valuable feedback by specifying the reason that you are uninstalling Comodo Internet Security Essentials:



- Click 'Next' to complete the uninstall:



That's it! Click 'Finish' to close the program.

Back to top

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**