



# 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

COMODO

### **Table of Contents**

Comodo Internet Security Essentials	3
What is Comodo Internet Security Essentials?	3
How do I install Comodo Internet Security Essentials?	4
What is a man-in-the-middle attack?	6
How does Comodo Internet Security Essentials protect me from a man-in-the-middle attack?	7
What is the install location of Comodo Internet Security Essentials?	8
How do I update CISE?	8
Understanding alerts and configuring exceptions	14
How do I view CISE help?	
How do I view the version number and release notes?	18
How do I remove Comodo Internet Security Essentials?	19
About Comodo Security Solutions	23

# **Comodo Internet Security Essentials**

- What is Comodo Internet Security Essentials?
- How do I install Comodo Internet Security Essentials?
- What is a man-in-the-middle attack?
- How does Comodo Internet Security Essentials protect me from a man-in-the-middle attack?
- What is the install location of Comodo Internet Security Essentials?
- How do I update CISE?
- Understanding alerts and configuring exceptions
- How do I view CISE help?
- How do I view the version number and release notes?
- How do I remove 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

COMODO

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.

#### COMODO Creating Trust Online\*

Browse
nstall

- 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:

COMODO Creating Trust Online\*



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:

➀ Malware embeds a fake trusted root certificate in user's certificate store. (7)Browser shows trusted lock because the fake root Malicious Software certificate has already been in stalled on endpoint installed Local 2 Machine 6 User requests access to https://www.shop.com but in fact connects to a Proxy re-encrypts the data with MITM server set up by fake certificate for Fake the attacker. www.shop.com and relays it www.shop.com back to user over 'secure' connection. This maintains the illusion that the use is connected to the genuine website All HTTPS traffic between the user and 3 the real website is intercepted and decrypted by the MITM server. This can include credit card data, social security MITM server detects a HTTPS request, generates a fake certificate for www.shop.com numbers and other confidential data and sends it to the browser thus establishing a 'trusted' and secure connection. www.shop.com MITM Web Genuine www.shop.com Server web site (4) MITM server simultaneously impersonates end-user Internet by negotiating a separate connection to www.shop.com, requesting its (genuine) certificate. It takes the user's passwords to login at the genuine website

Back to top

COMODO Creating Trust Online

# 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

COMODO Creating Trust Online

# 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:

COMODO

COMODO Internet Security Essentials	? -	×
	Check	for Updates
Internet Security Essentials	Online	Help 🗟
Internet Security Essentials protects you from man-in-the-middle attacks (MIT online banking and shopping sessions by verifying that sites you connect to a SSL certificates.	About M) auring re using trus	sted
Enable protection ()		

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

COMODO Internet Security Essentials	?	×
Internet Security Essentials		
Updates for Internet Security Essentials are available By clicking "Apply" button you consent that you have read and accepted Comodo Internet Security Essentials <u>License Agreement</u> and <u>Privacy Policy</u>		
Release not	es pply	

Click 'Apply'

•

Updates will be automatically installed if available:



Click the 'Finish' button to finalize the installation.

сомодо



• 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:

сомодо

COMODO Creating Trust Online\*

COMODO Internet Security Essentials ? -	×
Internet Security Essentials	
Internet Security Essentials protects you from man-in-the-middle attacks (MITM) during online banking and shopping sessions by verifying that sites you connect to are using truster SSL certificates.	d
Enable protection ()	
Automatically install program updates (recommended) i Define excluded certificates i	
+ X X Add Edit Remove	
Issued to	
Define excluded websites 🕡	
+     ★       Add     Edit       Remove	
U Website	
OK Cancel	

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

COMODO

COMODO Internet Security Essentials	?	×
Updates for your computer are availan Keep your computer protected against man-in-t attacks (MITM)	<b>ble</b> he-mic <u>Lear</u>	idle <u>n More</u>
We recommend you to install this update to stay protected latest threats and to ensure the best system performance.	from th	he
By clicking "Update Now", you consent that you have read a Internet Security Essentials License Agreement and Priva	and acc acy Pc	epted
	Release	Notes
Remind me in:		
30 minutes		•
Postpone Upo	late no	w

- 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:

COMODO Creating Trust Online\*



- · 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:

COMODO Creating Trust Online\*

COMODO Internet Security Essentials	? >	×
<b>Restart Computer</b> You need to restart your computer to process.	complete the installatio	'n
[obsolete_versions]COMODO Internet Security h updates as version you were running had critica must be patched.	nas applied automatic I vulnerabilities and	
Remind me in: 15 minutes 🔻	Release notes	
Postpone	Restart now	

- · 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:

COMODO

COM	1000 Internet Security Essentials ? 🗙
<b>A</b>	Internet Security Essentials has detected that an untrusted root certificate "DO_NOT_TRUST_FiddlerRoot" is being used between "IEXPLORE.EXE" and "www.hdfcbank.com". This means that an unauthorized third party may be intercpeting your traffic. You should block the connection if you don't recognize the certificate, otherwise you may add this certificate to the exclusion list, if you think it's coming from a trusted application.
IEXPLO	DRE.EXE O
What	t would you like to do?
œ.	Protect me and block the website access
<b>.</b>	Add certificate to exclusions list and continue
$\rightarrow$	Continue browsing this time only

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 certificate 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:

COMODO Creating Trust Online\*

certificate, otherwise you may add this certificate to e if you think it's coming from a trusted application.	
	www.hdfcbank
What would you like to do?	<b>→</b> ۞
Protect me and block the website access	

This will open the CISE configuration screen:

COMODO Internet Security Essentials ? - ×
Internet Security Essentials
Internet Security Essentials protects you from man-in-the-middle attacks (MITM) during online banking and shopping sessions by verifying that sites you connect to are using trusted SSL certificates.
Enable protection (i)
Automatically install program updates (recommended) (i) Define excluded certificates (i)
+ X X Add Edit Remove
Issued to
Define excluded websites 🕡
+ X X Add Edit Remove
U Website
OK Cancel

- 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:

Add Excluded Certificate	?	×
<ul> <li>Select the certificate you want to exclude from the list of currently untrusted root certificates</li> </ul>		
DO_NOT_TRUST_FiddlerRoot		
© Type in the name (Common Name) of the root certificate you wish exclude	1 to	
Apply Close	2	

 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:

Add Excluded Website		?	×
Type in the website name you wish	to exclude (e.g. www.	websitename.com	1)
example.com			
	Apply	Close	
	Apply	Close	

сомоло



- 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

COMODO Internet Security Essentials	? - >	:	
		Updates	
Internet Security Essentials	Online He	Online Help	
	About	~	
Internet Security Essentials protects you from man-in-the-middle attacks (MITM) during online banking and shopping sessions by verifying that sites you connect to are using trusted SSL certificates.			
Enable protection ()			
Automatically install program updates (recommended) ()		cate to ects it i	

#### 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':

COMODO

OMODO Internet Security Essentials	<u>? - X</u>
	Check for Updates
Internet Security Essentials	Online Help
	About 📐
and a band in a state of the second state of t	
SSL certificates.	as it is
SSL certificates.	as it is

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.

	COMODO Comodo Internet Security Essentials Product Version:1.3.436779.133	? <u>Release Note</u>	×
Patents Pending. Copyright 2005-2011	7 СОМОДО		

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'

#### Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Organize 🔻 Uninstall				
Name	Publisher			
3 Intel® USB 3.0 eXtensible Host Controller Driver	Intel Corporation			
Internet Security Essentials	Comodo			
🕌 Java 8 Update 77	Oracle Corporation			
📕 Lenovo Auto Scroll Utility				

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:

СОМОДО

 Back
 X

Click 'Next' to complete the uninstall:

COMODO Creating Trust Online\*

COMODO Internet Security Essentials

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

Back to top

COMODO Creating Trust Online\*



# **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