

8549167



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

November 29, 2024

**THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE
RECORDS OF THIS OFFICE OF THE FILE WRAPPER AND CONTENTS
OF:**

APPLICATION NUMBER: 16/141,378

FILING DATE: *September 25, 2018*

PATENT NUMBER: 11178104

ISSUE DATE: *November 16, 2021*



Certified by

Katherine Kelly Vidal

Performing the Functions and Duties of the
Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	Not Yet Assigned
Filing Date	Herewith
First Named Inventor	Glenn Coleman
Title	NETWORK ISOLATION WITH CLOUD NETWORKS
Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned
Attorney Docket Number	LCOM_ENT_CLOUD_US01

SIGNATURE of Applicant or Patent Practitioner

Signature	/Benjamin Chalfin/	Date (Optional)	2018-09-25
Name	Benjamin Chalfin	Registration Number	74,181
Title (if Applicant is a juristic entity)	Patent Practitioner		
Applicant Name (if Applicant is a juristic entity)	L3 Technologies, Inc.		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.



*Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)



I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above:

15027

OR



I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:



The address associated with the above-mentioned Customer Number

OR



The address associated with Customer Number:

OR

Firm or Individual Name	
Address	
City	State Zip
Country	
Telephone	Email

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

L3 Technologies, Inc.



Inventor or Joint Inventor (title not required below)



Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)



Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)



Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature	Date (Optional)	7-27-17
Name	Donald L. Letizia	
Title	VP, General Counsel CSO	

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.



Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**In re Application of:
L3 Technologies, Inc.**

For: NETWORK ISOLATION WITH CLOUD NETWORKS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**AUTHORIZATION TO TREAT A REPLY AS
INCORPORATING AN EXTENSION OF TIME UNDER C.F.R. § 1.136(a)(3)**

Sir/Madame:

The Commissioner is hereby requested to grant an extension of time for the appropriate length of time, should one be necessary, in connection with this filing or any further filing submitted to the U.S. Patent and Trademark Office in the above-identified application during the pendency of this application. The Commissioner is further authorized to charge any fees related to any such extension of time to Deposit Account No. 50-5519.

Date: September 25, 2018

/Benjamin Chalfin/
Name: Benjamin Chalfin
Registration No.: 74,181

Electronic Patent Application Fee Transmittal

Application Number:

Filing Date:

Title of Invention:

NETWORK ISOLATION WITH CLOUD NETWORKS

First Named Inventor/Applicant Name:

Glenn Coleman

Filer:

Benjamin S. Chalfin/melissa overline

Attorney Docket Number:

LCOM_ENT_CLOUD_US01

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
UTILITY APPLICATION FILING	1011	1	300	300
UTILITY SEARCH FEE	1111	1	660	660
UTILITY EXAMINATION FEE	1311	1	760	760

Pages:

Claims:

Miscellaneous-Filing:

Petition:

Patent-Appeals-and-Interference:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1720

Electronic Acknowledgement Receipt

EFS ID:	33823526
Application Number:	16141378
International Application Number:	
Confirmation Number:	2440
Title of Invention:	NETWORK ISOLATION WITH CLOUD NETWORKS
First Named Inventor/Applicant Name:	Glenn Coleman
Customer Number:	15027
Filer:	Benjamin S. Chalfin/melissa overline
Filer Authorized By:	Benjamin S. Chalfin
Attorney Docket Number:	LCOM_ENT_CLOUD_US01
Receipt Date:	25-SEP-2018
Filing Date:	
Time Stamp:	16:19:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 1720
RAM confirmation Number	092618INTEFSW16204800
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		LCOM_ENT_CLOUD_US01_AS_ FILED_SPECIFICATION.pdf	221169	yes	35
			71925bb218bcb5f398ca83c6cc0200acb2a d930a		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Abstract		35	35	
	Claims		31	34	
	Specification		1	30	
Warnings:					
Information:					
2	Drawings-only black and white line drawings	LCOM_ENT_CLOUD_US01_AS_ FILED_DRAWINGS.pdf	313209	no	4
			310d5ed559ab04e938eac7f4fe1b8a6e00ee a1f3		
Warnings:					
Information:					
3	Oath or Declaration filed	LCOM_ENT_CLOUD_US01_AS_ FILED_Executed_Declarations. pdf	328765	no	3
			91b3cdf69dc32b39d0573f2d7220ae037be b6fe6		
Warnings:					
Information:					
4	Application Data Sheet	LCOM_ENT_CLOUD_US01_AS_ FILED_ADS.pdf	102621	no	9
			78d63431f2c72e2f88df5cfa765de06d307c 25fb		
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					

5	Power of Attorney	LCOM_ENT_CLOUD_US01_AS_FILED_POA.pdf	240257	no	2
			af56790d1591528353dd9a6db93afc5e7fd085e1		
Warnings:					
Information:					
6	Authorization for Extension of Time all replies	LCOM_ENT_CLOUD_US01_AS_FILED_EOT_Authorization.pdf	69349	no	1
			ed3b635630fff31a857d4b627f1d1c32ec190787		
Warnings:					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	34867	no	2
			a9503bc5d04c17a25991ed3a842b146ac12ac2d4		
Warnings:					
Information:					
Total Files Size (in bytes):			1310237		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

ABSTRACT

Systems and methods are disclosed for a sandbox based network isolation system configured to protect cloud based assets. A host computer system may include a processor and a memory. The host computer system may include a workspace. One or more applications may run in the workspace via a first memory space (e.g., a trusted memory space). The host computer system may include an isolated computing environment. One or more isolated applications may run in the isolated computing environment via a second memory space (e.g., an untrusted memory space). The isolated computing environment may be isolated from the workspace by an internal isolation firewall. The internal isolation firewall may prevent communication between the isolated computing environment and the workspace.

CLAIMS

What Is Claimed:

1. A host computer system comprising a processor and memory, the processor configured to:
 - implement a workspace, wherein the workspace is configured to enable operation of a first set of one or more applications or processes via a first memory space;
 - implement an isolated computing environment, the isolated computing environment being configured to enable operation of a second set of one or more applications or processes via a second memory space, wherein the isolated computing environment is configured to access an Internet-based cloud service via at least one application of the second set of applications;
 - isolate the isolated computing environment from the workspace using an internal isolation firewall; and
 - communicate with at least one proxy server in order to access the Internet-based cloud service, wherein the isolated computing environment is configured to authenticate with an authentication device in order to allow communication between the at least one application and the Internet-based cloud service.
2. The system of claim 1, wherein the processor is configured to access the Internet-based cloud service via one or more of a local area network (LAN), a wide area network (WAN), a cellular network, a Wi-Fi network, a digital subscribers line (DSL) network, a cloud computing network, a data center, or a satellite network.
3. The system of claim 1, wherein the Internet-based cloud service comprises one or more of an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS).
4. The system of claim 1, wherein the processor is configured to select the at least one proxy server from a plurality of candidate proxy servers, the plurality of proxy servers comprising at least one Internet-based proxy server or at least one local network-based proxy server.

5. The system of claim 4, wherein the processor is configured to determine whether to send web traffic to the local network-based proxy server or the Internet-based proxy server based on a location of the host computer system.
6. The system of claim 4, wherein the processor is configured to determine whether to send web traffic to the local network-based proxy server or the Internet-based proxy server based on an identity of a network to which the host computer system is connected.
7. The system of claim 4, wherein the processor is configured to determine whether to send web traffic to the local network-based proxy server or the Internet-based proxy server based on the identity of the at least one application running in the isolated computing environment.
8. The system of claim 1, wherein the internal isolation firewall is configured to segregate the first memory space from the second memory space and is configured to enforce policies for communication between the first memory space and the second memory space.
9. The system of claim 8, wherein the internal isolation firewall is further configured to prompt a user of the host computer system to allow communication between the first memory space and the second memory space.
10. A cloud computing system comprising:
 - a cloud computing network, the cloud computing network comprising at least one server, wherein the server comprises a first set of one or more applications or processes running in a workspace and a second set of one or more applications or processes running in an isolated computing environment, and the server comprises an internal firewall to isolate the workspace from the isolated computing environment; and
 - at least one proxy configured to control communication between the server and at least one Internet resource, wherein the proxy is configured to allow communication between the second set of one or more applications or processes running in the isolated computing environment and the at least one Internet resource and to block communication between the first set of one or more applications or processes running in the workspace and the at least one Internet resource.

11. The system of claim 10, wherein the server is configured to perform at least one processing task on behalf of a client device.
12. The system of claim 11, wherein the at least one proxy comprises a first proxy and a second proxy, and the server is configured to determine whether to send traffic to the first proxy or the second proxy.
13. The system of claim 12, wherein the server is configured to determine whether to send traffic to the first proxy or the second proxy based on user-provided credentials.
14. The system of claim 10, further comprising a border firewall configured to segregate the cloud computing network from one or more Internet destinations.
15. The system of claim 10, wherein the internal firewall is further configured to allow communication between the workspace and the isolated computing environment on a condition that the communication is in a predetermined format.
16. The system of claim 11, wherein the server is further configured to receive input data from the client device and send one or more data communications to the client device.
17. The system of claim 11, wherein the at least one processing task performed on behalf of the client device comprises a processing task for an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS).
18. The system of claim 10, wherein the isolated computing environment is implemented using one or more of a sandboxed computing environment or a virtual machine.
19. A method implemented in a host computer system comprising a processor and a memory, the method comprising:
 - implementing a workspace, wherein the workspace is configured to enable operation of a first set of one or more applications or processes via a first memory space;
 - implementing an isolated computing environment, the isolated computing environment being configured to enable operation of a second set of one or more applications or processes via

a second memory space, wherein the isolated computing environment is configured to access an Internet-based cloud service via at least one application of the second set of applications;

isolating the isolated computing environment from the workspace using an internal isolation firewall; and

communicating with at least one proxy server in order to access the Internet-based cloud service, wherein the isolated computing environment is configured to authenticate with an authentication device in order to allow communication between the at least one application and the Internet-based cloud service.

20. The method of claim 19, wherein the Internet-based cloud service comprises one or more of an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS).

NETWORK ISOLATION WITH CLOUD NETWORKS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of U.S. Provisional Application Serial No. 62/563,237, filed September 26, 2017, the contents of which are incorporated by reference herein.

BACKGROUND

[0002] The Internet provides access to a large number of systems from which beneficial and/or harmful data may be retrieved by a host computer system attached to and communicating over the Internet. Harmful data that can be accessed through the Internet includes a variety of viral software constructs, generally referred to as malicious software or malware. Malware may be downloaded to a host computer system unintentionally, for example, by and/or without the knowledge of the user of the host computer system.

[0003] A host computer system that has downloaded malware may be referred to as an infected host computer system. An infected host computer system may result in possible security losses, reduction of efficiency, and/or malfunctions. Security losses may include, but are not limited to, the loss of some or all data that is accessible by the infected host computer system, the installation of additional malware onto the infected host computer system, and/or the loss of command and control of the infected host computer system. Reduction of efficiency may be incurred from, but not limited to, additional processor demand, additional memory usage, and/or additional network access by the executing malware

[0004] The security and privacy of the user of the infected host computer system may be compromised by malware. Both information located on the infected host computer system and/or information stored on or communicated via a local area network may be susceptible to attack by the malware. In many instances, an infected host computer may be used by the malware as a vehicle to stage an attack on other network resources that are accessible from the

infected host computer system. Such an attack method is often undetected by the user of the host computer system and/or network administrators.

[0005] An infected host computer system may lose command and control. The loss of command and control of the infected host computer system may include performing one or more actions the author of the downloaded malware may desire. For example, the malware may perform a reconnaissance of the infected host computer system, determine system privileges, access local files, access security tokens, and/or attempt infection or access of other network resources accessible from the infected computer system

SUMMARY OF THE INVENTION

[0006] Systems and methods are disclosed for a sandbox based network isolation system configured to protect cloud based assets. A host computer system may include a processor and a memory. The host computer system may include a workspace. One or more applications may run in the workspace via a first memory space (e.g., a trusted memory space). The host computer system may include an isolated computing environment. One or more isolated applications may run in the isolated computing environment via a second memory space (e.g., an untrusted memory space). The isolated computing environment may be isolated from the workspace by an internal isolation firewall. The internal isolation firewall may prevent communication between the isolated computing environment and the workspace. The internal isolation firewall may segregate the first memory space from the second memory space using a sandbox. The sandbox may enforce one or more policies for communication between the first memory space and the second memory space. For example, the internal isolation firewall may allow communication between the isolated computing environment and the workspace if the user of the host computer system allows the communication. The host computer system may prompt the user to allow the communication.

[0007] The isolated applications may have access to one or more Internet destinations (e.g., untrusted Internet destinations). The isolated applications may communicate with the Internet destinations via an authentication device (e.g., a proxy server). For example, the authentication device may prevent the isolated applications from communicating with the Internet destinations until after the isolated computing environment has authenticated with the authentication device. There may be more than one (e.g., two) authentication devices, which may include, for example, an Internet-based proxy server and a local network-based proxy server. The host computer

system may determine which authentication device to send web traffic to based on, for instance, the network and/or the application.

[0008] The isolated applications may include an application that accesses an Internet-based cloud service via a network. The network may be, for example, a local area network (LAN), a wide area network (a WAN), a cellular network, a Wi-Fi network, a digital subscribers line (DSL) network, a cloud computing network, a data center, and/or a satellite network. The host computer system may be connected to multiple networks at the same time. For example, the host computer system may be simultaneously connected to a Wi-Fi network and a LAN. The Internet-based cloud service may be, for example, an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), and/or a Platform as a Service (PaaS).

[0009] A cloud computing system may include a cloud computing network and one or more proxies. The cloud computing network may include a server. server may include one or more (e.g., two) sets of applications. For example, one set of applications (e.g., trusted applications) may run in a workspace and one set of applications (e.g., isolated applications) may run in an isolated computing environment. The server may include an internal firewall that isolates the workspace from the isolated computing environment. The internal firewall may allow communication between the workspace and the isolated computing environment if, for example, the communication is in a predetermined format. The isolated computing environment may be implemented using, for example, a sandboxed computing environment and/or a virtual machine. The cloud computing system may include a border firewall that segregates the cloud computing network from one or more internet destinations.

[0010] The server may perform a processing task on behalf of a client device. For example, the server may receive input data from the client device and may send data to the client device. The processing task may include one or more of an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), and/or a Platform as a Service (PaaS).

[0011] The proxies may control communication between the server and one or more Internet resources. For example, the proxies may allow communication between the isolated applications and the Internet resources, and may block communication between the trusted applications and the Internet resources. The proxies may include a first proxy and a second proxy, and the server may determine whether to send traffic to the first proxy or the second proxy based on, for example, user-provided credentials.

[0012] A host computer system may include a processor and a memory that may be configured to implement a first memory space, a second memory space, and/or a first firewall. The first memory space may be configured to enable storage and/or operation of a workspace.

The workspace may be configured to execute a first set of one or more applications and processes running on an operating system of the host computer system;

[0013] The second memory space may be configured to enable storage and/or operation of a second set of one or more applications and processes associated with a sandboxed computing environment. The sandboxed computing environment may be configured to run on the operating system. The second set of one or more applications and processes may be configured to access the Internet and/or other untrusted resources (*e.g.*, an untrusted network destination). The sandboxed computing environment may be enforced via a sandbox container process that may segregate the workspace associated with the first memory space from the sandboxed computing environment associated with the second memory space. The sandbox container process may be configured to prevent data from being communicated between the sandboxed computing environment and the workspace, for example, without an explicit user input. The sandboxed computing environment may be configured to determine whether to send web traffic to a proxy device (*e.g.*, such as a network-based web proxy), a first internet-based web proxy, and/or a second internet-based web proxy.

[0014] The first firewall may be configured to operate between the workspace of the first memory space and a network (*e.g.*, a local area network (LAN), a wide area network (WAN), a cellular network, a Wi-Fi network, a digital subscribers line (DSL) network, a cloud computing network, a data center, an ad-hoc network, a satellite network, a cable modem network, *etc.*). The first firewall may be a host-based firewall. The first firewall may be configured to determine whether the host computer system is connected to a trusted network or an untrusted network. The first firewall may implement a first configuration when the host computer system is connected to the trusted network. The first configuration may be associated with blocking incoming traffic to the host computer system that does not come from one or more predefined devices and/or via one or more predefined ports. The first firewall may implement a second configuration when the host computer system is connected to the untrusted network. In the second configuration, the first firewall may prevent unauthorized communication between the first set of one or more applications and processes and one or more untrusted network destinations.

[0015] The sandboxed computing environment may be configured to determine whether to send web traffic to a network-based web proxy, a first internet-based web proxy, and/or a second internet-based web proxy. For example, the sandboxed computing environment may be configured to send the web traffic to the first internet-based web proxy when the host computer system is connected to a trusted network and the sandboxed computing environment may be

configured to send the web traffic to the second internet-based web proxy when the host computer system is connected to an untrusted network. As another example, the sandboxed computing environment may be configured to send the web traffic to the network-based web proxy when the host computer system is connected to a trusted network and the sandboxed computing environment may be configured to send the web traffic to the first internet-based web proxy when the host computer system is connected to an untrusted network. As another example, the sandboxed computing environment may be configured to send the web traffic to the first internet-based web proxy when the host computer system is connected to a trusted network and when the host computer system is connected to an untrusted network. .

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] FIG. 1 depicts an example host computer system.

[0017] FIG. 2 depicts an example host computer system connected to a local area network (LAN), the example host computer system using a sandbox based network isolation system.

[0018] FIG. 3 depicts an example host computer system connected to a wide area network (WAN), the example host computer system using a sandbox based network isolation system.

[0019] FIG. 4 depicts an example enterprise network.

DETAILED DESCRIPTION

[0020] Systems and methods are disclosed for a sandbox based network isolation system configured to utilize and/or protect cloud based assets. For example, the sandbox based network isolation may protect cloud provided networks. The sandbox based network isolation may protect one or more assets within the cloud provided networks. For example, the one or more assets may include servers, server networks, storage devices, storage networks, enterprise networks, local networks, and/or data centers. The one or more assets may implement the sandbox based network isolation system. The sandbox based network isolation system may isolate a host computing system's communication with one or more untrusted network destinations. The sandbox based network isolation system may protect the host machine from one or more of command and control infection, data exfiltration, or general automated infection that can occur from communicating with the untrusted network destinations. For example, the sandbox based network isolation system may restrict web related traffic between the one or more cloud based assets and untrusted network destinations to a separate, authenticated channel (*e.g.*, between protected and/or trusted devices within the network and an intermediate device). As

another example, the sandbox based network isolation system may restrict traffic (*e.g.*, web related traffic) between devices (*e.g.*, cloud-based devices) using one or more cloud based assets.

[0021] A cloud based asset may securely browse, access, and/or communicate with untrusted network destinations, including but not limited to resources accessible via the Internet. The cloud based asset may be connected to a network (*e.g.*, a local area network (LAN), a wide area network (WAN), a cellular network, a Wi-Fi network, a digital subscribers line (DSL) network, a cloud computing network, a data center, an ad-hoc network, a satellite network, a cable modem network, *etc.*). The cloud-based asset may be a host computer system that is a physical machine, a virtual machine, or a physical machine with a virtual machine operating thereon. The cloud-based asset may include, for example, a server. The isolation may be enforced via the host computer system itself and/or via one or more network entities located within the network.

[0022] A device with a sandbox based network isolation system may travel between, connect to, and/or communicate with more than one network environment. For example, a device with a sandbox based network isolation system may travel between, connect to, and/or communicate with one or more of a LAN, a WAN, a WWAN, a cellular network, a digital subscriber line (DSL) network, a Wi-Fi network, a LPWA network, a satellite network, an infrastructure as a service (IaaS) network, a Software as a Service (SaaS) network), a platform as a service (PaaS) network, and/or the like. The device may be configured to provide network isolation by using a host-based firewall, an internal isolation firewall, and/or a segregation of memory space. The host-based firewall may enable network isolation of the device across different network environments. For example, the host-based firewall may prevent communications from other devices in the different network environments.

[0023] A device may be configured to use one or more proxy devices to access untrusted network destinations. For example, the device may use a first proxy device when connected to a trusted network. The device may use a second proxy device when connected to an untrusted network. The first proxy device may be an intermediate proxy device, for example, such as a network-based web proxy or an internet-based (*e.g.*, cloud-based) web proxy. The second proxy device may be an internet-based web proxy. As another example, the device may use a single internet-based (*e.g.*, cloud-based) web proxy whether connected to a trusted network or an untrusted network.

[0024] Internet isolation, or also known herein as communication isolation, may isolate communications associated with one or more web-based applications (*e.g.*, Internet-based cloud services) from other network communications. For example, the web-based applications may communicate via a first communication channel and the other network communications may use

one or more other communication channels. The first communication channel may be isolated from the one or more other communication channels. The first communication channel may be established with a web proxy. The web-based applications may include web browsers, file transfer applications, email applications, chat or instant messaging applications, peer-to-peer (P2P) file sharing applications, automatic web backup applications (*e.g.*, to cloud services), anti-virus and other security applications, collaboration software applications, remote desktop applications, screen and resource sharing applications, gaming applications, applications that rely on cloud resources for processing resources, and/or the like. Examples of web browsers may include Internet Explorer, Safari, Mozilla, Chrome, *etc.* The file transfer applications may include FileZilla, WinSCP, CyberDuck, FireFTP, *etc.* The collaboration software applications may include WebEx, LiveMeeting, HP Virtual Room, *etc.* As may be appreciated, many of these types of applications rely on robust communication networks that allow the application to connect to and communicate with remote locations. However, such reliance can create avenues of attack for malware and other exploits that can utilize the capacities and resources offered to these applications as a means to attack and or control the host computing system.

[0025] Systems and methods are described to provide a layer of isolation between these diverse types of applications and untrusted network destinations in order to prevent malware from effectively exfiltrating data from the host computer system and/or establishing command and control channels with an attacker resources in order to attempt to gain control of the host computing system. For example, the communication isolation may protect a network from a computer system operating within the network, that runs a collaboration software. The computer system may isolate the collaboration software from other applications and/or processes operating on the computer system.

[0026] Communication isolation may be provided via untrusted memory space segregation. The host computer system may have a sandbox protected application or process and/or an internal isolation firewall running thereon. For example, one or more of the web browsers, file transfer applications, email applications, chat or instant messaging application, P2P file sharing applications, automatic web backup application, anti-virus and other security applications, collaboration software applications, remote desktop applications, screen and resource sharing applications, gaming applications, applications that rely on cloud resources for processing resources, and/or the like may wholly or partially be contained in a sandboxed computing environment. In an example, other isolation methods such as operating the applications within a virtual machine may be used.

[0027] The sandbox protected application or process may operate within a sandboxed computing environment (e.g., an isolated computing environment). The sandboxed computing environment may include resources (e.g., a limited set of resources) allocated for operation of a sandbox container process. The sandboxed computing environment may be enforced via the sandbox container process. The sandbox container process may be a security mechanism used to separate the sandboxed computing environment from other applications and/or processes that may be running on a workspace of the host computer system. The sandboxed container process may be configured to enable one or more applications and/or processes (e.g., such as a browser process) being executed within the sandboxed computing environment to access the resources allocated for operation of the sandbox container process. For example, the one or more applications and/or processes being operated within the sandboxed computing environment may be allowed to access memory associated with the sandboxed computing environment. The memory associated with the sandboxed computing environment may be separate from memory that is configured to enable storage and operation of the workspace.

[0028] The terms “sandboxed computing environment” and “isolated computing environment” may be used interchangeably herein. For example, they may refer to a memory space that is isolated (e.g., by use of an internal isolation firewall) from another memory space (e.g., a workspace). Applications running in the isolated computing environment may be able to interact with one or more Internet resources, for example via one or more proxy servers and/or authentication devices. An isolated computing environment may be implemented using a sandbox container and/or other isolation techniques such as a virtual machine.

[0029] The workspace may include one or more processes operating within the operating system that are not restricted by the sandbox container process. The operating system of the host computer system may include a set of resources configured to enable operation of the workspace and the sandbox container process.

[0030] The sandbox container process may have access to one or more operating system and/or kernel processes in order to enforce isolation between the workspace associated with the first memory space and the sandboxed computing environment associated with the second memory space. The sandbox container process may enforce the segregation using techniques such as namespace isolation such that processes running in the sandboxed computing environment in the second memory space are restricted from accessing the first memory space including the workspace (e.g., and vice versa). The sandbox container process may restrict access to certain resources by processes running in the sandboxed computing environment. The sandboxed container process may allow the workspace and the sandboxed computing

environment to share access to the host operating system and host operating resources (e.g., including the kernel and libraries) while enforcing the segregation of the memory spaces access by the workspace and the sandboxed computing environment. In this manner, the sandbox container process may permit isolation of the sandboxed computing environment without requiring the sandboxed computing environment to boot a separate operating system, load separate libraries, *etc.*, which would require separate private memory for those files.

[0031] The one or more processes or applications operating within the sandboxed computing environment may be permitted to access untrusted network destinations via an intermediate connection device. The intermediate connection device may be a web proxy or a proxy server, for example. The intermediate connection device may include one or more (e.g., two) proxy servers. For example, the intermediate connection device may include a network-based proxy server and an Internet-based proxy server. The one or more processes or applications operating within the sandboxed computing environment may connect to the untrusted network destinations as a dedicated network interface device with using a specific Internet Protocol (IP) address. The one or more processes or applications operating within the sandboxed computing environment may be referred to as sandboxed processes or applications. The host computer system may maintain a list of untrusted network destinations and/or a list of trusted network destinations. The list of trusted network destinations may be a whitelist. The list of untrusted network destinations may be a blacklist. The whitelist and the blacklist may be refined based on username and/or machine identification (ID). For example, the lists of trusted and untrusted network destinations may be different for different users and/or machines associated with a respective network. The whitelist and/or the blacklist may be associated with one or more access levels. For example, a first whitelist and a first blacklist may be assigned to a first access level. An untrusted network destination may be an untrusted resource, an untrusted device, an untrusted website, and/or the like. Since the untrusted network destinations may be sources of malware, the one or more processes or applications operating within the sandboxed computing environment may be allowed to communicate with the untrusted network destination(s), but other communication from the host computer system (*e.g.*, communications originating from outside the sandboxed computing environment such as from within the workspace) to the untrusted network destination(s) may be prevented.

[0032] Communication isolation may be provided via a host-based firewall. The host-based firewall may be configured to prevent unauthorized communication between applications and/or processes operating in the workspace of the host computer system to other devices on the network over which the host computer is communicating. The host-based firewall may be

configured to block incoming communications to the workspace of the host computer system, except for predetermined trusted devices and/or predetermined network ports. The host-based firewall may allow outgoing communications to be sent from a process in the workspace to a non-web-based (*e.g.*, LAN destination) destination and/or a web-based (*e.g.*, LAN destination) destination that are considered trusted.

[0033] Communication isolation may be provided via an internal isolation firewall. The internal isolation firewall may enable separation between the sandboxed computing environment and the workspace. The applications and/or processes operating within the sandboxed computing environment may be prevented from accessing any additional resources of the host computer system or may be prevented from accessing any additional resources of the host computer system without explicit user action. For example, the internal isolation firewall may generate a command prompt that enables a user selection if an application and/or process operating within the sandboxed computing environment is requesting access to resources outside of the sandbox memory space. By prompting the user to confirm that the applications and/or processes operating within the sandboxed computing environment are permitted to access additional resources outside the sandbox memory space, malware that is designed to attempt to remain transparent to the user may be limited to operation within the sandboxed computing environment. Thus, the malware within the sandboxed computing environment may be unable to access other resources available to the host system generally, such as local area networks and secure memory regions.

[0034] The internal isolation firewall may allow certain actions to be performed with approval of the user of the host system. For example, an application and/or process operating within the sandboxed computing environment may be allowed access to the host system to perform one or more of a cut or copy of data, a paste of data, a printing of data to a local printer, a file transfer, and/or the like. The host computer system may prevent one or more other transfers of data between the sandboxed computing environment and the workspace except those user initiated actions described herein. For example, the sandbox container process may prevent unauthorized data transfers between the sandboxed computing environment and the workspace.

[0035] FIG. 1 illustrates an example of a host computer system that may implement one or more applications in a sandboxed environment. For example, a Host Computer System 10 may include one or more Processor(s) 12, Memory 14, one or more Input and/or Output (I/O) Devices 16, and one or more Network Interface Adapter(s) 18. Generally, the Host Computer System 10 may be any computing device capable of communicating over a network and/or performing processing tasks. Although the examples set forth herein may be described in terms general

purpose computing workstations, the systems and methods disclosed herein may be equally applicable to any computing device or communication device for which internet isolation is desired. For example, the systems and methods disclosed herein may be applicable for providing sandbox based internet isolation for cell phones, pagers, personal computers (PCs), laptops, vehicles, kiosks, facilities, servers, workstations, tablets, smartphones, routers, controllers, microcontrollers, and/or any other processing and/or communication device.

[0036] Processor(s) 12 may include one or more of a general purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Array (FPGA) circuits, any other type of integrated circuit (IC), a state machine, and/or the like. The Processor(s) 12 may perform data processing, input/output processing, instantiate operating system(s), execute application(s), and/or any other functionality that enables the use of sandbox isolation of one or more applications and/or processes.

[0037] Memory 14 may include volatile and/or non-volatile memory. Memory 14 may include read-only memory (ROM), random access memory (RAM), a register, cache memory, semiconductor memory devices, magnetic media such as, but not limited to, internal hard disks and removable disks, magneto-optical media, and/or optical media such as CD-ROM disks, and/or digital versatile disks (DVDs), and/or the like. Memory 14 may be configured to store computer readable instructions that when implemented by Processor(s) 12 may cause Processor(s) 12 to implement one or more of the functions or procedures described herein. For example, Memory 14 may be configured to store software code implemented by Processor(s) 12 that instantiate a restricted operating system environment for operation of the sandboxed browser and/or other sandboxed applications(s) and/or process(es). The software may restrict sandbox-based access to one more file descriptors, memory, file system space, etc. For example, the applications and/or processes operating within the sandboxed computing environment may be permitted to certain portions of Memory 14 but may not be allowed access to other portions of Memory 14. As an example, Memory 14 may be partitioned into a first memory space and a second memory space. The first memory space may be configured to enable storage and/or operation of a workspace configured to execute a first set of one or more applications and/or processes running on the operating system of the Host Computer System 10. The second memory space may be configured to enable storage and/or operation of a second set of one or more applications and/or processes running within the sandboxed computing environment. The sandboxed computing environment may be enforced via a sandbox container process. The

sandbox container process may segregate the workspace associated with the first memory space from the sandboxed computing environment associated with the second memory space. For example, the sandbox container process may include an internal isolation firewall. The internal isolation firewall may enforce the segregation of the first and second memory spaces.

[0038] The Host Computer System 10 may include I/O Device(s) 16. The I/O Devices 16 may include one or more of a monitor, keyboard, mouse, touchscreen interface, digital camera, a digital display, a graphical user interface, and/or the like. The I/O Device(s) 16 can allow user interaction with the Host Computer System 10, for example to allow certain interactions between an application or a process operating within the sandboxed computing environment and non-sandboxed resources.

[0039] The Network Interface Adapter(s) 18 may be configured to allow communication between the Host Computer System 10 and other devices. The Network Interface Adapter(s) 18 may include one or more wired and/or wireless communication devices.

[0040] The sandbox container process may be configured to protect the host computer system from one or more malware toolsets. For example, the Network Interface Adapter(s) 18 may include one or more of a modem, Ethernet adapter, radio, wired and/or wireless transceiver, computer port, network socket, network interface controller, and/or the like. The Processor(s) 12 may maintain rules related to access to the Network Interface Adapter(s) 18 for both access via the sandboxed computing environment and via the workspace. Further, the Processor(s) 12 may enforce a host-based firewall that implements additional rules related to access to the Network Interface Adapter(s) 18.

[0041] As described herein, a sandbox protected application or process may be used for communicating with untrusted sources, such as Internet based resources. In this manner, if malware is transferred back to the host computer system due to interactions with the untrusted source, the malware may be isolated to the sandboxed computing environment, which may make it difficult for the malware to infect the workspace of the host computer system. For example, the sandbox container process may prevent the malware toolset from performing a reconnaissance of the host computer system to assess what data is available from the host computer system, such as computing resources, files, network information, additional network connectivity, *etc.* The sandbox container process (*e.g.*, the internal isolation firewall) may prevent the data on the host computer system from being reported back to the remote device that sent the malware to the host computer and/or any other remote devices.

[0042] The sandbox container process may prevent the malware toolset from determining user system privileges of the host computer system, which can be used to access data on any

associated network or local area network. For example, applications and/or processes operating within the sandboxed computing environment may not have access and/or authorization to such host computer configurations.

[0043] The sandbox container process may prevent the malware toolset from accessing local files stored on the host computer system. For example, the sandbox container process may isolate the first memory space from the second memory space. Such isolation can help prevent the malware from attempting to transmit such information back to the remote device that is the source of the malware. For example, the malware toolset may attempt to transmit a local security database from which additional user credentials can be derived, including potential privileged user credentials. These user credentials may be used by the malware to attempt to gain access to other resources on any associated network or the local area network. Where the user credentials are for a privileged user account, these credentials may be used to gain privileged access to other resources on any associated network or local area network.

[0044] The sandbox container process may prevent the malware toolset from accessing a security token and/or hash of the host computer user from the memory of the host computer system and/or a network data stream. This security token or hash can be used to gain access to other resources on any associated network or the local area network. Where the security token or hash is for a privileged user account, this security token or hash may be used to gain privileged access to other resources on any associated network or local area network.

[0045] The sandbox container process may prevent the malware toolset from enabling remote control and/or access of the host computer system by a remote device that is unknown to the user. When malware enables remote control and/or access, the remote device may be able to control one or more (*e.g.*, all) operations of an infected host computer system and perform whatever alternative uses that an enslaved, infected host computer system can perform. For example, a remote device may download additional data to an infected host computer system, access other websites for denial of service attacks, and/or convert the infected host computer system into a source of malicious software from which toolsets or secondary payloads are downloaded to other, subsequently infected, host computer systems.

[0046] FIG. 2 depicts an example host computer system 212 connected to a local area network (LAN) 210, the example host computer system 212 using a sandbox based network isolation system. The LAN 210 may include a plurality of physical and/or virtual devices. The LAN 210 may include a plurality of host computer systems. The host computer system 212 may transmit electrical data signals to one or more other host computer systems on the LAN 210. Each of the host computer systems may be identified by a unique local area network address.

The LAN 210 may include a router, a border firewall 238, and/or a LAN-based web proxy 236. The host computer system 212 may send web traffic (*e.g.*, to one or more trusted URLs) and/or non-web traffic to a trusted network 230 via the operating system 226. The host computer system 212 may send web traffic to one or more untrusted network destinations (*e.g.*, untrusted URLs) using one or more of the border firewall 238, the LAN-based web proxy 236, a first internet-based web proxy 234, and/or another proxy device (*e.g.*, such as second internet-based web proxy 240). For example, the host computer system 212 may access the internet 242 and/or a device on the internet 242 via the trusted network 230, the border firewall 238, the LAN-based web proxy 236, the first internet-based web proxy 234, and/or another proxy device.

[0047] The host computer system 212 may include a host-based firewall 214, an operating system 226, a sandboxed computing environment (*e.g.*, an isolated computing environment) 220, an internal isolation firewall (*e.g.*, an internal firewall) 218, and a workspace 216. The host computer system 212 may be any host computer system, such as a cell phone, a pager, a personal computer (PC), a laptop, a vehicle computer system, a kiosk computer system, a server, a workstation, a tablet, a smartphone, a router, a controller, a microcontroller, and/or any other processing and/or communication device. The host computer system 212 may be a cloud based asset. The host computer system 212 may be operatively connected with one or more user-accessible data entry devices, a display device viewable by a user, and/or a computer-accessible data storage. One or more application programs may run on the operating system 226.

[0048] As an example, the host computer system 212 may be a PC, with 4 GB RAM and 146 GB hard disk computer-accessible storage, a monitor, a keyboard, and a mouse. The operating system 226 may be Windows-based, Linux-Based, Macintosh-based, and/or the like. The computer-accessible storage may store data corresponding to one or more software programs (*e.g.*, computer-readable instructions) stored on the host computer system 212 for common operation. The software programs may include word processing programs, accounting programs, remote connectivity programs, and/or other types of applications.

[0049] The host computer system 212 may be configured to isolate communication with untrusted network destinations. The host computer system 212 may isolate communication with untrusted network destinations using one or more of the host-based firewall 214, a border firewall 238, a LAN-based web proxy 236, the first internet-based web proxy 234, the second internet-based web proxy 240, an internal isolation firewall 218, or a segregation of untrusted memory space.

[0050] The host-based firewall 214 may enable isolation of the host computer system's communication with one or more untrusted network destinations by preventing lateral

communication with other devices connected to a trusted network 230. For example, the host computer system 212 may receive untrusted traffic from the trusted network 230. The host-based firewall 214 may be configured to block the untrusted traffic from the trusted network 230. The host-based firewall 214 may be configured to block all incoming traffic from the trusted network 230. The host-based firewall 214 may be configured to allow traffic received by the host computer system 212 via one or more predetermined devices and/or ports. One or more devices (*e.g.*, predetermined devices) connected to the trusted network 230 may bypass the host-based firewall 214, for example, using a predetermined set of protocols and/or ports.

[0051] The host-based firewall 214 may be implemented using software and/or hardware. For example, the host-based firewall 214 may be implemented using software that is commercially available, for example, such as Symantec Endpoint Protection, MacAfee Host Based Security Systems, *etc.* The host-based firewall 214 may be implemented using software inherent in the operating system 226 of the host computer system 212, for example the Windows operating system firewall. The host-based firewall 214 may be implemented using software for configuring and/or implementing restrictive ingress and/or egress policies on the host computer system 212.

[0052] The trusted network 230 may be a virtual-based network, a hardware-based network, a cloud based network, or a combination thereof. The trusted network 230 may be configured as a cloud provided network, a server network, a data center network, a storage network, an enterprise network, a local network, an office network, or a combination thereof. The trusted network 230 may manage a plurality of assets, that may include one or more of virtual-based assets, hardware-based assets, or cloud-based assets.

[0053] The sandboxed computing environment 220 may include resources (*e.g.*, a limited set of resources) allocated to operation of a sandbox container process. The sandboxed computing environment 220 may be enforced via the sandbox container process. The sandbox container process may be a security mechanism used to separate resources associated with the sandboxed computing environment 220 from other applications and/or processes that may be running on a workspace 216 of the host computer system 212. The sandboxed container process may be configured to enable one or more applications and/or processes (*e.g.*, such as a browser process) being executed within the sandboxed computing environment 220 to access the resources allocated for operation of the sandbox container process. For example, the one or more applications and/or processes being operated within the sandboxed computing environment 220 may be allowed to access memory associated with the sandboxed computing environment 220.

The memory associated with the sandboxed computing environment 220 may be separate from memory that is configured to enable storage and operation of the workspace.216.

[0054] The workspace 216 may include one or more processes operating within the operating system 226 that are not restricted by the sandbox container process. The operating system 226 of the host computer system 212 may include a set of resources configured to enable operation of the workspace 216 and the sandbox container process.

[0055] The LAN-based web proxy 236 may enable isolation of the host computer system 212 from one or more untrusted network destinations. The LAN-based web proxy 236 may be configured to allow one or more processes and/or applications (*e.g.*, such as a browser process, an email process, *etc.*) operating within the sandboxed computing environment 220 of the host computer system 212 to access an untrusted network destination. A sandbox container process may enable the sandboxed computing environment 220. The sandbox container process may authenticate with the LAN-based web proxy 236 on behalf of the one or more processes and/or applications operating within the sandboxed computing environment. The sandbox container process may be configured to authenticate with the LAN-based web proxy 236 using preconfigured credentials stored, for example, within an encrypted configuration file. When the sandbox container process has successfully authenticated with the LAN-based web proxy 236, the LAN-based web proxy 236 may allow the one or more processes and/or applications operating within the sandboxed computing environment 220 to access the untrusted network destination.

[0056] The internet-based web proxies 234, 240 may enable isolation of the host computer system 212 from one or more untrusted network destinations. The internet-based web proxies 234, 240 may be configured to allow one or more processes and/or applications (*e.g.*, such as a browser process, an email process, *etc.*) operating within the sandboxed computing environment 220 of the host computer system 212 to access an untrusted network destination. A sandbox container process may enable the sandboxed computing environment 220.

[0057] The host computer system 212 may be pre-configured to use one or more of the internet-based web proxies 234, 240. For example, the host computer system 212 may be pre-configured with a configuration file associated with one or more of the internet-based web proxies 234, 240. The host computer system 212 may search for the internet-based web proxies 234, 240. For example, the host computer system 212 may perform a domain name server (DNS) search to find the internet-based web proxy 234. The LAN 200 may provide a load balanced solution to establish connection with the internet based web proxies 234, 240. The sandbox container process may authenticate with one or more of the internet-based web proxies

234, 240 on behalf of the one or more processes and/or applications operating within the sandboxed computing environment 220. The sandbox container process may be configured to authenticate with one or more of the internet-based web proxies 234, 240 using preconfigured credentials stored, for example within an encrypted configuration file. When the sandbox container process has successfully authenticated with one or more of the internet-based web proxy 234, 240, the internet-based web proxies 234, 240 may allow the one or more processes and/or applications operating within the sandboxed computing environment 220 to access the untrusted network destination.

[0058] To which web proxy the sandboxed computing environment 220 sends web traffic may depend on whether the host computer system 212 is connected to a trusted network or an untrusted network. When the host computer system 212 is connected to a trusted network (*e.g.*, such as LAN 210), the sandboxed computing environment 220 may send web traffic to the first internet-based web proxy 234 and/or the LAN-based web proxy 236. When the host computer system 212 is connected to an untrusted network, the sandboxed computing environment 220 may send web traffic to the first internet-based web proxy 234 and/or the second internet-based web proxy 240. As an example, the sandboxed computing environment 220 may be configured to use the same internet-based web proxy (*e.g.*, such as internet-based web proxy 234) when the host computer system 212 is connected to a trusted network or an untrusted network. As another example, the sandboxed computing environment 220 may be configured to use the first internet-based web proxy 234 when the host computer system 212 is connected to a trusted network (*e.g.*, such as LAN 210) and may be configured to use the second internet-based web proxy 240 when the host computer system 212 is connected to an untrusted network. As another example, the sandboxed computing environment 220 may be configured to use the first internet-based web proxy 234 and/or the LAN-based web proxy 236 when the host computer system 212 is connected to a trusted network (*e.g.*, such as LAN 210) and may be configured to use the second internet-based web proxy 240 when the host computer system 212 is connected to an untrusted network.

[0059] The internet-based web proxy 234 may enable isolation of host computer system 244 from one or more untrusted network destinations. For example, host computer systems (*e.g.*, such as host computer system 244) that are connected to untrusted networks may send web related (*e.g.*, untrusted) traffic to the internet-based web proxy 234. For example, the host computer system 244 may be configured to enable a sandboxed computing environment (*e.g.*, such as the sandboxed computing environment 220) via a sandbox container process. The internet-based web proxy 234 may be configured to allow one or more processes and/or

applications (*e.g.*, such as a browser process, an email process, *etc.*) operating within the sandboxed computing environment of the host computer system 244 to access an untrusted network destination.

[0060] The LAN 210 may be accessed (*e.g.*, remotely accessed) by a host computer system 244 (*e.g.*, such as host computer system 212). The host computer system 244 may access the LAN 210 via a VPN connection. The VPN connection may enable the connectivity and features associated with a direct connection to the LAN 210. The host computer system 244 may be configured to locally connect to the LAN 210. When the host computer system 244 is remotely connected to the LAN 210, the sandboxed computing environment may be configured to send web traffic to a first internet-based web proxy 234 and/or a second internet-based web proxy 240. For example, when the host computer system 244 is connected to an untrusted network, the sandboxed computing environment may send the web traffic to the first internet-based web proxy 234 and/or the second internet-based web proxy 240. As an example, the sandboxed computing environment may be configured to use the same internet-based web proxy (*e.g.*, such as internet-based web proxy 234) when the host computer system 244 is connected to a trusted network or an untrusted network. As another example, the sandboxed computing environment may be configured to use the first internet-based web proxy 234 when the host computer system 244 is connected to a trusted network (*e.g.*, such as LAN 210) and may be configured to use the second internet-based web proxy 240 when the host computer system 244 is connected to an untrusted network. As another example, the sandboxed computing environment may be configured to use the first internet-based web proxy 234 and/or a network-based web proxy (*e.g.*, such as the LAN-based web proxy 236) when the host computer system 244 is connected to a trusted network (*e.g.*, such as LAN 210) and may be configured to use the second internet-based web proxy 240 when the host computer system 244 is connected to an untrusted network. As another example, the sandbox computing environment may be configured to use the network-based web proxy when the host computer system 244 is connected to an untrusted network with an encrypted connection channel (*e.g.*, a VPN connection) to a trusted network (*e.g.*, LAN 210) and may be configured to use one or more of the internet-based web proxies 234, 240 when connected to an untrusted network without an encrypted connection channel to a trusted network (*e.g.*, LAN 210).

[0061] The LAN 210 may be accessed (*e.g.*, remotely accessed) by the host computer system 244. The host computer system 244 may access the LAN 210 via a VPN connection. The VPN connection may enable the connectivity and features associated with a direct connection to the LAN 210.

[0062] The host computer system 244 may be pre-configured to use the internet-based web proxy 234. For example, the host computer system 244 may be pre-configured with a configuration file associated with the internet-based web proxy 234. The host computer system 244 may search for the internet-based web proxy 234. For example, the host computer system 244 may perform a domain name server (DNS) search to find the internet-based web proxy 234. The host computer system 244 may perform a local host lookup, reference a configuration file, *etc.* to determine information needed to find the internet-based web proxy 234. The sandbox container process operating within the host computer system 244 may authenticate with the internet-based web proxy 234 on behalf of the one or more processes and/or applications operating within the sandboxed computing environment. The sandbox container process may be configured to authenticate with the internet-based web proxy 234 using preconfigured credentials stored, for example, within an encrypted configuration file. When the sandbox container process has successfully authenticated with the internet-based web proxy 234, the internet-based web proxy 234 may allow the one or more processes and/or applications operating within the sandboxed computing environment to access the untrusted network destination.

[0063] The proxy devices (*e.g.*, such as internet-based web proxy 234, LAN-based web proxy 236, and/or internet-based web proxy 240) may be configured to enforce a blacklist for host computer systems connected to untrusted networks. For example, the host computer systems on untrusted networks may send web related traffic to the internet-based web proxy 234, for example, via the internet 242. The internet-based web proxy 234 may allow or prevent the web related traffic based on the network destination. If the network destination is on the blacklist, the internet-based web proxy 234 may block the web related traffic. As described herein, the blacklist may be tailored based on one or more of the network to which the host computer system is connected, a host computer system ID, the user, the access level associated with the user, *etc.*

[0064] The border firewall 238 may enable isolation of the host computer system 212 (*e.g.*, the workspace 216) from one or more untrusted network destinations (*e.g.*, Internet destinations). The border firewall 238 may be configured to restrict traffic to the untrusted network destinations (*e.g.*, the Internet 242) from the LAN-based web proxy 236 and/or the trusted network 230. The host computer systems 212 may access a whitelisted web server and/or an untrusted web server via a web proxy device, for example, via the border firewall 238. The border firewall 238 may be configured to block communication between the host computer system 212 and one or more untrusted network destinations, for example, the Internet 242. For example, the border firewall 238 may be configured to block untrusted traffic that is not routed

through the LAN-based web proxy 236. The border firewall 238 may be configured to block untrusted traffic that is not received from one or more predetermined devices. The border firewall 238 may be configured to block untrusted traffic that is not received via one or more predetermined network ports.

[0065] The host computer system 212 may enable the host-based firewall 214. The host-based firewall 214 may prohibit and/or prevent communication (*e.g.*, direct communication) between the host computer system 212 and other devices on the network 230. Each device on the trusted network 230 may include a host-based firewall (*e.g.*, such as the host-based firewall 214). The host-based firewall 214 may prohibit and/or prevent communication (*e.g.*, direct communication) between the host computer system 212 and other devices within the trusted network 230. For example, the host-based firewall 214 may be configured to block incoming traffic from the other devices within the trusted network 230. The host-based firewall 214 may allow traffic received by the host computer system 212 via one or more predetermined devices and/or ports. For example, one or more devices (*e.g.*, predetermined devices) on the trusted network 230 may bypass the host-based firewall 214, for example, using a predetermined set of protocols and/or ports.

[0066] The host-based firewall 214 may be implemented using software and/or hardware. For example, the host-based firewall 214 may be implemented using software that is commercially available, for example, such as Symantec Endpoint Protection, MacAfee Host Based Security Systems, *etc.* The host-based firewall 214 may be implemented using software inherent in the operating system 226 of the host computer system 212, for example the Windows operating system firewall. The host-based firewall 214 may be implemented using software for configuring and/or implementing restrictive ingress and/or egress policies on the host computer system 212.

[0067] The host computer system 212 may run the sandboxed computing environment 220. The sandboxed computing environment 220 may run within the operating system 226 of the host computer system 212. For example, the sandboxed computing environment 220 may be configured to run within a second memory space of the host computer system 212. A first memory space may be configured to enable storage and operation of a workspace configured to execute a first set of one or more applications and/or processes running on the operating system 226 of the host computer system 212. For example, a browser process may operate within the sandboxed computing environment 220. The sandboxed computing environment 220 may be prohibited from communicating with other devices within the network 230. The browser process

operating within the sandboxed computing environment 220 may be configured to enable access to untrusted network destinations.

[0068] Browser solutions running within the workspace 216 of the host computer system 212 may be utilized for communication between the host computer system 212 and trusted network destinations. For example, the one or more applications or processes running within the workspace 216 of the host computer system 212 may access the trusted network destinations.

[0069] The sandboxed computing environment 220 and/or the sandbox container process may be implemented using software and/or hardware. For example, the sandboxed computing environment 220 and/or the sandbox container process may be implemented using software that is commercially available, for example, such as Invincea Endpoint Protection, Tanium Endpoint Platform, Bromium Advanced Endpoint Security, *etc.*

[0070] The sandboxed computing environment 220 may provide separate and/or isolated memory space from the workspace 216 of the host computer system 212. For example, the sandboxed computing environment 220 may be enforced using a sandbox container process. The sandbox container process may segregate the workspace 216 from the sandboxed computing environment 220. The first memory space (*e.g.*, the workspace memory) may enable storage and/or operation of the workspace 216. The operating system 226 may enable operation of the sandboxed computing environment 220. The second memory space may enable storage and/or operation of one or more applications and/or processes associated with the sandboxed computing environment 220. For example, the second memory space may be reserved for storage and/or operation of the applications and/or processes running within the sandboxed computing environment 220.

[0071] The sandbox container process may isolate the first memory space and the second memory space. For example, the sandbox container process may enable the internal isolation firewall 218. The internal isolation firewall 218 may enforce a separation of the first and second memory spaces. For example, the internal isolation firewall 218 may allow a predefined set of processes to be executed within the sandboxed computing environment 220. The internal isolation firewall 218 may prevent execution, in the sandboxed computing environment 220, of any processes outside of the predefined set of processes. The second memory space may be referred to as a separate and/or isolated memory space. The sandbox container process may segregate the second memory space, any additional processes and/or memory usage required for usage of untrusted network destination related content during an established communication session. Separation and/or isolation of computer resources may be referred to as a virtual air gapped solution. The first memory space and the second memory space may be separate

physical memory locations. The first memory space and the second memory space may be collocated on a physical memory.

[0072] The host computer system 212 may be configured to connect to the trusted network 230 or an untrusted network. When the host computer system 212 is connected to the trusted network 230, the host-based firewall 214 may implement a first configuration. When the host computer system 212 is connected to the untrusted network, the host-based firewall 214 may implement a second configuration. The first configuration may be associated with blocking incoming traffic to the host computer system 212 that does not come from one or more predefined devices and/or via one or more predefined ports. In the first configuration, the host-based firewall 214 may allow outgoing traffic to be sent from one or more processes or applications in the workspace 216, for example irrespective of the type of communication protocol used. In an example, the second configuration may be associated with preventing one or more applications and/or processes operating on the workspace 216 of the host computer system 212 from communicating with one or more untrusted destinations. In an example, the second configuration may be associated with blocking all incoming traffic from the untrusted network to the host computer system 212.

[0073] When the host-based firewall 214 is configured in the second configuration, the host-based firewall 214 may allow one or more of the applications and/or process operating within the workspace 216 to communicate with a trusted network destination on condition that a predetermined set of communication protocols. The predetermined set of protocols may include communicating with the trusted network destination via a VPN client associated with the workspace 216. The trusted network destination may be located on the trusted network 230. The VPN client may be configured to establish an encrypted communication system with the trusted network destination via the untrusted network. For example, the second configuration of the host-based firewall 214 may enable one or more applications and/or processes operating within the workspace 216 to access the trusted network 230 via the untrusted network and/or the Internet 242 using the VPN client.

[0074] In this manner, the host-based firewall 214 can allow the processes or applications of the workspace 216 to send outgoing communications without restriction when implementing the first configuration (*e.g.*, when connected to the trusted LAN), but may limit outgoing communications from the processes or applications of the workspace 216 to communications to trusted destinations that also utilize a predetermined protocol in order to communicate with the trusted destination. In both the first and second configurations, the host-based firewall 214 may

block incoming communications to the workspace 216 unless the communication is from a trusted destination and uses a predetermined communication protocol.

[0075] If malware in a sandboxed computing environment 220 is able to access the resources, assets, and/or files of the operating system 226, the host computer system 212 may be considered infected and untrusted. For example, the malware may bypass the internal isolation firewall 218 via explicit user input. The host-based firewall 214 may prohibit the introduced malware from communicating with any other device on the trusted network 230. For example, the host-based firewall 214 may be configured to block incoming traffic from the trusted network 230.

[0076] Malware may be introduced to the operating system 226 from a source other than communication with the Internet 242. For example, malware may be introduced to the operating system 226 via an infected email, an infected USB memory stick, and/or another infected hardware device.

[0077] An infected and/or untrusted host computer system (*e.g.*, regardless of the introduced malware's vector) may have no communication (*e.g.*, direct communication) with the Internet 242. For example, the border firewall 238, the internal isolation firewall 218, and/or a proxy device (*e.g.*, such as LAN-based web proxy 236, internet-based web proxy 234, internet-based web proxy 240, *etc.*) may prevent the infected and/or untrusted host computer system from communicating with the Internet 242. Without a connection to (*e.g.*, communication with) the Internet 242, the introduced malware may be prevented from performing many toolset functions described herein or any other function that an enslaved, infected and/or untrusted host computer system may perform. Without a connection to the Internet 242, the introduced malware may not be able to transfer any data from the infected and/or untrusted host computer system to the Internet 242.

[0078] The host computer system 212 and/or the trusted network 230 may limit the adverse effects associated with a received malware. For example, the host computer system 212 and/or the trusted network 230 may prevent the received malware from using its vector to communicate data from the host computer system 212.

[0079] An author of the malware may not be aware of any level of efficacy of the introduced malware and/or its successful attack vector. The host computer system 212 and/or the trusted network 230 may prevent data of an infected and/or untrusted host computer system that may have been compromised and/or collected by the malware from being communicated to the author of the malware. For example, the host computer system 212 may prevent communication

between an infected and/or untrusted host computer system and the Internet 242 (*e.g.*, the author of the malware via the Internet 242).

[0080] FIG. 3 depicts an example host computer system 312 (*e.g.*, such as the host computer system 212 shown in FIG. 2) connected to a wide area network (WAN) 300, the example host computer system 312 using a sandbox based network isolation system. The WAN 310 may include one or more trusted LANs 310A, 310B. The trusted LANs 310A, 310B may access a trusted WAN 340. The trusted WAN 340 may operate within the WAN 300. Trusted LAN 310A and trusted LAN 310B may be connected to each other, for example, via an inter-site connection. Trusted LAN 310A and trusted LAN 310B may include a plurality of physical and/or virtual devices. For example, trusted LAN 310A may include a host computer system 312. The host computer systems may transmit electrical data signals to one or more other host computer systems on the trusted LAN 310A.

[0081] The host computer system 312 may include a host-based firewall 314, an operating system 326, a sandboxed computing environment 320, an internal isolation firewall 318, and a workspace 316. The host computer system 312 may be any host computer system, such as a cell phone, a pager, a personal computer (PC), a laptop, a vehicle computer system, a kiosk computer system, a server, a workstation, a tablet, a smartphone, a router, a controller, a microcontroller, and/or any other processing and/or communication device. The host computer system 312 may be a cloud-based asset. The host computer system 312 may be a physical machine, a virtual machine, or a physical machine with a virtual machine operating thereon. The host computer system 312 may be operatively connected with one or more user-accessible data entry devices, a display device viewable by a user, and/or a computer-accessible data storage. One or more application programs may run on the operating system 326.

[0082] As an example, the host computer system 312 may be a PC, with 4 GB RAM and 146 GB hard disk computer-accessible storage, a monitor, a keyboard, and a mouse. The operating system 326 may be Windows-based, Linux-Based, Macintosh-based, and/or the like. The computer-accessible storage may store data corresponding to one or more software programs (*e.g.*, computer-readable instructions) stored on the host computer system 312 for common operation. The software programs may include word processing programs, accounting programs, remote connectivity programs, and/or other types of applications.

[0083] The host computer system 312 may be configured to isolate communication with untrusted network destinations. The host computer system 312 may isolate communication with untrusted network destinations using one or more of the host-based firewall 314, a LAN border firewall 334, a LAN-based web proxy 336, a first internet-based web proxy 346, a second

internet-based web proxy 352, the internal isolation firewall 318, or a segregation of untrusted memory space.

[0084] The host-based firewall 314 may enable isolation of the host computer system's communication with one or more untrusted network destinations by preventing lateral communication with other devices connected to a trusted network 332. For example, the host computer system 312 may receive untrusted traffic from the trusted network 332. The host-based firewall 314 may be configured to block the untrusted traffic from the trusted network 332. The host-based firewall 314 may be configured to block all incoming traffic from the trusted network 332. The host-based firewall 314 may be configured to allow traffic received by the host computer system 312 via one or more predetermined devices and/or ports. One or more devices (*e.g.*, predetermined devices) connected to the trusted network 330 may bypass the host-based firewall 314, for example, using a predetermined set of protocols and/or ports.

[0085] The trusted LAN 310A may be a virtual-based network, a hardware-based network, a cloud based network, or a combination thereof. The trusted LAN 310A may be configured as a cloud provided network, a server network, a data center network, a storage network, an enterprise network, a local network, an office network, or a combination thereof. The trusted LAN 310A may manage a plurality of cloud-based assets. Each of the cloud-based assets may be a host computer system that may be a physical machine, a virtual machine, or a physical machine with a virtual machine operating thereon. The trusted LAN 310A may communicate with the trusted WAN 340 (*e.g.*, one or more devices on the trusted WAN 340). For example, one or more devices (*e.g.* such as the host computer system 312) may send trusted and/or untrusted traffic to the trusted WAN 340. A WAN border firewall 344 may be configured to restrict traffic to one or more untrusted network destinations (*e.g.*, the Internet 348) from a WAN-based web proxy 342 and/or the trusted WAN 340. The trusted WAN 340 may access a whitelisted web server and/or an untrusted web server via a web proxy device, for example, via the WAN border firewall 344. The WAN border firewall 344 may be configured to block communication between the trusted WAN 340 and the one or more untrusted network destinations, for example the Internet 348. For example, the WAN border firewall 344 may be configured to block untrusted traffic that is not routed through the WAN-based web proxy 342, LAN based proxies, such for example 336, and/or predetermined devices. The WAN border firewall 344 may allow untrusted traffic that has been routed through the WAN-based web proxy 342, LAN based proxies, such for example 336, and/or predetermined devices to access the one or more untrusted network destinations.

[0086] Each host computer system on the trusted LAN 310A may be identified by a unique local area network address. The trusted LAN 310A may include a router and/or a trusted network 332 (*e.g.*, such as trusted network 230 shown in FIG. 2). The host computer system 312 may send web traffic and/or non-web traffic to the trusted network 332, for example, via the router. The trusted LAN 310A may send web traffic to one or more untrusted network destinations using one or more of the trusted network 332, a LAN border firewall 334, a LAN-based web proxy 336 (*e.g.*, such as LAN-based web proxy 236 shown in FIG. 2), the trusted WAN 340, the WAN border firewall 344, the WAN-based web proxy 342, or an internet-based web proxy 346 (*e.g.*, such as the internet-based web proxy 234 shown in FIG. 2). For example, the trusted LAN 310A may access the internet 348 and/or a device on the internet 348 via the trusted WAN 340, the WAN border firewall 344, and/or the WAN-based web proxy 342.

[0087] The web traffic sent by the host computer system 312 to the trusted network 332 may be destined for trusted destinations. The trusted LAN 310A may enable a connection to a cloud-based computing system. The connection to the cloud-based computing system may be a direct connection and/or a connection through WAN 300. For example, the trusted LAN 310A may enable a connection to a cloud-based computing system using one or more of the trusted network 332, the LAN border firewall 334, the LAN-based web proxy 336, the trusted WAN 340, the WAN border firewall 344, the WAN-based web proxy 342, or the internet-based web proxy 346. The trusted LAN 310A may be part of a cloud interexchange. The trusted LAN 310A may be part of a cloud “meet me” point of presence.

[0088] The host computer system 312 may determine whether to send web traffic intended for an untrusted network destination to a LAN-based web proxy 336 or to the trusted WAN 340. The trusted WAN 340 may forward the web traffic received from the host computer system 312 to the WAN-based web proxy 342 or the internet-based web proxy 346. The trusted WAN 340 may determine which web proxy to forward the web traffic based on a configuration associated with the host computer system 312 and/or the trusted LAN 310A. The trusted WAN 340 may determine which web proxy to forward the web traffic based on the untrusted network destination.

[0089] The trusted WAN 340 may be pre-configured to use the internet-based web proxy 346. For example, the trusted WAN 340 may be pre-configured with a configuration file associated with the internet-based web proxy 346. The trusted WAN 340 may search for the internet-based web proxy 346. For example, the trusted WAN 340 may perform a domain name server (DNS) search to find the internet-based web proxy 346. The trusted WAN 340 may provide a load balanced solution to establish connection with the internet-based web proxy 346.

[0090] A device (*e.g.*, such as the host computer system 312) on the trusted WAN 340 may determine which web proxy to send web traffic. For example, the device may include a sandboxed computing environment (*e.g.*, such as the sandboxed computing environment 220). When the device is connected to a trusted network (*e.g.*, such as trusted WAN 340), the sandboxed computing environment may send the web traffic to the first internet-based web proxy 346 and/or the WAN-based web proxy 342. When the device is connected to an untrusted network, the sandboxed computing environment may send the web traffic to the first internet-based web proxy 346 and/or the second internet-based web proxy 352. As an example, the sandboxed computing environment may be configured to use the same internet-based web proxy (*e.g.*, such as internet-based web proxy 346) when the device is connected to a trusted network or an untrusted network. As another example, the sandboxed computing environment may be configured to use the first internet-based web proxy 346 when the device is connected to a trusted network (*e.g.*, such as trusted WAN 340) and may be configured to use the second internet-based web proxy 352 when the device is connected to an untrusted network. As another example, the sandboxed computing environment may be configured to use the first internet-based web proxy 346 and/or the WAN-based web proxy 342 when the device is connected to a trusted network (*e.g.*, such as trusted WAN 340) and may be configured to use the second internet-based web proxy 352 when the device is connected to an untrusted network.

[0091] As another example, the sandbox computing environment may be configured to use the WAN-based web proxy 342 when the host computer system 350 is connected to an untrusted network with an encrypted connection channel (*e.g.*, a VPN connection) to a trusted network (*e.g.*, WAN 300) and may be configured to use one or more of the internet-based web proxies 346, 352 when connected to an untrusted network without an encrypted connection channel to a trusted network (*e.g.*, WAN 300).

[0092] The WAN 300, the trusted WAN 340, the trusted LAN 310A, and/or the trusted LAN 310B may be accessed (*e.g.*, remotely accessed) by a host computer system 350 (*e.g.*, such as host computer system 212 shown in FIG.2 and/or host computer system 312 shown in FIG. 3). The host computer system 350 may access one or more of the WAN 300, the trusted WAN 340, the trusted LAN 310A, and/or the trusted LAN 310B via a VPN connection. The VPN connection may enable the connectivity and features associated with a direct connection to the WAN 300, the trusted WAN 340, the trusted LAN 310A, and/or the trusted LAN 310B. The host computer system 350 may be configured to locally connect to one or more of the trusted LANs 310A, 310B. When the host computer system 350 is remotely connected to one or more of the WAN 300, the trusted WAN 340, the trusted LAN 310A, and/or the trusted LAN 310B,

the sandboxed computing environment may be configured to send web traffic to a first internet-based web proxy 346 and/or a second internet-based web proxy 352. For example, when the host computer system 350 is connected to an untrusted network, the sandboxed computing environment may send the web traffic to the first internet-based web proxy 346 and/or the second internet-based web proxy 352. As an example, the sandboxed computing environment may be configured to use the same internet-based web proxy (*e.g.*, such as internet-based web proxy 346) when the host computer system 350 is connected to a trusted network or an untrusted network. As another example, the sandboxed computing environment may be configured to use the first internet-based web proxy 346 when the host computer system 350 is connected to a trusted network (*e.g.*, such as trusted LAN 310A or trusted LAN 310B) and may be configured to use the second internet-based web proxy 352 when the host computer system 350 is connected to an untrusted network. As another example, the sandboxed computing environment may be configured to use the first internet-based web proxy 346 and/or a network-based web proxy when the host computer system 350 is connected to a trusted network (*e.g.*, such as trusted LAN 310A or trusted LAN 310B) and may be configured to use the second internet-based web proxy 352 when the host computer system 350 is connected to an untrusted network.

[0093] The trusted WAN 340 may support a plurality of trusted LANs (*e.g.*, such as trusted LAN 310A and trusted LAN 310B). The WAN-based web proxy 342 may be configured to enable access to one or more untrusted network destinations. The WAN-based web proxy 342 may enforce a blacklist associated with the trusted WAN 340, one or more of the trusted LANs, and/or one or more host computer systems.

[0094] FIG. 4 depicts an example enterprise network configuration. For example, one or more trusted networks (*e.g.*, trusted networks 410A, 410B) may be configured to access the Internet 420 (*e.g.*, a trusted or untrusted network destination). Each of the trusted networks 410A, 410B may be a trusted LAN (*e.g.*, such as trusted LAN 310A shown in FIG. 3) or a trusted WAN (*e.g.*, such as trusted WAN 340 shown in FIG. 3). The trusted networks 410A, 410B may be connected, for example, via an inter-site connection. Network traffic may be sent between the trusted networks 410A, 410B. For example, a device on the trusted network 410A may communicate with a device on the trusted network 410B.

[0095] Each of the trusted networks 410A, 410B may include a plurality of host computer systems (*e.g.*, such as host computer system 212 shown in FIG. 2 and/or host computer system 312 shown in FIG. 3). Each host computer system of a respective trusted network may be configured to send electrical data signals to one or more other host computer systems on the respective trusted network. For example, the host computer systems of the LAN 410A may send

data to each other. Each of the host computer systems may be identified by a unique local area network address. The trusted networks 410A, 410B (*e.g.*, each host computer system in the trusted networks 410A, 410B) may send web traffic and/or non-web traffic to another trusted network (not shown) and/or to the Internet 420. The web traffic sent to the other trusted network and/or the Internet 420 may be destined for trusted destinations.

[0096] One or more of the trusted networks 410A, 410B may be accessed (*e.g.*, remotely accessed) by a host computer system 426 (*e.g.*, such as host computer system 212 shown in FIG.2 and/or host computer system 312 shown in FIG. 3). The host computer system 426 may access one or more of the trusted networks 410A, 410B via a VPN connection. The VPN connection may enable the connectivity and features associated with a direct connection to the trusted networks 410A, 410B. The host computer system 426 may be configured to locally connect to one or more of the trusted networks 410A, 410B. When the host computer system 426 is remotely connected to one or more of the trusted networks 410A, 410B, the sandboxed computing environment may be configured to send web traffic to a first internet-based web proxy 422 and/or a second internet-based web proxy 424. For example, when the host computer system 426 is connected to an untrusted network, the sandboxed computing environment may send the web traffic to the first internet-based web proxy 422 and/or the second internet-based web proxy 424. As an example, the sandboxed computing environment may be configured to use the same internet-based web proxy (*e.g.*, such as internet-based web proxy 422) when the host computer system 426 is connected to a trusted network or an untrusted network. As another example, the sandboxed computing environment may be configured to use the first internet-based web proxy 422 when the host computer system 426 is connected to a trusted network (*e.g.*, such as trusted network 410A or trusted network 410B) and may be configured to use the second internet-based web proxy 424 when the host computer system 426 is connected to an untrusted network. As another example, the sandboxed computing environment may be configured to use the first internet-based web proxy 422 and/or a network-based web proxy when the host computer system 426 is connected to a trusted network (*e.g.*, such as trusted network 410A or trusted network 410B) and may be configured to use the second internet-based web proxy 424 when the host computer system 426 is connected to an untrusted network.

[0097] A sandbox based network isolation system may be used to prevent malware from establishing command and control on a computer system (*e.g.*, a desktop computer, a laptop computer, a tablet, a mobile phone, *etc.*). For example, the sandbox based network isolation system may be configured to operate on a computer system running Windows, Linux, MacOS, iOS, Android, Windows Mobile, and/or some other operating system.

[0098] A sandbox based network isolation system may prevent malware from moving from a first computer system to a second computer system on the same network environment. For example, when a computer system in a network environment is infected with malware, the sandbox based network isolation system may prevent proliferation of the malware within the network environment.

[0099] A sandbox based network isolation system may increase the security posture of an enterprise network (*e.g.*, a WAN, a LAN, and/or a VM infrastructure). For example, the sandbox based network isolation system may protect the enterprise network from malware, command and control attacks, viruses, and/or data exfiltration attacks.

[0100] The terms used herein should be seen to be terms of description rather than of limitation. It is understood that those of skill in the art with this disclosure may devise alternatives, modifications, or variations of the principles of the invention. It is intended that all such alternatives, modifications, or variations be considered as within the spirit and scope of this invention, as defined by the following claims.

[0101] Embodiments may take the form of a tangible computer-usable or computer-readable medium providing program code for use by or in connection with a computer or any instruction execution system. Examples of a computer-usable or computer-readable medium include tangible computer media such as semiconductor or solid state memory, magnetic tape, a removable computer diskette, a random access memory (RAM), a read-only memory (ROM), a rigid magnetic disk and an optical disk. Current examples of optical disks include compact disk-read only memory (CD-ROM), compact disk-read/write (CD-R/W) and DVD. A processor may be configured to execute instructions stored in memory to perform the various functions and/or functional modules described herein.

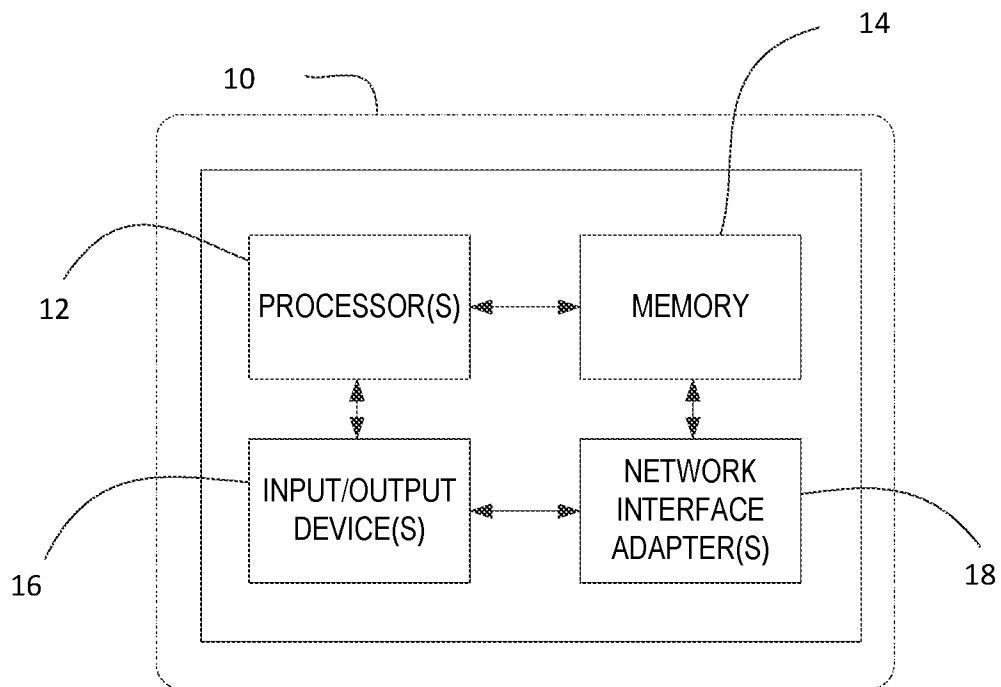


FIG. 1

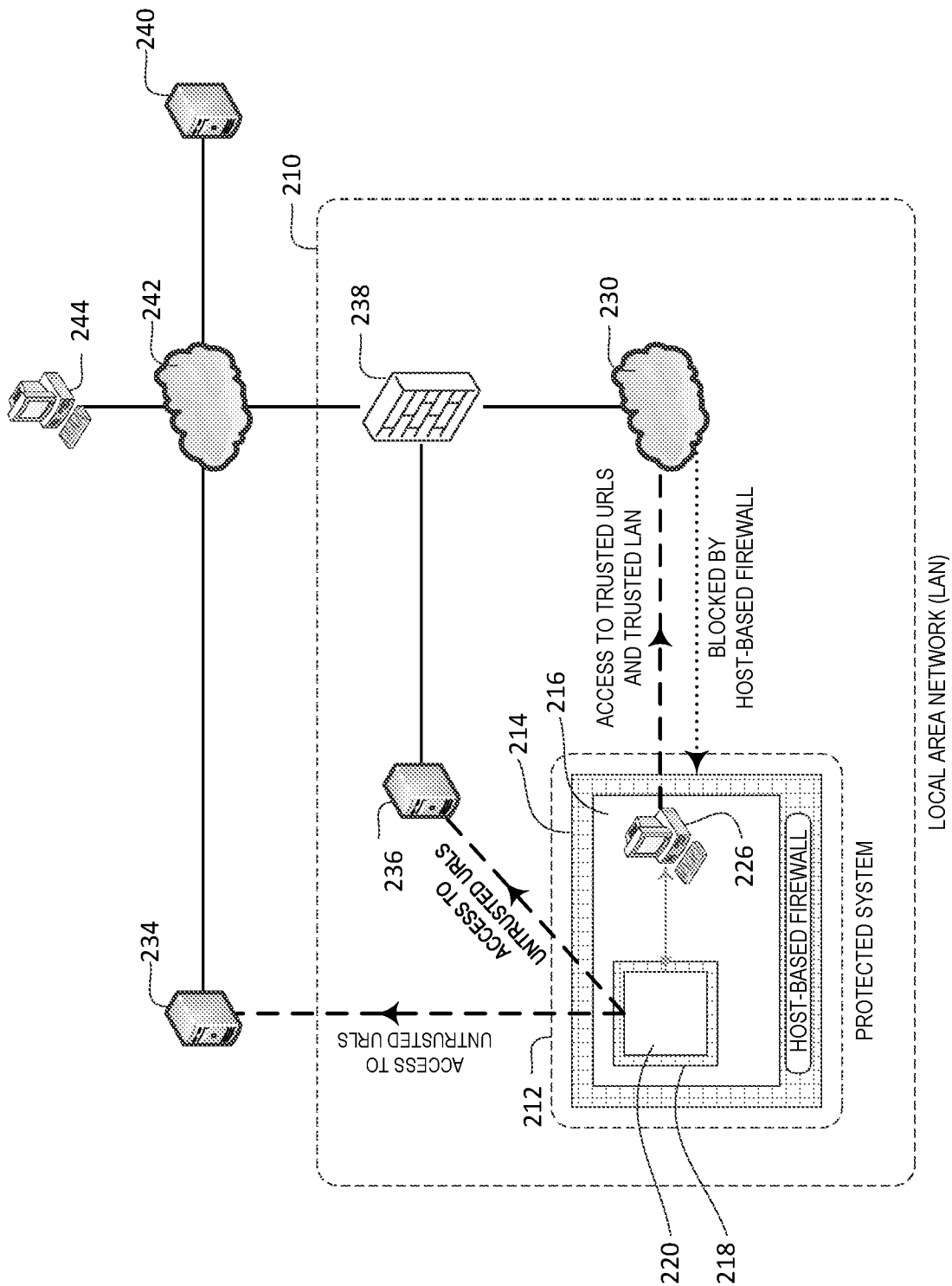


FIG. 2

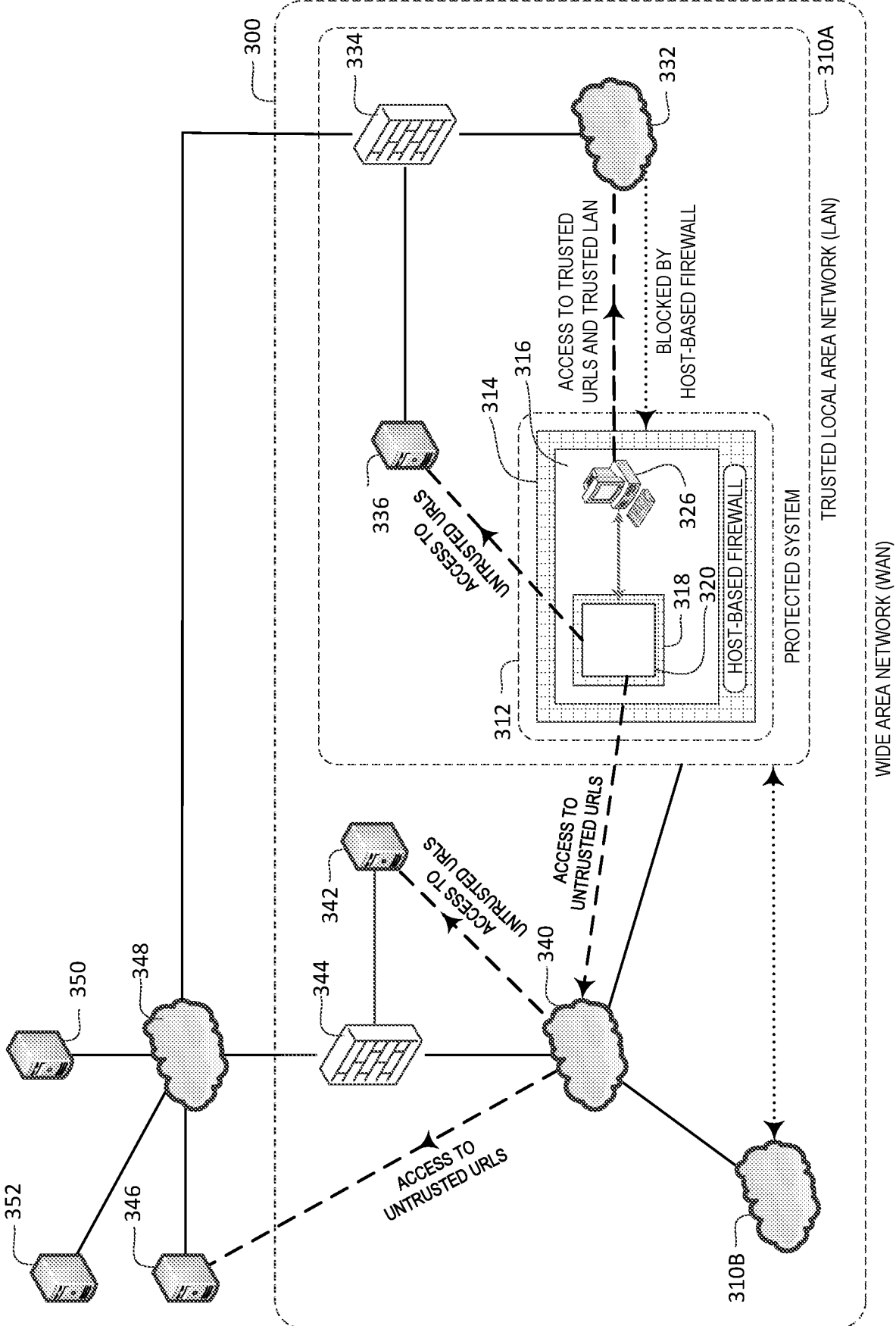


FIG. 3

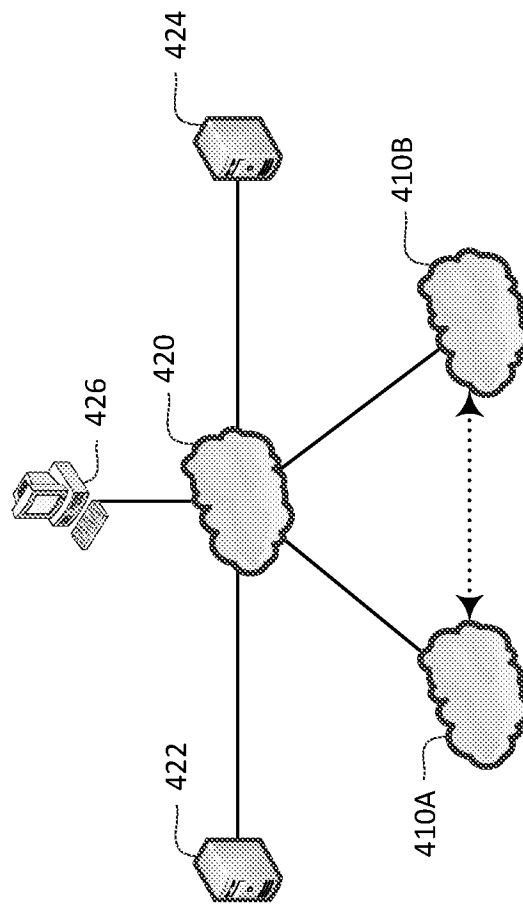


FIG. 4

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of
Invention **NETWORK ISOLATION WITH CLOUD NETWORKS**

As the below named inventor, I hereby declare that:

This declaration

is directed to: ☒ The attached application, or

☐ United States application or PCT international application number _____

filed on _____

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I have reviewed and understand the contents of the above-identified application, including the claims.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Glenn Coleman

Date: 11 Sep 2018

Signature: [Signature]

Note: An application data sheet (PTO/AIA/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional Substitute Form for PTO/SB/AIA01 for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of
Invention **NETWORK ISOLATION WITH CLOUD NETWORKS**

As the below named inventor, I hereby declare that:

This declaration

is directed to:

☒ The attached application, or

☐ United States application or PCT international application number _____
filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I have reviewed and understand the contents of the above-identified application, including the claims.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Peter Martz

Date:

9/11/10

Signature:



Note: An application data sheet (PTO/AIA/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional Substitute Form for PTO/SB/AIA01 for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of
Invention **NETWORK ISOLATION WITH CLOUD NETWORKS**

As the below named inventor, I hereby declare that:

This declaration

is directed to: ☒ The attached application, or

☐ United States application or PCT international application number _____
filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I have reviewed and understand the contents of the above-identified application, including the claims.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Kenneth Moritz

Date: 9-11-18

Signature: *Kenneth Moritz*

Note: An application data sheet (PTO/AIA/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional Substitute Form for PTO/SB/AIA01 for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	LCOM_ENT_CLOUD_US01
		Application Number	
Title of Invention	NETWORK ISOLATION WITH CLOUD NETWORKS		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.</p> <p>This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

Secrecy Order 37 CFR 5.2:

☐	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	---

Inventor Information:

Inventor 1					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Glenn		Coleman		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Berwyn	State/Province	PA	Country of Residence	US
Mailing Address of Inventor:					
Address 1	600 Third Avenue				
Address 2					
City	New York	State/Province	NY		
Postal Code	10016	Country	US		
Inventor 2					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Peter		Martz		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Marlton	State/Province	NJ	Country of Residence	US
Mailing Address of Inventor:					
Address 1	600 Third Avenue				
Address 2					
City	New York	State/Province	NY		
Postal Code	10016	Country	US		
Inventor 3					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Kenneth		Moritz		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	LCOM_ENT_CLOUD_US01	
		Application Number		
Title of Invention	NETWORK ISOLATION WITH CLOUD NETWORKS			

City	Lansdowne	State/Province	PA	Country of Residence	US
------	-----------	----------------	----	----------------------	----

Mailing Address of Inventor:

Address 1	600 Third Avenue				
Address 2					
City	New York			State/Province	NY
Postal Code	10016		Country	US	
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.					<input type="button" value="Add"/>

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).			
☐ An Address is being provided for the correspondence Information of this application.			
Customer Number	15027		
Email Address		<input type="button" value="Add Email"/>	<input type="button" value="Remove Email"/>

Application Information:

Title of the Invention	NETWORK ISOLATION WITH CLOUD NETWORKS		
Attorney Docket Number	LCOM_ENT_CLOUD_US01	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	4	Suggested Figure for Publication (if any)	2

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	LCOM_ENT_CLOUD_US01
		Application Number	
Title of Invention	NETWORK ISOLATION WITH CLOUD NETWORKS		

Representative Information:

<p>Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.</p>			
Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	15027		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	62563237	2017-09-26
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	LCOM_ENT_CLOUD_US01
		Application Number	
Title of Invention	NETWORK ISOLATION WITH CLOUD NETWORKS		

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

<p>This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.</p> <p>☐ NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.</p>	
--	--

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	LCOM_ENT_CLOUD_US01
	Application Number	
Title of Invention	NETWORK ISOLATION WITH CLOUD NETWORKS	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	LCOM_ENT_CLOUD_US01
		Application Number	
Title of Invention	NETWORK ISOLATION WITH CLOUD NETWORKS		

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.			
Applicant 1			
<p>If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.</p>			
<input type="button" value="Clear"/>			
☐ Assignee	☐ Legal Representative under 35 U.S.C. 117	☐ Joint Inventor	
☒ Person to whom the inventor is obligated to assign.		☐ Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
Name of the Deceased or Legally Incapacitated Inventor: <input type="text"/>			
If the Applicant is an Organization check here. ☒			
Organization Name	L3 Technologies, Inc.		
Mailing Address Information For Applicant:			
Address 1	600 Third Avenue		
Address 2			
City	New York	State/Province	NY
Country	US	Postal Code	10016
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button.			

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	LCOM_ENT_CLOUD_US01
		Application Number	
Title of Invention	NETWORK ISOLATION WITH CLOUD NETWORKS		

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

Organization Name L3 Technologies, Inc.

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1		600 Third Avenue	
Address 2			
City	New York	State/Province	NY
Country ⁱ	US	Postal Code	10016
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). However, if this Application Data Sheet is submitted with the **INITIAL** filing of the application **and** either box A or B is **not** checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Benjamin Chalfin/		Date (YYYY-MM-DD)	2018-09-25
First Name	Benjamin	Last Name	Chalfin	Registration Number
74181				

Additional Signature may be generated within this form by selecting the Add button.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	LCOM_ENT_CLOUD_US01
		Application Number	
Title of Invention	NETWORK ISOLATION WITH CLOUD NETWORKS		

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

- 1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
- 2 A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
- 3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
- 4 A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
- 5 A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
- 6 A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
- 7 A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
- 8 A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
- 9 A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 16/141,378				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300			
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	660			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760			
TOTAL CLAIMS (37 CFR 1.16(j))	20	minus 20 = *			OR	x 100 =	0.00			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *				x 460 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL		TOTAL	1720			
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.										



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
16/141,378	09/25/2018	1652	1720	LCOM_ENT_CLOUD_US01	20	3

CONFIRMATION NO. 2440

FILING RECEIPT



0000000103088038

15027
Condo Roccia Koptiw LLP
1800 JFK Boulevard
Suite 1700
Philadelphia, PA 19103

Date Mailed: 10/17/2018

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Glenn Coleman, Berwyn, PA;
Peter Martz, Marlton, NJ;
Kenneth Moritz, Lansdowne, PA;

Applicant(s)

L3 Technologies, Inc., New York, NY;

Assignment For Published Patent Application

L3 Technologies, Inc., New York, NY

Power of Attorney: The patent practitioners associated with Customer Number 15027

Domestic Priority data as claimed by applicant

This appln claims benefit of 62/563,237 09/26/2017

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 10/16/2018

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/141,378**

Projected Publication Date: 03/28/2019

Non-Publication Request: No

Early Publication Request: No
Title

NETWORK ISOLATION WITH CLOUD NETWORKS

Preliminary Class

435

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	REQUEST ID
16/141,378		1652	73876

PAIR Correspondence Address/Fee Address Change

The following fields have been changed to Customer Number 158266 on 10/17/2018 via Private PAIR in view of the certification copied below that authorized the change.

• Correspondence Address

The address for Customer Number 158266 is:

158266

Condo Roccia Koptiw LLP

1800 JFK Boulevard

Suite 1700

Philadelphia, PA 19103

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

An attorney or Agent of Record registered to practice before the Patent and Trademark Office who has been given power of attorney in this application

Signature:	/Joseph R. Klinicki/
Name:	Joseph R. Klinicki
Registration Number:	68505



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	REQUEST ID
16/141,378		1652	73876

PAIR Correspondence Address/Fee Address Change

The following fields have been changed to Customer Number 158266 on 10/17/2018 via Private PAIR in view of the certification copied below that authorized the change.

- Maintenance Fee Address

The address for Customer Number 158266 is:

158266

Condo Roccia Koptiw LLP

1800 JFK Boulevard

Suite 1700

Philadelphia, PA 19103

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

An attorney or Agent of Record registered to practice before the Patent and Trademark Office who has been given power of attorney in this application

Signature:	/Joseph R. Klinicki/
Name:	Joseph R. Klinicki
Registration Number:	68505

CD Submission Review Results

Internal Worksheet Only - Do Not Scan

Application Number

16141378

Receipt Date

Sep 25, 2018

☒New
Application☐Response To
Notice

Date Of Response

☐

Jumbo – Large tables are included on the CD

☒**There are no problems with the CDs in the submission.****Items checked below are to be selected in the PALM Pre-Exam CD problem list.**

Omitted Items

☐	Files on compact disc are unreadable:
☐	Disc(s) of either set not readable:
☐	Disc(s) do not contain file names listed:
☐	Amended CD missing unamended files
☐	Missing compact discs

Missing Parts

☐	Disc(s) do not contain file names listed
☐	Discs contains files that are non-ASCII files:
☐	Only one copy of the CD, no duplicate:
☐	Wrong media type, e.g., CD-RW:
☐	The transmittal letter and specification do not list information:
☐	Both disc(s) contain unreadable files:
☐	One disc(s) contain unreadable files:
☐	Compact disc(s) contain viruses, but are still readable:
☐	EFS/Paper Submission:
☐	Table does not maintain data in proper alignment:
☐	Not proper subject matter for CD's:

Informality

☐	No statement in transmittal letter that CD's are the same:
☐	No incorporation by reference statement for the CD's:
☐	CD's not labeled "Copy 1" and "Copy 2":
☐	Deficient CD packaging:
☐	Deficient Labeling on CD's:
☐	The transmittal letter does not list information:
☐	The specification does not list information:
☐	Table less than 51 pages submitted on CD:

File Directory Attachment

☐	Copy of file directory listing is attached and should be mailed to applicant
☐	Copy of file directory listing is not attached
☐	Copy of file directory listing is not attached because it is over one page long

Additional Comments

Internal Worksheet Only - Do Not Scan

SCORE Placeholder Sheet for IFW Content

Application Number: 16141378

Document Date: 09/25/2018

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access SCORE content via eDAN using the Supplemental Content tab, or via the SCORE web page.
- External customers may access SCORE content via PAIR using the Supplemental Content tab.

Substitute for 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>				Complete if Known	
				Application Number	16/141,378
				Filing Date	September 25, 2018
				First Named Inventor	Coleman, Glenn
				Art Unit	2491
Examiner Name	PATEL, ASHOKKUMAR B				
Sheet	1	of	2	Attorney Docket Number	LCOM_ENT_CLOUD_US01

U. S. PUBLICATION AND PATENT DOCUMENTS				
Examiner Initials	Cite No.	Document Number	Publication or Grant Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
		Number – Kind Code (if known)		
	1	7,478,330 B1	01-13-2009	Branson et al.
	2	7,698,442 B1	04-13-2010	Krishnamurthy et al.
	3	7,805,516 B2	09-28-2010	Kettler et al.
	4	2002/0069369 A1	06-06-2002	Tremain et al.
	5	2006/0070066 A1	03-30-2006	Grobman, Steven L.
	6	2007/0220187 A1	09-20-2007	Kates, Lawrence
	7	2007/0260873 A1	11-08-2007	Hatfalvi et al.
	8	2008/0028401 A1	01-31-2008	Geisinger, Nile Josiah
	9	2008/0201711 A1	08-21-2008	Amir Husain, Syed M.
	10	2008/0256536 A1	10-16-2008	Zhao et al.
	11	2009/0172781 A1	07-02-2009	Masuoka et al.
	12	2009/0328038 A1	12-31-2009	Yamada et al.
	13	2010/0138829 A1	06-03-2010	Hanquez et al.
	14	2010/0138830 A1	06-03-2010	Astete et al.
	15	2010/0223613 A1	09-02-2010	Schneider, James P.
	16	2010/0251329 A1	09-30-2010	Wei, Coach
	17	2012/0023593 A1	01-26-2012	Puder et al.

FOREIGN PATENT DOCUMENTS					
Examiner Initials	Cite No.	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T
		Country Code- Number - Kind Code (if known)			
	18	RU 2406138 C1	12-10-2010	Samsung Electronics Co., Ltd.	X

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

Substitute for 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>				Complete if Known	
				Application Number	16/141,378
				Filing Date	September 25, 2018
				First Named Inventor	Coleman, Glenn
				Art Unit	2491
Examiner Name	PATEL, ASHOKKUMAR B				
Sheet	2	of	2	Attorney Docket Number	LCOM_ENT_CLOUD_US01

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author, title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), Volume-issue Number(s), publisher, city and/or country where published.	T
	19	BARNET, MARK, "Praktikum Po Zaszchite Seti Kompanii", Windows IT Pro/RE, November-December 2006, pp. 79-81	
	20	BURNETT, MARK, "How I Secured One Company's Network", Using Log Parser, Virtualization, and A Little Psychology, September 17, 2006, 4 pages	
	21	LAVERICK, MIKE, "Hypervisor Management and Optimization for Advanced Virtualization", E-book, TechTarget, 2010, 13 pages	
	22	LI et al., "VSITE: A Scalable and Secure Architecture for Seamless L2 Enterprise Extension in the Cloud", 6th IEEE Workshop on Secure Network Protocols (NPSec), October 2010, pp. 31-36	
	23	REUBEN, JENNI SUSAN, "A Survey on Virtual Machine Security", TKK T-110.5290 Seminar on Network Security, October 11-12, 2007, 5 pages	
	24	VILLENEUVE, NART, "Command and Control in the Cloud", Malware Explorer, October 22, 2010, 3 pages	
	25	WIKIPEDIA, "Computer Networking", Available at https://en.wikipedia.org/wiki/Computer_network , December 2010, 19 pages	
	26	WIKIPEDIA, "Computer Security", Available at https://en.wikipedia.org/wiki/Computer_security , retrieved on December 2010, 27 pages	
	27	WIKIPEDIA, "Cyber Security Standards", Available at https://en.wikipedia.org/wiki/Cyber_security_standards , retrieved on December 2010, 9 pages	
	28	WIKIPEDIA, "HTTP Secure", Available at https://en.wikipedia.org/wiki/HTTPS , retrieved on December 2010, 9 pages	
	29	WIKIPEDIA, "Hypervisor", Available at < https://en.wikipedia.org/wiki/Hypervisor > , retrieved on December 2010, 6 pages	
	30	WIKIPEDIA, "Internet Protocol", Available at https://en.wikipedia.org/wiki/Internet_Protocol , retrieved on December 2010, 5 pages	
	31	WIKIPEDIA, "Multiprotocol Label Switching", Available at < https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching > , retrieved on December 2010, 8 pages	
	32	WIKIPEDIA, "Network Address Translation", Available at https://en.wikipedia.org/wiki/Network_address_translation , December 2010, 12 pages	
	33	WIKIPEDIA, "Security-Focused Operating System", Available at https://en.wikipedia.org/wiki/Security-focused_operating_system , retrieved on December 2010, 9 pages	
	34	WIKIPEDIA, "Virtual Desktop", Available at https://en.wikipedia.org/wiki/Virtual_desktop , retrieved on December 2010, 5 pages	
	35	WIKIPEDIA, "Virtual Private Network", Available at https://en.wikipedia.org/wiki/Virtual_private_network , retrieved on December 2010, 9 pages	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

Практикум по защите сети компании

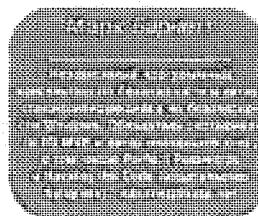
*С применением Log Parser, виртуализации
и небольшой доли психотерапии*

Отражение попыток проникновения в сеть —

процесс бесконечный. Благодаря значительному прогрессу последних лет защита сетей стабильно находится на приемлемом уровне, хотя иногда приходится поступиться удобством работы и совместимостью. Для одной из компаний такая цена показалась слишком высокой. Мне удалось смягчить проблему неудобства для одного из клиентов, не жертвуя безопасностью.

Ситуация

Недавно одна компания пригласила меня на работу в качестве консультанта. Специфика этого предприятия такова, что сотрудникам постоянно приходится посещать множество различных Web-узлов. Руководство поощряет использование компьютеров для игр, общения и других занятий, способствующих творческому подходу к работе. Проблема заключалась в том, что со времени выпуска Windows и Server 2003 Service Pack 1 (SP1) XP SP2 сотрудникам не удавалось добиться корректной работы многих



посещаемых ими Web-узлов. В службу поддержки постоянно шли обращения за помощью для установки компонентов ActiveX, устранения проблем с зонами, активизации всплывающих

окон и настройки параметров для файлов-«маяков» — всех элементов, необходимых для функционирования Web-узлов.

Иногда пользователи проявляли инициативу и самостоятельно ослабляли режим безопасности. Смягчение защиты не прошло без последствий: несмотря на такие базовые меры предосторожности, как брандмауэры, сканирование почтовых сообщений в поисках вирусов и автоматические обновления, компания стала чаще подвергаться атакам «шпионов», вирусов и других вредных программ.

Моя задача состояла не в том, чтобы укрепить Windows, а в том, чтобы изменить установленный в компании режим безопасности, дабы сотрудникам было удобнее работать с операционной системой, по возможности не поступившись безопасностью. Компания поставила ряд условий: решение должно быть простым и не требо-

вать серьезной перестройки сети, оно не должно требовать переобучения администраторов или существенно повышать их нагрузку. Одним словом, компании был нужен компонент, который легко добавить к существующей сетевой инфраструктуре.

Я объяснил заказчику опасность ослабления мер защиты браузера и других программ. Например, пользователь может посетить Web-узел, который использует какое-нибудь уязвимое место в Microsoft Internet Explorer (IE), чтобы установить программу сбора информации о нажатиях на клавиши. В результате злоумышленник сможет перехватывать все данные, вводимые с клавиатуры. С этого момента пароли и любая другая конфиденциальная информация будут находиться под угрозой. Такая опасность возникает постоянно. Или пользователь неосторожно установит шпионскую программу, которая существенно снизит быстродействие системы или сделает ее неработоспособной.

Я предложил применить обычную процедуру укрепления защиты Windows, но руководители компании быстро отвергли этот вариант. Им хотелось, чтобы меры безопасности были изменены ровно настолько, чтобы не влиять на работоспособность и сохранить удобство использования. Сотрудники компании должны полностью задействовать ресурсы Internet, не подвергаясь при этом опасности.

Достаточно было пройти по офису, чтобы получить представление о задаче, которую предстояло решать: я увидел окна программы мгновенного обмена сообщениями, открытые на многих компьютерах, панели задач со множеством пиктограмм и USB-концентраторы, подключенные к самым разнообразным устройствам. Стало очевидно: компьютер был центральным звеном профессиональной деятельности этих высококвалифицированных, творческих пользователей. Один из руководителей сказал, что ему хотелось бы иметь две отдельные сети: одну безопасную, для работы, и равноценную

сеть для доступа в Internet. Как выяснилось, в его замысле было рациональное зерно.

Виртуальное решение

Я обдумал идею двух отдельных сетей. Всем известно, что строить две отдельные сети непрактично, но идея заинтересовала меня. Существует много способов изолировать сети с единым соединением. Моей первой мыслью было поэкспериментировать с виртуальной тестовой сетью с использованием виртуальных машин (VM). Я постоянно прибегаю к этому приему для исследований и тестирования.

Затем я понял, что моя идея с тестовой сетью была уже сама по себе решением. Я мог быстро построить параллельную сеть из виртуальных машин и обеспечить любой уровень изоляции.

Сначала виртуальная сеть должна была сосуществовать с основной, но я намеревался использовать технологию виртуализации, чтобы направлять сетевой трафик в виртуальные машины на каждом настольном компьютере. Таким образом можно достичь достаточно хорошей изоляции виртуальных машин, назначив им IP-адреса из отдельной подсети и защитив трафик основной сети с помощью протокола IPsec. Этот подход не помешает злоумышленнику специально атаковать основную сеть, но успешно изолирует угрозы, исходящие от вредных программ.

Большое достоинство виртуальных машин заключается в том, что пользователь, заподозривший угрозу безопасности системы или просто нестабильность работы, может вернуться к чистому образу системы за несколько секунд. Пользователи могут сколько угодно экспериментировать с виртуальными машинами, не подвергая риску стабильность рабочей системы.

Конечно, ни одна компания, продукт или технология не гарантируют полной безопасности. Глубокое проникновение взломщика в VM до уровня базовой операционной системы грозит крупными неприятностями.

Для данного решения важно сформировать хороший уровень изоляции. Цель — сбалансировать риск и удобство использования и изолировать риск, чтобы свести к минимуму влияние мер безопасности на сеть компании. Кроме того, у администратора появляется способ быстро идентифицировать опасность и восстанавливать системы после аварий.

Подсеть VM

Я начал планирование с самого низкого уровня изоляции — виртуальной сети. Сеть можно было бы изолировать физически, но для простоты виртуальные машины были размещены в отдельной подсети. Это решение не идеально, но, по крайней мере, благодаря уникальным IP-адресам проще настроить брандмауэр, маршрутизаторы и систему обнаружения несанкционированного доступа для особого подхода к подсети VM. Организовав особую подсеть для виртуальных машин, можно без труда идентифицировать любые проблемы, исходящие от этих машин. Но главное, можно применить строгие правила брандмауэра, которые позволяют уменьшить риск, не влияя на просмотр Web.

Для виртуальных машин была выделена сеть 10.1.0.0/16, так как в качестве основной сети компании использовалась подсеть 192.168.0.0/16. Для этой подсети был выделен специальный порт маршрутизатора, а тщательно составленные правила брандмауэра ограничили сетевые соединения от виртуальных машин.

Физические сетевые адаптеры — общие для виртуальных и базовых машин, поэтому необходим DHCP-сервер, который будет присваивать IP-адреса только виртуальным машинам. VMware располагает DHCP-функцией для гостевых операционных систем, но с главного маршрутизатора нельзя отличить трафик виртуальных машин от трафика базового компьютера. Поскольку уже планировалось использовать IPsec, я решил настроить DHCP-сервер, который может уста-

навливать связь только с системами, аутентифицированными через протокол IPsec.

Я осознал, что решение задействовать IPsec может противоречить требованию малой нагрузки для администраторов. По итогам анализа риска было решено использовать аутентификацию IPsec с общим ключом, чтобы обеспечить необходимый уровень изоляции без разрывания инфраструктуры открытых ключей. Сведения о применении IPsec для изоляции домена приведены в статье Microsoft «Server and Domain Isolation» по адресу <http://www.microsoft.com/technet/itsolutions/network/sdiso/default.mspx>.

Настройка браузера

Значительная часть проекта заключалась в настройке браузеров таким образом, чтобы пользователи не чувствовали стеснения, несмотря на принятые меры безопасности. Самым очевидным решением было ослабить некоторые параметры безопасности, чтобы ограничения IE меньше сказывались на таких задачах, как установка Java или загрузка и запуск компонента ActiveX.

Чтобы достичь нужного баланса, мне пришлось настроить политики зоны, выбираемой по умолчанию. Вместо того чтобы блокировать компоненты или запретить сценарии, я настроил браузер на запрос разрешения перед выполнением этих действий. Однако скоро выяснилось, что в таком случае пользователи будут получать множество раздражающих запросов

даже при просмотре самых обычных Web-узлов.

Поэтому пришлось понаблюдать за некоторыми пользователями во время их работы с Internet. Большинство пользователей применяли те или иные приемы для обхода ограничений безопасности — использовали браузер Mozilla Firefox или Opera либо добавляли узлы в доверенный список IE. Но каждый сотрудник мог быстро назвать один или два узла, корректной работы которых не удавалось добиться никакими средствами. Это распространенная ситуация, когда узел в надежной зоне пытается загрузить компонент (например, Java) из узла в ограниченной зоне.

Я заметил, что пользователи не нуждались в неограниченном доступе в Internet — достаточно нескольких базовых компонентов, работающих с разнообразными Web-узлами. Кроме того, необходимые компоненты были весьма обычными, и их безопасность общепризнанна: в частности, Adobe Acrobat, Adobe ShockWave Player, Macromedia Flash и Apple QuickTime.

Я понял, что не нужно существенно менять политики безопасности, достаточно заранее установить типичные компоненты, чтобы создавалось впечатление, будто защитные ограничения сняты. Вероятно, можно даже применить более строгие меры безопасности, создав у пользователей иллюзию, что они ослаблены. В конце концов, пользователи протестовали не против защитных мер; они просто хотели, чтобы работали нужные Web-узлы.

Я мог заранее установить наиболее широко применяемые компоненты и внести в список надежных наиболее часто посещаемые узлы. Эти две меры обеспечили бы пользователям нужный уровень совместимости и снизили вероятность встречи с новым компонентом, требующим установки; одновременно отпала бы необходимость в полной отмене ограничений на компоненты ActiveX.

Чтобы все узлы могли использовать эти компоненты, я настроил групповую политику, позволив пользователям устанавливать компоненты ActiveX, но только из заранее подготовленного списка. Выяснив, какие компоненты установлены в различных системах, я вручную составил список, показанный в таблице. Затем я установил эти компоненты как одобренные администратором с помощью инструмента Profile Manager из комплекта Internet Explorer Administration Kit (IEAK)6SP1.

Заполнение зон

Составить список доверенных узлов было довольно сложно. Все сотрудники посещали обычные Web-узлы, но, чтобы избежать проблем совместимости, желательно, чтобы список узлов был исчерпывающим. Для подготовки этого списка использовалась бесплатная утилита Log Parser компании Microsoft.

Сначала я составил запрос, чтобы извлечь текущие списки доверенных узлов из десятка систем в сети. Вместе они точно отражали картину обращений в Web для всей сети. На каждой системе была запущена следующая команда Log Parser (вводится одной строкой):

Список типовых программ, используемых компонентами ActiveX	
Компонент ActiveX	URL
Adobe Systems Adobe Acrobat	http://www.adobe.com/products/acrobat
Adobe Systems Adobe Flash Player	http://www.adobe.com/products/flashplayer
Adobe Systems Macromedia	http://www.adobe.com/products/authorware/productinfo/webplayer
Authorware Web Player	
Apple Computer QuickTime	http://www.apple.com/quicktime/download/win.html
Microsoft DirectX	http://www.microsoft.com/windows/directx/default.mspx
Microsoft Office Viewers and Updates	http://office.microsoft.com/en-us/officeupdate
Microsoft Update	http://update.microsoft.com/microsoftupdate
Microsoft Windows Genuine Advantage Tool	http://www.microsoft.com/genuine/default.mspx
Sun Microsystems Java Software	http://java.com/en/download/index.jsp

```
C:\>logparser «SELECT DISTINCT
EXTRACT_TOKEN(Path, 8, '\\')
As Domain INTO
TrustedSites-
%COMPUTERNAME%.txt
FROM 'HKCU\Software\Microsoft\
Windows\CurrentVersion\
Internet Settings\ZoneMap\
EscDomains'
WHERE ValueName LIKE
'http%' -> -o:NAT -rtp:1
-headers:off
```

Данный запрос извлекает имена доменов из списка узлов в разделе реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\EscDomains` и сохраняет этот список имен в текстовом файле в текущем каталоге.

После того как были получены списки из каждого опрошенного компьютера, я поместил все списки в каталог и проанализировал их с помощью команды

```
CA>logparser «SELECT Text AS
Domain, Count(*) AS Total INTO
TrustedSites.txt FROM
TrustedSites*.txt GROUP BY
Domain HAVING Total > 1
ORDER BY Total DESC»
-i:txtline -o:nat -rtp:1
```

Этот запрос собирает доменные имена из всех списков доверенных узлов и сортирует их по частоте использования на всех компьютерах. При этом исключаются доменные имена, которые встречаются в списке лишь один раз. В результате получился список из нескольких сотен доменных имен. Я вручную просмотрел список и удалил явно неподходящие домены, в частности известные порнографические и шпионские сайты. В конечном итоге список доверенных сайтов стал похож на список 500 лучших Web-узлов.

Я решил, что нет причин запрещать какие-либо узлы из доменов, внесенных в список. Поэтому вместо того, чтобы разрешать [www.microsoft.com](http://www.microsoft.com/support/microsoft.com), windowsupdate.microsoft.com и download.microsoft.com, можно использовать универсальный символ и разрешить `*.microsoft.com`. Благодаря универсальным символам значительно проще ввести список в реестр.

Чтобы составить список, который легко импортировать в реестр, я запустил еще один запрос Log Parser, но на этот раз формат вывода был более сложным. Для подготовки правильно форматированного .reg-файла я построил файл шаблона, сохранив текст, показанный на экране, в файле с именем `reg.tpl`. В следующей команде параметр `-tpl` используется для форматирования вывода с применением указанного шаблона:

```
<LPHEADER>
Windows Registry Editor Version 5.00
</LPHEADER>

<LPBODY>
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\EscDomains\%Domain%]
"http"=dword:00000002
"https"=dword:00000002
</LPBODY>
<LPFOOTER>
</LPFOOTER>
```

Экран

Шаблон для создания .reg-файла

```
CA> logparser «SELECT Domain
INTO TrustedSites.reg FROM
TrustedSites.txt» -itsv
-iSeparator:space -nSep:2
-nFields:2 -o:tpl -tpl:reg.tpl
```

В результате был получен файл `TrustedSites.reg`, который можно добавить в реестр двойным щелчком мыши.

Заполняя список доверенных узлов, я подумал, что полезно подготовить и список запрещенных узлов. Эта задача оказалась гораздо проще, так как подготовительная работа уже была сделана. Чтобы добавить узлы в зону `Restricted Sites`, я использовал несколько программ, которые добавляют собственные списки запрещенных узлов, в том числе `IESPYAD` (по адресу <http://www.spywarewarrior.com/uiuc/resource.htm>), которая добавляет список известных опасных узлов и доменов в зону `Restricted Sites` браузера IE. В Firefox нет зоны, соответствующей `Restricted Sites`.

Построение виртуальной машины

Подготовленный шаблон VM был базовым экземпляром XP SP2. Ради простоты для задания политики безопасности использовался встроенный шаблон безопасности `securows.inf`. Виртуальные машины нуждаются в эффективной защите от опасных программ, поэтому я загрузил несколько бесплатных программ для борьбы с вирусами и другими вредителями: `Javacool Software SpywareBlaster`, `Clam Antivirus`, бета-версию `Microsoft Windows Defender` и `Spybot-Search & Destroy`. Многие функции этих программ перекрываются, что обеспечивает более надежную защиту.

После того как была завершена настройка и укреплена безопасность операционной системы, я установил новейшие исправления и новую учетную запись для регистрации пользователей. Вместо того чтобы управлять вторым набором учетных данных для каждого пользователя, я создал одну учетную запись пользователя в базовом образе, установил образ на каждом компьютере и потребовал, чтобы пользователи изменили пароль при следующей регистрации. При первом запуске виртуальной машины пользователи должны назначить пароль для учетной записи. Полностью управляемый домен, выделенный для виртуальных машин, обеспечил бы более тщательный контроль над каждой учетной записью, но применение одной учетной записи — простое решение, соответствующее поставленной цели.

Виртуальное создание выходов

Назначив базовые политики безопасности — а я убедил руководство компании запретить приложения для одноранговых сетей, обычный источник шпионских программ, — и проведя начальное обучение пользователей, я развернул образ на компьютерах сети. Поначалу некоторые пользователи выражали недовольство, но быстро успокоились после того, как привыкли работать с VM, и особенно когда обнаружили, что Web-узлы работают безупречно. В результате сотрудники компании получили удобный, а администраторы — безопасный доступ в Internet. ☺



- App Management
- Patch Management
- Policy Management
- Software Deployment

[View all articles](#)
[Manage your Desktop Control](#)
[HOME](#) > [SYSTEMS MANAGEMENT](#) > [NETWORKING](#) > [HOW I SECURED ONE COMPANY'S NETWORK](#)

How I Secured One Company's Network

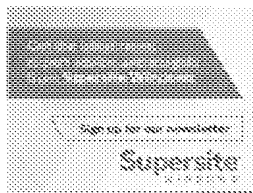
Using Log Parser, virtualization, and a little psychology

Mark Burnett | [Windows IT Pro](#)

Sep 17, 2008

TWITTER 

COMMENTS 0



Keeping malware from infecting networks is a never-ending battle. Over the past few years, the IT world has made great progress in maintaining acceptable network defenses, although sometimes at the expense of usability and compatibility. For one company, that was too great a price to pay. Here's how I lowered the usability cost of malware prevention for one of my clients while maintaining security.

The Situation

Recently, a company hired me as a security consultant. Due to the nature of my client's business, employees spend a lot of time on many different Web sites. The company encourages employees to use their computers to play, to communicate with others, and to do whatever else is needed to foster creativity. Its problem was that ever since the release of Windows Server 2003 Service Pack 1 (SP1) and XP SP2, employees couldn't get the Web sites they visited to work properly.

Support incidents piled up as employees requested help to install ActiveX components, troubleshoot zone issues, enable pop-ups, and adjust cookie settings--whatever it took to get Web sites to work.

Sometimes users went ahead and eased security settings themselves. This relaxed security had consequences: Despite taking such basic precautions as using firewalls, email virus scanning, and automatic updates, the company still experienced an increase in spyware, viruses, and other malware-related incidents.

However, my job wasn't to harden Windows, but rather to relax some of the company's OS security defaults to improve usability while sacrificing as little security as possible. The company set some guidelines for my solution: It had to be simple and not require a major network overhaul, and it couldn't add significant administrative training or overhead. In short, the company wanted something I could easily attach to the existing network infrastructure.

I explained the risks involved with relaxing security restrictions on Web browsers and other software. For example, a user might visit a Web site that exploited some unpatched vulnerability in Microsoft Internet Explorer (IE) to install a keylogger on the user's system, giving the attacker access to everything the user typed on the keyboard. From that point on, user's passwords and just about any sensitive information typed would be at risk--it happens all the time. Or a user might inadvertently install spyware that significantly slowed the system or made it unusable.

I proposed my standard Windows lockdown procedure, but management quickly shot that down. The company wanted me to relax security just enough to get everything working but without affecting usability--it wanted to fully use the Internet without being vulnerable to it.

As I walked through the office, I caught a glimpse of the challenge before me: I saw IM windows open on many desktops, elaborate custom desktop themes, system trays loaded with icons, and USB hubs connecting devices of all varieties. One thing was clear: These were highly skilled, creative users whose work lives were centered on their PC. One executive told me he wished he could just have two separate networks: a safe one for work and a compatible one for Internet access. Turns out he was on to something.

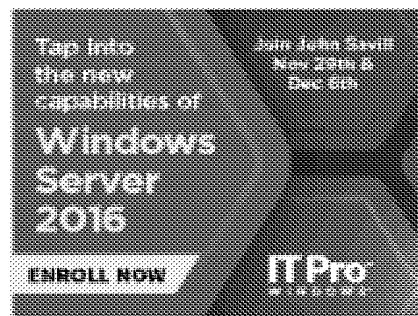
Windows Server 2016 Class

Windows Server 2016 Deep Dive with John Savill

Live Online Training on November 29th and December 6th

Register by November 22nd and Save 20%!

Windows Server 2016 offers a multitude of feature enhancements in addition to enabling new types of computing with technologies such as Nano Server and containers. During this two-day training all of the key new capabilities of Windows Server 2016 will be explored in addition to how they can be used in customer environments.

[REGISTER NOW](#)


Access Denied

Reason: Matched categories:
Web and Email Mark
Sites that are associa
URL: <http://forms.windowsit>
Options: CPA Global's policy fo
believe your access to
to it for a legitimate bu
requesting access.

Join the Conversation

Virtual Solution

I contemplated the idea of having two separate networks. We all knew that building two separate networks simply wasn't practical, but the idea intrigued me—there are plenty of ways to isolate networks on a single connection. My first thought was to experiment with a virtual test network using virtual machines (VMs)—something I do all the time for research and testing.

Then I realized that my test-network idea itself was the solution. I could quickly build an entire parallel network made up of VMs that could easily accommodate any level of isolation.

The virtual network would initially coexist with the main network, but I would use virtualization technology to direct that network's traffic to VMs running on each desktop. We could achieve reasonably good isolation of the VMs by assigning IP addresses from a separate subnet and using IPsec to secure the traffic on the main network. Although this approach wouldn't stop a malicious hacker from specifically targeting the main network, it would work well for isolating malware threats.

A big bonus of using VMs was that if users at any time felt their system security was compromised or otherwise unstable, they could revert to a clean master image in a matter of seconds. Users could play with—or destroy—VMs to their heart's content without threatening the stability of their work system.

Of course, no company, product, or technology can guarantee total security. If someone has hacked the VM to the extent that they can access the host, you probably have bigger concerns anyway.

The point with this solution was to add a pretty good layer of isolation. The goal was to balance risk and usability and to isolate the risk to minimize the effect on the company's network. Furthermore, we would have a method to quickly identify and recover from security incidents.

VM Subnet

I started my planning at the lowest level of isolation: the virtual network. Although I could have physically isolated the network, for simplicity I placed the VMs on their own subnet. The solution wasn't perfect, but at least the unique IP addresses would help me configure the firewall, routers, and intrusion detection systems to treat the VM subnet differently. By having a unique subnet for the VMs, I could easily identify any problems originating from those machines. Best of all, I knew I could enforce strict firewall rules that could limit security problems without affecting Web browsing.

I went with a 10.1.0.0/16 network for use with the VMs, because the company used the 192.168.0.0/16 subnet for its main network. I dedicated a router port to that subnet and carefully built firewall rules to limit network communications from the VMs.

Because the VMs shared the physical network adaptors with the host machines, I needed a DHCP server that would give IP addresses only to the VMs. VMware has a DHCP feature for guest OSs, but from the main router I wouldn't be able to distinguish VM traffic from the host's traffic. Since I was already planning to use IPsec, my solution was to configure a DHCP server that could only communicate with other systems authenticated via IPsec.

As for my decision to use IPsec, I knew it might conflict with the requirement of low administrative overhead. After analyzing the risks, I decided to use IPsec authenticating with a shared key, which would achieve the isolation I needed but wouldn't require implementing a public key infrastructure. (For information on configuring IPsec, see "Using IP Security Policies to Restrict Access to a Server," March 2005, InstantDoc ID 45217; for information on using IPsec for domain isolation, see the Microsoft article "Server and Domain Isolation" at <http://www.microsoft.com/technet/solutions/network/sdiso/default.mspx>.)

Browser Configuration

A big part of the project involved configuring browsers so that users felt unobstructed even though we maintained some level of security. The most obvious solution was to relax some of the security settings so that IE was less restrictive about such tasks as installing Java or downloading and running an ActiveX component.

To achieve this balance, I had to adjust the default zone policies. Rather than blocking components and disabling scripting, I adjusted the settings to prompt before taking these actions. However, it didn't take long for me to realize that users would experience a lot of annoying prompts, even when browsing the most common Web sites.

Consequently, I stepped back and monitored a handful of users as they used the Internet. Most users had developed some kind of workaround to cope with security restrictions—either using Mozilla Firefox or Opera to access some sites or adding sites to the trusted-



Get answers to questions, share tips, and engage with the IT professional community at myITForum.

Are you a data center professional? Join APCOM for the best data center insights.

Looking to get things done in web development? Hot Scripts offers tens of thousands of scripts you can use.

Database administrator? dbforums offers community insight on everything from ASP to Oracle, and get the latest news from Data Center Knowledge.



Penton® SmartReach™

Data & direct marketing programs, all in one place!



sites list in IE. But every user was quick to point out one or two sites that didn't work no matter what. This scenario often arose when a Web site that was in the Trusted Sites zone tried to download a component—such as Java—from a Web site in a restricted zone.

I noticed that users didn't need unrestricted Internet access—they just needed a few basic components to be able to work with a variety of Web sites. Furthermore, the components they needed were quite common and widely accepted as safe to install: Adobe Acrobat, Adobe Shock-Wave Player, Macromedia Flash, and Apple QuickTime, among others.

It occurred to me that I didn't have to significantly change security policies—I could simply preinstall the most common components to give the appearance that I'd removed security restrictions. In fact, I could probably increase security while giving users the illusion that I had relaxed it. After all, it wasn't the security restrictions that users disliked; they just needed Web sites to work. I could preinstall the most common components and prepopulate the trusted-sites list with the most commonly visited sites. Doing these two things would give users the compatibility they needed while making it less likely that they'd encounter a new component that needed to be installed, and I wouldn't have to completely remove the restrictions on ActiveX components.

To enable all sites to use these components, I configured Group Policy to let users install ActiveX components, but only those that were on the preapproved list. I manually compiled the list of components shown in Table 1 by looking at the components installed on various systems. I then installed the components as administrator-approved components using the Profile Manager tool from the Internet Explorer Administration Kit (IEAK) 6 SP1.

Populated Zones

Populating the trusted-sites list was a bit complicated. Everyone visited common Web sites, but to avoid compatibility problems, I wanted the list of sites to be comprehensive. To generate the list, I used Microsoft's free Log Parser utility.

I started by writing a query to pull the current trusted-sites list from a dozen systems on the network that together closely reflected overall network usage. On each system, I ran the following Log Parser command (which must be typed all on one line):

```
C:\>logparser "SELECT DISTINCT                                EXTRACT_TOKEN(Path, 8, '\\')                                As Domain INTO
```

This query extracts domain names from the list of hosts in the `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings\ZoneMap\EscDomains` registry key and saves the list of names to a text file in the current directory.

After collecting a list from each queried computer, I placed all the lists in a directory and parsed them with the command

```
C:\>logparser "SELECT Text AS                                Domain, Count(*) AS Total INTO                                TrustedSites.txt FROM
```

This query gathers the domain names from all the trusted-sites lists and sorts them by frequency of use across all machines, excluding those domain names that appear just once on a list. The aggregate list consisted of several hundred trusted domain names. I manually reviewed the list and removed domains that were obviously inappropriate, such as known porn or spyware sites. In the end, my trusted-sites list probably read a lot like a list of the top 500 Web sites.

I realized that there was no reason not to accept all hosts for each domain on the list. So rather than allowing `www.microsoft.com`, `sup.port.microsoft.com`, `windowsupdate.microsoft.com`, and `download.microsoft.com`, for example, I could use a wildcard and allow `*.microsoft.com`. Using wildcards made putting my list back into the registry much simpler.

To make a list I could easily import to the registry, I ran yet another Log Parser query, but this time the output format was a bit more complicated. To create a properly formatted .reg file, I created a template file by saving the text shown in Figure 1 to a file named `reg.tpl`. The following command uses the `-tpl` parameter to format the output using the specified template:

```
C:\> logparser "SELECT Domain                                INTO TrustedSites.reg FROM                                TrustedSites.txt" -i:tsv
```

This action creates a file, `Trusted-Sites.reg`, which you can double-click to add to the registry.

Because I was populating the trusted-sites list, I also thought it prudent to populate the restricted-sites list. This task was much easier, because the work had already been done for me. To add sites to the Restricted Sites zone, I used several other programs that add their own lists of restricted sites, including `IESPYAD` (available at <http://www.spywarewarrior.com/nuuc/resource.htm>), which adds a list of known undesirable sites and domains to IE's Restricted Sites zone. (There is no equivalent to a

Restricted Sites zone in Firefox.)

Building the VMs

The VM template I built was just a basic XP SP2 installation. To keep things simple, I used the built-in securewpa.inf security template to set the system's security policy.

Because the VMs needed effective protection from malware threats, I loaded several free antivirus and antimalware applications: Javacool Software SpywareBlaster, Clam AntiVirus, the Microsoft Windows Defender beta, and Spybot-Search & Destroy. Many of these tools' features overlapped, which I felt made the coverage more comprehensive.

After I hardened and preconfigured the OS, I installed the latest patches and created a new account for users to log on to. Rather than managing a second set of account credentials for each user, I created one user account on the base image, installed the image on every machine, and required the user to change the password at the next logon. When users first boot their VM, they have to set a password on that account. Although a fully managed domain dedicated to the VMs would have allowed more precise control over each account, using one account was a simple solution that still met the design goals.

(Virtual) Mission Accomplished

After establishing some basic security policies—I convinced company management to forbid the use of peer-to-peer applications, a common source of spyware—and conducting some basic user training, I deployed the image across the network. Initially, there was some user resistance, but that quickly disappeared after users became comfortable using the VMs, and especially after they found that most of their Web sites worked without any problems. To the users, I made the Internet work; to the administrators, I made it work securely.

TWEET | 3+1

Please Log in or Register to post comments.

Related Articles

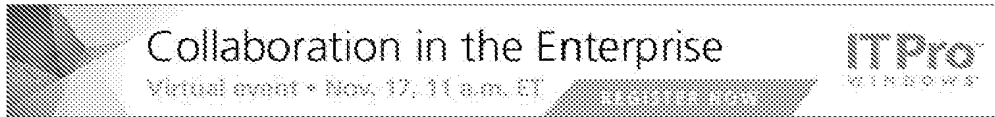
Reduce Admin Risks

How I Secured One Company's Network

2008: A Great Year for Windows IT Innovation 3

2006: A Great Year for Windows IT Innovation 3

Industry Briefings - 28 Nov 2008



Collaboration in the Enterprise

Virtual event • Nov. 17, 11 a.m. ET

REGISTER NOW

ITPro
WINDOWS

WindowsITPro.com

Windows Exchange Server SharePoint Virtualization Cloud Systems Management

Site Features

Contact Us

Awards

Community Sponsors

Media Center

RSS

Sitemap

Site Archive

View Mobile Site

Penton

Privacy Policy

Terms of Service

Advertise

Follow Us

Search WindowsITPro.com



Related Sites

DevPro SharePoint Pro SQL Server Pro SuperSite for Windows IT/Dev Connections myITForum

TAKE STOCK
OF YOUR RAM

EVALUATE CPU NEEDS

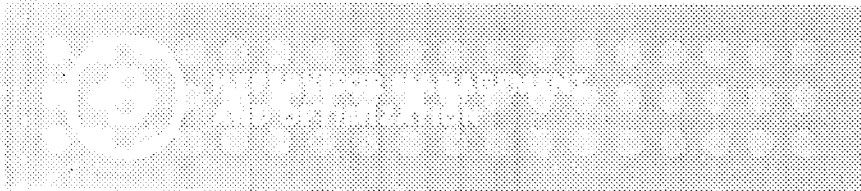
SIZE UP YOUR NETWORK

HYPERVISOR TEARDOWN:
VENDOR BY VENDOR

Hypervisor management and optimization

All hypervisors essentially do the same job, but not in the same way. The three top hypervisors all have differences that require specific management tactics.

BY MIKE LAVERICK



HYPERVISOR management and optimization

TAKE STOCK
OF YOUR RAM

BY MIKE LAVERICK

EVALUATE
CPU NEEDS

SIZE UP
YOUR NETWORK

VMWARE ESX

MICROSOFT
HYPER-V

CITRIX
XENSERVER

THERE ARE A few best practices and recommendations you can follow to optimize and maintain the three core data center hypervisors—VMware ESX, Microsoft Hyper-V and Citrix XenServer.

On the surface, the discussion of hypervisor optimization might seem trivial since hypervisors are fairly basic and don't come with the usual baggage that a full-blown operating system has. But it is possible to modify key default settings and tweak various vendors' hypervisors. A little research reveals that there is a marked difference in recommendations and best practices from one hypervisor to another. No matter which hypervisor you select to manage your virtual machines (VMs), all three platforms have similar resource demands as well as challenges to solve.

The easiest way to control these demands is to systematically ex-

plore the four-core resources of any system: memory, CPU, disk utilization and network resources.

TAKE STOCK OF YOUR RAM

RAM is the key resource to consider before purchasing a hypervisor, mainly because it's what most people run out of first. It's very common for virtualized environments to run low on memory long before they run out of CPU cycles. Failure to purchase the correct amount of memory for current and future demands can lead to unwanted and expensive consequences—having to upgrade your memory and having to purchase additional hosts.

In general, you can say that the right amount of memory to purchase is as much as you can afford. But that's a rather simplistic view considering that a server has a finite number of DIMM slots, and the



jump from 2 GB, 4 GB, 8 GB and 16 GB DIMMs is not a small one from a cost perspective.

In the long run, having fewer servers with a large amount of memory will be more cost efficient than having more smaller servers, especially when you consider the total cost of power, cooling and licensing. In the case of VMware, for example, this total cost is bound to the number of completed sockets in a rack-mounted server or chassis of blades.

TAKE STOCK
OF YOUR RAM

EVALUATE
CPU NEEDS

SIZE UP
YOUR NETWORK

VMWARE ESX

MICROSOFT
HYPER-V

CITRIX
XENSERVER

EVALUATE CPU NEEDS

Despite the rise of four-core and six-core CPUs, the more VMs you create with more than one vCPU, the more work the underlying hypervisor has to do to schedule each CPU within the guest vCPU. Therefore, on a VM level, be careful about the excessive use of multiple vCPUs within a VM because it may not produce the performance dividend you're looking for.

Additionally, the excessive use of vCPU can increase scheduling collisions—more than one vCPU executes on the same core at the same time. In general, this isn't a bad thing in its own right; it forms the bedrock of server consolidation where two, three and four VMs share the same underlying physical CPU. But resources do not scale to "infinity and beyond," so it's important not to overuse the physical CPUs.

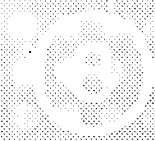
Closely examine your virtual

machines and the software applications they contain and ask if virtual symmetric multiprocessing, or SMP, will really pay any dividends. A legacy service that isn't multiprocessor aware will simply not use all of the CPU efficiently.

Pound for pound,
x64 OSes come
with greater
virtualization
overhead, re-
quiring more
memory just to
power on the VM.

Additionally, you may be attracted to the performance gains that x64 OSes can deliver from both a memory and CPU perspective. But you may discover that your application doesn't notice all of the benefits of the new architecture because it is 32-bit infrastructure. Pound for pound, x64 OSes come with greater virtualization overhead, requiring more memory just to power on the virtual machine. The question to ask is, "Will my application run on 32-bit architecture in a way that the vendor will support?"

Finally, if you're working with a hypervisor that doesn't allow for intelligent placement of the virtual machine on the correct host, then



it's up to you to blend the VMs on an array of hosts. It makes no sense to put two or more resource-intensive VMs on the same physical host. You want to avoid excessive over-

It makes no sense to put two or more resource-intensive VMs on the same physical host.

older Xeon and Opteron chipsets.

In the past, most virtualization specialists would have recommended disabling Hyper-Threading on physical CPUs, but recent enhancements on the Intel Nehalem CPUs indicate that Hyper-Threading is back and worth enabling for most workloads.

Most vendors often have a confusing array of different CPU specifications for the same rack-mounted server or blade. Often, there can be a huge price difference between one CPU type and another—with an almost negotiable gain in performance. You can find some helpful information online regarding which processor works well in virtualized environments.

SIZE UP YOUR NETWORK

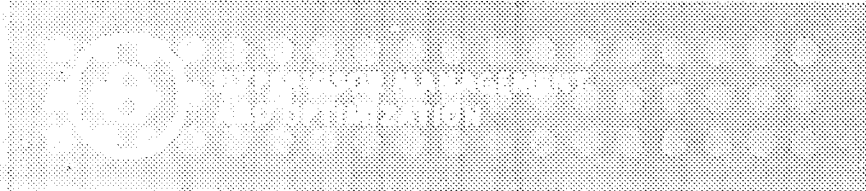
From a network perspective, I recommend using discrete and different network interfaces for each type of traffic that you intend to push in and out of the physical box. Each type of traffic should reside in its own broadcast domain, ideally using

subscription or “contention,” which degrades performance when too many virtual machines try to access the same physical CPU.

In short, if you think your workload is going to be CPU bound, then the amount of onboard memory cache on the CPU will make more of a difference than the overall amount of CPU cycles.

Additionally, the new Intel Nehalem and AMD Shanghai processors offer significant CPU gains over

VLAN TAGGING is a process in which the hypervisor adds an additional identifier to Ethernet frames. These packets are “tagged” in such a way that when the packets arrive at the physical network switch, it can read the data and send the frame to the appropriate network. The process of VLAN tagging significantly reduces the number of physical network interface cards (NICs) that a hypervisor needs.



VLANs and VLAN tagging to maintain network boundaries.

The features you select will ultimately dictate the number of physical network interface cards (NICs) you need and whether the traffic they carry requires redundancy and fault-tolerance. Generally, the following numbers are recommended:

**TAKE STOCK
OF YOUR RAM**

**EVALUATE
CPU NEEDS**

**SIZE UP
YOUR NETWORK**

VMWARE ESX

**MICROSOFT
HYPER-V**

**CITRIX
XENSERVER**

- At least one NIC for management traffic
- At least two NICs connected for VM traffic
- At least two NICs connected for any IP-based storage system used (network-attached storage or iSCSI)
- At least one NIC for any live migration or VMotion feature

Hypervisors network demands alone can be daunting. It's possible for network traffic to be "blended" together, so it's not uncommon for organizations to also use the management network to carry out live migration tasks. As a network gateway, the management network isn't heavily used, which is a shame because it would be suitable as spare bandwidth for something else the network needs. However, most hypervisor vendors caution that this is against best practices.

So companies will inevitably have to make compromises based on cost, performance and security. For example, it's less expensive to drive live migration traffic across a man-

agement network, but that has its security consequences. Most live migration traffic is unencrypted and contains sensitive VM memory data. With that said, most management networks are secured and private.

Few customers have experienced poor network performance in the virtual data center. In these few instances, however, the root cause was attributed to external configuration issues such as poor DNS queries and structures or out-of-date routing table settings that needed immediate attention.

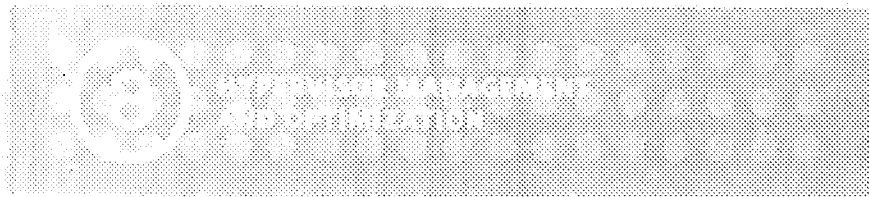
HYPERVISOR TEARDOWN: VENDOR BY VENDOR

All hypervisors essentially have the same job—spawn virtual machines and allocate a slice of memory, CPU, disk space and network usage to the workload. And while there are some fundamental aspects of hypervisors where performance optimization will be very similar, not all hypervisors are the same architecturally. In some cases, vendor-specific tweaking is required to gain the most from the virtualization layer you have selected.

Here's a look at the three biggest hypervisors by vendor and considerations when implementing each.

VMware ESX

Generally recognized to have one of the smallest hypervisor footprints on the market, the actual amount of



space VMware ESX consumes depends on which flavor of ESX you purchase.

ESX Classic, which has a fully interactive service console, is commonly recognized as the more mature cousin to ESXi. Despite VMware Inc.'s publically stated position that ESXi is the future of its hypervisor, you're more likely to see ESX Classic in most data centers.

The Classic edition allocates a block of memory to the ancillary management front end called the service console. With the amount of memory in most hosts moving from 32 GB to the 64 GB or 72 GB range,

it's good practice to max out the amount of memory assigned to it. Currently, VMware assigns a block of memory to the service console on a sliding scale with 300 MB allocated on an 8 GB server and up to 703 MB allocated to a 128 GB server.

I recommend allocating the maximum of 800 MB to the service console when possible to reduce the impact of management agents that are installed on it. The value can be adjusted by modifying the settings in the Configuration tab as well as the Memory option in the Hardware pane (**FIGURE 1**).

Adopting the ESXi version of the

TAKE STOCK
OF YOUR RAM

EVALUATE
CPU NEEDS

SIZE UP
YOUR NETWORK

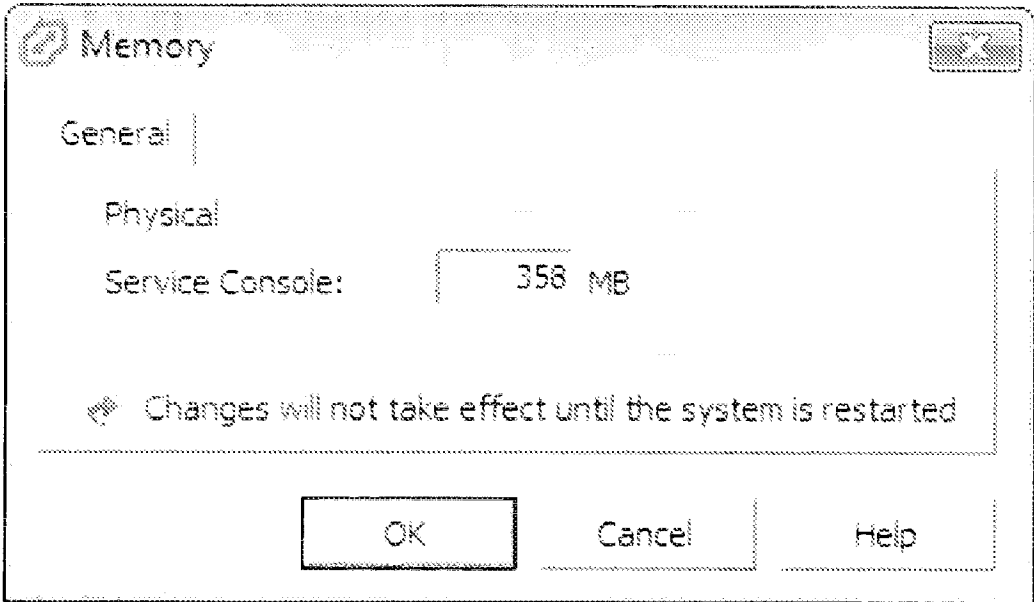
VMWARE ESX

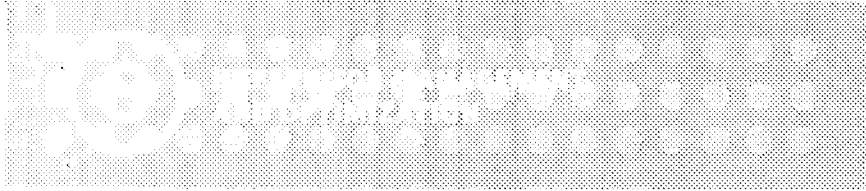
MICROSOFT
HYPER-V

CITRIX
XENSERVER

FIGURE 1:

Use VMware ESX's Configuration tab to adjust the value of memory allotted to the host.





TAKE STOCK
OF YOUR RAM

EVALUATE
CPU NEEDS

SIZE UP
YOUR NETWORK

VMWARE ESX

MICROSOFT
HYPER-V

CITRIX
XENSERVER

platform will avoid this issue altogether. Since it doesn't have a service console, you don't need to worry about configuration issues.

ESXi can be run completely from either USB or SD memory cards, which complete the boot process. Once loaded in memory, ESXi presents a smaller attack service area that should leave it less vulnerable to attacks and easier to patch, and it makes VMware ESXi an attractive option for many data centers. However, VMware claims that it will not produce the service console edition forever.

► **Buying the right amount**

of CPUs: From a CPU perspective, you must select an x64 process because VMware no longer produces a 32-bit version of its platform. I recommend buying the CPU that has the largest onboard memory cache you can reasonably afford. With that said, available memory probably matters more than overall speed.

Although ESX will manage the mapping of VM memory to physical memory using its internal memory management unit (MMU), it's better to have a CPU that offers this MMU functionality as a hardware-assist feature. Intel VT-X CPU, which possesses Extended Page Tables (EPTs) and the AMD CPU, which possesses AMD-V and Rapid Virtualization Indexing (RVI) support, both have this capability.

Additionally, if you want to take advantage of VMware's fault tolerance feature, you should look for a CPU that supports the vLockstep attribute, which allows for the successful mirroring of the primary and mirrored secondary virtual machine.

A common problem with enabling VMware fault tolerance is that using power-saving features like Intel SpeedStep and AMD PowerNow can undermine the feature's reliability. As a general rule, review the BIOS settings that control these features sets.

► **Storage recommendations for**

ESX: I also recommend that businesses using ESX Classic edition use a boot-from-SAN configuration as well as USB or SD cards to boot ESXi systems. The goal should be to use a stateless ESX host in which there is no configuration or end-user data held on the host itself.

When comparing SAN boot or USB boot, SAN booting is more complicated and troublesome from a configuration perspective. It involves a complex interlocking series of settings from the server BIOS, HBA and LUN as well as LUN masking. In the future, VMware will likely support the Preboot Execution Environment (PXE) booting for ESX.

● **Microsoft Hyper-V**

Microsoft Hyper-V is available in several formats: as a standalone

platform, in graphical user interface (GUI) mode Standard edition, Enterprise edition and Datacenter edition. You have the option to run them all in a core mode where the graphical shell is suppressed in favor of a command-line-only distribution.

For corporate customers, the standalone model will probably be insufficient given that it is limited to addressing 32 GB of RAM. A more appealing version would be to run the server core versions of either the

Enterprise or Datacenter edition, which come with generous licensing conditions that allow unlimited copies of the Datacenter edition. That way, companies can create VMs without worrying about the licensing implication of VM sprawl.

As is the case with VMware ESXi, running a stripped down version of Hyper-V also reduces the attack surface from a security perspective and frees up valuable resources.

Currently, Microsoft Hyper-V



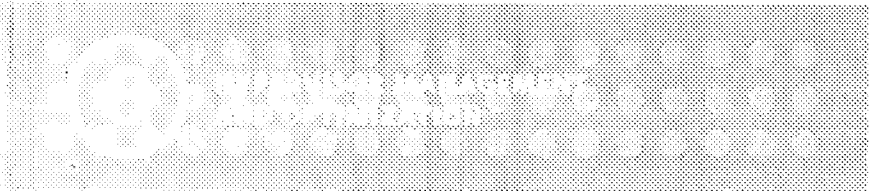
The history of storage protocol wars

FROM A DISK perspective, although storage vendors battle over which is better—Fibre Channel, iSCSI or NFS—each method offers about the same performance characteristics. The correct argument is more about usability, manageability, features and quality of support than raw throughput.

As is the case with CPU resources, you want to avoid oversubscribing the same LUN/volume while storing too many VMs on the same underlying spindles. In the case of excessive IOPS, it's possible to dedicate an entire LUN/volume and the bandwidth of your Fibre Channel HBAs or network interface cards to service read/writes.

Disk I/O rarely constitutes a bottleneck unless excessive queue depths are being created from storing too many virtual machines on too few LUNs/volumes without sufficient spindles.

Organizations often ask what the optimum LUN/volume size is. I don't recommend any hard and fast numbers; however, between 500 GB and 1,500 GB is a safe bet. Using less than 500 GB creates a situation where you need to manage too many volumes that will fill up rapidly. Additionally, creating LUNS/volumes in excess of 1.5 TB usually wastes space, which causes you to run out of IOPS before reaching capacity. ■



does not support memory over-commitment, so optimizing your memory efficiency is critical. Microsoft has indicated that Service Pack 1 will offer a feature for handling memory over-commitment called "Dynamic Memory."

• Network selection and performance:

From a network perspective, it's important to choose synthetic devices over emulated devices when possible. Microsoft doesn't use this specific terminology in the Hyper-V suite, but in parts of the user interface that concern networking, these appear as "Network Adapter" and "Legacy Network Adapter." You can switch from one to the other after you have installed the Integration Components to the VM.

Use both synthetic devices with integration tools to get the best performance from a CPU perspective.

Microsoft recommends using versions of Windows that have been "enlightened" for use on Hyper-V such as Windows Vista, Windows 7 and Windows Server 2008. Older Windows OSes such as Windows 2000 and NT4 lack these enhancements.

At the physical level, Hyper-V will need a significant number of physical NICs—especially if you're using IP-based technologies such as iSCSI. As a rule of thumb, use up to two quad-port NICs to complement the two onboard network interfaces common on most rack-mounted

servers. There also may be extreme cases where you'll want to adjust the guest OS's ReceiveBufferSize and SendBufferSize in the Microsoft registry. If you have a large network load, you might experience heavy traffic loss combined with subsequent retransmits. Microsoft recom-

Although dynamic disks offer better disk space utilization, they're not without a performance hit. Use fixed disks for production VMs and dynamic virtual disks for test and dev

mends increasing the buffer size on a per-virtual-machine basis from 1 MB to 2 MB to alleviate this.

Although dynamic disks offer better disk space utilization, they're not without a performance hit. The best bet is to use fixed disks for production VMs and use dynamic virtual disks for desktops, test and development environments where raw I/O may be less of a pain point.

At the upper end, many people

TAKE STOCK
OF YOUR RAM

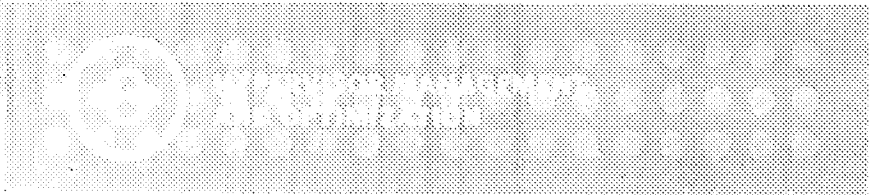
EVALUATE
CPU NEEDS

SIZE UP
YOUR NETWORK

VMWARE ESX

MICROSOFT
HYPER-V

CITRIX
XENSERVER



TAKE STOCK
OF YOUR RAM

EVALUATE
CPU NEEDS

SIZE UP
YOUR NETWORK

VMWARE ESX

MICROSOFT
HYPER-V

CITRIX
XENSERVER

recommend using the Pass-Thru Disk format (PTD), which gives a Hyper-V host the capacity to present LUNs/volumes directly to the virtual machine.

At the disk-level, Microsoft recommends using fixed virtual disks over the newer Dynamic VHD format. With fixed disks, a virtual disk is created upfront as a flat file whenever a VM is created. This means that a 30 GB virtual disk would consume 30 GB of physical storage.

With a dynamic disk, a 30 GB virtual disk would use just a couple of megabytes of physical storage and would grow dynamically on demand as data is written inside it. This represents a better use of physical disk space because you don't waste space storing empty blocks of data that are waiting for the VM to write to them.

- **Hyper-V trouble spots:** Antivirus software configuration can be an area of contention in Microsoft Hyper-V because it can degrade performance. When correctly configured, Hyper-V should not be used as a workstation nor should it access the Internet from its management network. Of course, some data center policies may be non-negotiable, so if you're forced to install an AV product, the general guidelines should not include these locations or these executables until a systemwide scan has been completed:

- Default and custom VM configuration directory, such as C:\ProgramData\Microsoft\Windows\Hyper-V
- Custom VM configuration directories, such as C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks
- Snapshot directories
- Vmms.exe and Vmwp.exe

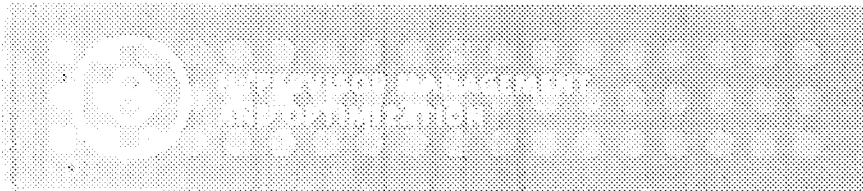
☉ Citrix XenServer

There are several tricks for tuning XenServer specifically for virtual desktop loads, and many of Citrix Systems Inc.'s performance optimization methods center on the company's long history of delivering a client experience to end users.

One of the downsides of virtual desktops is that they consume resources even when end users aren't connected to them.

In XenServer 5.6, Citrix introduced Dynamic Memory Control (DMC), which frees an administrator from allocating a fixed amount of memory to the virtual desktop before powering it on. This could possibly solve the virtual machine memory management paradox—allocating a large amount of memory to VMs will improve their performance, but reduce the number of VMs per host.

Allocating a small amount of memory increases the consolidation ratio but reduces performance. The problem is that you never quite



know how much memory a VM needs, when it needs it or if it will only need it for a certain period of time, such as when the user is connected to his virtual desktop.

Configuring XenServer's Dom0:

XenServer has a privilege VM called Dom0. It acts like a broker for all network communication from VMs to the physical world. Each VM lives inside a DomU, and network communication occurs from the netfront component in DomU to its netback component in Dom0. So, a bottleneck could occur if the Dom0 isn't configured correctly.

Each VM that's created (DomU) will use 6 MB of RAM at power on, and although this isn't a huge amount of memory, the RAM allocation that

comes from the Dom0 partition can add up. At boot up, Dom0 receives an allocation of 752 MB; Dom0

You never quite know how much memory a VM needs, when it needs it or if it will only need it for a certain period of time.

takes 400 MB of this for itself, leaving approximately 352 MB from which each VM (DomU) can take its 6 MB. Once you reach about 60

TAKE STOCK
OF YOUR RAM

EVALUATE
CPU NEEDS

SIZE UP
YOUR NETWORK

VMWARE ESX

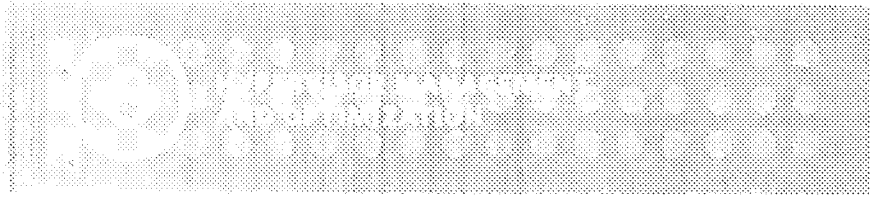
MICROSOFT
HYPER-V

CITRIX
XENSERVER

Storage and capacity planning library

WHEN YOU START researching storage optimization and planning your virtual environment capacity for Citrix XenServer, look to these resources for help.

- ◉ [XenServer Performance Monitoring for Scalability Testing](#)
- ◉ [Evaluate Performance of Block Type Storage Repositories for XenServer](#)
- ◉ [Proper Storage Allocation for Hosted Virtual Desktops](#)
- ◉ [Software iSCSI Storage Repository Detachment](#)



TAKE STOCK
OF YOUR RAM

EVALUATE
CPU NEEDS

SIZE UP
YOUR NETWORK

VMWARE ESX

MICROSOFT
HYPER-V

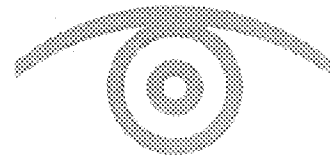
CITRIX
XENSERVER

VMs, the memory pool is full.

This situation is common in a hypervisor; organizations that previously used different versions of VMware ESX will know it has a memory reservation for its management layer. Of course, Microsoft Hyper-V needs a chunk of memory just to be viable. The memory allocations in Citrix XenServer are much more specific. However, incorrect planning can reduce VM performance and degrade the manageability of the host through the XenAPI. And, in a worst-case scenario, it can crash XenServer.

If your performance woes are not RAM related but IOPS bound, I recommend that you avoid individual commands that let you monitor network and disk activity such as **iostat**, **hdparm**, **dd**, **tcpdump**, **netstat** and **ifconfig**. Focus instead on Citrix's various "shell scripts," which pull all of these tools together into handy scripts that send out all of the data you actually need. ■

Mike Laverick is a professional instructor with 15 years experience in technologies such as Novell, Windows and Citrix, and he has been involved with the VMware community since 2003. Laverick is a VMware forum moderator and member of the London VMware User Group Steering Committee. He is also the owner and author of the virtualization website and blog RTFM Education, where he publishes free guides and utilities aimed at VMware ESX/VirtualCenter users. In 2009, Laverick received the VMware vExpert award and helped found the Irish and Scottish user groups. He has had books published on VMware Virtual Infrastructure 3, VMware vSphere4 and VMware Site Recovery Manager.



SearchServerVirtualization.com

Cathy Gagne

Editorial Director

cgagne@techtarget.com

Jo Maitland

Executive Editor

jmaitland@techtarget.com

Colin Steele

Site Editor

csteele@techtarget.com

Michelle Boisvert

Managing Editor

mboisvert@techtarget.com

Martha Moore

Copy Editor

mmoore@techtarget.com

Linda Koury

Art Director of Digital Content

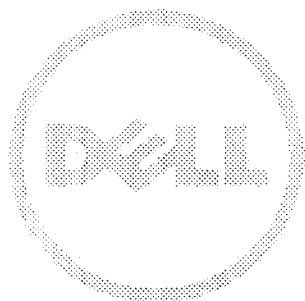
lkoury@techtarget.com

Marc Laplante

Publisher

mlaplante@techtarget.com

©2010 TECHTARGET. ALL RIGHTS RESERVED.



- Virtualization: Consolidation to Cloud Foundation
- Forecast: Cloudy with a Chance of Virtualization
- Implementing and Expanding a Virtualized Environment

About Dell, Inc.:

Dell Inc. (NASDAQ: DELL) listens to customers and delivers innovative technology and services they trust and value. Uniquely enabled by its direct business model, Dell is a leading global systems and services company and No. 34 on the Fortune 500. For more information, visit www.dell.com, or to communicate directly with Dell via a variety of online channels, go to www.dell.com/dellshares. To get Dell news direct, visit www.dell.com/RSS.

VSITE: a scalable and secure architecture for seamless L2 enterprise extension in the cloud

Li Erran Li

Bell Labs, Alcatel-Lucent
600 Mountain Ave, Murray Hill, NJ 07974
Email: erranli@research.bell-labs.com

Thomas Woo

Bell Labs, Alcatel-Lucent
600 Mountain Ave, Murray Hill, NJ 07974
Email: woo@research.bell-labs.com

Abstract—This paper presents an end-to-end architecture, called VSITE, for seamless integration of cloud resources into an enterprise's intranet at layer 2. VSITE allows a cloud provider to carve out its resources to serve multiple enterprises simultaneously while maintaining isolation and security. Resources (allocated to an enterprise) in the cloud provider appears "internal" to the enterprise. VSITE achieves this abstraction through the use of VPN technologies, the assignment of different VLANs to different enterprises, and the encoding of enterprise IDs in MAC addresses. Unlike traditional layer 2 VPN technology such as VPLS, VSITE suppresses layer 2 MAC learning related broadcast traffic from reaching the remote sites. VSITE makes use of location IP (represents location area) for scalable migration support. The MAC or IP address of a VM is not visible in data center core. VSITE hypervisor enforces security mechanisms to prevent enterprises from attacking one another. Thus, VSITE is scalable, secure and efficient, and it facilitates common data center operation such as VM migration. Because VSITE extends enterprise network at layer 2, this offers transparency to most existing applications and presents an easy migration path for an enterprise to leverage cloud computing resources.

Index Terms—seamless L2 network extension, multi-tenant data center, cloud computing

I. INTRODUCTION

A particularly important form of cloud computing is called Infrastructure as a Service (IaaS), which refers to the provision of raw resources such as compute and storage servers from a cloud. Amazon's Elastic Cloud Computing (EC2) solution is a well-known example of IaaS cloud computing. In such a solution, a user is allocated compute/storage resources in the cloud where she can use for launching applications of her choice.

For most enterprises, IaaS represents an intriguing option for scaling their computing needs. Specifically, an enterprise can choose to build its internal infrastructure to satisfy only the average demand, and augment that with resources from an IaaS cloud on an on-demand basis to address demand burst above the average. To enable live VM migration and minimize application configuration it is essential that the network extension can be reached in layer 2.

A public data center needs to accommodate a large number of enterprises (tenants). These tenants need to be logically isolated. Assign each tenant a VLAN throughout the data center is not a scalable solution. There are only 4096 VLANs. It is possible to use VLAN stacking where the outer VLAN ID will be shared by many enterprises, and the inner VLAN

ID identifies each enterprise. However, in this case, each enterprise's L2 broadcast traffic will be flooded throughout the outer VLAN and can potentially be visible throughout the data center.

It is tempting to reuse VPLS technology to interconnect an enterprise with its cloud provider. However, VPLS floods L2 broadcasts from the public data center to the enterprise, vice versa. Each VM can potentially appear in the L2 forwarding table of each switch in the enterprise.

In this paper, we provide a systematic treatment of issues related to supporting seamless enterprise cloud computing and present a scalable architecture, called VSITE¹. VSITE uses a protocol similar to recent CISCO OTV [1] for scalable connection between enterprise networks and cloud resources. The MAC information is exchanged between the cloud edge switch and the enterprise customer edge switch. This is much more scalable than VPLS which uses MAC learning.

VSITE uses VLANs to logically separate enterprises. Unlike Cloudnet [11], VSITE does not assign global VLAN IDs (visible throughout a data center) to enterprises. Instead, VSITE assigns local VLAN IDs that are local to a data center edge location. To ensure packets from one enterprise never reach another enterprise, we encode enterprise IDs in MAC addresses. Specifically, the hypervisor of a VM will ensure that packets can only be sent to or received from MAC addresses of the same enterprise.

VSITE makes minimal assumption of data center internals. VSITE uses Ethernet over IP (e.g. Ethernet over GRE or EnterIP protocol) encapsulation to traverse the **data center core**. VSITE only assumes Ethernet at **data center edge**. L3 switches connect data center edge with data center core².

VSITE introduces the concept of location IP for scalable VM migration. Specifically, each VM has a location IP (locIP). locIP is the IP of any L3 switch that interconnects data center edge and core. The hypervisor of a VM looks up a directory server for the locIP of the destination VM if it is not known. Only the location area of a VM needs to be aware of its current location.

VSITE makes the following contributions:

- VSITE makes public cloud data center resources appear "internal" to an enterprise. VSITE provides a set of

¹A patent based on this work was filed in September 2009

²VSITE design also works well if both core and edge are Ethernet.

networking mechanisms that solves the address space, security and scalability issues.

- VSITE enables dynamic and scalable service offering. Dynamic creation, removal or migration operations on VMs only involves updating the directory service and the relevant elements such as logical customer premise edge router (CE), and the configuration of the hypervisor of a server. Migration within the data center edge is seamless.
- VSITE does not require changes to switches and routers. All the changes are relegated to the CEs and the hypervisors. The overhead is the directory query when information are not cached.
- VSITE prevents L2 attacks such as ARP attacks, MAC flooding attacks performed by one enterprise from adversely impacting other enterprises.

The rest of the paper is organized as follows. In section II, we present the architecture and its design principles. We illustrate the details of VSITE control and data plane in Section III and IV. We then discuss issues in Section V, VI, related work in Section VII and conclude our paper in Section VIII.

II. THE VSITE ARCHITECTURE

The problem of creating a cloud extension to an enterprise is a multifaceted one. A complete solution will touch on resource allocation (e.g., where and how the cloud resources are allocated), networking, monitoring, migration, reporting, etc. We focus mostly on networking and security in this paper as it lays the foundation for most other components.

We begin by defining a *virtual stub* network or *vstub* to be the logical network inside the cloud infrastructure formed by the collection of resources allocated to a specific enterprise. A virtual stub network is logically isolated from resources outside the stub in that resources within a stub can communicate freely while no traffic can cross the stub boundary. Essentially, a stub network is like a virtual private subcloud inside the cloud infrastructure.

We break up the problem of seamless enterprise cloud extension into three components: **virtual stub creation**, and **virtual stub attachment** and **virtual stub isolation and scalability**. We present the overview of VSITE architecture, design considerations and architecture entities.

A. The End-to-End Picture

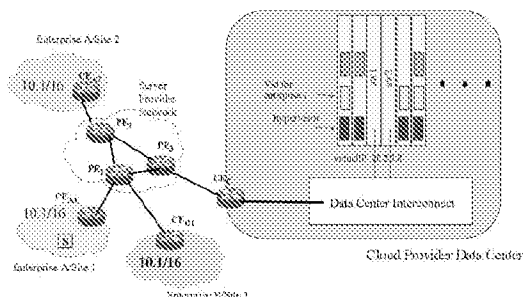


Fig. 1. End-to-end architecture

Figure 1 shows the different components that comprise the end-to-end problem of extending an enterprise into the cloud.

Starting from the left are the physical enterprise sites. Two different enterprises *A* and *B* are shown here, with enterprise *A* having two existing sites *A1* and *A2*.

Virtual Stub Attachment: Connectivity between different enterprise sites including vstub are provided over the service provider network. This is typically provided using some form of VPN technologies. Using standard terminology, CE (customer edge) routers in enterprise sites interface to PE (provider edge) routers in the service provider network to create VPN connectivity. These VPN solutions can include IPsec, Layer 3 MPLS VPN, and Layer 2 VPN such as VPLS, OTV [1]. For example, in a site extension using L3 MPLS VPN case, the stub site will be given an IP subnet prefix that is within the space of the enterprise, all resources within the stub site will be allocated an IP address within that subnet. The subnet prefix is advertised via BGP within the MPLS VPN to all other sites within the enterprise, which then establishes reachability to the stub site. Communication between internal and stub site resources proceeds via standard MPLS encapsulation as defined for L3 MPLS VPN. Some technologies such as IPsec VPN and Cisco OTV [1] do not require special support from Internet service providers. That is, PE routers do not have any specific VPN state.

A virtual stub attachment connects a virtual stub to the enterprise VPN which extends over the service provider network and reach all enterprise sites.

Virtual Stub Creation: A cloud provider is shown on the right side of Figure 1. In fact, it shows a data center of the cloud provider. The cloud provider can be the service provider or a third party provider, and there can be multiple physical data centers. The cloud provider data center interfaces to the service provider network just like an enterprise site. The data center hosts the physical resources such as the compute and storage servers. Typically, these resources are hosted in chassis-based servers (i.e., blade servers) and are virtualized. A blade server has multiple slots each of which can hold a physical server blade. These blades are redundantly connected to a pair of embedded switch within the chassis. Each server blade runs a *hypervisor* which in turn hosts *virtual machines* (VMs) that can be allocated to an enterprise. The different resources inside a data center is connected by a data center network.

In simple terms, a virtual stub network begins at a data center CE, and extends over the data center network to reach all the VMs allocated to an enterprise.

Virtual Stub Isolation and Scalability: Virtual stubs between different enterprise sites must be isolated by default. A cloud provider must be able to support a large number of vstubs. One can make use of VLANs to isolate different enterprises. However, there are only 4096 IDs. VLAN stacking can increase the number of VLANs to 4096*4096. However, broadcast traffic of VLANs can seriously stress the data center networks. All broadcast traffic with the same outer VLAN ID will reach all ports configured with that VLAN ID.

As VMs are created or terminated dynamically in a much

shorter time scale, traditional MAC learning can seriously impact the underlying network: (1) broadcast traffic will reach all switches with the same VLAN configured (2) end host MAC entries will populate switch MAC forwarding tables.

B. Design Considerations

In the following, we look at the key technical requirements and motivate the specific VSITE design feature that address it.

VM configuration transparency and mobility: Many applications may require layer 2 connectivity to different application components, e.g. L2 reachability among front end or backend servers in three-tiered applications. L2 connectivity also makes it easy to support VM mobility. Thus, we choose L2 vstub attachment. Among L2 technologies, there are VPLS, pseudo-wire and OTV. Pseudo-wire is a point-to-point solution. We would like to interconnect multiple sites of a given enterprise. Thus, we choose multipoint-to-multipoint solutions. We make use of OTV-like protocols (OTV is proprietary). The key advantage of OTV-like protocols is that it exchanges MAC addresses among sites using a control plane protocol. This eliminates the cross-site MAC learning related flooding which increases the scalability of vstub attachment.

To further support VM configuration transparency, a VM's hypervisor will intercept the VM's DHCP and ARP messages. A VM will be configured the same way as if it is in the enterprise.

Data center scalability: Each VM is configured with its enterprise IP (entIP). Rapid shrinking or growing of virtual machines (VM) as well as rapid VM migration calls for the separation of names from locations. For each VM, we associate it with a location IP (locIP). One option for locIP is to use the L3 switch IP (note that L2 switch ports are not configured with IP addresses) to which the VM logically connects. If the server hosting a VM is multi-homed to more than one rack switch, then locIP is the virtual IP of the switch master (switches are configured in master or slave by virtual router redundancy protocol (VRRP)).

Note that, we could have used server virtual NIC IP as locIP of an VM. Virtual NIC using NIC teaming technique can provide fault tolerance against one NIC failure. However, VM mobility is handled better when the locIP is the switch IP. If a VM migrates to a different server behind the same switch, then there is no need for routing updates as the locIP does not change.

A specific VM's MAC address is only visible within its location area (the data center edge). We only assume the data center edge is Ethernet. The limited VM MAC visibility increases the scalability of data center core. At the same time, it supports VM mobility much better as the locIP stays the same within the location area.

Data center core transparency: There are two main reasons that we want VSITE to be data center core transparent (i.e. data center core is agnostic of vstub). The first is scalability. Limiting VM's MAC within the edge increases data center core scalability. The second is to accommodate different data center designs. Data center core is still evolving, and there are

many competing technologies, some are composed of purely L2 nodes, some are L3 nodes, and some even propose the use of optical switches [10], [3].

Traffic separation and security: A vstub can be part of an enterprise VLAN logically. To support this, we organize a vstub in a VLAN in the data center. This VLAN does not reach into data center core. In order to support a large number of vstubs, VLAN ID has only local significance. Thus, the VLAN ID of a vstub can be different from the VLAN ID of its enterprise portion. The data center CE does the translation. We will discuss the details later.

Since VLAN IDs are not assigned to enterprises statically, there may be transient situations where traffic of VMs of one enterprise gets sent to VMs of a different enterprise (due to VLAN ID reuse). To prevent this, we choose to encode enterprise ID in the MAC address. There are many encoding schemes. The simplest one is to partition the 48 bit MAC address into a x bit portion which uniquely identifies the enterprise, and a $48 - x$ bit portion that identifies a VM that is local to ToR switch.

Other encoding schemes are possible. All we need is that we should be able to easily figure out the enterprise a given MAC address belongs to. The hypervisor of a VM will check the validity of MAC addresses. That is, if a VM sends a packet to a VM of a different enterprise, the hypervisor will drop the packet. Similarly, if the hypervisor receives a packet where the source and destination enterprise ID are different, the packet will be dropped. Note that VMs in enterprise site should follow the same MAC addressing scheme as in their vstubs. Ideally, the allocations should be coordinated. If not, then the data center CE has to map each VM's MAC in the enterprise site to a unique one that conforms to the addressing scheme.

C. VSITE Architecture Entities

A number of entities work together to create the VSITE architecture. We describe these entities and their roles here.

Cloud Manager: The cloud manager takes enterprise customer requests, and creates vstubs. This includes instantiating the VMs, configuring appropriate network elements such as cloud data center CE.

Directory Server: On an enterprise basis, there is a mapping from entIP to locIP and MAC, possible other information such as VLAN ID. Such mappings are collected in a directory server maintained by the cloud provider; and like a DNS server, queries can be made to retrieve the current mapping.

Cloud Data Center CE (CE_c): Typically, a site CE serves as a gateway for a single enterprise site. In the cloud data center case, its CE must support virtualization as it provides gateway functions for multiple tenants. Cloud data center CE communicates with the directory server to retrieve the up-to-date mapping. Cloud data center CE implements OTV-like protocol which exchanges MAC reachability information with enterprise CE and directory server.

Hypervisor: We assume a hypervisor understands (i.e., is configured with) the enterprise information for each VM it hosts. Specifically, it knows the enterprise membership (i.e., enterprise ID) for each VM, and their corresponding security

parameters. A hypervisor is also responsible for intercepting certain traffic (e.g., L2 broadcast), ARP request and DHCP request. The hypervisor communicates with VSITE data plane to assign an appropriate MAC address for a VM. The hypervisor also relays DHCP messages to DHCP servers.

III. VSITE CONTROL PLANE

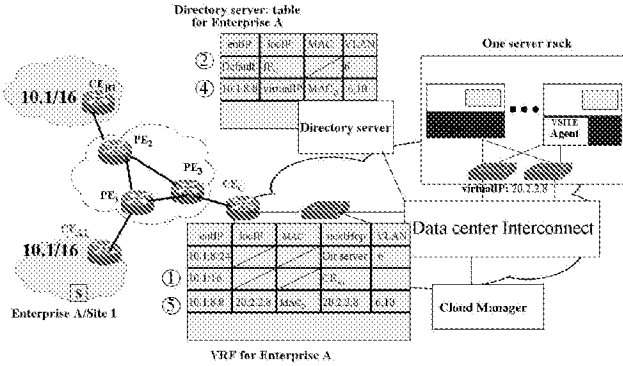


Fig. 2. VSITE control plane

VSITE control plane is shown in Figure 2. An enterprise can request cloud resources via a web portal or programmatic API. These interface to a cloud manager that kicks off actions within the cloud to instantiate/remove a vstub and/or add/subtract resources from a vstub. Such a manager should have interface for an enterprise to configure address plan for its vstub (including internal DHCP server addresses), VM images, security keys, etc.

The intelligence of deciding which data center and servers should specific resources be allocated from is beyond the scope of this paper. We focus on the networking actions that tie those resources into the enterprise once they are allocated.

We describe the typical control plane scenarios below.

vstub Instantiation: As shown in Figure 2, for enterprise A to dynamically instantiate a subnet (say 10.1.8/24) in the cloud provider, a logical CE (virtual router) will be created in CE_C if it does not exist. Once the logical CE is created, a routing entry for the subnet will be configured in the enterprise's VRF table of CE_C . The provider-facing interface of enterprise A's CEs (such as CE_{A1}) will be properly configured. A default entry mapping all enterprise address to the logical CE's IP_C will be installed at the directory server. Packets originating from a vstub VM to an internal enterprise address now will be forwarded to the logical CE, which will then forward it to the enterprise.

VM Instantiation: A VM is identified by its entIP, MAC, and locIP. All these information are obtained during the boot process. Upon booting, the VSITE hypervisor intercepts the DHCP request and relays it to a previously configured per-enterprise DHCP server. If the server sits inside the enterprise, the packet will be properly tunneled to CE_C first using the regular tunneling procedure (will become clear in the next section). The locIP is the address of the switch to which the host hypervisor homes. The entIP, locIP and MAC mapping

is then installed in the directory server (step 4). The directory server may optionally install a routing entry in routing table of the logical CE (step 5).

Any ARP request will also be intercepted by the hypervisor and answered with the destination MAC address retrieved from the directory server.

IV. VSITE DATA PLACE

VSITE data plane is shown in Figure 3. VSITE data plane makes use of the following techniques:

- Ethernet frame are carried using Ethernet over IP protocols such as Ethernet over GRE or EtherIP protocol (RFC3378) between CE_{A1} and CE_C , between CE_C and top-of-rack (ToR) switch (assume ToR is its locIP). For example, CE_C encapsulates the Ethernet frame received from CE_{A1} with an IP header destined to ToR switch of destination (the protocol field of IP header is 97 for EtherIP).
- Since ToR switch will remove the IP header and process the Ethernet frame. To prevent multiple enterprises from using overlapping VLAN IDs, The VLAN ID has to be translated into a locally unique one. This is done at data center CE for traffic from enterprise site. For an Ethernet frame from cloud VMs, the translation is done at the hypervisor, and the Ethernet frame is then encapsulated with an outer IP header.
- For the MAC address of a VM, we can identify which enterprise it belongs to.

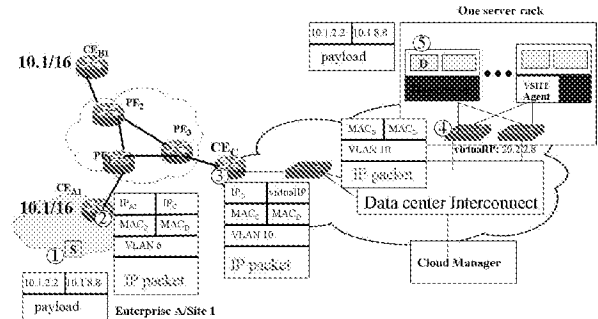


Fig. 3. VSITE data plane

Inbound traffic: Figure 3 illustrates our data plane when S sends a packet to D in the vstub. To avoid excessive ARP flooding CE_{A1} is configured to be the ARP proxy for IP prefixes in the cloud. CE_{A1} and CE_C exchange MAC reachability information using OTV control plane protocol. ARP request from S will be answered by CE_{A1} with D 's MAC address MAC_D . After obtaining destination MAC, S sends its packet (Step 1). When CE_{A1} receives the packet from S , it consults its MAC routing table for destination D . The outgoing interface is the IP address of cloud CE CE_C . Thus, the Ethernet frame is encapsulated with an IP header with destination CE_C (Step 2). The packet is then routed to CE_C . Packets received at CE_C are first decapsulated. They then get encapsulated with another IP header. For each packet, the source is the CE itself,

the destination is the locIP of the destination. The MAC is the MAC of the destination. We need to translate the VLAN to a locally unique one. VLAN 6 is translated into VLAN 10. The VRF entry for MAC_D is kept up-to-date by the directory server. These are done in Step 3. The packet is then sent to the ToR switch. When the ToR switch receives the packet, it will remove the IP header and forwarding in layer 2 (Step 4). Since MAC_D is unique, the packet will be sent directly to the hypervisor of D .

Outbound traffic: When the hypervisor receives a packet from a VM with source, 10.1.8.8 and destination 10.1.2.2. It checks whether it has an entry in its forwarding table. If not, it queries the directory server for the destination locIP . The locIP is the IP of CE_C . The packet is then encapsulated with an IP header (destination is locIP) and routed. Because VM D 's default gateway is its ToR switch, the MAC layer of the hypervisor will append a MAC header with VLAN 10 and its ToR's MAC as L2 destination. Upon receipt at the logical CE, the packet will first be decapsulated, then encapsulated with another IP header (destination CE_{A1}) before routed to the enterprise site with prefix 10.1/16.

Cloud internal traffic: If the source and destination have the same locIP , then the packet will be sent in layer 2 with the appropriate source MAC and destination MAC as well as VLAN ID in the header. If they are different, then the process is the same as outbound traffic except that the locIP and destination MAC will correspond to the destination VM's locIP and destination VM's MAC.

A. VLAN issues

VLAN processing: VM D needs to join in its appropriate VLAN through the hypervisor. Each local switch will only need to be configured with the VLANs of its attached VMs.

Reuse of VLAN ID: VLAN ID may be reused. If a VLAN ID gets reassigned from enterprise A to B due to VM shutdown or migration, VMs of enterprise A may have stale entries and still send packets to VMs of the same VLAN ID in a particular location. However, since the MAC address of different enterprises are partitioned. The packets from enterprise A will be dropped at the destination hypervisor. If MAC address filtering is enabled on VLANs, then enterprise A's packet will be dropped at ToR because the MAC does not match enterprise B (the VLAN is currently allocated to B).

V. DISCUSSION

A. Security

vstub attachment security: By default, an OTV like protocol only transport Ethernet frames across geographically separated data centers. It does not specify virtual private connection. However, this can be easily achieved by using IPsec encapsulation between CE_{A1} and CE_C .

VM attack from other tenants: The hypervisor implements a virtual switch with VLAN support. Broadcast and multicast traffic is only sent to the VMs with the same VLAN ID of the same enterprise. Recall that we encode enterprise ID in the MAC address. Thus, it is not possible to carry out MAC

address spoofing attack without compromising the hypervisor. We assume the hypervisor is secure.

It is not possible for a VM to impersonate as a VM of another enterprise. The hypervisor knows which VM belongs to which enterprise. It is also not possible to carry out a DDoS attack. The attacker's hypervisor will drop those packets.

VM attacks through covert channels have been uncovered recently [8]. Our design mitigates these attacks as VMs do not have cloud provider's publicly reachable IP addresses configured. Since these VMs are configured with enterprise IP addresses, in most cases, these VMs should not be reachable from Internet hosts. Thus, inducing workload by VMs of other tenants is not possible. Covert channels attacks are hard to rule out as pointed out in [8]. Thus, to be free from these attacks, VMs of different tenants should not co-locate at the same physical machine.

VLAN networking attack from other tenants: In traditional Ethernet, it is possible to mount MAC flooding attack of one VLAN from hosts belong to another VLAN. MAC flooding exhaust MAC forwarding table entries. Thus, MAC frames whose destinations are kicked out the table will have to be flooded throughout the VLAN. The problem is that forwarding table of different VLANs are shared. In VSITE, all Ethernet frames have to go through the hypervisor. Hypervisor will drop frames with invalid MAC addresses. In VSITE, data center edge switches are designed to hold maximum MAC entries if all physical machines in the edge are instantiated with the maximum number of VMs.

B. Ethernet data center core and edge

In the case that both core and edge are Ethernet, all we need is to replace the current encapsulation protocol with MACinMAC protocol. Instead of location IP, we will have location MAC. Note that currently most data center switches do not support MACinMAC.

C. Bandwidth isolation

Bandwidth isolation will depend on the bandwidth allocation scheme. If each enterprise is allocated a pre-specified amount of total bandwidth, then we can use cloud-wide rate limiting [7] to achieve bandwidth isolation.

Cloud provider may not fix the bandwidth allocation for each enterprise. Rather it may just enforce fairness. Fairness can be enforced in VSITE by fair bandwidth allocation among VLANs. In particular, each enterprise gets the same weight (if all enterprises have the same priority). This weight is split among all VLANs of the enterprise. A control protocol can adjust the weight in switches (e.g. ToR switch).

D. L2 broadcast

L2 broadcast of a VLAN is nicely supported in VSITE. If S broadcasts, CE_{A1} will encapsulate the Ethernet frame with the IP address of CE_C (if there are multiple MAC forwarding entries for the broadcast address, it will be done for each entry). The packet will be routed first to CE_C , then ToR switch where it will be released into L2.

When VM D broadcasts, each VM in the local VLN 10 will receive the packet. When ToR receives the packet, it will be transported to CE_C using Ethernet over IP protocol. This in turn gets sent to CE_A .

VI. IMPLEMENTATION AND SCALABILITY

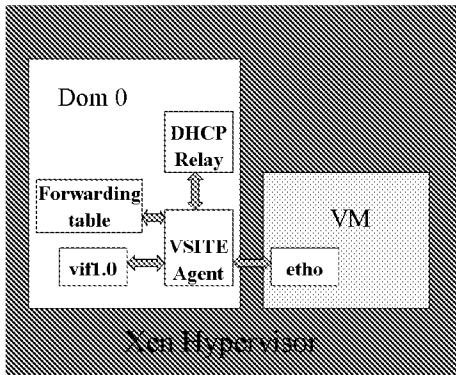


Fig. 4. VSITE hypervisor implementation in Xen

An example Xen-based implementation of our hypervisor is shown in Figure 4. The key operation in control plane is a directory query when a forwarding entry is not found. This has been shown to be very scalable [4]. The operations in the data plane are IP encapsulation. This overhead is small.

We briefly discuss the scalability of our solution here. Suppose a large data center design [9] is built with 100 containers, each container having 32 racks and each rack containing 64 servers, which yields a total number of 204,800 physical servers. Assuming each server can host 8 VMs; each rack can hold 2 /24 subnets if every address is allocated, and 4 /24 subnets if only half of each subnet is allocated. Assume we need ToR switches as the locIPs. With all ToR switches in a rack sharing one virtual IP (using VRRP), this results in 100*32 locIP and at most 3200*4 subnets. Each subnet can be used to extend a VLAN from an enterprise. L2 traffic for a VLAN is confined to reach only the 64 servers in the rack.

VII. RELATED WORK

The work most closely related to ours is CloudNet [11], Amazon VPC and VPN-Cubed [2]. CloudNet relies on the VLAN feature for tenant separation and thus is much less scalable in terms of the number of virtual private clouds (VPCs) or enterprises it can support. In addition, VPLS flood L2 broadcast to the enterprise. Amazon VPC offers seamless extension in L3. Not much technical details are known. VPN-Cubed is a commercial product; it is basically an overlay solution.

Other related work are data center networking [4], [6], [5]. The idea of separating location address from actual address has been applied in these data center networking papers. However, they do not discuss any support for private address space and security isolation among enterprise users.

VIII. CONCLUSION AND FUTURE WORK

Today's enterprises can benefit significantly if resources can be tapped seamlessly and dynamically from a public cloud. We study the problem of providing such cloud extension in this paper. We divide the problem into two related parts: vstub creation and vstub attachment, which adds significant clarity to the whole design space. We then present a scalable and secure architecture called VSITE that offers a layer 2 solution for enterprise vstub construction. VSITE uses a combination of location IP and enterprise ID (encapsulated in MAC) to tunnel enterprise packets with potentially overlapping addresses. A key design goal of VSITE is to minimize the impact of VM dynamics on the underlying network configuration thus making it highly scalable. We are implementing VSITE in our test network.

IX. ACKNOWLEDGMENT

We thank Terry Lam from UCSD for helpful comments.

REFERENCES

- [1] Cisco. Overlay transport virtualization (otv). http://www.cisco.com/en/US/prod/sw/switches/ps9441/nexus7000_promo.html.
- [2] C. F. T. Corp. Vpn-cubed: customer controlled security for the cloud. http://www.cohesiveft.com/Cube/VPN/VPN-Cubed_Custom_Enterprise_Configuration/.
- [3] N. Farrington and et al. Helios: A hybrid electrical/optical switch architecture for modular data centers. In *ACM SIGCOMM*, 2010.
- [4] A. Greenberg, N. Jain, S. Kandula, C. Kim, P. Lahiri, D. Maltz, P. Patel, and S. Sengupta. V12: A scalable and flexible data center network. In *ACM SIGCOMM*, 2009.
- [5] C. Kim, M. Caesar, and J. Rexford. Floodless in seattle: a scalable ethernet architecture for large enterprises. In *ACM SIGCOMM*, 2008.
- [6] A. Pamboris, N. Farrington, N. Huang, P. Miri, S. Radhakrishnan, V. Subramanya, and A. Vahdat. Portland: A scalable fault-tolerant layer 2 data center network fabric. In *ACM SIGCOMM*, 2009.
- [7] B. Raghavan, K. Vishwanath, S. Ramabhadran, K. Yocum, and A. C. Snoeren. Cloud control with distributed rate limiting. In *ACM SIGCOMM*, 2007.
- [8] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In *ACM CCS*, 2009.
- [9] R. systems. Ice cube modular data center.
- [10] G. Wang and et al. c-through: Part-time optics in data centers. In *ACM SIGCOMM*, 2010.
- [11] T. Wood, A. Gerber, K. K. Ramakrishnan, and J. V. D. Merwe. The case for enterprise-ready virtual private clouds. In *USENIX HotCloud*, 2009.

A Survey on Virtual Machine Security

Jenni Susan Reuben
Helsinki University of Technology
jreubens@cc.hut.fi

Abstract

Virtualization plays a major role in helping the organizations to reduce the operational cost, and still ensuring improved efficiency, better utilization and flexibility of existing hardware. "Virtualization is both an opportunity and a threat - says Patrick Lin, Senior director of Product Management for VMware" [4]. This paper presents a literature study on various security issues in virtualization technologies. Our study focus mainly on some open security vulnerabilities that virtualization brings to the environment. We concentrate on security issues that are unique for virtual machines. The security threats presented here are common to all the virtualization technologies available in the market, they are not specific to a single virtualization technology. We provide an overview of various virtualization technologies available in the market at the first place together with some security benefits that comes together with virtualization. Finally we provide a detailed discussion of several security holes in the virtualized environment.

KEYWORDS: Virtualization, Security, Threats, Benefits.

1 Introduction

Virtualization - A technology that has an enormous effect in today's IT world. It is a technique that divides a physical computer into several partly or completely isolated machines commonly known as virtual machines (VM) or guest machines. Multiple of these virtual machines can run on a host computer, each possessing its own operating system and applications. This gives an illusion to the processes on these virtual machines as if they are running on a physical computer, but in reality they are sharing the physical hardware of the host machine. The software that allows multiple operating systems to use the hardware of the physical machine is called a hypervisor or a control program. Hypervisors sit between the operating system of the host machine and the virtual environment. There are various virtualization technologies available in the market, having their own merits and demerits.

In non-virtual environment, the applications running on the machine can see each other, and in some cases can even communicate with each other, whereas in virtual environment [7] the programs running in one guest machine are isolated from the programs running in another guest machine, in other words guest machines "provide what appear to be independent coexisting computers" [7] to their running programs. The degree of isolation should be strong enough that

the vulnerabilities in one virtual machine should not affect either the virtual machines or the underlying host machine.

The computer that is being virtualized is of no difference from the computer that is not virtualized. The virtualized environment is vulnerable to all the traditional attacks and exploits that are common to the normal environment. The case is even worse in the virtualized environment, where there are several virtual computers running. The security expectations are higher in here because "there are more systems to protect" [4], more possible points of entry, more holes to patch and there are more interconnection points in the virtualized environment [4]. Attackers and Hackers are already been actively developing new malware programs for virtual machine environment. "Root kit infections, malware that detects a virtual environment and modifies itself accordingly" [4, 11] are some of them. "Low-level hypervisor attacks, and deployment of malicious virtual systems" [4] are few possible attacks that are unique to this environment.

On the other hand new security protection programs are also emerging in the market every now and then from different vendors, but most of these security solutions are mainly focused on hypervisor. Since hypervisor is a new layer between the host's OS and virtual environment, it creates new opportunities for the malicious programs. And more over, hypervisor is basically a software program, so it has all the traditional software bugs and the security vulnerabilities as any software have. One of such product that hits the market recently is SHype [4], a new secure hypervisor that binds security policies to the virtual environment. A good debate on recent security solutions can be found on [10].

However, virtual machine security is more than just deploying a secure hypervisor to the environment. Virtualization technologies are still evolving. Newer versions with added features are introduced before the security consequences of the older version has been fully studied. This work analyzes the general security threats in a virtual environment and suggests possible solutions for few of the mentioned threats.

Understanding of virtualization technologies greatly helps to understand the security consequences that occur in the environment. Sec. 3 discuss the back ground of various virtualization technologies together with some security benefits offered by these virtualization technologies and finally Sec. 4 analyze the security issues concerning virtualization.

2 Research Methodology

This paper is a literature survey that analyse various issues concerning security in virtual machine environment. This

work provides an overview of security consequences arises in a virtualized environment. However this paper does not provide one perfect solution for all the described threats. But do provide an understanding of how these threats can be avoided while implementing virtualization.

3 Background

Virtualization was first developed in 1960's by IBM Corporation, originally to partition large mainframe computer into several logical instances and to run on single physical mainframe hardware as the host. This feature was invented because maintaining the larger mainframe computers became cumbersome. The scientist realized that this capability of partitioning allows multiple processes and applications to run at the same time, thus increasing the efficiency of the environment and decreasing the maintainance overhead. By day to day development, virtualization technologies has rapidly attains popularity in computing, in fact it is now proven to be a fundamental building block for today's computing [14].

Although the main focus of this paper is to provide an overview of security vulnerabilities in a virtual environment. It is worth mentioning some of the security benefits that comes together with virtualization.

Two primary benefits offered by any virtualization technology are 1.Resource sharing and 2.Isolation. Resource sharing - Unlike in non-virtualized environment where all the resources are dedicated to the running programs, in virtualized environment the VMs shares the physical resources such as memory, disk and network devices of the underlying host. The resources are allocated to the virtual machine on request. Hypervisors plays a significant role in resource allocation.

Isolation - One of the key issue in virtualization, provides isolation between virtual machines that are running on the same physical hardware. Programs running in one virtual machine cannot see programs running in another virtual machine. This is contrast to non-virtual environment where the running programs can see each other and if allowed can communicate with each other.

Virtualization provides a facility of restoring a clean non infected environment even the underlying system is infected by malicious programs. Since, Virtualization provides an isolated environment this can be used for debugging malicious programs. and also to test new applications.

Virtualization can be done in several ways. There are various virtualization technologies available in the market that helps to virtualize the environment. Depending on the needs and goals of the organization, one virtualization technology is better than the other. This section gives an overview of some of the existing virtualization technologies.

Before going into the details of different virtualization technologies, Fig. 1 gives a basic idea of a virtual machine environment.

In Fig. 1 [6] there are two virtual machines running on top of a physical computer possessing their own operating system and applications. Every guest machines appears to be an independent computer for their running processes. As already mentioned, Hypervisor layer is the host software layer

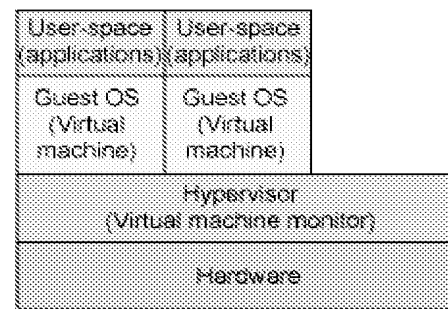


Figure 1: Overview of a virtual machine environment

that provides the ability to run multiple operating system on a physical hardware. It sits between the host physical hardware and the guest machines.

3.1 Full virtualization

In this approach the hypervisor simulates several logical instances of completely independent virtual computers possessing its own virtual resources. These virtual resources included IO ports and DMA channels. Therefore, each virtual machine can run any operating system supported by the underlying hardware. Besides the fact, that this is the most commonly used virtualization technology, true full virtualization where the virtual processors have to reproduce the CPU operations of the host machine is hard to achieve. More over, the overhead of handling these CPU operations makes true full virtualization difficult to manage. However the virtual machine environment that provides "enough representation of the underlying hardware to allow guest operating systems to run without modification can be considered to provide "Full Virtualization" [7].

In this kind of setup the I/O devices are allotted to the guest machines by imitating the physical devices in the virtual machine monitor; interacting with these devices in the virtual environment are then directed to the real physical devices either by the host operating system driver or by the "hypervisor driver [7].

3.2 Paravirtualization

Unlike full virtualization, in paravirtualization the running guest OS should be modified in order to be operated in the virtual environment. Paravirtualization is a subset of server virtualization, which provides a thin software interface between the host hardware and the modified guest OS. An interesting fact in this technology is that the guest machines are aware of the fact that they are running in a virtualized environment.

One of the main characteristics of paravirtualization technology is, the virtual machine monitor is simple which allows paravirtualization to achieve performance closer to non-virtualized hardware.

Device interaction in paravirtualized environment is very similar to the device interaction in full virtualized environment, the virtual devices in paravirtualized environment also rely on physical device drivers of the underlying host [8].

3.3 Application virtualization

In Application virtualization, the user is able to run a server application locally using the local resources without needing the complexity of completely installing this application on his/her computer. Such virtualized applications are designed to run in a small virtual environment containing the only the resources needed for the application to execute. Thus in application virtualization each user have an isolated application environment virtually. This small isolated virtual environment acts as a layer between the application and the host operating system [8].

3.4 Hardware support virtualization

This approach has recently gains attention when Intel and AMD released their processors with inbuilt hardware which supports virtualization. The hardware support virtualization architecture creates a trusted "root mode" and an untrusted "non-root mode". The hypervisor resides in the root mode whereas all the guest operating systems reside in the non-root mode. Hypervisor is responsible for resource allocation and I/O device interaction. Since the hypervisor reside in the root mode the guest operating systems calls out for the hypervisor in order to process their requests for resources by means of a special virtualization instruction known as hypercalls [7].

3.5 Resource virtualization

Virtualizing system specific resources such as "storage volumes, name spaces and the network resources [8]" is known as resource virtualization. There are various approaches to perform resource virtualization. Some of them are,

- Aggregating many individual components into larger resource pool
- Grid computing or computer clusters where multiple discrete computers are combined to form a large super-computers with enormous resources
- partitioning a single resource such as disk space into number of smaller and easily accessible resources of same type

3.5.1 Storage virtualization

Storage virtualization is a form of Resource virtualization, where a logical storage is created by abstracting all the physical storage resources that are scattered over the network. First the physical storage resources are aggregated to form a storage pool which then forms the logical storage. This logical storage which is the aggregation of scattered physical resources appears to be a single monolithic storage device to the user.

4 Security vulnerabilities in virtualization

Most of security flaws identified in a virtual machine environment are very similar to the security flaws associated with

any physical system. The following are some general flaws that are unique [9] to the virtual environment.

4.1 Communication between VMs or Between VMs and host

One of the primary benefits that virtualization bring is isolation. This benefit, if not carefully deployed become a threat to the environment. Isolation should be carefully configured and maintained in a virtual environment to ensure that the applications running in one VM dont have access to the applications running in another VM. Isolation should be strongly maintained that break-in into one virtual machine should not provide access either to virtual machines in the same environment or to the underlying host machine.

Shared clipboard in virtual machine is a useful feature that allows data to be transferred between VMs and the host. But this useful feature can also be treated as a gateway for transferring data between cooperating malicious program in VMs. In worst case, it is used to "exfiltrate data to/from the host operating system [7]".

In some VM technologies, the VM layer is able to log keystrokes and screen updates across the virtual terminals, provided that the host operating system kernel has given necessary permission. These captured logs are stored out in the host, which creates an opportunity to the host to monitor even the logs of encrypted terminal connections inside the VMs.

Some virtualization avoids isolation, in order to support applications designed for one operating system to be operated on another operating system, this solution completely exploits the security bearers in both the operating systems. This kind of system, where there is no isolation between the host and the VMs gives the virtual machines an unlimited access to the host's resources, such as file system and networking devices. In which case the host's file system becomes vulnerable [7].

4.2 VM Escape

Virtual machines are allowed to share the resources of the host machine but still can provide isolation between VMs and between the VMs and the host. That is, the virtual machines are designed in a way that a program running in one virtual machine cannot monitor, or communicate either with programs running in other VMs or with the programs running in the host. But in reality the organizations compromise isolation. They configure flexible isolation to meet their organization needs which exploits the security of the systems. New software bugs were already introduced to compromise isolation [2].

One such example of this kind of attack is VM escape. VM escape is one of the worst case happens if the isolation between the host and between the VMs is compromised. In VM escape, the program running in a virtual machine is able to completely bypass the virtual layer (hypervisor layer), and get access to the host machine. Since the host machine is the root, the program which gain access to the host machine also gains the root privileges basically escapes from the virtual

machine privileges. This result in complete break down in the security framework of the environment [7].

This problem can be solved by properly configuring the host/guest interaction.

4.3 VM monitoring from the host

Host machine in the virtual environment is considered to be the control point and there are implications that enable the host to monitors and communicate with the VM applications up running. Therefore it is more necessary to strictly protect the host machines than protecting distinctive VMs.

Different virtualization technologies have different implications for the host machine to influence the VMs up running in the system. Following are the possible ways for the host to influence the VMs [7].

- The host can start, shutdown, pause and restart the VMs.
- The host can able to monitor and modify the resources available for the virtual machines.
- The host if given enough rights can monitor the applications running inside the VMs.
- The host can view, copy, and likely to modify the data stored in the virtual disks assigned to the VMs.

And particularly, in general all the network traffic to/from the VMs pass through the host, this enables the host to monitor all the network traffic for all its VMs. In which case if a host is compromised then the security of the VMs is under question. Basically in all virtualization technologies, the host machines are given some sort of basic rights to control some actions such as resource allocations of the VMs running on top. But care should be taken when configuring the VM environment so that enough isolation should be provided which avoids the host being a gateway for attacking the virtual machine [7].

4.4 VM monitoring from another VM

As mentioned several times earlier in Sec. 3 and in Sec. 4 isolation plays a vital role in virtualization. It is considered as a threat when one VM without any difficult may be allowed to monitor resources of another VM. Thanks to today's modern CPUs, which comes with a built in memory protection feature. The hypervisor who is responsible for memory isolation can make use of this feature; this memory protection feature prevents one VM seeing the other VM's memory resources. And more over the VMs does not have the possibility to directly access the file system of the host machine, so its impossible for a VM to access the virtual disk allocated to another VM on the host.

When comes to the network traffic, isolation completely depends on the connection (network) setup of the virtualized environment. If the host machine is connected to the guest machine by means of physical dedicated channel, then its unlikely that the guest machine can sniff packets to the host and vice versa. However in reality the VMs are linked to the host machine by means "virtual hub" or by a virtual switch.

In which case, it enables the guest machines to sniff packets in the network or even worse that the guest machines can use ARP poisoning to redirect the packets going to and coming from another guest [7].

Authenticating the network traffic could be a solution the problem described above.

4.5 Denial of Service

In virtual machine architecture the guest machines and the underlying host share the physical resources such as CPU, memory disk, and network resource. So it is possible for a guest to impose a denial of service attack to other guests residing in the same system.

Denial of service attack in virtual environment can be described as an attack when a guest machine takes all the possible resources of the system. Hence, the system denies the service to other guests that are making request for resources, this is because there is no resource available for other guests.

The best approach to prevent a guest consuming all the resources is to limit the resources allocated to the guests. Current virtualization technologies offer a mechanism to limit the resources allocated to each guest machines in the environment. Therefore the underlying virtualization technology should be properly configured, which can then prevent one guest consuming all the available resources, there by preventing the denial of service attack [7].

4.6 Guest-to-Guest attack

As mentioned in Sec. 4.3 it is important to prevent the host machine than the individual VMs. If an attacker gains the administrator privileges of the hardware then its likely that the attacker can break-in into the virtual machines. It is termed as guest-to-guest attack because the attacker can able to hop from one virtual machine to another virtual machine provided that the underlying security framework is already broken [4].

4.7 External Modification of a VM

There are some sensitive applications exists which rely on the infrastructure of the VM environment. These applications running inside a virtual machine requires the virtual machine to be a trusted environment to execute that application. If a VM is modified for some reason, the applications can still be able to run on the VM but the trust is broken. Sudhakar and Andrew [3] in their paper emphasis more attacks on application virtualization.

A best solution for this problem is to digitally sign the VM and validating the signature prior to the execution of this sensitive applications [7].

4.8 External modification of the hypervisor

As mentioned earlier in Sec. 4.4 hypervisor is responsible for providing isolation between the guest machines. The VMs are said to be completely isolated or "self protected" [7, 2] only if the underlying hypervisor behaves well. A badly behaved hypervisor will break the security model of the system.

There are several solutions exists for this problem, one of the recommended solution is to use secure hypervisor like SHype [4] to ensure security in the hypervisor layer. Another solution is to protect the hypervisor from unauthorized modifications [7] or enable the guest machines to validate the hypervisor.

5 Conclusion

The paper has presented some of the security flaws in the virtual machine environment. Some of the threats presented here may be considered as benefits in some situations, but they are presented here so that proper care should be taken while designing and implementing the virtual environment.

Virtualization brings very little added security to the environment. One of the key issue is that everyone should be aware of the fact that virtual machines represent the logical instance of an underlying system. So many of the traditional computer threats apply the same to the virtual machines also. Another issue that makes the security consequences difficult to understand is that, there are so many different types of virtualization technologies available in the market. Each of it has its own merits and demerits, each virtualization deployment is different depending on the need for the virtualization. It is common that any single virtualization technology will not provide shield to all the security issues arise. However, the key to create a good virtualization environment is to study carefully the environment that is to be virtualized, the needs and goals of the organization, and taking into consideration all the possible security issues that puts the virtual machines at risk. Finally carefully design the virtual environment with the help of correct virtualization technology that matches the goals.

Majority of the security issues presented here concerns the security of the host and the hypervisor. If the host or the hypervisor is compromised then the whole security model is broken. Attacks against the hypervisor becoming more popular among the attackers realm [11]. Therefore after setting up the environment, care should be taken to ensure that the hypervisor is secure enough to the newly emerging threats, if not patches has to be done. Patches should be done frequently so that the risk of hypervisor being compromised will be avoided [5].

Virtualization is a powerful solution to reduce the operational costs in today's computing but if done wrong it become as a threat to the environment. While implementing, exaggerate the security model to with stand the attacks. And as mentioned earlier keep monitoring for new developments that emerges in this field and continue to stay up to date.

References

- [1] P. Ferrie. *Attacks on virtual Machine Emulators*. SYMANTEC ADVANCED THREAT RESEARCH. http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf.
- [2] T. Garfinkel and M. Rosenblum. *When Virtual is Harder than Real: Security Challenges in Virtual Machine Bases computing Environments*. Stanford University Department of Computer Science. <http://www.stanford.edu/~talg/papers/HOTOS05/virtual-harder-hotos05.pdf>.
- [3] S. Govindavajhala and A. W. Appel. *Using Memory Errors to Attack a Virtual Machine*. Princeton University. <http://www.cs.princeton.edu/sip/pub/memerr.pdf>.
- [4] K. J. Higgins. Vm's create potential risks. Technical report, darkREADING, 2007. http://www.darkreading.com/document.asp?doc_id=117908.
- [5] B. Huston. Security tip: 3 steps towards securing virtual machines. *Security*, September 2007. http://security.itworld.com/4367/nlssecurity071009/page_1.html.
- [6] M. Jones. *Discover the Linux Kernel Virtual Machine*. IBM. <http://www-128.ibm.com/developerworks/linux/library/l-linux-kvm/>.
- [7] J. Kirch. Virtual machine security guidelines. *The center for Internet Security*, September 2007. http://www.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf.
- [8] A. Mann. The pros and cons of virtualization. *BTQ*, 2007. <http://www.btquarterly.com/?mc=pros-cons-virtualization\&page=virt-view%research>.
- [9] D. Marshall. Whitepaper: Virtual machine security guidelines. *InfoWorld*, September 2007. http://weblog.infoworld.com/virtualization/archives/2007/09/whitepaper_%virt.html.
- [10] E. Messmer. Security in the 'virtual machine'? *NETWORKWORLD*, April 2006. <http://www.networkworld.com/weblogs/security/012014.html>.
- [11] R. Naraine. Vm rootkits: The next big threat. *eWeek*, March 2006. <http://www.eweek.com/article2/0,1759,1936666,00.asp>.
- [12] R.P.Goldberg. Architecture of virtual machines. In *Proceedings of the workshop on virtual computer systems*, pages 74 – 112. THE ACM, 1973.
- [13] R.P.Goldberg. Survey of virtual machine research. In *Computer*, volume 7, pages 34–35. IEEE, June 1974.
- [14] VMware. *VMware security center*. <http://www.vmware.com/support/security.html>.



Espacenet

Bibliographic data: RU2406138 (C1) — 2010-12-10

SECURITY SYSTEM FOR VIRTUAL COMPUTER SYTEM

Inventor(s): ANDREEV STANISLAV VALER EVICH [RU]; DRAGAL CHUK VLADISLAV KONSTANTINOVICH [RU]; POPOV EVGENIJ ALEKSANDROVICH [RU] ± (Андреев Станислав Валерьевич (RU), ; Драгальчук Владислав Константинович (RU), ; Попов Евгений Александрович (RU))

Applicant(s): SAMSUNG ELECTRONICS CO LTD [KR] ± (KORPORATSIJA "SAMSUNG EHLEKTRONIKS KO., LTD.")

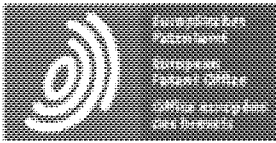
Classification: - **international:** **G06F12/08; G06F21/20**
- **cooperative:**

Application number: RU20090123225 20090618

Priority number(s): RU20090123225 20090618

Abstract of RU2406138 (C1)

FIELD: information technology. ^ SUBSTANCE: security system for a virtual computer system having a hardware part connected to at least one virtual machine through a virtual machine monitor which has a security policy control module, connected to a security subsystem having connected adjustment module and at least one security module connected to the virtual machine. ^ EFFECT: high efficiency and short response time. ^ 3 dwg



Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION RU2406138

SYSTEM OF SECURITY OF THE VIRTUALIZED COMPUTER SYSTEM

The invention relates to the security of computer systems, namely, to the security systems of virtualized computer systems, and can be used in computer devices of various types with different architectural and operating systems that support virtualization capabilities.

The approach to virtualization capabilities associated with a virtual machine monitor (VMM) is in fact a typical way to create multiple virtual machines on a single real hardware platform. A virtual machine monitor is a computer program that performs full or partial monitoring of the resources of a real computer system. It provides an isolated environment by virtualizing hardware resource data. A virtualized environment is called a virtual machine (VM). A virtual machine can access virtual resources. Attempts to access virtual resources for virtual machines are controlled by the security subsystem. At the same time, from the point of view of the security subsystem, the virtual machine is the subject of the operation of circulation, and the resource to which it refers, the object. The security subsystem contains several (one or more) different elements, called security modules. When a virtual machine monitor organizes access to system resources, security modules decide to access subjects to objects based on the loaded security policy.

The security subsystem receives these decisions in a certain sequence and takes the final decision on their basis. In existing virtualization systems, the security module interrogation sequence is hard-coded. The performance aspect is not taken into account or it is determined empirically in determining this sequence. Since decisions can be made very often and the sequence of interrogation of security modules may not be optimal, this can lead to a significant deterioration in the system's performance: a reduction in overall performance and response time.

The Xen virtualization system with the sHype security subsystem, developed by IBM, is well known (cf. Research Report RC23629: R.Sailer, T.Jaeger, E.Valdez, R.Perez, S.Berger, JL Griffin, L. van Doorn: Building a MAC-based Security Architecture for the Xen Opensource Hypervisor [1] and the Research Report RC23511: R.Sailer, E.Valdez, T.Jaeger, R.Perez, L. van Doorn, JLGriffin, S.Berger: sHype: Secure Hypervisor Approach to Trusted Virtualized Systems [2]). The sHype architecture (IBM) supports the implementation of various security modules (Chinese Wall, Biba, Bell-LaPadula, etc.).

The closest to the claimed invention is the security system of a virtualized computer system described in patent EP 2,037,657 [3], comprising a hardware associated with at least one virtual machine via a virtual machine monitor, wherein the virtual machine is configured to forward an access request to a virtual machine monitor configured to process the access request. This system was chosen as a prototype of the claimed invention.

The architecture of the analog and prototype systems described above assumes that the sequence of obtaining solutions from the security modules is based on the required security and is hard-coded. The performance aspect is not taken into account or it is determined empirically, which may not correspond to the real state. In systems with this architecture, overall system performance and system response time may deteriorate, especially if several complex security modules are used. In addition, this architecture does not provide functionality for recording events that occur in the security system.

The aim of the claimed invention is to create a security system for a virtualized computer system with increased performance and reduced response time.

The task is solved by creating an optimized sequence of polling the security modules and interrogating the modules in this sequence, and all modules are not required to be polled, if, after polling some modules, the information received is sufficient to make a decision. In addition, the subsystem of security added the ability to register events occurring in it. Event logging functions facilitate the administration of the security subsystem.

The technical result is achieved by creating a security system of a virtualized computer system comprising a hardware associated with at least one virtual machine through a virtual machine monitor that includes a security policy management module connected to a security subsystem

comprising a tuning module connected to each other and, at least one security module connected to the virtual machine, wherein the virtual machine is configured to forward the request access to the virtual machine monitor configured to process the access request, wherein the security subsystem is configured to interrogate the security modules, obtain permission from them and, based on the received decisions on the admission of the final approval decision, and the tuning module is executed with the ability to implement the function to configure the collection of information on the number of polls of each security module and the time spent on each of the polls, and with the possibility of determining on

For a better understanding of the claimed invention, a detailed description thereof will now be given with the corresponding drawings.

1. General scheme of the security system of the virtualized computer system according to the invention.

Fig. 2. Detailed scheme of the security system of the virtualized computer system according to the invention.

FIG. 3. The algorithm of the security system operation of the virtualized computer system according to the invention.

Let us consider the principle of functioning of the claimed invention. The claimed security system of the virtualized computer system (FIGS. 1-3) comprises a hardware part 1 associated with at least one virtual machine 2 via a virtual machine monitor 3 that contains a security policy management module 4 connected to a security subsystem 5 comprising connected to each other by the tuning module 6 and at least one security module 7 connected to the virtual machine 2. The tuning module 6 provides functions for setting up and recording events. The functions of both types can be independently activated or deactivated by the security policy management module 4. The configuration functions have several modes.

Disabled - the security subsystem 5 operates in the normal mode (as if there were no configuration functions in the system).

Enabled - the security subsystem 5 constantly performs self-tuning (described later in this section).

Automatic mode - self-tuning of the subsystem 5 is initially enabled. The tuning module 6 checks the overhead for performing self-tuning. If the overhead of self-tuning exceeds its benefit (that is, determine the appropriateness of using self-tuning), self-tuning is turned off altogether or for a certain period of time.

For each access request, security modules 7 return an access decision. When the building function is enabled, the tuning module 6 collects information about the access decision requests. For each returned access decision, this information contains the number of polls of the security modules and the time spent by each module to determine its solution. Then, on demand or after a certain time interval (i.e., periodically), the tuning module determines the optimal polling sequence of the security modules 7, which has the minimum expected execution time. Thus, the frequently called security modules 7 and modules, for which time is wasted, will be called among the first in the security module polling sequence. At the same time, restrictions on the permutation of security modules 7 in the polling sequence can be imposed.

The event logging functions of the security subsystem 5 can be turned on or off depending on the needs. This makes it possible to collect some information: subjects, objects, module solutions and final solutions. This information can be used for profiling and tracing the security subsystem, as well as for determining the correct configuration of the security subsystem and its verification.

Let us consider a preferred embodiment of the claimed invention. The virtualization system (FIG. 1) is a set of virtual machines 2 operating on any equipment with any architecture 1 and in any operating system. Each virtual machine 2 is independent and protected from the rest. The virtual machine monitor 3 ensures that this set of virtual machines 2 works correctly. All security information for virtual machines 2 and other resources is located inside the virtual machine monitor 3 and is protected from virtual machines 2.

Each virtual machine 2 can access various objects (virtual resources) that correspond to the real resources of the hardware part 1 of the system. When the virtual machine 2 tries to access the object, the access request is sent to the security subsystem 5 of the virtual machine monitor 3 (FIG. 2). The security subsystem 5 polls the security modules 7 and makes the final decision. Interrogation of all security modules 7 in a certain sequence may not be required - the final decision is available from the moment when the information received from the interrogated security modules 7 becomes sufficient to make a final decision.

Security subsystem 5 contains a configuration module 6 that performs setup functions (for self-tuning of the security subsystem) and event logging functions (for profiling / tracing the security subsystem). The functions of both types can be independently activated or deactivated by the policy management module.

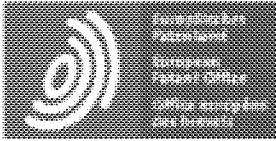
For each access request, security modules 7 return an access decision. When the tuning functions are turned on, the tuning module 6 collects information about the access decision requests. For each returned access decision, this information contains the number of polls of the security modules 7 and the time taken by each module to generate the solution. Then, on demand or after a time interval (i.e., periodically), the tuning module determines the optimal polling sequence of the security modules 7, which has the minimum expected execution time. Thus, frequently called modules 7 and modules 7, which are spent time consuming, will be interrogated among the first in the sequence of polling the security modules. At the same time, restrictions on the permutation of security modules 7 in the polling sequence can be imposed.

Thus, tuning functions increase the performance of the security subsystem.

If the registration of events is activated, it enables you to collect information: subjects, objects, module solutions and final decisions. This information can be used for profiling and tracing the security subsystem, and can also help in creating the correct configuration of the security subsystem.

The proposed system provides high performance of the security subsystem. In addition, it offers additional functionality - the ability to log events of the security subsystem. This information can be very useful for properly configuring the security subsystem in a virtualization system.

While the foregoing embodiment has been set forth to illustrate the present invention, it will be appreciated by those skilled in the art that various modifications, additions and substitutions are possible without departing from the scope and spirit of the present invention disclosed in the appended claims.



Patent Translate

Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

CLAIMS RU2406138

A security system of a virtualized computer system comprising a hardware associated with at least one virtual machine through a virtual machine monitor that includes a security policy management module connected to a security subsystem comprising a connected setup module and at least one a security module coupled to the virtual machine, wherein the virtual machine is configured to direct the access request to the virtual machine monitor configured with the ability to process an access request, while the security subsystem is configured to interrogate security modules, obtain permission from them and, on the basis of decisions obtained, allow the final approval decision, and the configuration module is configured to: configure information gathering the number of polls of each security module and the time spent on each of the surveys, and the ability to determine, on the basis of the information collected, the optimal follower



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: 2009123225/08, 18.06.2009

(24) Дата начала отсчета срока действия патента:
18.06.2009

(45) Опубликовано: 10.12.2010 Бюл. № 34

(56) Список документов, цитированных в отчете о
поиске: RU 2007137570 A, 20.04.2009. US
2009133097 A1, 21.05.2009. CN 101425027 A,
06.05.2009. CN 101414913 A, 22.04.2009.Адрес для переписки:
119331, Москва, а/я 88, В.Н.Рослову

(72) Автор(ы):

Андреев Станислав Валерьевич (RU),
Драгальчук Владислав Константинович
(RU),
Попов Евгений Александрович (RU)

(73) Патентообладатель(и):

Корпорация "САМСУНГ ЭЛЕКТРОНИКС
Ко., Лтд." (KR)

(54) СИСТЕМА БЕЗОПАСНОСТИ ВИРТУАЛИЗОВАННОЙ КОМПЬЮТЕРНОЙ СИСТЕМЫ

(57) Реферат:

Изобретение относится к области безопасности компьютерных систем, а именно к системам безопасности виртуализованных компьютерных систем. Техническим результатом является высокая производительность и уменьшение времени отклика. Система безопасности виртуализованной компьютерной системы

содержит аппаратную часть, связанную с, по меньшей мере, одной виртуальной машиной через монитор виртуальной машины, который содержит модуль управления политиками безопасности, соединенный с подсистемой безопасности, содержащей соединенные между собой пастроечный модуль и, по меньшей мере, один модуль безопасности, соединенный с виртуальной машиной. 3 ил.

RU 2 406 138 C1

RU 2 406 138 C1



Фиг. 1



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(51) Int. Cl.
G06F 21/20 (2006.01)
G06F 12/08 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: 2009123225/08, 18.06.2009

(24) Effective date for property rights:
18.06.2009

(45) Date of publication: 10.12.2010 Bull. 34

Mail address:
119331, Moskva, a/ja 88, V.N.Roslovu

(72) Inventor(s):

Andreev Stanislav Valer'evich (RU),
Dragal'chuk Vladislav Konstantinovich (RU),
Popov Evgenij Aleksandrovich (RU)

(73) Proprietor(s):

Korporatsija "SAMSUNG EhLEKTRONIKS Ko.,
Ltd." (KR)

(54) SECURITY SYSTEM FOR VIRTUAL COMPUTER SYTEM

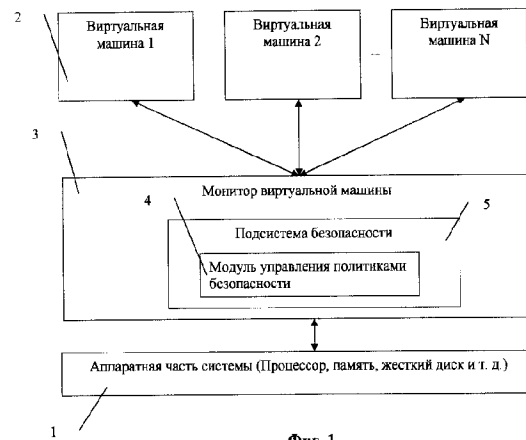
(57) Abstract:

FIELD: information technology.

SUBSTANCE: security system for a virtual computer system having a hardware part connected to at least one virtual machine through a virtual machine monitor which has a security policy control module, connected to a security subsystem having connected adjustment module and at least one security module connected to the virtual machine.

EFFECT: high efficiency and short response time.

3 dwg



Фиг. 1

Изобретение относится к области безопасности компьютерных систем, а именно к системам безопасности виртуализованных компьютерных систем, и может применяться в компьютерных устройствах различного типа с разными архитектурными и операционными системами, которые поддерживают возможности виртуализации.

Подход к возможностям виртуализации, связанный с монитором виртуальной машины (VMM - virtual machine monitor), фактически является типичным путем для создания нескольких виртуальных машин на единой реальной аппаратной платформе.

Монитор виртуальной машины - это компьютерная программа, которая осуществляет полный или частичный контроль ресурсов реальной компьютерной системы. Она предоставляет изолированное окружение путем виртуализации данных аппаратных ресурсов. Виртуализованное окружение называется виртуальной машиной (VM - virtual machine). Виртуальная машина может обращаться к виртуальным ресурсам. Попытки обращения виртуальных машин к виртуальным ресурсам контролируются подсистемой безопасности. При этом, с точки зрения подсистемы безопасности, виртуальная машина является субъектом операции обращения, а ресурс, к которому она обращается, объектом. Подсистема безопасности содержит несколько (один или более) различных элементов, называемых модулями безопасности. Когда монитор виртуальной машины организывает доступ к ресурсам системы, модули безопасности принимают решение о доступе субъектов к объектам на основе загруженной политики безопасности. Подсистема безопасности получает эти решения в определенной последовательности и принимает на их основе окончательное решение. В существующих системах виртуализации последовательность опроса модулей безопасности жестко закодирована. Аспект производительности не учитывается или она определяется эмпирически при определении данной последовательности. Поскольку решения могут приниматься очень часто и последовательность опроса модулей безопасности может быть неоптимальной, то это может привести к значительному ухудшению характеристик системы: уменьшению общей производительности и времени отклика.

Известна система виртуализации Xen с sHype подсистемой безопасности, разработанной фирмой IBM (см. Research Report RC23629: R.Sailer, T.Jaeger, E.Valdez, R.Perez, S.Berger, J.L.Griffin, L. van Doorn: Building a MAC-based Security Architecture for the Xen Opensource Hypervisor [1] и Research Report RC23511: R.Sailer, E.Valdez, T.Jaeger, R.Perez, L. van Doorn, J.L.Griffin, S.Berger: sHype: Secure Hypervisor Approach to Trusted Virtualized Systems [2]). Архитектура sHype (фирмы IBM) поддерживает реализацию различных модулей безопасности (Chinese Wall, Biba, Bell-LaPadula и т.д.).

Наиболее близкой к заявленному изобретению является система безопасности виртуализованной компьютерной системы, описанная в патенте EP 2037657 [3], содержащая аппаратную часть, связанную, по меньшей, с одной виртуальной машиной через монитор виртуальной машины, при этом виртуальная машина выполнена с возможностью направления запроса доступа в монитор виртуальной машины, выполненный с возможностью обработки запроса доступа. Данная система выбрана в качестве прототипа заявленного изобретения.

Описанная выше архитектура систем аналога и прототипа предполагает, что последовательность получения решений от модулей безопасности основана на требуемой безопасности и жестко закодирована. Аспект производительности не учитывается или она определяется эмпирически, что может не соответствовать реальному состоянию. В системах с такой архитектурой может произойти ухудшение

общей производительности системы и времени отклика системы, особенно если используется несколько сложных модулей безопасности. Кроме того, данная архитектура не обеспечивает функциональности для регистрации событий, происходящих в системе безопасности.

5 Задачей заявленного изобретения является создание системы безопасности виртуализированной компьютерной системы с увеличенной производительностью и уменьшенным временем отклика.

Поставленная задача решена за счет формирования оптимизированной
10 последовательности опроса модулей безопасности и опроса модулей в данной последовательности, при этом опрос всех модулей не требуется, если после опроса некоторых модулей полученной информации достаточно для принятия решения. Кроме того, в подсистему безопасности добавлена возможность регистрации происходящих в ней событий. Функции регистрации событий облегчают
15 администрирование подсистемы безопасности.

Технический результат достигается благодаря созданию системы безопасности виртуализированной компьютерной системы, содержащей аппаратную часть, связанную с, по меньшей мере, одной виртуальной машиной через монитор виртуальной
20 машины, который содержит модуль управления политиками безопасности, соединенный с подсистемой безопасности, содержащей соединенные между собой настроечный модуль и, по меньшей мере, один модуль безопасности, соединенный с виртуальной машиной, причем виртуальная машина выполнена с возможностью направления запроса доступа в монитор виртуальной машины, выполненный с
25 возможностью обработки запроса доступа, при этом подсистема безопасности выполнена с возможностью опроса модулей безопасности, получения от них решений о допуске и с возможностью принятия на основе полученных решений о допуске окончательного решения о допуске, а настроечный модуль выполнен с возможностью
30 реализации функции настройки сбора информации о количестве опросов каждого модуля безопасности и времени, израсходованном на каждый из опросов, и с возможностью определения на основе собранной информации оптимальной последовательности опроса модулей безопасности, при которой часто вызываемые модули и модули, на которые тратится мало времени, вызывают в числе первых.

35 Для лучшего понимания заявленного изобретения далее приводится его подробное описание с соответствующими чертежами.

Фиг.1. Общая схема системы безопасности виртуализированной компьютерной системы согласно изобретению.

40 Фиг.2. Подробная схема системы безопасности виртуализированной компьютерной системы согласно изобретению.

Фиг.3. Алгоритм работы системы безопасности виртуализированной компьютерной системы согласно изобретению.

Рассмотрим принцип функционирования заявленного изобретения. Заявленная
45 система безопасности виртуализированной компьютерной системы (Фиг.1-3) содержит аппаратную часть 1, связанную с, по меньшей мере, одной виртуальной машиной 2 через монитор 3 виртуальной машины, который содержит модуль 4 управления политиками безопасности, соединенный с подсистемой 5 безопасности, содержащей соединенные между собой настроечный модуль 6 и, по меньшей мере, один модуль 7
50 безопасности, соединенный с виртуальной машиной 2. Настроечный модуль 6 обеспечивает функции настройки и регистрации событий. Функции обоих типов могут быть независимо активированы или деактивированы модулем 4 управления

политиками безопасности. Функции настройки имеют несколько режимов.

Выключен - подсистема 5 безопасности работает в обычном режиме (как если бы в системе не существовало функций настройки).

5 Включен - подсистема 5 безопасности постоянно выполняет самонастройку (описанную ниже в этом разделе).

Автоматический режим - изначально включена самонастройка подсистемы 5. Настроечный модуль 6 проверяет накладные расходы на выполнение самонастройки. Если накладные расходы самонастройки превышают ее выгоду (то есть определяют
10 целесообразность использования самонастройки), то самонастройку выключают совсем или на определенный период времени.

На каждый запрос доступа модули 7 безопасности возвращают решение о доступе. Когда функция застройки включена, настроечный модуль 6 собирает информацию о запросах решения о доступе. Для каждого возвращенного решения о доступе данная
15 информация содержит количество опросов модулей безопасности и время, израсходованное каждым модулем на выработку его решения. Затем по запросу или через определенный временной интервал (то есть периодически) настроечный модуль определяет оптимальную последовательность опроса модулей 7 безопасности, которая имеет минимальное ожидаемое время выполнения. Таким образом, часто
20 вызываемые модули 7 безопасности и модули, на выполнение которых тратится мало времени, будут вызваны в числе первых в последовательности опроса модулей безопасности. При этом на перестановку модулей 7 безопасности в последовательности опроса могут накладываться определенные ограничения.

25 Функции регистрации событий подсистемы 5 безопасности могут быть включены или выключены в зависимости от потребностей. Это дает возможность собирать некоторую информацию: субъекты, объекты, решения модулей и окончательные решения. Данная информация может быть использована для профилирования и трассировки подсистемы безопасности, а также для определения правильной
30 конфигурации подсистемы безопасности и ее проверки.

Рассмотрим предпочтительный вариант выполнения заявленного изобретения. Система виртуализации (Фиг.1) представляет собой набор виртуальных машин 2, работающих на любом оборудовании с любой архитектурой 1 и в любых
35 операционных системах. Каждая виртуальная машина 2 независима и защищена от остальных. Монитор 3 виртуальной машины обеспечивает правильную работу данного набора виртуальных машин 2. Вся информация по безопасности, предназначенная для виртуальных машин 2 и других ресурсов, находится внутри монитора 3 виртуальной машины и защищена от виртуальных машин 2.
40

Каждая виртуальная машина 2 может получить доступ к различным объектам (виртуальным ресурсам), которые соответствуют реальным ресурсам аппаратной части 1 системы. Когда виртуальная машина 2 пытается получить доступ к объекту, запрос доступа посылают в подсистему 5 безопасности монитора 3 виртуальной
45 машины (Фиг.2). Подсистема 5 безопасности опрашивает модули 7 безопасности и принимает окончательное решение. Опрос всех модулей 7 безопасности в определенной последовательности может не требоваться - окончательное решение доступно с того момента, когда информации, полученной от опрошенных модулей 7 безопасности, становится достаточно для принятия окончательного решения.
50

Подсистема 5 безопасности содержит настроечный модуль 6, который выполняет настроечные функции (для самонастройки подсистемы безопасности) и функции регистрации событий (для профилирования/трассировки подсистемы безопасности).

Функции обоих типов могут быть независимо активированы или деактивированы модулем управления политиками безопасности.

На каждый запрос доступа модули 7 безопасности возвращают решение о доступе. Когда настроечные функции включены, настроечный модуль 6 собирает информацию о запросах решения о доступе. Для каждого возвращенного решения о доступе эта информация содержит количество опросов модулей 7 безопасности и время, затраченное каждым модулем на выработку решения. Затем по запросу или через временной интервал (то есть периодически) настроечный модуль определяет оптимальную последовательность опроса модулей 7 безопасности, которая имеет минимальное ожидаемое время выполнения. Таким образом, часто вызываемые модули 7 и модули 7, на выполнение которых тратится мало времени, будут опрашиваться в числе первых в последовательности опроса модулей безопасности. При этом на перестановку модулей 7 безопасности в последовательности опроса могут накладываться определенные ограничения.

Таким образом, настроечные функции повышают производительность подсистемы безопасности.

Если регистрация событий активирована, то она дает возможность собирать информацию: субъекты, объекты, решения модулей и окончательные решения. Данная информация может быть использована для профилирования и трассировки подсистемы безопасности, а также может помочь при создании правильной конфигурации подсистемы безопасности.

Предложенная система обеспечивает высокую производительность подсистемы безопасности. Кроме того, она предлагает дополнительную функциональность - возможность регистрации событий подсистемы безопасности. Данная информация может быть очень полезна для правильного конфигурирования подсистемы безопасности в системе виртуализации.

Хотя указанный выше вариант выполнения изобретения был изложен с целью иллюстрации настоящего изобретения, специалистам ясно, что возможны разные модификации, добавления и замены, не выходящие из объема и смысла настоящего изобретения, раскрытого в прилагаемой формуле изобретения.

Формула изобретения

Система безопасности виртуализированной компьютерной системы, содержащая аппаратную часть, связанную с, по меньшей мере, одной виртуальной машиной через монитор виртуальной машины, который содержит модуль управления политиками безопасности, соединенный с подсистемой безопасности, содержащей соединенные между собой настроечный модуль и, по меньшей мере, один модуль безопасности, соединенный с виртуальной машиной, причем виртуальная машина выполнена с возможностью направления запроса доступа в монитор виртуальной машины, выполненный с возможностью обработки запроса доступа, при этом подсистема безопасности выполнена с возможностью опроса модулей безопасности, получения от них решений о допуске и с возможностью принятия на основе полученных решений о допуске окончательного решения о допуске, а настроечный модуль выполнен с возможностью реализации функции настройки: сбора информации о количестве опросов каждого модуля безопасности и времени, израсходованном на каждый из опросов, и с возможностью определения на основе собранной информации оптимальной последовательности опроса модулей безопасности, при которой часто вызываемые модули и модули, на которые тратится мало времени, вызывают в числе

первых.

5

10

15

20

25

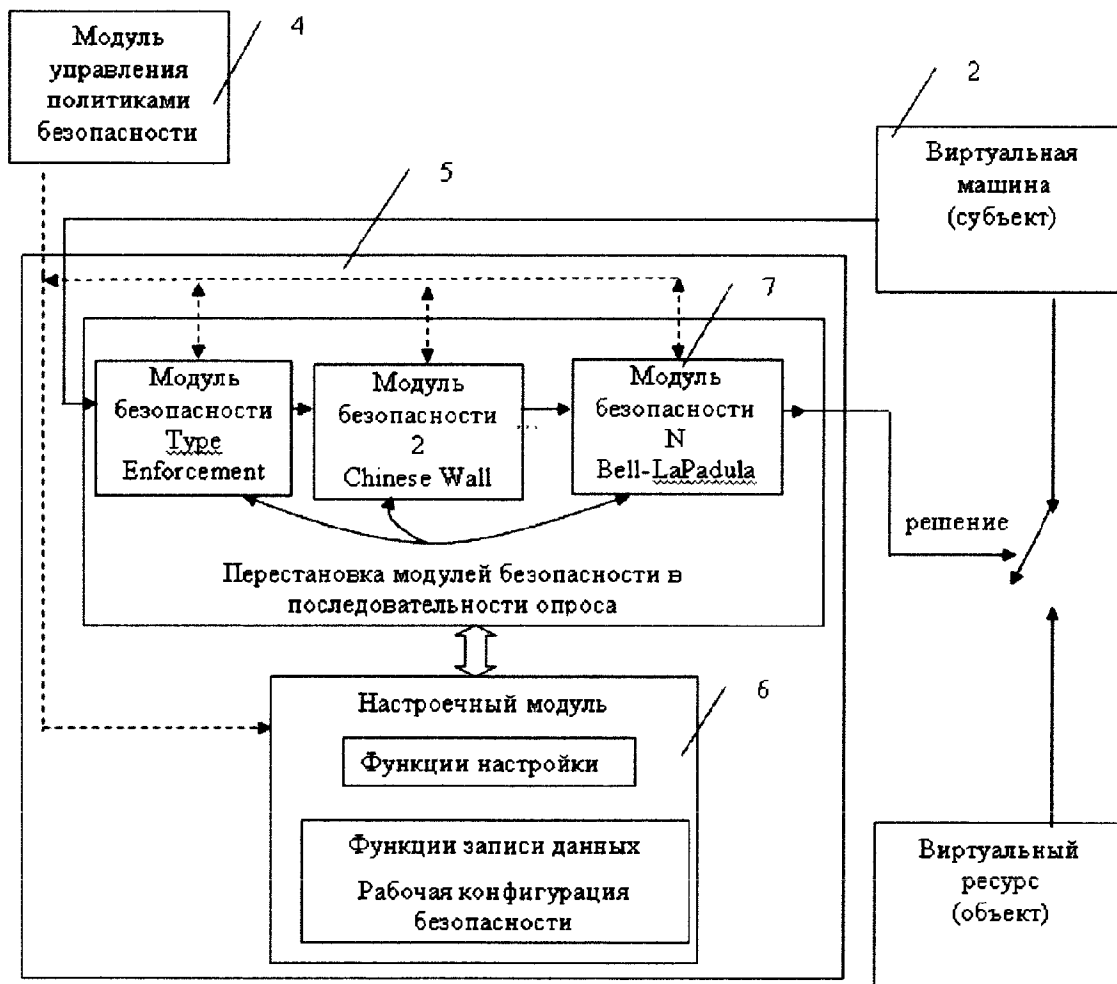
30

35

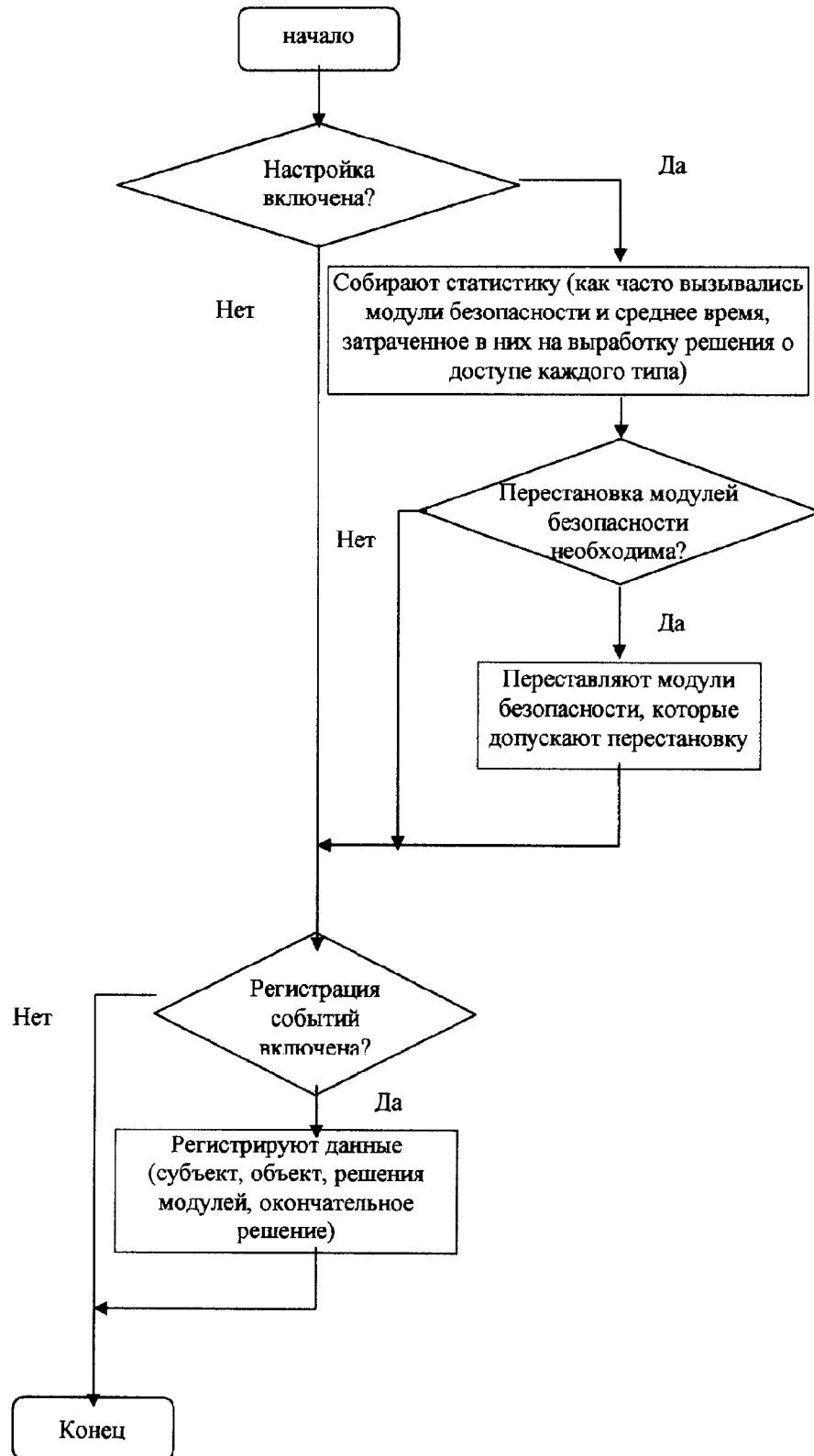
40

45

50



Фиг. 2



Фиг. 3

Malware Explorer | Nart Villeneuve

Command and Control in the Cloud

Posted by nart on October 22nd, 2010. No comments... »

Tags: Malware, Social Engineering.

In “Shadows in the Cloud: An investigation into cyber espionage 2.0” my co-authors and I analyzed the command and control infrastructure of a network that extracted secret, confidential and restricted documents from the Indian government and military. The *Shadow Network* used a complex and tiered command and control infrastructure that leveraged Twitter, Google Groups, Blogspot, Baidu Blogs, blog.com and Yahoo! Mail in order to maintain persistent control over the compromised computers. As we noted in the report, the use of these services as elements of command and control is certainly not new:

The use of social networking sites as elements of command and control for malware networks is not novel. The attackers leverage the normal operation of these systems in order to maintain control over compromised system. In 2009, researchers found that Twitter, Jaiku, Tumblr, Google Groups, Google AppEngine and Facebook had all been used as the command and control structure for malware. In August 2009, Arbor Networks' Jose Nazario found that Twitter was being used as a command and control component for a malware network. In this case, the malware was an information stealer focused on extracting banking credentials from compromised computers located mostly in Brazil. Twitter was not the only channel being used by the attackers. They also used accounts on Jaiku and Tumblr (Nazario 2009a). Furthermore, Arbor Networks found another instance of malware that used the Google AppEngine to deliver malicious URLs to compromised computers (Nazario 2009b). The Unmask Parasites blog found that obfuscated scripts embedded in compromised web sites used the Twitter API to obscure their activities. While the method was clever, the code was unreliable and appeared to have been abandoned by the attackers (Unmask Parasites 2009). Symantec found that Google Groups were being used as command and control for another instance of malware. In this case, a private Google group was used by the attackers to send commands to compromised computers which then uploaded their responses to the same Group (Symantec 2009a). Symantec also found an instance of malware that used Facebook status messages as a mechanism of command and control. (Symantec 2009b). The use of these social networking and Web 2.0 tools allows the attackers to leverage the normal operation of these tools to obscure the command and control functions of malware.

Earlier this year, Sunbelt found a Twitter botnet creator and Trend Micro reports that the “Here You Have” worm used Gmail accounts. As we found with the *Shadow Network* malware authors learn from each other. And in the case of the *Shadow Network* they didn't just use one service they used six of them, including Yahoo! Mail. And while indiscriminate malware may be rather noisy, the malware used in targeted attacks tends to be (but is certainly not always) more discrete.

A recent sample posted at contagiodump.blogspot.com caught my attention for this very reason. The sample, “Conference Information_2010 IFANS Conference on Global Affairs (1001).pdf” (which was sent from 221.9.247.17 and was detected by 14 /43 (32.6%) AV products at Virustotal) arrived with the subject line “Nuclear Challenges and Responses in the Century” and exploited a vulnerability in Adobe Reader/Acrobat (CVE-2010-2883) to drop malware on the targets' computers. For those of you who follow Mila's awesome blog, this scenario is hardly surprising.

Pages

About
Writing

Search

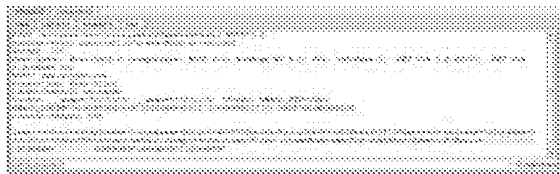
Tweets by @nartv

Meta

RSS
RSS (comments)
Log in

But a few things caught my attention. There were references in the strings dumped from a file the malware created (syschk.ocx) that referenced GMail (mail.google.com) and DriveHQ (drivehq.com), which describes itself as a “cloud based storage, backup, group sharing and collaboration service.” When you look at the traffic generated by the malware you’ll see connections to these locations.

There is nothing about these locations that is very suspicious — everyone checks their GMail right? Moreover, the connection to GMail is SSL encrypted.



Using Burp (which made the process very simple) I MITM’d the traffic between the malware and GMail. The malware logs in to the GMail account and sends an email to another GMail address. The content of this email is encrypted. However, I believe that what it is sending — although this is just a hunch — is the content of another file the malware generates: form.ocx. This file contains what appears to be a unique ID assigned by the malware, the hostname and IP address, the default home page of the default browser and a listing of installed programs on the computer. The end of the file contains information about executables the malware has impacted. In addition to the encrypted message sent through the GMail account, the Unique ID in form.ocx appears at the beginning of the message.

```
IEXPLORE.EXE done
CHROME.EXE done
FIREFOX.EXE done

C:\WINDOWS\system32\form.ocx
Infect OK!
```

I have not looked into what exactly the malware does to these applications, but it basically disables the operation of FireFox and Chrome and instead connect to the Gmail account when you try to start these applications. Internet Explorer seems to function normally.

The connection to fuechei.chang.drivehq.com results in the download of an additional file rename.ocx which appears to be very similar, when its strings are compared with, syschk.ocx. It then renames syschk.ocx to syschk.ocx1. You can see that this correlates with text in the strings dumped from syschk.ocx.

```
%s\rename.ocx
http://%s/rename
%s\syschk.ocx1
```

After the initial connections to GMail and DriveHQ the malware went quiet. I never did get it to connect again.

As network defenses continue to include traffic analysis, I believe that we will continue to see a move toward using popular services, especially web mail as command and control elements. Unlike connections to well-known dynamic DNS services like 3322.org or abnormal connections to geographic regions, connections to GMail and other popular services do not necessarily stand out. Moreover, the connections to the services, such as GMail are encrypted, further obfuscating the malicious activity that is occurring.

Post a comment.

Name (required)

Mail (will not be published) (required)

Website

Submit Comment

Except where otherwise noted, content on this site is licensed under a [Creative Commons License](#).

Computer network

A **computer network**, or **data network**, is a digital telecommunications network which allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections (data links) between nodes. These data links are established over cable media such as wires or optic cables, or wireless media such as WiFi.

Network computer devices that originate, route and terminate the data are called network nodes.^[1] Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other. In most cases, application-specific communications protocols are layered (i.e. carried as payload) over other more general communications protocols. This formidable collection of information technology requires skilled network management to keep it all running reliably.

Computer networks support an enormous number of applications and services such as access to the World Wide Web, digital video, digital audio, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications as well as many others. Computer networks differ in the transmission medium used to carry their signals, communications protocols to organize network traffic, the network's size, topology, traffic control mechanism and organizational intent. The best-known computer network is the Internet.

Contents

History

Properties

Network packet

Network topology

Network links

- Wired technologies

- Wireless technologies

- Exotic technologies

Network nodes

- Network interfaces

- Repeaters and hubs

- Bridges

- Switches

- Routers

- Modems

- Firewalls

Network structure

- Common layouts

- Overlay network

Communication protocols

- IEEE 802

- Ethernet

- Wireless LAN

- Internet Protocol Suite

- SONET/SDH

- Asynchronous Transfer Mode

Cellular standards

Geographic scale

Organizational scope

Intranet

Extranet

Internetwork

Internet

Darknet

Routing

Network service

Network performance

Quality of service

Network congestion

Network resilience

Security

Network security

Network surveillance

End to end encryption

SSL/TLS

Views of networks

Journals and newsletters

See also

References

Further reading

External links

History

The chronology of significant computer-network developments includes:

- In the late 1950s, early networks of computers included the U.S. military radar system Semi-Automatic Ground Environment (SAGE).
- In 1959, Anatolii Ivanovich Kitov proposed to the Central Committee of the Communist Party of the Soviet Union a detailed plan for the re-organisation of the control of the Soviet armed forces and of the Soviet economy on the basis of a network of computing centres, the OGAS.^[2]
- In 1960, the commercial airline reservation system semi-automatic business research environment (SABRE) went online with two connected mainframes.
- In 1963, J. C. R. Licklider sent a memorandum to office colleagues discussing the concept of the "Intergalactic Computer Network", a computer network intended to allow general communications among computer users.
- In 1964, researchers at Dartmouth College developed the Dartmouth Time Sharing System for distributed users of large computer systems. The same year, at Massachusetts Institute of Technology, a research group supported by General Electric and Bell Labs used a computer to route and manage telephone connections.
- Throughout the 1960s, Paul Baran, and Donald Davies independently developed the concept of packet switching to transfer information between computers over a network. Davies pioneered the implementation of the concept with the NPL network, a local area network at the National Physical Laboratory (United Kingdom) using a line speed of 768 kbit/s.^{[3][4][5]}
- In 1965, Western Electric introduced the first widely used telephone switch that implemented true computer control.
- In 1966, Thomas Marill and Lawrence G. Roberts published a paper on an experimental wide area network (WAN) for computer time sharing.^[6]
- In 1969, the first four nodes of the ARPANET were connected using 50 kbit/s circuits between the University of California at Los Angeles, the Stanford Research Institute, the University of California at Santa Barbara, and the University of Utah.^[7] Leonard Kleinrock carried out theoretical work to model the performance of packet-switched

networks, which underpinned the development of the ARPANET.^{[8][9]} His theoretical work on hierarchical routing in the late 1970s with student Farouk Kamoun remains critical to the operation of the Internet today.

- In 1972, commercial services using X.25 were deployed, and later used as an underlying infrastructure for expanding TCP/IP networks.
- In 1973, the French CYCLADES network was the first to make the hosts responsible for the reliable delivery of data, rather than this being a centralized service of the network itself.^[10]
- In 1973, Robert Metcalfe wrote a formal memo at Xerox PARC describing Ethernet, a networking system that was based on the Aloha network, developed in the 1960s by Norman Abramson and colleagues at the University of Hawaii. In July 1976, Robert Metcalfe and David Boggs published their paper "Ethernet: Distributed Packet Switching for Local Computer Networks"^[11] and collaborated on several patents received in 1977 and 1978. In 1979, Robert Metcalfe pursued making Ethernet an open standard.^[12]
- In 1976, John Murphy of Datapoint Corporation created ARCNET, a token-passing network first used to share storage devices.
- In 1995, the transmission speed capacity for Ethernet increased from 10 Mbit/s to 100 Mbit/s. By 1998, Ethernet supported transmission speeds of a Gigabit. Subsequently, higher speeds of up to 100 Gbit/s were added (as of 2016). The ability of Ethernet to scale easily (such as quickly adapting to support new fiber optic cable speeds) is a contributing factor to its continued use.^[12]

Properties

Computer networking may be considered a branch of electrical engineering, electronics engineering, telecommunications, computer science, information technology or computer engineering, since it relies upon the theoretical and practical application of the related disciplines.

A computer network facilitates interpersonal communications allowing users to communicate efficiently and easily via various means: email, instant messaging, online chat, telephone, video telephone calls, and video conferencing. A network allows sharing of network and computing resources. Users may access and use resources provided by devices on the network, such as printing a document on a shared network printer or use of a shared storage device. A network allows sharing of files, data, and other types of information giving authorized users the ability to access information stored on other computers on the network. Distributed computing uses computing resources across a network to accomplish tasks.

A computer network may be used by security hackers to deploy computer viruses or computer worms on devices connected to the network, or to prevent these devices from accessing the network via a denial-of-service attack.

Network packet

Computer communication links that do not support packets, such as traditional point-to-point telecommunication links, simply transmit data as a bit stream. However, most information in computer networks is carried in *packets*. A network packet is a formatted unit of data (a list of bits or bytes, usually a few tens of bytes to a few kilobytes long) carried by a packet-switched network. Packets are sent through the network to their destination. Once the packets arrive they are reassembled into their original message.

Packets consist of two kinds of data: control information, and user data (payload). The control information provides data the network needs to deliver the user data, for example: source and destination network addresses, error detection codes, and sequencing information. Typically, control information is found in packet headers and trailers, with payload data in between.

With packets, the bandwidth of the transmission medium can be better shared among users than if the network were circuit switched. When one user is not sending packets, the link can be filled with packets from other users, and so the cost can be shared, with relatively little interference, provided the link isn't overused. Often the route a packet needs to take through a network is not immediately available. In that case the packet is queued and waits until a link is free.

Network topology

The physical layout of a network is usually less important than the topology that connects network nodes. Most diagrams that describe a physical network are therefore topological, rather than geographic. The symbols on these diagrams usually denote network links and network nodes.

Network links

The transmission media (often referred to in the literature as the *physical media*) used to link devices to form a computer network include electrical cable, optical fiber, and radio waves. In the OSI model, these are defined at layers 1 and 2 — the physical layer and the data link layer.

A widely adopted *family* of transmission media used in local area network (LAN) technology is collectively known as Ethernet. The media and protocol standards that enable communication between networked devices over Ethernet are defined by IEEE 802.3. Ethernet transmits data over both copper and fiber cables. Wireless LAN standards use radio waves, others use infrared signals as a transmission medium. Power line communication uses a building's power cabling to transmit data.

Wired technologies

The orders of the following wired technologies are, roughly, from slowest to fastest transmission speed.

- Coaxial cable is widely used for cable television systems, office buildings, and other work-sites for local area networks. The cables consist of copper or aluminum wire surrounded by an insulating layer (typically a flexible material with a high dielectric constant), which itself is surrounded by a conductive layer. The insulation helps minimize interference and distortion. Transmission speed ranges from 200 million bits per second to more than 500 million bits per second.
- ITU-T G.hn technology uses existing home wiring (coaxial cable, phone lines and power lines) to create a high-speed (up to 1 Gigabit/s) local area network
- Twisted pair wire is the most widely used medium for all telecommunication. Twisted-pair cabling consist of copper wires that are twisted into pairs. Ordinary telephone wires consist of two insulated copper wires twisted into pairs. Computer network cabling (wired Ethernet as defined by IEEE 802.3) consists of 4 pairs of copper cabling that can be utilized for both voice and data transmission. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. The transmission speed ranges from 2 million bits per second to 10 billion bits per second. Twisted pair cabling comes in two forms: unshielded twisted pair (UTP) and shielded twisted-pair (STP). Each form comes in several category ratings, designed for use in various scenarios.
- An optical fiber is a glass fiber. It carries pulses of light that represent data. Some advantages of optical fibers over metal wires are very low transmission loss and immunity from electrical interference. Optical fibers can simultaneously carry multiple wavelengths of light, which greatly increases the rate that data can be sent, and helps enable data rates of up to trillions of bits per second. Optic fibers can be used for long runs of cable carrying very high data rates, and are used for undersea cables to interconnect continents. There are two types of transmission of fiber optics, Single-mode fiber (SMF) and Multimode fiber (MMF). Single-mode fiber has the advantage of being able to sustain a coherent signal for dozens or even a hundred kilometers. Multimode fiber is cheaper to terminate but is limited to a few hundred or even only a few dozens of meters, depending on the data rate and cable grade.^[13]

 Bundle of glass threads with light emitting from the ends
Fiber optic cables are used to transmit light from one computer/network node to another

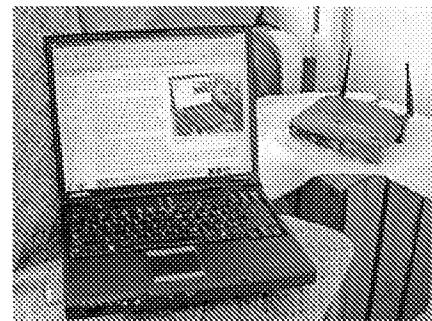
 World map with red and blue lines
2007 map showing submarine optical fiber telecommunication cables around the world.

Price is a main factor distinguishing wired- and wireless-technology options in a business. Wireless options command a price premium that can make purchasing wired computers, printers and other devices a financial benefit. Before making the decision to purchase hard-wired technology products, a review of the restrictions and limitations of the selections is necessary. Business and employee needs may override any cost considerations.^[14]

Wireless technologies

- Terrestrial microwave – Terrestrial microwave communication uses Earth-based transmitters and receivers resembling satellite dishes. Terrestrial microwaves are in the low gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 48 km (30 mi) apart.

- *Communications satellites* – Satellites communicate via microwave radio waves, which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically in geosynchronous orbit 35,400 km (22,000 mi) above the equator. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.
- *Cellular and PCS systems* use several radio communications technologies. The systems divide the region covered into multiple geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area.
- *Radio and spread spectrum technologies* – Wireless local area networks use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. IEEE 802.11 defines a common flavor of open-standards wireless radio-wave technology known as Wifi.
- *Free-space optical communication* uses visible or invisible light for communications. In most cases, line-of-sight propagation is used, which limits the physical positioning of communicating devices.



Computers are very often connected to networks using wireless links

Exotic technologies

There have been various attempts at transporting data over exotic media:

- IP over Avian Carriers was a humorous April fool's Request for Comments, issued as RFC 1149 (<https://tools.ietf.org/html/rfc1149>). It was implemented in real life in 2001.^[15]
- Extending the Internet to interplanetary dimensions via radio waves, the Interplanetary Internet.^[16]

Both cases have a large round-trip delay time, which gives slow two-way communication, but doesn't prevent sending large amounts of information.

Network nodes

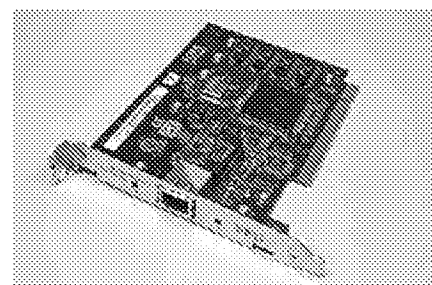
Apart from any physical transmission media there may be, networks comprise additional basic system building blocks, such as network interface controllers (NICs), repeaters, hubs, bridges, switches, routers, modems, and firewalls. Any particular piece of equipment will frequently contain multiple building blocks and perform multiple functions.

Network interfaces

A network interface controller (NIC) is computer hardware that provides a computer with the ability to access the transmission media, and has the ability to process low-level network information. For example, the NIC may have a connector for accepting a cable, or an aerial for wireless transmission and reception, and the associated circuitry.

The NIC responds to traffic addressed to a network address for either the NIC or the computer as a whole.

In Ethernet networks, each network interface controller has a unique Media Access Control (MAC) address—usually stored in the controller's permanent memory. To avoid address conflicts between network devices, the Institute of Electrical and Electronics Engineers (IEEE) maintains and administers MAC address uniqueness. The size of an Ethernet MAC address is six octets. The three most significant octets are reserved to identify NIC manufacturers. These manufacturers, using only their assigned prefixes, uniquely assign the three least-significant octets of every Ethernet interface they produce.



An ATM network interface in the form of an accessory card. A lot of network interfaces are built-in.

Repeaters and hubs

A repeater is an electronic device that receives a network signal, cleans it of unnecessary noise and regenerates it. The signal is retransmitted at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable that runs longer than 100 meters. With fiber optics, repeaters can be tens or even hundreds of kilometers apart.

A repeater with multiple ports is known as an Ethernet hub. Repeaters work on the physical layer of the OSI model. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay that affects network performance and may affect proper function. As a result, many network architectures limit the number of repeaters that can be used in a row, e.g., the Ethernet 5-4-3 rule.

Hubs and repeaters in LANs have been mostly obsoleted by modern switches.

Bridges

A network bridge connects and filters traffic between two network segments at the data link layer (layer 2) of the OSI model to form a single network. This breaks the network's collision domain but maintains a unified broadcast domain. Network segmentation breaks down a large, congested network into an aggregation of smaller, more efficient networks.

Bridges come in three basic types:

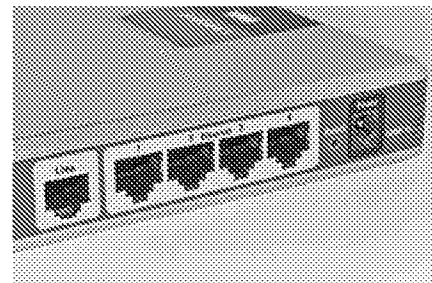
- **Local bridges:** Directly connect LANs
- **Remote bridges:** Can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced with routers.
- **Wireless bridges:** Can be used to join LANs or connect remote devices to LANs.

Switches

A network switch is a device that forwards and filters OSI layer 2 datagrams (frames) between ports based on the destination MAC address in each frame.^[17] A switch is distinct from a hub in that it only forwards the frames to the physical ports involved in the communication rather than all ports connected. It can be thought of as a multi-port bridge.^[18] It learns to associate physical ports to MAC addresses by examining the source addresses of received frames. If an unknown destination is targeted, the switch broadcasts to all ports but the source. Switches normally have numerous ports, facilitating a star topology for devices, and cascading additional switches.

Routers

A router is an internetworking device that forwards packets between networks by processing the routing information included in the packet or datagram (Internet protocol information from layer 3). The routing information is often processed in conjunction with the routing table (or forwarding table). A router uses its routing table to determine where to forward packets. A destination in a routing table can include a "null" interface, also known as the "black hole" interface because data can go into it, however, no further processing is done for said data, i.e. the packets are dropped.



A typical home or small office router showing the ADSL telephone line and Ethernet network cable connections

Modems

Modems (MODulator-DEModulator) are used to connect network nodes via wire not originally designed for digital network traffic, or for wireless. To do this one or more carrier signals are modulated by the digital signal to produce an analog signal that can be tailored to give the required properties for transmission. Modems are commonly used for telephone lines, using a Digital Subscriber Line technology.

Firewalls

A firewall is a network device for controlling network security and access rules. Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in cyber attacks.

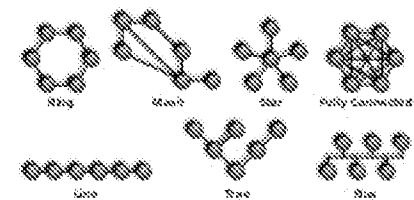
Network structure

Network topology is the layout or organizational hierarchy of interconnected nodes of a computer network. Different network topologies can affect throughput, but reliability is often more critical. With many technologies, such as bus networks, a single failure can cause the network to fail entirely. In general the more interconnections there are, the more robust the network is; but the more expensive it is to install.

Common layouts

Common layouts are:

- A bus network: all nodes are connected to a common medium along this medium. This was the layout used in the original Ethernet, called 10BASE5 and 10BASE2. This is still a common topology on the data link layer, although modern physical layer variants use point-to-point links instead.
- A star network: all nodes are connected to a special central node. This is the typical layout found in a Wireless LAN, where each wireless client connects to the central Wireless access point.
- A ring network: each node is connected to its left and right neighbour node, such that all nodes are connected and that each node can reach each other node by traversing nodes left- or rightwards. The Fiber Distributed Data Interface (FDDI) made use of such a topology.
- A mesh network: each node is connected to an arbitrary number of neighbours in such a way that there is at least one traversal from any node to any other.
- A fully connected network: each node is connected to every other node in the network.
- A tree network: nodes are arranged hierarchically.

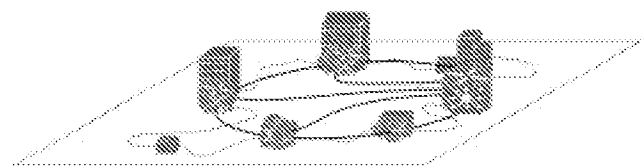


Common network topologies

Note that the physical layout of the nodes in a network may not necessarily reflect the network topology. As an example, with FDDI, the network topology is a ring (actually two counter-rotating rings), but the physical topology is often a star, because all neighboring connections can be routed via a central physical location.

Overlay network

An overlay network is a virtual computer network that is built on top of another network. Nodes in the overlay network are connected by virtual or logical links. Each link corresponds to a path, perhaps through many physical links, in the underlying network. The topology of the overlay network may (and often does) differ from that of the underlying one. For example, many peer-to-peer networks are overlay networks. They are organized as nodes of a virtual system of links that run on top of the Internet.^[19]



A sample overlay network

Overlay networks have been around since the invention of networking when computer systems were connected over telephone lines using modems, before any data network existed.

The most striking example of an overlay network is the Internet itself. The Internet itself was initially built as an overlay on the telephone network.^[19] Even today, each Internet node can communicate with virtually any other through an underlying mesh of sub-networks of wildly different topologies and technologies. Address resolution and routing are the means that allow mapping of a fully connected IP overlay network to its underlying network.

Another example of an overlay network is a distributed hash table, which maps keys to nodes in the network. In this case, the underlying network is an IP network, and the overlay network is a table (actually a map) indexed by keys.

Overlay networks have also been proposed as a way to improve Internet routing, such as through quality of service guarantees to achieve higher-quality streaming media. Previous proposals such as IntServ, DiffServ, and IP Multicast have not seen wide acceptance largely because they require modification of all routers in the network. On the other hand, an overlay network can be incrementally deployed on end-hosts running the overlay protocol software, without cooperation from Internet service providers. The overlay network has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes that a message traverses before it reaches its destination.

For example, Akamai Technologies manages an overlay network that provides reliable, efficient content delivery (a kind of multicast). Academic research includes end system multicast,^[20] resilient routing and quality of service studies, among others.

Communication protocols

A communication protocol is a set of rules for exchanging information over a network. In a protocol stack (also see the OSI model), each protocol leverages the services of the protocol layer below it, until the lowest layer controls the hardware which sends information across the media. The use of protocol layering is today ubiquitous across the field of computer networking. An important example of a protocol stack is HTTP (the World Wide Web protocol) running over TCP over IP (the Internet protocols) over IEEE 802.11 (the Wi-Fi protocol). This stack is used between the wireless router and the home user's personal computer when the user is surfing the web.

Communication protocols have various characteristics. They may be connection-oriented or connectionless, they may use circuit mode or packet switching, and they may use hierarchical addressing or flat addressing.

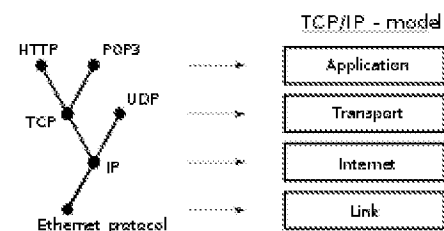
There are many communication protocols, a few of which are described below.

IEEE 802

IEEE 802 is a family of IEEE standards dealing with local area networks and metropolitan area networks. The complete IEEE 802 protocol suite provides a diverse set of networking capabilities. The protocols have a flat addressing scheme. They operate mostly at levels 1 and 2 of the OSI model.

For example, MAC bridging (IEEE 802.1D) deals with the routing of Ethernet packets using a Spanning Tree Protocol. IEEE 802.1Q describes VLANs, and IEEE 802.1X defines a port-based Network Access Control protocol, which forms the basis for the authentication mechanisms used in VLANs (but it is also found in WLANs) – it is what the home user sees when the user has to enter a "wireless access key".

Ethernet



The TCP/IP model or Internet layering scheme and its relation to common protocols often layered on top of it.

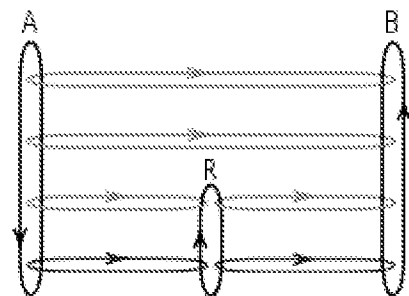


Figure 4. Message flows (A-B) in the presence of a router (R), red flows are effective communication paths, black paths are across the actual network links.

Ethernet, sometimes simply called *LAN*, is a family of protocols used in wired LANs, described by a set of standards together called IEEE 802.3 published by the Institute of Electrical and Electronics Engineers.

Wireless LAN

Wireless LAN, also widely known as WLAN or WiFi, is probably the most well-known member of the IEEE 802 protocol family for home users today. It is standardized by IEEE 802.11 and shares many properties with wired Ethernet.

Internet Protocol Suite

The Internet Protocol Suite, also called TCP/IP, is the foundation of all modern networking. It offers connection-less as well as connection-oriented services over an inherently unreliable network traversed by data-gram transmission at the Internet protocol (IP) level. At its core, the protocol suite defines the addressing, identification, and routing specifications for Internet Protocol Version 4 (IPv4) and for IPv6, the next generation of the protocol with a much enlarged addressing capability.

SONET/SDH

Synchronous optical networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers. They were originally designed to transport circuit mode communications from a variety of different sources, primarily to support real-time, uncompressed, circuit-switched voice encoded in PCM (Pulse-Code Modulation) format. However, due to its protocol neutrality and transport-oriented features, SONET/SDH also was the obvious choice for transporting Asynchronous Transfer Mode (ATM) frames.

Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) is a switching technique for telecommunication networks. It uses asynchronous time-division multiplexing and encodes data into small, fixed-sized cells. This differs from other protocols such as the Internet Protocol Suite or Ethernet that use variable sized packets or frames. ATM has similarity with both circuit and packet switched networking. This makes it a good choice for a network that must handle both traditional high-throughput data traffic, and real-time, low-latency content such as voice and video. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins.

While the role of ATM is diminishing in favor of next-generation networks, it still plays a role in the last mile, which is the connection between an Internet service provider and the home user.^[21]

Cellular standards

There are a number of different digital cellular standards, including: Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), cdmaOne, CDMA2000, Evolution-Data Optimized (EV-DO), Enhanced Data Rates for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), Digital Enhanced Cordless Telecommunications (DECT), Digital AMPS (IS-136/TDMA), and Integrated Digital Enhanced Network (iDEN).^[22]

Geographic scale

A network can be characterized by its physical capacity or its organizational purpose. Use of the network, including user authorization and access rights, differ accordingly.

Nanoscale network

A nanoscale communication network has key components implemented at the nanoscale including message carriers and leverages physical principles that differ from macroscale communication mechanisms. Nanoscale communication extends communication to very small sensors and actuators such as those found in biological systems and also tends to operate in environments that would be too harsh for classical communication.^[23]

Personal area network

A personal area network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and even video game consoles. A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters.^[24] A wired PAN is usually constructed with USB and FireWire connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.

Local area network

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as a home, school, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Wired LANs are most likely based on Ethernet technology. Newer standards such as ITU-T G.hn also provide a way to create a wired LAN using existing wiring, such as coaxial cables, telephone lines, and power lines.^[25]

The defining characteristics of a LAN, in contrast to a wide area network (WAN), include higher data transfer rates, limited geographic range, and lack of reliance on leased lines to provide connectivity. Current Ethernet or other IEEE 802.3 LAN technologies operate at data transfer rates up to 100 Gbit/s, standardized by IEEE in 2010.^[26] Currently, 400 Gbit/s Ethernet is being developed.

A LAN can be connected to a WAN using a router.

Home area network

A home area network (HAN) is a residential LAN used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a cable TV or digital subscriber line (DSL) provider.

Storage area network

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network by other devices. The cost and complexity of SANs dropped in the early 2000s to levels allowing wider adoption across both enterprise and small to medium-sized business environments.

Campus area network

A campus area network (CAN) is made up of an interconnection of LANs within a limited geographical area. The networking equipment (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling, etc.) are almost entirely owned by the campus tenant / owner (an enterprise, university, government, etc.).

For example, a university campus network is likely to link a variety of campus buildings to connect academic colleges or departments, the library, and student residence halls.

Backbone network

A backbone network is part of a computer network infrastructure that provides a path for the exchange of information between different LANs or sub-networks. A backbone can tie together diverse networks within the same building, across different buildings, or over a wide area.

For example, a large company might implement a backbone network to connect departments that are located around the world. The equipment that ties together the departmental networks constitutes the network backbone. When designing a network backbone, network performance and network congestion are critical factors to take into account. Normally, the backbone network's capacity is greater than that of the individual networks connected to it.

Another example of a backbone network is the Internet backbone, which is the set of wide area networks (WANs) and core routers that tie together all networks connected to the Internet.

Metropolitan area network

A Metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.

Wide area network

A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances. A WAN uses a communications channel that combines many types of media such as telephone lines, cables, and air waves. A WAN often makes use of transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

Enterprise private network

An enterprise private network is a network that a single organization builds to interconnect its office locations (e.g., production sites, head offices, remote offices, shops) so they can share computer resources.

Virtual private network

A virtual private network (VPN) is an overlay network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point.

Global area network

A global area network (GAN) is a network used for supporting mobile across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is handing off user communications from one local coverage area to the next. In IEEE Project 802, this involves a succession of terrestrial wireless LANs.^[27]

Organizational scope

Networks are typically managed by the organizations that own them. Private enterprise networks may use a combination of intranets and extranets. They may also provide network access to the Internet, which has no single owner and permits virtually unlimited global connectivity.

Intranet

An intranet is a set of networks that are under the control of a single administrative entity. The intranet uses the IP protocol and IP-based tools such as web browsers and file transfer applications. The administrative entity limits use of the intranet to its authorized users. Most commonly, an intranet is the internal LAN of an organization. A large intranet typically has at least one web server to provide users with organizational information. An intranet is also anything behind the router on a local area network.

Extranet

An extranet is a network that is also under the administrative control of a single organization, but supports a limited connection to a specific external network. For example, an organization may provide access to some aspects of its intranet to share data with its business partners or customers. These other entities are not necessarily trusted from a security standpoint. Network connection to an extranet is often, but not always, implemented via WAN technology.

Internetwork

An internetwork is the connection of multiple computer networks via a common routing technology using routers.

Internet

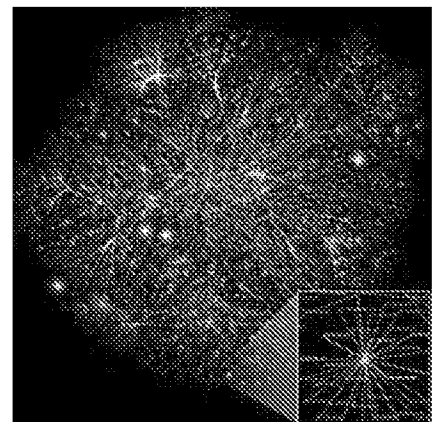
The Internet is the largest example of an internetwork. It is a global system of interconnected governmental, academic, corporate, public, and private computer networks. It is based on the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the United States Department of Defense. The Internet is also the communications backbone underlying the World Wide Web (WWW).

Participants in the Internet use a diverse array of methods of several hundred documented, and often standardized, protocols compatible with the Internet Protocol Suite and an addressing system (IP addresses) administered by the Internet Assigned Numbers Authority and address registries. Service providers and large enterprises exchange information about the reachability of their address spaces through the Border Gateway Protocol (BGP), forming a redundant worldwide mesh of transmission paths.

Darknet

A darknet is an overlay network, typically running on the Internet, that is only accessible through specialized software. A darknet is an anonymizing network where connections are made only between trusted peers — sometimes called "friends" (F2F)^[28] — using non-standard protocols and ports.

Darknets are distinct from other distributed peer-to-peer networks as sharing is anonymous (that is, IP addresses are not publicly shared), and therefore users can communicate with little fear of governmental or corporate interference.^[29]



Partial map of the Internet based on the January 15, 2005 data found on [opte.org](http://www.opte.org) (<http://www.opte.org/maps/>). Each line is drawn between two nodes, representing two IP addresses. The length of the lines are indicative of the delay between those two nodes. This graph represents less than 30% of the Class C networks reachable.

Routing

Routing is the process of selecting network paths to carry network traffic. Routing is performed for many kinds of networks, including circuit switching networks and packet switched networks.

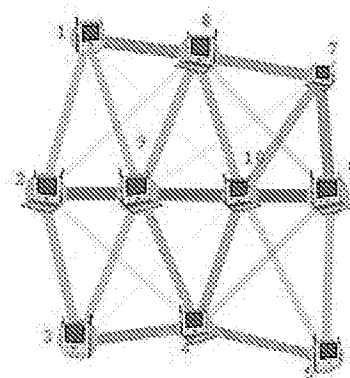
In packet switched networks, routing directs packet forwarding (the transit of logically addressed network packets from their source toward their ultimate destination) through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. The routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing.

There are usually multiple routes that can be taken, and to choose between them, different elements can be considered to decide which routes get installed into the routing table, such as (sorted by priority):

1. *Prefix-Length*: where longer subnet masks are preferred (independent if it is within a routing protocol or over different routing protocol)
2. *Metric*: where a lower metric/cost is preferred (only valid within one and the same routing protocol)
3. *Administrative distance*: where a lower distance is preferred (only valid between different routing protocols)

Most routing algorithms use only one network path at a time. Multipath routing techniques enable the use of multiple alternative paths.

Routing, in a more narrow sense of the term, is often contrasted with bridging in its assumption that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within localized environments.



Routing calculates good paths through a network for information to take. For example, from node 1 to node 6 the best routes are likely to be 1-8-7-6 or 1-8-10-6, as this has the thickest routes.

Network service

Network services are applications hosted by servers on a computer network, to provide some functionality for members or users of the network, or to help the network itself to operate.

The World Wide Web, E-mail,^[30] printing and network file sharing are examples of well-known network services. Network services such as DNS (Domain Name System) give names for IP and MAC addresses (people remember names like "nm.lan" better than numbers like "210.121.67.18"),^[31] and DHCP to ensure that the equipment on the network has a valid IP address.^[32]

Services are usually based on a service protocol that defines the format and sequencing of messages between clients and servers of that network service.

Network performance

Quality of service

Depending on the installation requirements, network performance is usually measured by the quality of service of a telecommunications product. The parameters that affect this typically can include throughput, jitter, bit error rate and latency.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network, viz. ATM:

- Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads.^[33] Other types of performance measures can include the level of noise and echo.
- ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.^[34]

There are many ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modelled instead of measured. For example, state transition diagrams are often used to model queuing performance in a circuit-switched network. The network planner uses these diagrams to analyze how the network performs in each state, ensuring that the network is optimally designed.^[35]

Network congestion

Network congestion occurs when a link or node is carrying so much data that its quality of service deteriorates. Typical effects include queueing delay, packet loss or the blocking of new connections. A consequence of these latter two is that incremental increases in offered load lead either only to small increase in network throughput, or to an actual reduction in network throughput.

Network protocols that use aggressive retransmissions to compensate for packet loss tend to keep systems in a state of network congestion—even after the initial load is reduced to a level that would not normally induce network congestion. Thus, networks using these protocols can exhibit two stable states under the same level of load. The stable state with low throughput is known as *congestive collapse*.

Modern networks use congestion control, congestion avoidance and traffic control techniques to try to avoid congestion collapse. These include: exponential backoff in protocols such as 802.11's CSMA/CA and the original Ethernet, window reduction in TCP, and fair queueing in devices such as routers. Another method to avoid the negative effects of network congestion is implementing priority schemes, so that some packets are transmitted with higher priority than others. Priority schemes do not solve network congestion by themselves, but they help to alleviate the effects of congestion for some services. An example of this is 802.1p. A third method to avoid network congestion is the explicit allocation of network resources to specific flows. One example of this is the use of Contention-Free Transmission Opportunities (CFTXOPs) in the ITU-T G.hn standard, which provides high-speed (up to 1 Gbit/s) Local area networking over existing home wires (power lines, phone lines and coaxial cables).

For the Internet, RFC 2914 (<https://tools.ietf.org/html/rfc2914>) addresses the subject of congestion control in detail.

Network resilience

Network resilience is "the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation."^[36]

Security

Network security

Network security consists of provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and its network-accessible resources.^[37] Network security is the authorization of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority. Network security is used on a variety of computer networks, both public and private, to secure daily transactions and communications among businesses, government agencies and individuals.

Network surveillance

Network surveillance is the monitoring of data being transferred over computer networks such as the Internet. The monitoring is often done surreptitiously and may be done by or at the behest of governments, by corporations, criminal organizations, or individuals. It may or may not be legal and may or may not require authorization from a court or other independent agency.

Computer and network surveillance programs are widespread today, and almost all Internet traffic is or could potentially be monitored for clues to illegal activity.

Surveillance is very useful to governments and law enforcement to maintain social control, recognize and monitor threats, and prevent/investigate criminal activity. With the advent of programs such as the Total Information Awareness program, technologies such as high speed surveillance computers and biometrics software, and laws such as the Communications Assistance For Law Enforcement Act, governments now possess an unprecedented ability to monitor the activities of citizens.^[38]

However, many civil rights and privacy groups—such as Reporters Without Borders, the Electronic Frontier Foundation, and the American Civil Liberties Union—have expressed concern that increasing surveillance of citizens may lead to a mass surveillance society, with limited political and personal freedoms. Fears such as this have led to numerous lawsuits such as *Hepting v. AT&T*.^{[38][39]} The hacktivist group Anonymous has hacked into government websites in protest of what it considers "draconian surveillance".^{[40][41]}

End to end encryption

End-to-end encryption (E2EE) is a digital communications paradigm of uninterrupted protection of data traveling between two communicating parties. It involves the originating party encrypting data so only the intended recipient can decrypt it, with no dependency on third parties. End-to-end encryption prevents intermediaries, such as Internet providers or application service providers, from discovering or tampering with communications. End-to-end encryption generally protects both confidentiality and integrity.

Examples of end-to-end encryption include HTTPS for web traffic, PGP for email, OTR for instant messaging, ZRTP for telephony, and TETRA for radio.

Typical server-based communications systems do not include end-to-end encryption. These systems can only guarantee protection of communications between clients and servers, not between the communicating parties themselves. Examples of non-E2EE systems are Google Talk, Yahoo Messenger, Facebook, and Dropbox. Some such systems, for example LavaBit and SecretInk, have even described themselves as offering "end-to-end" encryption when they do not. Some systems that normally offer end-to-end encryption have turned out to contain a back door that subverts negotiation of the encryption key between the communicating parties, for example Skype or Hushmail.

The end-to-end encryption paradigm does not directly address risks at the communications endpoints themselves, such as the technical exploitation of clients, poor quality random number generators, or key escrow. E2EE also does not address traffic analysis, which relates to things such as the identities of the end points and the times and quantities of messages that are sent.

SSL/TLS

The introduction and rapid growth of e-commerce on the world wide web in the mid-1990s made it obvious that some form of authentication and encryption was needed. Netscape took the first shot at a new standard. At the time, the dominant web browser was Netscape Navigator. Netscape created a standard called secure socket layer (SSL). SSL requires a server with a certificate. When a client requests access to an SSL-secured server, the server sends a copy of the certificate to the client. The SSL client checks this certificate (all web browsers come with an exhaustive list of CA root certificates preloaded), and if the certificate checks out, the server is authenticated and the client negotiates a symmetric-key cipher for use in the session. The session is now in a very secure encrypted tunnel between the SSL server and the SSL client.^[13]

Views of networks

Users and network administrators typically have different views of their networks. Users can share printers and some servers from a workgroup, which usually means they are in the same geographic location and are on the same LAN, whereas a Network Administrator is responsible to keep that network up and running. A community of interest has less of a connection of being in a local area, and should be thought of as a set of arbitrarily located users who share a set of servers, and possibly also communicate via peer-to-peer technologies.

Network administrators can see networks from both physical and logical perspectives. The physical perspective involves geographic locations, physical cabling, and the network elements (e.g., routers, bridges and application layer gateways) that interconnect via the transmission media. Logical networks, called, in the TCP/IP architecture, subnets, map onto one or more transmission media. For example, a common practice in a campus of buildings is to make a set of LAN cables in each building appear to be a common subnet, using virtual LAN (VLAN) technology.

Both users and administrators are aware, to varying extents, of the trust and scope characteristics of a network. Again using TCP/IP architectural terminology, an intranet is a community of interest under private administration usually by an enterprise, and is only accessible by authorized users (e.g. employees).^[42] Intranets do not have to be connected to the Internet, but generally have a limited connection. An extranet is an extension of an intranet that allows secure communications to users outside of the intranet (e.g. business partners, customers).^[42]

Unofficially, the Internet is the set of users, enterprises, and content providers that are interconnected by Internet Service Providers (ISP). From an engineering viewpoint, the Internet is the set of subnets, and aggregates of subnets, which share the registered IP address space and exchange information about the reachability of those IP addresses using the Border Gateway Protocol. Typically, the human-readable names of servers are translated to IP addresses, transparently to users, via the directory function of the Domain Name System (DNS).

Over the Internet, there can be business-to-business (B2B), business-to-consumer (B2C) and consumer-to-consumer (C2C) communications. When money or sensitive information is exchanged, the communications are apt to be protected by some form of communications security mechanism. Intranets and extranets can be securely superimposed onto the Internet, without any access by general Internet users and administrators, using secure Virtual Private Network (VPN) technology.

Journals and newsletters

- Open Computer Science (<https://www.degruyter.com/view/j/comp>) (open access journal)

See also

- Comparison of network diagram software
- Cyberspace
- History of the Internet

- [Network simulation](#)
- [Network planning and design](#)
- [Network traffic control](#)
- [Minimum-Pairs Protocol](#)

References

1. *Computer network definition* (<https://web.archive.org/web/20120121061919/http://www.atis.org/glossary/definition.aspx?id=6555>), archived from the original (<http://www.atis.org/glossary/definition.aspx?id=6555>) on 2012-01-21, retrieved 2011-11-12
2. "История о том, как пионер кибернетики оказался не нужен СССР" (<http://ria.ru/technology/20100809/263341026.html>) [The story of how a cybernetics pioneer became unnecessary to the USSR]. *ria.ru* (in Russian). ММА «Россия сегодня». 2010-08-09. Retrieved 2015-03-04. "Главным делом жизни Китова, увы, не доведенным до практического воплощения, можно считать разработку плана создания компьютерной сети (Единой государственной сети вычислительных центров - ЕГСВЦ) для управления народным хозяйством и одновременно для решения военных задач. Этот план Анатолий Иванович предложил сразу в высшую инстанцию, направив в январе 1959 года письмо генсеку КПСС Никите Хрущеву. Не получив ответа (хотя начинание на словах было поддержано в различных кругах), осенью того же года он заново направляет на самый верх письмо, приложив к нему 200-страничный детальный проект, получивший название 'Красной книги'. [One can regard the magnum opus of Kitov's career as his elaboration of the plan – unfortunately never brought into practical form – for the establishment of a computer network (the Unified State Network of Computer Centres – EGSVTs) for the control of the national economy and simultaneously for the resolution of military tasks. Anatoliï Ivanovich presented this plan directly to the highest levels, sending a letter in January 1959 to the General Secretary of the Communist Party of the Soviet Union Nikita Khrushchev. Not receiving a reply (although supported in various circles), in the autumn of the same year he again sent a letter to the very top, appending a 200-page detailed project plan, called the 'Red Book']"
3. Isaacson, Walter (2014). *The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution* (<https://books.google.com/books?id=4V9koAEACAAJ&lpg=PP1&pg=PA245#v=onepage&q&f=false>). Simon and Schuster. pp. 237–246.
4. "Inductee Details - Paul Baran" (<http://www.invent.org/honor/inductees/inductee-detail/?IID=316>). National Inventors Hall of Fame. Retrieved 6 September 2017.
5. "Inductee Details - Donald Watts Davies" (<http://www.invent.org/honor/inductees/inductee-detail/?IID=328>). National Inventors Hall of Fame. Retrieved 6 September 2017.
6. Roberts, Larry; Marrill, Tom (October 1966). *Toward a Cooperative Network of Time-Shared Computers* (<http://www.packet.cc/files/toward-coop-net.html>). Fall AFIPS Conference.
7. Chris Sutton. "Internet Began 35 Years Ago at UCLA with First Message Ever Sent Between Two Computers" (<https://web.archive.org/web/20080308120314/http://www.engineer.ucla.edu/stories/2004/Internet35.htm>). *UCLA*. Archived from the original (<http://www.engineer.ucla.edu/stories/2004/Internet35.htm>) on March 8, 2008.
8. Gillies, James; Cailliau, Robert (2000). *How the Web was Born: The Story of the World Wide Web* (<https://books.google.com/books?id=pIH-JijUNS0C&lpg=PA25&ots=MKZi0F7pJN&pg=PA25#v=onepage&q&f=false>). Oxford University Press. p. 25. ISBN 0192862073.
9. C. Hempstead; W. Worthington (2005). *Encyclopedia of 20th-Century Technology* (https://books.google.com/books?id=2ZCNAgAAQBAJ&pg=PA574&hl=en&sa=X&redir_esc=y#v=onepage&q&f=false). Routledge
10. Bennett, Richard (September 2009). "Designed for Change: End-to-End Arguments, Internet Innovation, and the Net Neutrality Debate" (<https://www.itif.org/files/2009-designed-for-change.pdf>) (PDF). Information Technology and Innovation Foundation. p. 11. Retrieved 11 September 2017.
11. Ethernet: Distributed Packet Switching for Local Computer Networks (<http://www.acm.org/classics/apr96/>) Archived (<https://web.archive.org/web/20070807213308/http://www.acm.org/classics/apr96/>) 2007-08-07 at the *Wayback Machine*, Robert M. Metcalfe and David R. Boggs, Communications of the ACM (pp 395–404, Vol. 19, No. 5), July 1976.
12. Spurgeon, Charles E. (2000). *Ethernet The Definitive Guide*. O'Reilly & Associates. ISBN 1-56592-660-9.
13. 1961-, Meyers, Mike, (2012). *CompTIA Network+ exam guide : (exam N10-005)* (<https://www.worldcat.org/oclc/748332969>) (5th ed ed.). New York: McGraw-Hill. ISBN 9780071789226. OCLC 748332969 (<https://www.worldcat.org/oclc/748332969>)

14. [1] (<http://smallbusiness.chron.com/disadvantages-wired-technology-17833.html>), The Disadvantages of Wired Technology, Laura Acevedo, Demand Media.
15. "Bergen Linux User Group's CIP Implementation" (<http://www.blug.linux.no/rfc1149>). Blug.linux.no. Retrieved 2014-03-01.
16. A. Hooke (September 2000), *Interplanetary Internet* (<https://web.archive.org/web/20120113053223/http://www.ipnsig.org/reports/ISART9-2000.pdf>) (PDF), Third Annual International Symposium on Advanced Radio Technologies, archived from the original (<http://www.ipnsig.org/reports/ISART9-2000.pdf>) (PDF) on 2012-01-13, retrieved 2011-11-12
17. "Define switch" (<http://www.webopedia.com/TERM/s/switch.html>). WWW.Wikipedia.com. Retrieved April 8, 2008.
18. "What bridge devices and bridging do for computer networks" (http://compnetworking.about.com/cs/internetworkin/g/g/bldef_bridge.htm).
19. D. Andersen; H. Balakrishnan; M. Kaashoek; R. Morris (October 2001), *Resilient Overlay Networks* (<http://nms.lcs.mit.edu/papers/ron-sosp2001.html>), Association for Computing Machinery, retrieved 2011-11-12
20. "End System Multicast" (<https://web.archive.org/web/20050221110350/http://esm.cs.cmu.edu/>), project web site, Carnegie Mellon University. Archived from the original (<http://esm.cs.cmu.edu/>) on February 21, 2005. Retrieved May 25, 2013.
21. For an interesting write-up of the technologies involved, including the deep stacking of communication protocols used, see Martin, Thomas. "Design Principles for DSL-Based Access Solutions" (http://www.gsi.dit.upm.es/~legf/Varios/XDSL_MARTI.PDF) (PDF). Retrieved 18 June 2011.
22. Paetsch, Michael (1993): The evolution of mobile communications in the US and Europe. Regulation, technology, and markets. Boston, London: Artech House (The Artech House mobile communications library).
23. Nanoscale Communication Networks, Bush, S. F., ISBN 978-1-60807-003-9, Artech House, 2010. [2] (<https://www.amazon.com/Nanoscale-Communication-Networks-Stephen-Bush/dp/1608070034>)
24. "personal area network (PAN)" (http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci546288,00.html). Retrieved January 29, 2011.
25. *New global standard for fully networked home* (<https://web.archive.org/web/20090221090736/http://www.itu.int/ITU-T/newslog/New+Global+Standard+For+Fully+Networked+Home.aspx>), ITU-T, 2008-12-12, archived from the original (<http://www.itu.int/ITU-T/newslog/New+Global+Standard+For+Fully+Networked+Home.aspx>) on 2009-02-21, retrieved 2011-11-12
26. *IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force* (<http://www.ieee802.org/3/ba/>), retrieved 2011-11-12
27. "Mobile Broadband Wireless connections (MBWA)" (<http://grouper.ieee.org/groups/802/20/>). Retrieved 2011-11-12.
28. Mansfield-Devine, Steve (December 2009). "Darknets". *Computer Fraud & Security*. 2009 (12): 4–6. doi:10.1016/S1361-3723(09)70150-2 (<https://doi.org/10.1016/S1361-3723%2809%2970150-2>).
29. Wood, Jessica (2010). "The Darknet: A Digital Copyright Revolution" (<http://jolt.richmond.edu/v16i4/article14.pdf>) (PDF). *Richmond Journal of Law and Technology*. 16 (4). Retrieved 25 October 2011.
30. rfc5321
31. RFC 1035 (<https://tools.ietf.org/html/rfc1035>), *Domain names – Implementation and Specification*, P. Mockapetris (November 1987)
32. Peterson LL, Davie BS. (2011). *Computer Networks: A Systems Approach* (<https://books.google.com/books?id=BvaFreun1W8C&pg=PA372&lpg=PA372>).
33. *Teletraffic Engineering Handbook* (<https://web.archive.org/web/20070111015452/http://oldwww.com.dtu.dk/teletraff/handbook/telenook.pdf>) (PDF), ITU-T Study Group 2, archived from the original (<http://www.com.dtu.dk/teletraff/handbook/telenook.pdf>) (PDF) on 2007-01-11
34. *Telecommunications Magazine Online* (<http://www.telecommagazine.com/>), Americas January 2003, Issue Highlights, Online Exclusive: Broadband Access Maximum Performance, Retrieved on February 13, 2005.
35. "State Transition Diagrams" (https://web.archive.org/web/20031015010139/http://cne.gmu.edu/modules/os_perf/std.t.html). Archived from the original (http://cne.gmu.edu/modules/os_perf/std.t.html) on October 15, 2003. Retrieved July 13, 2003.
36. "Definitions: Resilience" (http://wiki.ittc.ku.edu/resilinetns_wiki/index.php/Definitions#Resilience) ResiliNets Research Initiative. Retrieved 2011-11-12.

37. Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attack". *Lecture Notes in Computer Science*. Lecture Notes in Computer Science. 3285: 317–323. doi:10.1007/978-3-540-30176-9_41 (https://doi.org/10.1007/978-3-540-30176-9_41). ISBN 978-3-540-23659-7.
38. "Is the U.S. Turning Into a Surveillance Society?" (https://www.aclu.org/privacy/gen/index.html). *American Civil Liberties Union*. Retrieved March 13, 2009.
39. "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society" (https://www.aclu.org/FilesPD/Fs/aclu_report_bigger_monster_weaker_chains.pdf) (PDF). *American Civil Liberties Union*. January 15, 2003. Retrieved March 13, 2009.
40. "Anonymous hacks UK government sites over 'draconian surveillance' " (http://www.zdnet.com/blog/security/anonymous-hacks-uk-government-sites-over-draconian-surveillance/11412), Emil Protalinski, ZDNet, 7 April 2012, retrieved 12 March 2013
41. Hacktivists in the frontline battle for the internet (https://www.theguardian.com/technology/2012/apr/20/hacktivists-battle-internet) retrieved 17 June 2012
42. RFC 2547 (https://tools.ietf.org/html/rfc2547)

⦿ This article incorporates public domain material from the General Services Administration document "Federal Standard 1037C" (http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm).

Further reading

- Shelly, Gary, et al. "Discovering Computers" 2003 Edition.
- Wendell Odom, Rus Healy, Denise Donohue. (2010) CCIE Routing and Switching. Indianapolis, IN: Cisco Press
- Kurose James F and Keith W. Ross : Computer Networking: A Top-Down Approach Featuring the Internet, Pearson Education 2005.
- William Stallings, *Computer Networking with Internet Protocols and Technology*, Pearson Education 2004.
- Important publications in computer networks
- Network Communication Architecture and Protocols: OSI Network Architecture 7 Layers Model
- Dimitri Bertsekas, and Robert Gallager, "Data Networks," Prentice Hall, 1992.

External links

- Networking (https://curlie.org/Computers/Software/Networking/) at Curlie (based on DMOZ)
 - IEEE Ethernet manufacturer information (http://standards.ieee.org/regauth/oui/oui.txt)
 - A computer networking acronym guide (http://www.ciena.com/insights/acronym-guide/)
-

Retrieved from "https://en.wikipedia.org/w/index.php?title=Computer_network&oldid=852171183"

This page was last edited on 27 July 2018, at 03:46 (UTC).

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.

Computer security

From Wikipedia, the free encyclopedia

Computer security, also known as **cyber security** or **IT security**, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide.^[1]

It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection,^[2] and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures.^[3]

The field is of growing importance due to the increasing reliance on computer systems and the Internet in most societies,^[4] wireless networks such as Bluetooth and Wi-Fi – and the growth of "smart" devices, including smartphones, televisions and tiny devices as part of the Internet of Things.

Contents

- 1 Vulnerabilities and attacks
 - 1.1 Backdoors
 - 1.2 Denial-of-service attack
 - 1.3 Direct-access attacks
 - 1.4 Eavesdropping
 - 1.5 Spoofing
 - 1.6 Tampering
 - 1.7 Privilege escalation
 - 1.8 Phishing
 - 1.9 Clickjacking
 - 1.10 Social engineering
- 2 Systems at risk
 - 2.1 Financial systems
 - 2.2 Utilities and industrial equipment
 - 2.3 Aviation
 - 2.4 Consumer devices
 - 2.5 Large corporations
 - 2.6 Automobiles
 - 2.7 Government
 - 2.8 Internet of Things and physical vulnerabilities
- 3 Impact of security breaches
- 4 Attacker motivation
- 5 Computer protection (countermeasures)
 - 5.1 Security by design
 - 5.2 Security architecture
 - 5.3 Security measures
 - 5.4 Vulnerability management
 - 5.5 Reducing vulnerabilities
 - 5.6 Hardware protection mechanisms
 - 5.7 Secure operating systems
 - 5.8 Secure coding
 - 5.9 Capabilities and access control lists

- 5.10 Response to breaches
- 6 Notable attacks and breaches
 - 6.1 Robert Morris and the first computer worm
 - 6.2 Rome Laboratory
 - 6.3 TJX customer credit card details
 - 6.4 Stuxnet attack
 - 6.5 Global surveillance disclosures
 - 6.6 Target and Home Depot breaches
 - 6.7 Ashley Madison breach
- 7 Legal issues and global regulation
- 8 Government
- 9 Actions and teams in the US
 - 9.1 Legislation
 - 9.2 Agencies
 - 9.3 Computer emergency readiness team
- 10 International actions
 - 10.1 Europe
- 11 National teams
 - 11.1 Canada
 - 11.2 China
 - 11.3 Germany
 - 11.4 India
 - 11.5 Pakistan
 - 11.6 South Korea
 - 11.7 Other countries
- 12 Modern warfare
- 13 Job market
- 14 Terminology
- 15 Scholars
- 16 See also
- 17 Further reading
- 18 References
- 19 External links

Vulnerabilities and attacks

A vulnerability is a system susceptibility or flaw. Many vulnerabilities are documented in the Common Vulnerabilities and Exposures (CVE) database. An *exploitable* vulnerability is one for which at least one working attack or "exploit" exists.^[5]

To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of the categories below:

Backdoors

A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration. They may have been added by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability.

Denial-of-service attack

Denial of service attacks are designed to make a machine or network resource unavailable to its intended users.^[6] Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points – and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet, but a range of other techniques are possible including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

Direct-access attacks

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, keyloggers, covert listening devices or using wireless mice.^[7] Even when the system is protected by standard security measures, these may be able to be by-passed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and Trusted Platform Module are designed to prevent these attacks.

Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as Carnivore and NarusInsight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware; TEMPEST is a specification by the NSA referring to these attacks.

Spoofing

Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security.^[8]

Tampering

Tampering describes a malicious modification of products. So-called "Evil Maid" attacks and security services planting of surveillance capability into routers^[9] are examples.

Privilege escalation

Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. So for example a standard computer user may be able to fool the system into giving them access to restricted data; or even to "become root" and have full unrestricted access to a system.

Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users.^[10] Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Preying on a victim's trusting, phishing can be classified as a form of social engineering.

Clickjacking

Clickjacking, also known as "UI redress attack" or "User Interface redress attack", is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page. This is done using multiple transparent or opaque layers. The attacker is basically "hijacking" the clicks meant for the top level page and routing them to some other irrelevant page, most likely owned by someone else. A similar technique can be used to hijack keystrokes. Carefully drafting a combination of stylesheets, iframes, buttons and text boxes, a user can be led into believing that they are typing the password or other information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

Social engineering

Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer.^[11]

A popular and profitable cyber scam involves fake CEO emails sent to accounting and finance departments. In early 2016, the FBI reported that the scam has cost US businesses more than \$2bn in about two years.^[12]

In May 2016, the Milwaukee Bucks NBA team was the victim of this type of cyber scam with a perpetrator impersonating the team's president Peter Feigin, resulting in the handover of all the team's employees' 2015 W-2 tax forms.^[13]

Systems at risk

Computer security is critical in almost any industry which uses computers. Currently, most electronic devices such as computers, laptops and cellphones come with built in firewall security software, but despite this, computers are not 100 percent accurate and dependable to protect our data (Smith, Grabosky & Urbas, 2004.) There are many different ways of hacking into computers. It can be done through a network system, clicking into unknown links, connecting to unfamiliar Wi-Fi, downloading software and files from unsafe sites, power consumption, electromagnetic radiation waves, and many more. However, computers can be protected through well built software and hardware. By having strong internal interactions of properties, software complexity can prevent software crash and security failure.^[14]

Financial systems

Web sites and apps that accept or store credit card numbers, brokerage accounts, and bank account information are prominent hacking targets, because of the potential for immediate financial gain from transferring money, making purchases, or selling the information on the black market.^[15] In-store payment systems and ATMs have also been tampered with in order to gather customer account data and PINs.

Utilities and industrial equipment

Computers control functions at many utilities, including coordination of telecommunications, the power grid, nuclear power plants, and valve opening and closing in water and gas networks. The Internet is a potential attack vector for such machines if connected, but the Stuxnet worm demonstrated that even equipment controlled by computers not connected to the Internet can be vulnerable to physical damage caused by malicious commands sent to industrial equipment (in that case uranium enrichment centrifuges) which are infected via removable media. In 2014, the Computer Emergency Readiness Team, a division of the Department of Homeland Security, investigated 79 hacking incidents at energy companies.^[16] Vulnerabilities in smart meters (many of which use local radio or cellular communications) can cause problems with billing fraud.^[17]

Aviation

The aviation industry is very reliant on a series of complex system which could be attacked.^[18] A simple power outage at one airport can cause repercussions worldwide,^[19] much of the system relies on radio transmissions which could be disrupted,^[20] and controlling aircraft over oceans is especially dangerous because radar surveillance only extends 175 to 225 miles offshore.^[21] There is also potential for attack from within an aircraft.^[22]

In Europe, with the (Pan-European Network Service)^[23] and NewPENS,^[24] and in the US with the NextGen program,^[25] air navigation service providers are moving to create their own dedicated networks.

The consequences of a successful attack range from loss of confidentiality to loss of system integrity, which may lead to more serious concerns such as exfiltration of data, network and air traffic control outages, which in turn can lead to airport closures, loss of aircraft, loss of passenger life, damages on the ground and to transportation infrastructure. A successful attack on a military aviation system that controls munitions could have even more serious consequences.

Consumer devices

Desktop computers and laptops are commonly infected with malware either to gather passwords or financial account information, or to construct a botnet to attack another target. Smart phones, tablet computers, smart watches, and other mobile devices such as Quantified Self devices like activity trackers have also become targets and many of these have sensors such as cameras, microphones, GPS receivers, compasses, and accelerometers which could be exploited, and may collect personal information, including sensitive health information. Wifi, Bluetooth, and cell phone networks on any of these devices could be used as attack vectors, and sensors might be remotely activated after a successful breach.^[26]

Home automation devices such as the Nest thermostat are also potential targets.^[26]

Large corporations

Large corporations are common targets. In many cases this is aimed at financial gain through identity theft and involves data breaches such as the loss of millions of clients' credit card details by Home Depot,^[27] Staples,^[28] and Target Corporation.^[29] Medical records have been targeted for use in general

identify theft, health insurance fraud, and impersonating patients to obtain prescription drugs for recreational purposes or resale.^[30]

Not all attacks are financially motivated however; for example security firm HBGary Federal suffered a serious series of attacks in 2011 from hacktivist group Anonymous in retaliation for the firm's CEO claiming to have infiltrated their group,^{[31][32]} and Sony Pictures was attacked in 2014 where the motive appears to have been to embarrass with data leaks, and cripple the company by wiping workstations and servers.^{[33][34]}

Automobiles

If access is gained to a car's internal controller area network, it is possible to disable the brakes and turn the steering wheel.^[35] Computerized engine timing, cruise control, anti-lock brakes, seat belt tensioners, door locks, airbags and advanced driver assistance systems make these disruptions possible, and self-driving cars go even further. Connected cars may use wifi and bluetooth to communicate with onboard consumer devices, and the cell phone network to contact concierge and emergency assistance services or get navigational or entertainment information; each of these networks is a potential entry point for malware or an attacker.^[35] Researchers in 2011 were even able to use a malicious compact disc in a car's stereo system as a successful attack vector,^[36] and cars with built-in voice recognition or remote assistance features have onboard microphones which could be used for eavesdropping.

A 2015 report by U.S. Senator Edward Markey criticized manufacturers' security measures as inadequate, and also highlighted privacy concerns about driving, location, and diagnostic data being collected, which is vulnerable to abuse by both manufacturers and hackers.^[37]

Government

Government and military computer systems are commonly attacked by activists^{[38][39][40][41]} and foreign powers.^{[42][43][44][45]} Local and regional government infrastructure such as traffic light controls, police and intelligence agency communications, personnel records, student records,^[46] and financial systems are also potential targets as they are now all largely computerized. Passports and government ID cards that control access to facilities which use RFID can be vulnerable to cloning.

Internet of Things and physical vulnerabilities

The Internet of Things (IoT) is the network of physical objects such as devices, vehicles, and buildings that are embedded with electronics, software, sensors, and network connectivity that enables them to collect and exchange data^[47] – and concerns have been raised that this is being developed without appropriate consideration of the security challenges involved.^{[48][49]}

While the IoT creates opportunities for more direct integration of the physical world into computer-based systems,^{[50][51]} it also provides opportunities for misuse. In particular, as the Internet of Things spreads widely, cyber attacks are likely to become an increasingly physical (rather than simply virtual) threat.^[52] If a front door's lock is connected to the Internet, and can be locked/unlocked from a phone, then a criminal could enter the home at the press of a button from a stolen or hacked phone. People could stand to lose much more than their credit card numbers in a world controlled by IoT-enabled devices. Thieves have also used electronic means to circumvent non-Internet-connected hotel door locks.^[53]

Medical devices have either been successfully attacked or had potentially deadly vulnerabilities demonstrated, including both in-hospital diagnostic equipment^[54] and implanted devices including pacemakers^[55] and insulin pumps.^[56]

Impact of security breaches

Serious financial damage has been caused by security breaches, but because there is no standard model for estimating the cost of an incident, the only data available is that which is made public by the organizations involved. "Several computer security consulting firms produce estimates of total worldwide losses attributable to virus and worm attacks and to hostile digital acts in general. The 2003 loss estimates by these firms range from \$13 billion (worms and viruses only) to \$226 billion (for all forms of covert attacks). The reliability of these estimates is often challenged; the underlying methodology is basically anecdotal."^[57]

However, reasonable estimates of the financial cost of security breaches can actually help organizations make rational investment decisions. According to the classic Gordon-Loeb Model analyzing the optimal investment level in information security, one can conclude that the amount a firm spends to protect information should generally be only a small fraction of the expected loss (i.e., the expected value of the loss resulting from a cyber/information security breach).^[58]

Attacker motivation

As with physical security, the motivations for breaches of computer security vary between attackers. Some are thrill-seekers or vandals, others are activists or criminals looking for financial gain. State-sponsored attackers are now common and well resourced, but started with amateurs such as Markus Hess who hacked for the KGB, as recounted by Clifford Stoll, in *The Cuckoo's Egg*.

A standard part of threat modelling for any particular system is to identify what might motivate an attack on that system, and who might be motivated to breach it. The level and detail of precautions will vary depending on the system to be secured. A home personal computer, bank, and classified military network face very different threats, even when the underlying technologies in use are similar.

Computer protection (countermeasures)

In computer security a countermeasure is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.^{[59][60][61]}

Some common countermeasures are listed in the following sections:

Security by design

Security by design, or alternately secure by design, means that the software has been designed from the ground up to be secure. In this case, security is considered as a main feature.

Some of the techniques in this approach include:

- The principle of least privilege, where each part of the system has only the privileges that are needed for its function. That way even if an attacker gains access to that part, they have only

limited access to the whole system.

- Automated theorem proving to prove the correctness of crucial software subsystems.
- Code reviews and unit testing, approaches to make modules more secure where formal correctness proofs are not possible.
- Defense in depth, where the design is such that more than one subsystem needs to be violated to compromise the integrity of the system and the information it holds.
- Default secure settings, and design to "fail secure" rather than "fail insecure" (see fail-safe for the equivalent in safety engineering). Ideally, a secure system should require a deliberate, conscious, knowledgeable and free decision on the part of legitimate authorities in order to make it insecure.
- Audit trails tracking system activity, so that when a security breach occurs, the mechanism and extent of the breach can be determined. Storing audit trails remotely, where they can only be appended to, can keep intruders from covering their tracks.
- Full disclosure of all vulnerabilities, to ensure that the "window of vulnerability" is kept as short as possible when bugs are discovered.

Security architecture

The Open Security Architecture organization defines IT security architecture as "the design artifacts that describe how the security controls (security countermeasures) are positioned, and how they relate to the overall information technology architecture. These controls serve the purpose to maintain the system's quality attributes: confidentiality, integrity, availability, accountability and assurance services".^[62]

Techopedia defines security architecture as "a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible." The key attributes of security architecture are:^[63]

- the relationship of different components and how they depend on each other.
- the determination of controls based on risk assessment, good practice, finances, and legal matters.
- the standardization of controls.

Security measures

A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following:

- User account access controls and cryptography can protect systems files and data, respectively.
- Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware- or software-based.
- Intrusion Detection System (IDS) products are designed to detect network attacks in-progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.
- "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected.

Today, computer security comprises mainly "preventive" measures, like firewalls or an exit procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and can be implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as Linux, built into the

operating system kernel) to provide real time filtering and blocking. Another implementation is a so-called "physical firewall", which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet.

Some organizations are turning to big data platforms, such as Apache Hadoop, to extend data accessibility and machine learning to detect advanced persistent threats.^{[64][65]}

However, relatively few organisations maintain computer systems with effective detection systems, and fewer still have organised response mechanisms in place. As result, as Reuters points out: "Companies for the first time report they are losing more through electronic theft of data than physical stealing of assets".^[66] The primary obstacle to effective eradication of cyber crime could be traced to excessive reliance on firewalls and other automated "detection" systems. Yet it is basic evidence gathering by using packet capture appliances that puts criminals behind bars.

Vulnerability management

Vulnerability management is the cycle of identifying, and remediating or mitigating vulnerabilities",^[67] especially in software and firmware. Vulnerability management is integral to computer security and network security.

Vulnerabilities can be discovered with a vulnerability scanner, which analyzes a computer system in search of known vulnerabilities,^[68] such as open ports, insecure software configuration, and susceptibility to malware

Beyond vulnerability scanning, many organisations contract outside security auditors to run regular penetration tests against their systems to identify vulnerabilities. In some sectors this is a contractual requirement.^[69]

Reducing vulnerabilities

While formal verification of the correctness of computer systems is possible,^{[70][71]} it is not yet common. Operating systems formally verified include seL4,^[72] and SYSGO's PikeOS^{[73][74]} – but these make up a very small percentage of the market.

Cryptography properly implemented is now virtually impossible to directly break. Breaking them requires some non-cryptographic input, such as a stolen key, stolen plaintext (at either end of the transmission), or some other extra cryptanalytic information.

Two factor authentication is a method for mitigating unauthorized access to a system or sensitive information. It requires "something you know"; a password or PIN, and "something you have"; a card, dongle, cellphone, or other piece of hardware. This increases security as an unauthorized person needs both of these to gain access.

Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Training is often involved to help mitigate this risk,^{[75][76]} but even in a highly disciplined environments (e.g. military organizations), social engineering attacks can still be difficult to foresee and prevent.

It is possible to reduce an attacker's chances by keeping systems up to date with security patches and updates, using a security scanner or/and hiring competent people responsible for security. The effects of data loss/damage can be reduced by careful backing up and insurance.

Hardware protection mechanisms

While hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process,^{[77][78]} hardware-based or assisted computer security also offers an alternative to software-only computer security. Using devices and methods such as dongles, trusted platform modules, intrusion-aware cases, drive locks, disabling USB ports, and mobile-enabled access may be considered more secure due to the physical access (or sophisticated backdoor access) required in order to be compromised. Each of these is covered in more detail below.

- USB dongles are typically used in software licensing schemes to unlock software capabilities,^[79] but they can also be seen as a way to prevent unauthorized access to a computer or other device's software. The dongle, or key, essentially creates a secure encrypted tunnel between the software application and the key. The principle is that an encryption scheme on the dongle, such as Advanced Encryption Standard (AES) provides a stronger measure of security, since it is harder to hack and replicate the dongle than to simply copy the native software to another machine and use it. Another security application for dongles is to use them for accessing web-based content such as cloud software or Virtual Private Networks (VPNs).^[80] In addition, a USB dongle can be configured to lock or unlock a computer.^[81]
- Trusted platform modules (TPMs) secure devices by integrating cryptographic capabilities onto access devices, through the use of microprocessors, or so-called computers-on-a-chip. TPMs used in conjunction with server-side software offer a way to detect and authenticate hardware devices, preventing unauthorized network and data access.^[82]
- Computer case intrusion detection refers to a push-button switch which is triggered when a computer case is opened. The firmware or BIOS is programmed to show an alert to the operator when the computer is booted up the next time.
- Drive locks are essentially software tools to encrypt hard drives, making them inaccessible to thieves.^[83] Tools exist specifically for encrypting external drives as well.^[84]
- Disabling USB ports is a security option for preventing unauthorized and malicious access to an otherwise secure computer. Infected USB dongles connected to a network from a computer inside the firewall are considered by the magazine Network World as the most common hardware threat facing computer networks.^[85]
- Mobile-enabled access devices are growing in popularity due to the ubiquitous nature of cell phones. Built-in capabilities such as Bluetooth, the newer Bluetooth low energy (LE), Near field communication (NFC) on non-iOS devices and biometric validation such as thumb print readers, as well as QR code reader software designed for mobile devices, offer new, secure ways for mobile phones to connect to access control systems. These control systems provide computer security and can also be used for controlling access to secure buildings.^[86]

Secure operating systems

One use of the term "computer security" refers to technology that is used to implement secure operating systems. In the 1980s the United States Department of Defense (DoD) used the "Orange Book"^[87] standards, but the current international standard ISO/IEC 15408, "Common Criteria" defines a number of progressively more stringent Evaluation Assurance Levels. Many common operating systems meet the EAL4 standard of being "Methodically Designed, Tested and Reviewed", but the formal verification

required for the highest levels means that they are uncommon. An example of an EAL6 ("Semiformally Verified Design and Tested") system is Integrity-178B, which is used in the Airbus A380^[88] and several military jets.^[89]

Secure coding

In software engineering, secure coding aims to guard against the accidental introduction of security vulnerabilities. It is also possible to create software designed from the ground up to be secure. Such systems are "secure by design". Beyond this, formal verification aims to prove the correctness of the algorithms underlying a system;^[90] important for cryptographic protocols for example.

Capabilities and access control lists

Within computer systems, two of many security models capable of enforcing privilege separation are access control lists (ACLs) and capability-based security. Using ACLs to confine programs has been proven to be insecure in many situations, such as if the host computer can be tricked into indirectly allowing restricted file access, an issue known as the confused deputy problem. It has also been shown that the promise of ACLs of giving access to an object to only one person can never be guaranteed in practice. Both of these problems are resolved by capabilities. This does not mean practical flaws exist in all ACL-based systems, but only that the designers of certain utilities must take responsibility to ensure that they do not introduce flaws.

Capabilities have been mostly restricted to research operating systems, while commercial OSs still use ACLs. Capabilities can, however, also be implemented at the language level, leading to a style of programming that is essentially a refinement of standard object-oriented design. An open source project in the area is the E language.

The most secure computers are those not connected to the Internet and shielded from any interference. In the real world, the most secure systems are operating systems where security is not an add-on.

Response to breaches

Responding forcefully to attempted security breaches (in the manner that one would for attempted physical security breaches) is often very difficult for a variety of reasons:

- Identifying attackers is difficult, as they are often in a different jurisdiction to the systems they attempt to breach, and operate through proxies, temporary anonymous dial-up accounts, wireless connections, and other anonymising procedures which make backtracing difficult and are often located in yet another jurisdiction. If they successfully breach security, they are often able to delete logs to cover their tracks.
- The sheer number of attempted attacks is so large that organisations cannot spend time pursuing each attacker (a typical home user with a permanent (e.g., cable modem) connection will be attacked at least several times per day, so more attractive targets could be presumed to see many more). Note however, that most of the sheer bulk of these attacks are made by automated vulnerability scanners and computer worms.
- Law enforcement officers are often unfamiliar with information technology, and so lack the skills and interest in pursuing attackers. There are also budgetary constraints. It has been argued that the high cost of technology, such as DNA testing, and improved forensics mean less money for other kinds of law enforcement, so the overall rate of criminals not getting dealt with goes up as the cost of the technology increases. In addition, the identification of attackers across a network may require logs from various points in the network and in many countries, the release of these records

to law enforcement (with the exception of being voluntarily surrendered by a network administrator or a system administrator) requires a search warrant and, depending on the circumstances, the legal proceedings required can be drawn out to the point where the records are either regularly destroyed, or the information is no longer relevant.

Notable attacks and breaches

Some illustrative examples of different types of computer security breaches are given below.

Robert Morris and the first computer worm

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers – the first internet "computer worm".^[91] The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.^[91]

Rome Laboratory

In 1994, over a hundred intrusions were made by unidentified crackers into the Rome Laboratory, the US Air Force's main command and research facility. Using trojan horses, hackers were able to obtain unrestricted access to Rome's networking systems and remove traces of their activities. The intruders were able to obtain classified files, such as air tasking order systems data and furthermore able to penetrate connected networks of National Aeronautics and Space Administration's Goddard Space Flight Center, Wright-Patterson Air Force Base, some Defense contractors, and other private sector organizations, by posing as a trusted Rome center user.^[92]

TJX customer credit card details

In early 2007, American apparel and home goods company TJX announced that it was the victim of an unauthorized computer systems intrusion^[93] and that the hackers had accessed a system that stored data on credit card, debit card, check, and merchandise return transactions.^[94]

Stuxnet attack

The computer worm known as Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges^[95] by disrupting industrial programmable logic controllers (PLCs) in a targeted attack generally believed to have been launched by Israel and the United States^{[96][97][98][99]} although neither has publicly acknowledged this.

Global surveillance disclosures

In early 2013, massive breaches of computer security by the NSA were revealed, including deliberately inserting a backdoor in a NIST standard for encryption^[100] and tapping the links between Google's data centres.^[101] These were disclosed by NSA contractor Edward Snowden.^[102]

Target and Home Depot breaches

In 2013 and 2014, a Russian/Ukrainian hacking ring known as "Rescator" broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards,^[103] and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers.^[104] Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee – meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Ashley Madison breach

In July 2015, a hacker group known as "The Impact Team" successfully breached the extramarital relationship website Ashley Madison. The group claimed that they had taken not only company data but user data as well. After the breach, The Impact Team dumped emails from the company's CEO, to prove their point, and threatened to dump customer data unless the website was taken down permanently. With this initial data release, the group stated "Avid Life Media has been instructed to take Ashley Madison and Established Men offline permanently in all forms, or we will release all customer records, including profiles with all the customers' secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails. The other websites may stay online."^[105] When Avid Life Media, the parent company that created the Ashley Madison website, did not take the site offline, The Impact Group released two more compressed files, one 9.7GB and the second 20GB. After the second data dump, Avid Life Media CEO Noel Biderman resigned, but the website remained functional.

Legal issues and global regulation

Conflict of laws in cyberspace has become a major cause of concern for computer security community. Some of the main challenges and complaints about the antivirus industry are the lack of global web regulations, a global base of common rules to judge, and eventually punish, cyber crimes and cyber criminals. There is no global cyber law and cybersecurity treaty that can be invoked for enforcing global cybersecurity issues.

International legal issues of cyber attacks are complicated in nature. Even if an antivirus firm locates the cyber criminal behind the creation of a particular virus or piece of malware or form of cyber attack, often the local authorities cannot take action due to lack of laws under which to prosecute.^{[106][107]} Authorship attribution for cyber crimes and cyber attacks is a major problem for all law enforcement agencies.

"[Computer viruses] switch from one country to another, from one jurisdiction to another – moving around the world, using the fact that we don't have the capability to globally police operations like this. So the Internet is as if someone [had] given free plane tickets to all the online criminals of the world."^[106] Use of dynamic DNS, fast flux and bullet proof servers have added own complexities to this situation.

Government

The role of the government is to make regulations to force companies and organizations to protect their systems, infrastructure and information from any cyber-attacks, but also to protect its own national infrastructure such as the national power-grid.^[108]

The question of whether the government should intervene or not in the regulation of the cyberspace is a very polemical one. Indeed, for as long as it has existed and by definition, the cyberspace is a virtual space free of any government intervention. Where everyone agree that an improvement on cybersecurity is more than vital, is the government the best actor to solve this issue? Many government officials and experts think that the government should step in and that there is a crucial need for regulation, mainly due to the failure of the private sector to solve efficiently the cybersecurity problem. R. Clarke said during a panel discussion at the RSA Security Conference in San Francisco, he believes that the "industry only responds when you threaten regulation. If industry doesn't respond (to the threat), you have to follow through."^[109] On the other hand, executives from the private sector agree that improvements are necessary, but think that the government intervention would affect their ability to innovate efficiently.

Actions and teams in the US

Legislation

The 1986 18 U.S.C. § 1030 (<https://www.law.cornell.edu/uscode/text/18/1030>), more commonly known as the Computer Fraud and Abuse Act is the key legislation. It prohibits unauthorized access or damage of "protected computers" as defined in 18 U.S.C. § 1030(e)(2) (https://www.law.cornell.edu/uscode/text/18/1030#e_2).

Although various other measures have been proposed, such as the "Cybersecurity Act of 2010 – S. 773" in 2009, the "International Cybercrime Reporting and Cooperation Act – H.R.4962"^[110] and "Protecting Cyberspace as a National Asset Act of 2010 – S.3480"^[111] in 2010 – none of these has succeeded.

Executive order 13636 *Improving Critical Infrastructure Cybersecurity* was signed February 12, 2013.

Agencies

The Department of Homeland Security has a dedicated division responsible for the response system, risk management program and requirements for cybersecurity in the United States called the National Cyber Security Division.^{[112][113]} The division is home to US-CERT operations and the National Cyber Alert System.^[113] The National Cybersecurity and Communications Integration Center brings together government organizations responsible for protecting computer networks and networked infrastructure.^[114]

The third priority of the Federal Bureau of Investigation (FBI) is to: *"Protect the United States against cyber-based attacks and high-technology crimes"*,^[115] and they, along with the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA) are part of the multi-agency task force, The Internet Crime Complaint Center, also known as IC3.^[116]

In addition to its own specific duties, the FBI participates alongside non-profit organizations such as InfraGard.^{[117][118]}

In the criminal division of the United States Department of Justice operates a section called the Computer Crime and Intellectual Property Section. The CCIPS is in charge of investigating computer crime and intellectual property crime and is specialized in the search and seizure of digital evidence in computers and networks.^[119]

The United States Cyber Command, also known as USCYBERCOM, is tasked with the defense of specified Department of Defense information networks and *"ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."*^[120] It has no role in the protection of civilian networks.^{[121][122]}

The U.S. Federal Communications Commission's role in cybersecurity is to strengthen the protection of critical communications infrastructure, to assist in maintaining the reliability of networks during disasters, to aid in swift recovery after, and to ensure that first responders have access to effective communications services.^[123]

The Food and Drug Administration has issued guidance for medical devices,^[124] and the National Highway Traffic Safety Administration^[125] is concerned with automotive cybersecurity. After being criticized by the Government Accountability Office,^[126] and following successful attacks on airports and claimed attacks on airplanes, the Federal Aviation Administration has devoted funding to securing systems on board the planes of private manufacturers, and the Aircraft Communications Addressing and Reporting System.^[127] Concerns have also been raised about the future Next Generation Air Transportation System.^[128]

Computer emergency readiness team

"Computer emergency response team" is a name given to expert groups that handle computer security incidents. In the US, two distinct organization exist, although they do work closely together.

- US-CERT: part of the National Cyber Security Division of the United States Department of Homeland Security.^[129]
- CERT/CC: created by the Defense Advanced Research Projects Agency (DARPA) and run by the Software Engineering Institute (SEI).

International actions

Many different teams and organisations exist, including:

- The Forum of Incident Response and Security Teams (FIRST) is the global association of CSIRTs.^[130] The US-CERT, AT&T, Apple, Cisco, McAfee, Microsoft are all members of this international team.^[131]
- The Council of Europe helps protect societies worldwide from the threat of cybercrime through the Convention on Cybercrime.^[132]
- The purpose of the Messaging Anti-Abuse Working Group (MAAWG) is to bring the messaging industry together to work collaboratively and to successfully address the various forms of messaging abuse, such as spam, viruses, denial-of-service attacks and other messaging exploitations.^[133] France Telecom, Facebook, AT&T, Apple, Cisco, Sprint are some of the members of the MAAWG.^[134]
- ENISA : The European Network and Information Security Agency (ENISA) is an agency of the European Union with the objective to improve network and information security in the European

Union.

Europe

CSIRTs in Europe collaborate in the TERENA task force TF-CSIRT. TERENA's Trusted Introducer service provides an accreditation and certification scheme for CSIRTs in Europe. A full list of known CSIRTs in Europe is available from the Trusted Introducer website.

National teams

Here are the main computer emergency response teams around the world. Most countries have their own team to protect network security.

Canada

On October 3, 2010, Public Safety Canada unveiled Canada's Cyber Security Strategy, following a Speech from the Throne commitment to boost the security of Canadian cyberspace.^[135]^[136] The aim of the strategy is to strengthen Canada's "cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world."^[136] Three main pillars define the strategy: securing government systems, partnering to secure vital cyber systems outside the federal government, and helping Canadians to be secure online.^[136] The strategy involves multiple departments and agencies across the Government of Canada.^[137] The Cyber Incident Management Framework for Canada outlines these responsibilities, and provides a plan for coordinated response between government and other partners in the event of a cyber incident.^[138] The Action Plan 2010–2015 for Canada's Cyber Security Strategy outlines the ongoing implementation of the strategy.^[139]

Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) is responsible for mitigating and responding to threats to Canada's critical infrastructure and cyber systems. The CCIRC provides support to mitigate cyber threats, technical support to respond and recover from targeted cyber attacks, and provides online tools for members of Canada's critical infrastructure sectors.^[140] The CCIRC posts regular cyber security bulletins on the Public Safety Canada website.^[141] The CCIRC also operates an online reporting tool where individuals and organizations can report a cyber incident.^[142] Canada's Cyber Security Strategy is part of a larger, integrated approach to critical infrastructure protection, and functions as a counterpart document to the National Strategy and Action Plan for Critical Infrastructure.^[137]

On September 27, 2010, Public Safety Canada partnered with STOP.THINK.CONNECT, a coalition of non-profit, private sector, and government organizations dedicated to informing the general public on how to protect themselves online.^[143] On February 4, 2014, the Government of Canada launched the Cyber Security Cooperation Program.^[144] The program is a \$1.5 million five-year initiative aimed at improving Canada's cyber systems through grants and contributions to projects in support of this objective.^[145] Public Safety Canada aims to begin an evaluation of Canada's Cyber Security Strategy in early 2015.^[137] Public Safety Canada administers and routinely updates the GetCyberSafe portal for Canadian citizens, and carries out Cyber Security Awareness Month during October.^[146]

China

China's network security and information technology leadership team was established February 27, 2014. The leadership team is tasked with national security and long-term development and co-ordination of major issues related to network security and information technology. Economic, political, cultural, social and military fields as related to network security and information technology strategy, planning and major macroeconomic policy are being researched. The promotion of national network security and information technology law are constantly under study for enhanced national security capabilities.

Germany

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

India

Some provisions for cybersecurity have been incorporated into rules framed under the Information Technology Act 2000.

The National Cyber Security Policy 2013 is a policy framework by Department of Electronics and Information Technology (DeitY) which aims to protect the public and private infrastructure from cyber attacks, and safeguard "information, such as personal information (of web users), financial and banking information and sovereign data".

The Indian Companies Act 2013 has also introduced cyber law and cyber security obligations on the part of Indian directors.

Pakistan

Cyber-crime has risen rapidly in Pakistan. There are about 34 million Internet users with 133.4 million mobile subscribers in Pakistan. According to Cyber Crime Unit (CCU), a branch of Federal Investigation Agency, only 62 cases were reported to the unit in 2007, 287 cases in 2008, ratio dropped in 2009 but in 2010, more than 312 cases were registered. However, there are many unreported incidents of cyber-crime.^[147]

"Pakistan's Cyber Crime Bill 2007", the first pertinent law, focuses on electronic crimes, for example cyber-terrorism, criminal access, electronic system fraud, electronic forgery, and misuse of encryption.^[147]

National Response Centre for Cyber Crime (NR3C) – FIA is a law enforcement agency dedicated to fight cybercrime. Inception of this Hi-Tech crime fighting unit transpired in 2007 to identify and curb the phenomenon of technological abuse in society.^[148] However, certain private firms are also working in cohesion with the government to improve cyber security and curb cyberattacks.^[149]

South Korea

Following cyberattacks in the first half of 2013, when government, news-media, television station, and bank websites were compromised, the national government committed to the training of 5,000 new cybersecurity experts by 2017. The South Korean government blamed its northern counterpart for these attacks, as well as incidents that occurred in 2009, 2011,^[150] and 2012, but Pyongyang denies the accusations.^[151]

Other countries

- CERT Brazil, member of FIRST (Forum for Incident Response and Security Teams)
- CARNet CERT, Croatia, member of FIRST
- AE CERT, United Arab Emirates
- SingCERT, Singapore
- CERT-LEXSI, France, Canada, Singapore
- INCIBE, Spain
- ID-CERT, Indonesia

Modern warfare

Cybersecurity is becoming increasingly important as more information and technology is being made available on cyberspace. There is growing concern among governments that cyberspace will become the next theatre of warfare. As Mark Clayton from the *Christian Science Monitor* described in an article titled "The New Cyber Arms Race":

In the future, wars will not just be fought by soldiers with guns or with planes that drop bombs. They will also be fought with the click of a mouse a half a world away that unleashes carefully weaponized computer programs that disrupt or destroy critical industries like utilities, transportation, communications, and energy. Such attacks could also disable military networks that control the movement of troops, the path of jet fighters, the command and control of warships.^[152]

This has led to new terms such as *cyberwarfare* and *cyberterrorism*. More and more critical infrastructure is being controlled via computer programs that, while increasing efficiency, exposes new vulnerabilities. The test will be to see if governments and corporations that control critical systems such as energy, communications and other information will be able to prevent attacks before they occur. As Jay Cross, the chief scientist of the Internet Time Group, remarked, "Connectedness begets vulnerability."^[152]

Job market

Cybersecurity is a fast-growing^[153] field of IT concerned with reducing organizations' risk of hack or data breach. According to research from the Enterprise Strategy Group, 46% of organizations say that they have a "problematic shortage" of cybersecurity skills in 2016, up from 28% in 2015.^[154] Commercial, government and non-governmental organizations all employ cybersecurity professionals. The fastest increases in demand for cybersecurity workers are in industries managing increasing volumes of consumer data such as finance, health care, and retail.^[155] However, the use of the term "cybersecurity" is more prevalent in government job descriptions.^[156]

Typical cybersecurity job titles and descriptions include:^[157]

Security analyst

Analyzes and assesses vulnerabilities in the infrastructure (software, hardware, networks), investigates using available tools and countermeasures to remedy the detected vulnerabilities, and recommends solutions and best practices. Analyzes and assesses damage to the data/infrastructure as a result of security incidents, examines available recovery tools and processes, and recommends solutions. Tests for compliance with security policies and procedures. May assist in the creation, implementation, and/or management of security solutions.

Security engineer

Performs security monitoring, security and data/logs analysis, and forensic analysis, to detect security incidents, and mounts incident response. Investigates and utilizes new technologies and processes to enhance security capabilities and implement improvements. May also review code or perform other security engineering methodologies.

Security architect

Designs a security system or major components of a security system, and may head a security design team building a new security system.

Security administrator

Installs and manages organization-wide security systems. May also take on some of the tasks of a security analyst in smaller organizations.

Chief Information Security Officer (CISO)

A high-level management position responsible for the entire information security division/staff. The position may include hands-on technical work.

Chief Security Officer (CSO)

A high-level management position responsible for the entire security division/staff. A newer position now deemed needed as security risks grow.

Security Consultant/Specialist/Intelligence

Broad titles that encompass any one or all of the other roles/titles, tasked with protecting computers, networks, software, data, and/or information systems against viruses, worms, spyware, malware, intrusion detection, unauthorized access, denial-of-service attacks, and an ever increasing list of attacks by hackers acting as individuals or as part of organized crime or foreign governments.

Student programs are also available to people interested in beginning a career in cybersecurity.^{[158][159]} Meanwhile, a flexible and effective option for information security professionals of all experience levels to keep studying is online security training, including webcasts.^{[160][161][162]}

Terminology

The following terms used with regards to engineering secure systems are explained below.

- Access authorization restricts access to a computer to group of users through the use of authentication systems. These systems can protect either the whole computer – such as through an interactive login screen – or individual services, such as an FTP server. There are many methods for identifying and authenticating users, such as passwords, identification cards, and, more recently, smart cards and biometric systems.
- Anti-virus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).
- Applications with known security flaws should not be run. Either leave it turned off until it can be patched or otherwise fixed, or delete it and replace it with some other application. Publicly known flaws are the main entry used by worms to automatically break into a system and then spread to other systems connected to it. The security website Secunia provides a search tool for unpatched known flaws in popular products.

- Authentication techniques can be used to ensure that communication end-points are who they say they are.
- Automated theorem proving and other verification tools can enable critical algorithms and code used in secure systems to be mathematically proven to meet their specifications.
- Backups are a way of securing information; they are another copy of all the important computer files kept in another location. These files are kept on hard disks, CD-Rs, CD-RWs, tapes and more recently on the cloud. Suggested locations for backups are a fireproof, waterproof, and heat proof safe, or in a separate, offsite location than that in which the original files are contained. Some individuals and companies also keep their backups in safe deposit boxes inside bank vaults. There is also a fourth option, which involves using one of the file hosting services that backs up files over the Internet for both business and individuals, known as the cloud.
 - Backups are also important for reasons other than security. Natural disasters, such as earthquakes, hurricanes, or tornadoes, may strike the building where the computer is located. The building can be on fire, or an explosion may occur. There needs to be a recent backup at an alternate secure location, in case of such kind of disaster. Further, it is recommended that the alternate location be placed where the same disaster would not affect both locations. Examples of alternate disaster recovery sites being compromised by the same disaster that affected the primary site include having had a primary site in World Trade Center I and the recovery site in 7 World Trade Center, both of which were destroyed in the 9/11 attack, and having one's primary site and recovery site in the same coastal region, which leads to both being vulnerable to hurricane damage (for example, primary site in New Orleans and recovery site in Jefferson Parish, both of which were hit by Hurricane Katrina in 2005). The backup media should be moved between the geographic sites in a secure manner, in order to prevent them from being stolen.
- Capability and access control list techniques can be used to ensure privilege separation and mandatory access control. This section discusses their use.
- Chain of trust techniques can be used to attempt to ensure that all software loaded has been certified as authentic by the system's designers.
- Confidentiality is the nondisclosure of information except to another authorized person.^[163]
- Cryptographic techniques can be used to defend data in transit between systems, reducing the probability that data exchanged between systems can be intercepted or modified.
- Cyberwarfare is an internet-based conflict that involves politically motivated attacks on information and information systems. Such attacks can, for example, disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems.
- Data integrity is the accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record.^[164]
- Encryption is used to protect the message from the eyes of others. Cryptographically secure ciphers are designed to make any practical attempt of breaking infeasible. Symmetric-key ciphers are suitable for bulk encryption using shared keys, and public-key encryption using digital certificates can provide a practical solution for the problem of securely communicating when no key is shared in advance.
- Endpoint security software helps networks to prevent exfiltration (data theft) and virus infection at network entry points made vulnerable by the prevalence of potentially infected portable computing devices, such as laptops and mobile devices, and external storage devices, such as USB drives.^[165]
- Firewalls are an important method for control and security on the Internet and other networks.

This is secret stuff, PSE do not...

→ **5a0 (k\$hQ% ...**

→ **This is secret stuff, PSE do not...**

Cryptographic techniques involve transforming information, scrambling it so it becomes unreadable during transmission. The intended recipient can unscramble the message; ideally, eavesdroppers cannot.

network firewall can be a communications processor, typically a router, or a dedicated server, along with firewall software. A firewall serves as a gatekeeper system that protects a company's intranets and other computer networks from intrusion by providing a filter and safe transfer point for access to and from the Internet and other networks. It screens all network traffic for proper passwords or other security codes and only allows authorized transmission in and out of the network. Firewalls can deter, but not completely prevent, unauthorized access (hacking) into computer networks; they can also provide some protection from online intrusion.

- Honey pots are computers that are either intentionally or unintentionally left vulnerable to attack by crackers. They can be used to catch crackers or fix vulnerabilities.
- Intrusion-detection systems can scan a network for people that are on the network but who should not be there or are doing things that they should not be doing, for example trying a lot of passwords to gain access to the network.
- A microkernel is the near-minimum amount of software that can provide the mechanisms to implement an operating system. It is used solely to provide very low-level, very precisely defined machine code upon which an operating system can be developed. A simple example is the early '90s GEMSOS (Gemini Computers), which provided extremely low-level machine code, such as "segment" management, atop which an operating system could be built. The theory (in the case of "segments") was that—rather than have the operating system itself worry about mandatory access separation by means of military-style labeling—it is safer if a low-level, independently scrutinized module can be charged **solely** with the management of individually labeled segments, be they memory "segments" or file system "segments" or executable text "segments." If software below the visibility of the operating system is (as in this case) charged with labeling, there is no theoretically viable means for a clever hacker to subvert the labeling scheme, since the operating system *per se* does **not** provide mechanisms for interfering with labeling: the operating system is, essentially, a client (an "application," arguably) atop the microkernel and, as such, subject to its restrictions.
- Pinging The ping application can be used by potential crackers to find if an IP address is reachable. If a cracker finds a computer, they can try a port scan to detect and attack services on that computer.
- Social engineering awareness keeps employees aware of the dangers of social engineering and/or having a policy in place to prevent social engineering can reduce successful breaches of the network and servers.

Scholars

- | | | |
|-----------------------|----------------------|-----------------------|
| ■ Ross J. Anderson | ■ Deborah Estrin | ■ Peter G. Neumann |
| ■ Annie Anton | ■ Joan Feigenbaum | ■ Susan Nycum |
| ■ Adam Back | ■ Ian Goldberg | ■ Roger R. Schell |
| ■ Daniel J. Bernstein | ■ Shafi Goldwasser | ■ Bruce Schneier |
| ■ Matt Blaze | ■ Lawrence A. Gordon | ■ Dawn Song |
| ■ Stefan Brands | ■ Peter Gutmann | ■ Gene Spafford |
| ■ L. Jean Camp | ■ Paul Kocher | ■ Joseph Steinberg |
| ■ Lance Cottrell | ■ Monica S. Lam | ■ Salvatore J. Stolfo |
| ■ Lorrie Cranor | ■ Butler Lampson | ■ Willis Ware |
| ■ Dorothy E. Denning | ■ Brian LaMacchia | ■ Moti Yung |
| ■ Peter J. Denning | ■ Carl Landwehr | |
| ■ Cynthia Dwork | ■ Kevin Mitnick | |

See also

- | | | |
|---------------|----------------------------|------------------------------------|
| ■ Attack tree | ■ CertiVox | ■ Comparison of antivirus software |
| ■ CAPTCHA | ■ Cloud computing security | |
| ■ CERT | ■ Common Criteria | |

- Content Disarm & Reconstruction
- Content security
- Countermeasure (computer)
- Cyber hygiene
- Cyber Insurance
- Cyber security standards
- Dancing pigs
- Data loss prevention software
- Data security
- Differentiated security
- Disk encryption
- Exploit (computer security)
- Fault tolerance
- Human–computer interaction (security)
- Identity management
- Identity theft
- Identity-based security
- Information security awareness
- Internet privacy
- IT risk
- Kill chain
- List of Computer Security Certifications
- Mobile security
- Network security
- Network Security Toolkit
- Next-Generation Firewall
- Open security
- OWASP
- Penetration test
- Physical information security
- Presumed security
- Privacy software
- Proactive cyber defence
- Risk cybernetics
- Sandbox (computer security)
- Separation of protection and security
- Software Defined Perimeter

Further reading

- Wu, Chwan-Hwa (John); Irwin, J. David (2013). *Introduction to Computer Networks and Cybersecurity*. Boca Raton: CRC Press. ISBN 978-1466572133.
- Lee, Newton (2015). *Counterterrorism and Cybersecurity: Total Information Awareness* (2nd ed.). Springer. ISBN 978-3-319-17243-9.
- Singer, P. W.; Friedman, Allan (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press. ISBN 978-0199918119.
- Kim, Peter (2014). *The Hacker Playbook: Practical Guide To Penetration Testing*. Seattle: CreateSpace Independent Publishing Platform. ISBN 978-1494932633.

References

1. Gasser, Morrie (1988). *Building a Secure Computer System* (PDF). Van Nostrand Reinhold. p. 3. ISBN 0-442-23022-2. Retrieved 6 September 2015.
2. "Definition of computer security". *Encyclopedia*. Ziff Davis, PCMag. Retrieved 6 September 2015.
3. Rouse, Margaret. "Social engineering definition". TechTarget. Retrieved 6 September 2015.
4. "Reliance spells end of road for ICT amateurs" (<http://www.theaustralian.com.au/technology/opinion/reliance-spells-end-of-road-for-ict-amateurs/story-e6frgb0o-1226636267865?nk=34fe4ab684629535daaf6a8fe6e6ef3d>), May 07, 2013, The Australian
5. "Computer Security and Mobile Security Challenges" (pdf). *researchgate.net*. Retrieved 2016-08-04.
6. "Distributed Denial of Service Attack". *csa.gov.sg*. Retrieved 12 November 2014.
7. Wireless mouse leave billions at risk of computer hack: cyber security firm (<http://gadgtecs.com/2016/03/30/wifi-mouse-leave-billions-risk-computer-hack/>)
8. [1] (<https://www.techopedia.com/definition/5398/spoofing>)
9. Gallagher, Sean (May 14, 2014). "Photos of an NSA "upgrade" factory show Cisco router getting implant". *Ars Technica*. Retrieved August 3, 2014.
10. "Identifying Phishing Attempts". Case.
11. Arcos Sergio. "Social Engineering" (PDF).
12. Scannell, Kara (24 Feb 2016). "CEO email scam costs companies \$2bn". *Financial Times* (25 Feb 2016). Retrieved 7 May 2016.
13. "Bucks leak tax info of players, employees as result of email scam". *Associated Press*. 20 May 2016. Retrieved 20 May 2016.
14. J. C. Willemssen, "FAA Computer Security". GAO/T-AIMD-00-330. Presented at Committee on Science, House of Representatives, 2000.
15. Financial Weapons of War, Minnesota Law Review (2016), available at: <http://ssrn.com/abstract=2765010>

16. Pagliery, Jose. "Hackers attacked the U.S. energy grid 79 times this year". *CNN Money*. Cable News Network. Retrieved 16 April 2015.
17. "Vulnerabilities in Smart Meters and the C12.12 Protocol". SecureState. 2012-02-16. Retrieved 4 November 2016.
18. P. G. Neumann, "Computer Security in Aviation," presented at International Conference on Aviation Safety and Security in the 21st Century, White House Commission on Safety and Security, 1997.
19. J. Zellan, Aviation Security. Hauppauge, NY: Nova Science, 2003, pp. 65–70.
20. "Air Traffic Control Systems Vulnerabilities Could Make for Unfriendly Skies [Black Hat] - SecurityWeek.Com".
21. "Hacker Says He Can Break Into Airplane Systems Using In-Flight Wi-Fi". *NPR.org*. 4 August 2014.
22. Jim Finkle (4 August 2014). "Hacker says to show passenger jets at risk of cyber attack". *Reuters*.
23. "Pan-European Network Services (PENS) - Eurocontrol.int".
24. "Centralised Services: NewPENS moves forward - Eurocontrol.int".
25. "NextGen Program About Data Comm - FAA.gov".
26. "Is Your Watch Or Thermostat A Spy? Cybersecurity Firms Are On It". *NPR.org*. 6 August 2014.
27. Melvin Backman (18 September 2014). "Home Depot: 56 million cards exposed in breach". *CNNMoney*.
28. "Staples: Breach may have affected 1.16 million customers' cards". *Fortune.com*. December 19, 2014. Retrieved 2014-12-21.
29. "Target security breach affects up to 40M cards". *Associated Press via Milwaukee Journal Sentinel*. 19 December 2013. Retrieved 21 December 2013.
30. Jim Finkle (23 April 2014). "Exclusive: FBI warns healthcare sector vulnerable to cyber attacks". *Reuters*. Retrieved 23 May 2016.
31. Bright, Peter (February 15, 2011). "Anonymous speaks: the inside story of the HBGary hack". *Arstechnica.com*. Retrieved March 29, 2011.
32. Anderson, Nate (February 9, 2011). "How one man tracked down Anonymous—and paid a heavy price". *Arstechnica.com*. Retrieved March 29, 2011.
33. Palilery, Jose (December 24, 2014). "What caused Sony hack: What we know now". *CNN Money*. Retrieved January 4, 2015.
34. James Cook (December 16, 2014). "Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far". *Business Insider*. Retrieved December 18, 2014.
35. Timothy B. Lee (18 January 2015). "The next frontier of hacking: your car". *Vox*.
36. Stephen Checkoway; Damon McCoy; Brian Kantor; Danny Anderson; Hovav Shacham; Stefan Savage; Karl Koscher; Alexei Czeskis; Franziska Roesner; Tadayoshi Kohno (2011). *Comprehensive Experimental Analyses of Automotive Attack Surfaces* (PDF). SEC'11 Proceedings of the 20th USENIX conference on Security. Berkeley, CA, US: USENIX Association. pp. 6–6.
37. Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk (PDF) (Report). 2015-02-06. Retrieved November 4, 2016.
38. "Internet strikes back: Anonymous' Operation Megaupload explained". *RT*. January 20, 2012. Archived from the original on May 5, 2013. Retrieved May 5, 2013.
39. "Gary McKinnon profile: Autistic 'hacker' who started writing computer programs at 14". *The Daily Telegraph*. London. 23 January 2009.
40. "Gary McKinnon extradition ruling due by 16 October". BBC News. September 6, 2012. Retrieved September 25, 2012.
41. Law Lords Department (30 July 2008). "House of Lords – Mckinnon V Government of The United States of America and Another". *Publications.parliament.uk*. Retrieved 30 January 2010. "15. ... alleged to total over \$700,000"
42. "NSA Accessed Mexican President's Email" (<http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html>), October 20, 2013, Jens Glüsing, Laura Poitras, Marcel Rosenbach and Holger Stark, *spiegel.de*
43. Sanders, Sam (4 June 2015). "Massive Data Breach Puts 4 Million Federal Employees' Records At Risk". *NPR*. Retrieved 5 June 2015.
44. Liptak, Kevin (4 June 2015). "U.S. government hacked; feds think China is the culprit". *CNN*. Retrieved 5 June 2015.
45. Sean Gallagher. "Encryption "would not have helped" at OPM, says DHS official".
46. "Schools Learn Lessons From Security Breaches". *Education Week*. 19 October 2015. Retrieved 23 May 2016.
47. "Internet of Things Global Standards Initiative". *ITU*. Retrieved 26 June 2015.

48. Singh, Jatinder; Pasquier, Thomas; Bacon, Jean; Ko, Hajoon; Eysers, David (2015). "Twenty Cloud Security Considerations for Supporting the Internet of Things". *IEEE Internet of Things Journal*: 1–1. doi:10.1109/JIOT.2015.2460333.
49. Chris Clearfield. "Why The FTC Can't Regulate The Internet Of Things". *Forbes*. Retrieved 26 June 2015.
50. "Internet of Things: Science Fiction or Business Fact?" (PDF). *Harvard Business Review*. Retrieved 4 November 2016.
51. Ovidiu Vermesan; Peter Friess. "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems" (PDF). River Publishers. Retrieved 4 November 2016.
52. Christopher Clearfield "Rethinking Security for the Internet of Things" Harvard Business Review Blog, 26 June 2013 (<http://blogs.hbr.org/2013/06/rethinking-security-for-the-in/>)
53. "Hotel room burglars exploit critical flaw in electronic door locks". *Ars Technica*. Retrieved 23 May 2016.
54. "Hospital Medical Devices Used As Weapons In Cyberattacks". *Dark Reading*. Retrieved 23 May 2016.
55. Jeremy Kirk (17 October 2012). "Pacemaker hack can deliver deadly 830-volt jolt". *Computerworld*. Retrieved 23 May 2016.
56. "How Your Pacemaker Will Get Hacked". *The Daily Beast*. Retrieved 23 May 2016.
57. Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). *The Economic Impact of Cyber-Attacks*. Congressional Research Service, Government and Finance Division. Washington DC: The Library of Congress.
58. Gordon, Lawrence; Loeb, Martin (November 2002). "The Economics of Information Security Investment". *ACM Transactions on Information and System Security*. **5** (4): 438–457. doi:10.1145/581271.581274.
59. RFC 2828 Internet Security Glossary
60. CNSS Instruction No. 4009 (http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf) dated 26 April 2010
61. InfosecToday Glossary (<http://www.infosec.today.com/Articles/Glossary.pdf>)
62. Definitions: IT Security Architecture (<http://www.opensecurityarchitecture.org/cms/definitions/it-security-architecture>). SecurityArchitecture.org, Jan, 2006
63. Janssen, Cory. "Security Architecture". *Techopedia*. Janalta Interactive Inc. Retrieved 9 October 2014.
64. "Cybersecurity at petabyte scale".
65. Woodie, Alex (9 May 2016). "Why ONI May Be Our Best Hope for Cyber Security Now". Retrieved 13 July 2016.
66. "Firms lose more to electronic than physical theft". Reuters.
67. Foreman, P: *Vulnerability Management*, page 1. Taylor & Francis Group, 2010. ISBN 978-1-4398-0150-5
68. Anna-Maija Juuso and Ari Takanen *Unknown Vulnerability Management*, Codenomicon whitepaper, October 2010 [2] (<http://www.codenomicon.com/solutions/unknown-vulnerability-management/>).
69. Alan Calder and Geraint Williams. *PCI DSS: A Pocket Guide, 3rd Edition*. ISBN 978-1-84928-554-4. "network vulnerability scans at least quarterly and after any significant change in the network"
70. Harrison, J. (2003). "Formal verification at Intel": 45–54. doi:10.1109/LICS.2003.1210044.
71. Umrigar, Zerkis D.; Pitchumani, Vijay (1983). "Formal verification of a real-time hardware design". *Proceeding DAC '83 Proceedings of the 20th Design Automation Conference*. IEEE Press. pp. 221–7. ISBN 0-8186-0026-8.
72. "Abstract Formal Specification of the seL4/ARMv6 API" (PDF). Retrieved May 19, 2015.
73. Christoph Baumann, Bernhard Beckert, Holger Blasum, and Thorsten Bormer Ingredients of Operating System Correctness? Lessons Learned in the Formal Verification of PikeOS (<http://www-wjp.cs.uni-saarland.de/publikationen/Ba10EW.pdf>)
74. "Getting it Right" (<http://www.ganssle.com/rants/gettingitright.htm>) by Jack Ganssle
75. Arachchilage, Nalin; Love, Steve; Scott, Michael (June 1, 2012). "Designing a Mobile Game to Teach Conceptual Knowledge of Avoiding 'Phishing Attacks'". *International Journal for e-Learning Security*. Infonomics Society. **2** (1): 127–132. Retrieved April 1, 2016.
76. Scott, Michael; Ghinea, Gheorghita; Arachchilage, Nalin (7 July 2014). *Assessing the Role of Conceptual Knowledge in an Anti-Phishing Educational Game* (pdf). Proceedings of the 14th IEEE International Conference on Advanced Learning Technologies. IEEE. p. 218. doi:10.1109/ICALT.2014.70. Retrieved April 1, 2016.
77. "The Hacker in Your Hardware: The Next Security Threat". *Scientific American*.
78. Waksman, Adam; Sethumadhavan, Simha (2010), "Tamper Evident Microprocessors" (PDF), *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, California
79. "Sentinel HASP HL". E-Spin. Retrieved 2014-03-20.
80. "Token-based authentication". SafeNet.com. Retrieved 2014-03-20.
81. "Lock and protect your Windows PC". TheWindowsClub.com. Retrieved 2014-03-20.

82. James Greene (2012). "Intel Trusted Execution Technology: White Paper" (PDF). Intel Corporation. Retrieved 2013-12-18.
83. "SafeNet ProtectDrive 8.4". SCMagazine.com. 2008-10-04. Retrieved 2014-03-20.
84. "Secure Hard Drives: Lock Down Your Data". PCMag.com. 2009-05-11.
85. "Top 10 vulnerabilities inside the network". Network World. 2010-11-08. Retrieved 2014-03-20.
86. "Forget IDs, use your phone as credentials". Fox Business Network. 2013-11-04. Retrieved 2014-03-20.
87. Lipner, Steve (2015). "The Birth and Death of the Orange Book". *IEEE Annals of the History of Computing*. **37** (2): 19–31. doi:10.1109/MAHC.2015.27.
88. Kelly Jackson Higgins (2008-11-18). "Secure OS Gets Highest NSA Rating, Goes Commercial". Dark Reading. Retrieved 2013-12-01.
89. "Board or bored? Lockheed Martin gets into the COTS hardware biz". VITA Technologies Magazine. December 10, 2010. Retrieved 9 March 2012.
90. Sanghavi, Alok (21 May 2010). "What is formal verification?". *EE Times Asia*.
91. Jonathan Zittrain, 'The Future of The Internet', Penguin Books, 2008
92. Information Security (<https://fas.org/irp/gao/aim96084.htm>). United States Department of Defense, 1986
93. "THE TJX COMPANIES, INC. VICTIMIZED BY COMPUTER SYSTEMS INTRUSION; PROVIDES INFORMATION TO HELP PROTECT CUSTOMERS" (Press release). The TJX Companies, Inc. 2007-01-17. Retrieved 2009-12-12.
94. Largest Customer Info Breach Grows (<http://www.myfoxtwincities.com/myfox/pages/Home/Detail?contentId=2804836&version=3&locale=EN-US&layoutCode=TSTY&pageId=1.1.1>). MyFox Twin Cities, 29 March 2007.
95. "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought". Business Insider. 20 November 2013.
96. Reals, Tucker (24 September 2010). "Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes?". CBS News.
97. Kim Zetter (17 February 2011). "Cyberwar Issues Likely to Be Addressed Only After a Catastrophe". Wired. Retrieved 18 February 2011.
98. Chris Carroll (18 October 2011). "Cone of silence surrounds U.S. cyberwarfare". Stars and Stripes. Retrieved 30 October 2011.
99. John Bumgarner (27 April 2010). "Computers as Weapons of War" (PDF). IO Journal. Retrieved 30 October 2011.
100. Newman, Lily Hay (9 October 2013). "Can You Trust NIST?". *IEEE Spectrum*.
101. "New Snowden Leak: NSA Tapped Google, Yahoo Data Centers" (<http://mashable.com/2013/10/30/nsa-google-yahoo-data-centers/>), Oct 31, 2013, Lorenzo Franceschi-Bicchierai, mashable.com
102. Seipel, Hubert. "Transcript: ARD interview with Edward Snowden". *La Foundation Courage*. Retrieved 11 June 2014.
103. Michael Riley; Ben Elgin; Dune Lawrence; Carol Matlack. "Target Missed Warnings in Epic Hack of Credit Card Data - Businessweek". *Businessweek.com*.
104. "Home Depot says 53 million emails stolen". *CNET*. CBS Interactive. 6 November 2014.
105. Mansfield-Devine, Steve (2015-09-01). "The Ashley Madison affair". *Network Security*. **2015** (9): 8–16. doi:10.1016/S1353-4858(15)30080-5.
106. "Mikko Hypponen: Fighting viruses, defending the net". TED.
107. "Mikko Hypponen – Behind Enemy Lines". Hack In The Box Security Conference.
108. "Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information". Government Accountability Office. Retrieved November 3, 2015.
109. Kirby, Carrie (June 24, 2011). "Former White House aide backs some Net regulation / Clarke says government, industry deserve 'F' in cybersecurity". *The San Francisco Chronicle*.
110. "Text of H.R.4962 as Introduced in House: International Cybercrime Reporting and Cooperation Act – U.S. Congress". OpenCongress. Retrieved 2013-09-25.
111. [3] (http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=4ee63497-ca5b-4a4b-9bb-a-04b7f4cb0123) Archived (https://web.archive.org/web/20120120040012/http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=4ee63497-ca5b-4a4b-9bba-04b7f4cb0123) January 20, 2012, at the Wayback Machine.
112. "National Cyber Security Division". U.S. Department of Homeland Security. Retrieved June 14, 2008.
113. "FAQ: Cyber Security R&D Center". U.S. Department of Homeland Security S&T Directorate. Retrieved June 14, 2008.
114. AFP-JiJi, "U.S. boots up cybersecurity center", October 31, 2009.

115. "Federal Bureau of Investigation – Priorities". Federal Bureau of Investigation.
116. Internet Crime Complaint Center (<http://www.ic3.gov/default.aspx>)
117. "Infragard, Official Site". *Infragard*. Retrieved 10 September 2010.
118. "Robert S. Mueller, III -- InfraGard Interview at the 2005 InfraGard Conference". *Infragard (Official Site) -- "Media Room"*. Retrieved 9 December 2009.
119. "CCIPS".
120. "U.S. Department of Defense, Cyber Command Fact Sheet". *stratcom.mil*. May 21, 2010.
121. "Speech:". Defense.gov. Retrieved 2010-07-10.
122. Shachtman, Noah. "Military's Cyber Commander Swears: "No Role" in Civilian Networks" (http://www.brookings.edu/opinions/2010/0923_military_internet_shachtman.aspx), The Brookings Institution (<http://www.brookings.edu/>), 23 September 2010.
123. "FCC Cybersecurity". FCC.
124. "Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication". Retrieved 23 May 2016.
125. "Automotive Cybersecurity - National Highway Traffic Safety Administration (NHTSA)". Retrieved 23 May 2016.
126. "U.S. GAO - Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen". Retrieved 23 May 2016.
127. Aliya Sternstein (4 March 2016). "FAA Working on New Guidelines for Hack-Proof Planes". *Nextgov*. Retrieved 23 May 2016.
128. Bart Elias (18 June 2015). "Protecting Civil Aviation from Cyberattacks" (PDF). Retrieved 4 November 2016.
129. Verton, Dan (January 28, 2004). "DHS launches national cyber alert system". *Computerworld*. IDG. Retrieved 2008-06-15.
130. "FIRST website".
131. "First members".
132. "European council".
133. "MAAWG".
134. "MAAWG".
135. "Government of Canada Launches Canada's Cyber Security Strategy". *Market Wired*. 3 October 2010. Retrieved 1 November 2014.
136. "Canada's Cyber Security Strategy". *Public Safety Canada*. Government of Canada. Retrieved 1 November 2014.
137. "Action Plan 2010–2015 for Canada's Cyber Security Strategy". *Public Safety Canada*. Government of Canada. Retrieved 3 November 2014.
138. "Cyber Incident Management Framework For Canada". *Public Safety Canada*. Government of Canada. Retrieved 3 November 2014.
139. "Action Plan 2010–2015 for Canada's Cyber Security Strategy". *Public Safety Canada*. Government of Canada. Retrieved 1 November 2014.
140. "Canadian Cyber Incident Response Centre". *Public Safety Canada*. Retrieved 1 November 2014.
141. "Cyber Security Bulletins". *Public Safety Canada*. Retrieved 1 November 2014.
142. "Report a Cyber Security Incident". *Public Safety Canada*. Government of Canada. Retrieved 3 November 2014.
143. "Government of Canada Launches Cyber Security Awareness Month With New Public Awareness Partnership". *Market Wired*. Government of Canada. 27 September 2012. Retrieved 3 November 2014.
144. "Cyber Security Cooperation Program". *Public Safety Canada*. Retrieved 1 November 2014.
145. "Cyber Security Cooperation Program". *Public Safety Canada*.
146. "GetCyberSafe". *Get Cyber Safe*. Government of Canada. Retrieved 3 November 2014.
147. "Cyber Security". *Tier3 — Cyber Security Services Pakistan*.
148. "National Response Centre For Cyber Crime".
149. "Cyber Security Services Pakistan". *Tier3 - Cyber Security Services Pakistan*.
150. "South Korea seeks global support in cyber attack probe". *BBC Monitoring Asia Pacific*. 7 March 2011.
151. Kwanwoo Jun (23 September 2013). "Seoul Puts a Price on Cyberdefense". *Wall Street Journal*. Dow Jones & Company, Inc. Retrieved 24 September 2013.
152. Clayton, Mark. "The new cyber arms race". *The Christian Science Monitor*. Retrieved 16 April 2015.
153. "Burning Glass Technologies, "Cybersecurity Jobs, 2015" ". July 2015. Retrieved 11 June 2016.
154. Oltsik, Jon. "Cybersecurity Skills Shortage Impact on Cloud Computing". *Network World*. Retrieved 2016-03-23.

155. [4] (<http://burning-glass.com/demand-for-cybersecurity-workers-outstripping-supply/>) Burning Glass Technologies, "Demand for Cybersecurity Workers Outstripping Supply," July 30, 2015, accessed 2016-06-11
156. de Silva, Richard (11 Oct 2011). "Government vs. Commerce: The Cyber Security Industry and You (Part One)". Defence IQ. Retrieved 24 Apr 2014.
157. "Department of Computer Science". Retrieved April 30, 2013.
158. "(Information for) Students". NICCS (US National Initiative for Cybercareers and Studies). Retrieved 24 April 2014.
159. "Current Job Opportunities at DHS". U.S. Department of Homeland Security. Retrieved 2013-05-05.
160. "Cybersecurity Training & Exercises". U.S. Department of Homeland Security. Retrieved 2015-01-09.
161. "Cyber Security Awareness Free Training and Webcasts". MS-ISAC (Multi-State Information Sharing & Analysis Center. Retrieved 9 January 2015.
162. "Security Training Courses". LearnQuest. Retrieved 2015-01-09.
163. "Confidentiality". Retrieved 2011-10-31.
164. "Data Integrity". Retrieved 2011-10-31.
165. "Endpoint Security". Retrieved 2014-03-15.

External links

 Media related to Computer security at Wikimedia Commons

- Computer security (<https://www.dmoz.org/Computers/Security/Policy/>) at DMOZ

Retrieved from "https://en.wikipedia.org/w/index.php?title=Computer_security&oldid=749456359"

Categories: Computer security | E-commerce | Secure communication | Computer network security | Crime prevention | National security | Cryptography | Computer security exploits | Cyberwarfare | Weapons countermeasures | Security technology | Cybercrime | Information governance

-
- This page was last modified on 14 November 2016, at 12:59.
 - Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Cyber security standards

From Wikipedia, the free encyclopedia

Cybersecurity standards (also styled **cyber security standards**)^[1] are techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organization.^[2] This environment includes users themselves, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. The principal objective is to reduce the risks, including prevention or mitigation of cyber-attacks. These published materials consist of collections of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies.

(Writing cybersecurity as two words (*cyber security*) or one (*cybersecurity*) depends on the institution.^[1] The spelling in Europe tends to consist of two words.^[3])

Contents

- 1 History
- 2 ETSI Cyber Security Technical Committee (TC CYBER)
- 3 ISO 27001 and 27002
- 4 *Standard of Good Practice*
- 5 NERC
- 6 NIST
- 7 ISO 15408
- 8 RFC 2196
- 9 ISA/IEC-62443 (formerly ISA-99)
- 10 IEC 62443 Conformity Assessment Program
- 11 IASME
- 12 See also
- 13 Notes
- 14 References
- 15 External links

History

Cybersecurity standards have existed over several decades as users and providers have collaborated in many domestic and international forums to effect the necessary capabilities, policies, and practices - generally emerging from work at the Stanford Consortium for Research on Information Security and Policy in the 1990s.^[4] Also many tasks that were once carried out by hand are now carried out by computer; therefore there is a need for information assurance (IA) and security.

A 2016 US security framework adoption study reported that 70% of the surveyed organizations see the NIST Cybersecurity Framework as the most popular best practice for computer security, but many note that it requires significant investment.^[5]

ETSI Cyber Security Technical Committee (TC CYBER)

IBM - Ex. 1002-Part 1 of 10, Page 170

IPR2025-00379 (IBM v. Croga)^{1/9}

TC CYBER is responsible for the standardisation of Cyber Security internationally and for providing a centre of relevant expertise for other ETSI committees.^[6] Growing dependence on networked digital systems has brought with it an increase in both the variety and quantity of cyber-threats. The different methods governing secure transactions in the various Member States of the European Union sometimes make it difficult to assess the respective risks and to ensure adequate security. Building on ETSI's world-leading expertise in the security of Information and Communications Technologies (ICT), it set up a new Cyber Security committee (TC CYBER) in 2014 to meet the growing demand for standards to protect the Internet and the communications and business it carries.

TC CYBER is working closely with relevant stakeholders to develop appropriate standards to increase privacy and security for organisations and citizens across Europe. The committee is looking in particular at the security of infrastructures, devices, services and protocols, as well as security tools and techniques to ensure security. It offers security advice and guidance to users, manufacturers and network and infrastructure operators. Its standards are freely available on-line. A principal work item effort is the production of a global cyber security ecosystem of standardization and other activities.^[7]

ISO 27001 and 27002

ISO/IEC 27001:2013, part of the growing ISO/IEC 27000 family of standards, is an information security management system (ISMS) standard published in October 2013 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements*.

ISO/IEC 27001:2013 formally specifies a management system that is intended to bring information security under explicit management control.

ISO/IEC 27002 incorporates mainly part 1 of the BS 7799 good security management practice standard. The latest versions of BS7799 is BS7799-3. Sometimes ISO/IEC 27002 is therefore referred to as ISO 17799 or BS 7799 part 1 and sometimes it refers to part 1 and part 7. BS 7799 part 1 provides an outline or good practice guide for cybersecurity management; whereas BS 7799 part 2 and ISO 27001 are normative and therefore provide a framework for certification. ISO/IEC 27002 is a high level guide to cybersecurity. It is most beneficial as explanatory guidance for the management of an organisation to obtain certification to the ISO 27001 standard. The certification once obtained lasts three years. Depending on the auditing organisation, no or some intermediate audits may be carried out during the three years.

ISO 27001 (ISMS) replaces BS 7799 part 2, but since it is backward compatible any organization working toward BS 7799 part 2 can easily transition to the ISO 27001 certification process. There is also a transitional audit available to make it easier once an organization is BS 7799 part 2-certified for the organization to become ISO 27001-certified. ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS). It states the information security systems required to implement ISO 27002 control objectives. Without ISO 27001, ISO 27002 control objectives are ineffective. ISO 27002 controls objectives are incorporated into ISO 27001 in Annex A.

ISO/IEC 21827 (SSE-CMM – ISO/IEC 21827) is an International Standard based on the Systems Security Engineering Capability Maturity Model (SSE-CMM) that can measure the maturity of ISO controls objectives.

Standard of Good Practice

In the 1990s, the Information Security Forum (ISF) published a comprehensive list of best practices for information security, published as the *Standard of Good Practice* (SoGP). The ISF continues to update the SoGP every two years (with the exception of 2013-2014); the latest version was published in 2016.

Originally the *Standard of Good Practice* was a private document available only to ISF members, but the ISF has since made the full document available for sale to the general public.

Among other programs, the ISF offers its member organizations a comprehensive benchmarking program based on the SoGP. Furthermore, it is important for those in charge of security management to understand and adhere to NERC CIP compliance requirements.

NERC

The North American Electric Reliability Corporation (NERC) addresses patching in NERC CIP 007-6 Requirement 2. Summarily, it requires Bulk Power System (BPS) Operators/Owners to identify the source or sources utilized to provide

Entire Security related patches for Cyber Assets utilized in the operation of the Registered Entities are required to check for new patches once every thirty five calendar days. Upon identification of a new patch, entities are required to evaluate applicability of a patch and then complete mitigation or installation activities within 35 calendar days of completion of assessment of applicability. e BPS.y

An initial attempt to create information security standards for the electrical power industry was created by NERC in 2003 and was known as NERC CSS (Cyber Security Standards).^[8] Subsequent to the CSS guidelines, NERC evolved and enhanced those requirements. The most widely recognized modern NERC security standard is NERC 1300, which is a modification/update of NERC 1200. The newest version of NERC 1300 is called CIP-002-3 through CIP-009-3 (CIP=Critical Infrastructure Protection). These standards are used to secure bulk electric systems although NERC has created standards within other areas. The bulk electric system standards also provide network security administration while still supporting best-practice industry processes.^[2]

NIST

1. The NIST Cybersecurity Framework (NIST CSF) "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes." It is intended to help private sector organizations that provide critical infrastructure with guidance on how to protect it, along with relevant protections for privacy and civil liberties.^[9]
2. Special publication 800-12 provides a broad overview of computer security and control areas. It also emphasizes the importance of the security controls and ways to implement them. Initially this document was aimed at the federal government although most practices in this document can be applied to the private sector as well. Specifically it was written for those people in the federal government responsible for handling sensitive systems.^[3]
3. Special publication 800-14 describes common security principles that are used. It provides a high level description of what should be incorporated within a computer security policy. It describes what can be done to improve existing security as well as how to develop a new security practice. Eight principles and fourteen practices are described within this document.^[4]
4. Special publication 800-26 provides advice on how to manage IT security. Superseded by NIST SP 800-53 rev3. This document emphasizes the importance of self assessments as well as risk

assessments. [5]

5. Special publication 800-37, updated in 2010 provides a new risk approach: "Guide for Applying the Risk Management Framework to Federal Information Systems"
6. Special publication 800-53 rev4, "Security and Privacy Controls for Federal Information Systems and Organizations", Published April 2013 updated to include updates as of January 15, 2014, specifically addresses the 194 security controls that are applied to a system to make it "more secure".
7. Special Publication 800-82, Revision 2, "Guide to Industrial Control System (ICS) Security", revised May 2015, describes how to secure multiple types of Industrial Control Systems against cyber attacks while considering the performance, reliability and safety requirements specific to ICS. [6]

ISO 15408

This standard develops what is called the "Common Criteria". It allows many different software applications to be integrated and tested in a secure way.

RFC 2196

RFC (Request For Comments) 2196 is memorandum published by Internet Engineering Task Force for developing security policies and procedures for information systems connected on the Internet. The RFC 2196 provides a general and broad overview of information security including network security, incident response, or security policies. The document is very practical and focusing on day-to-day operations.

ISA/IEC-62443 (formerly ISA-99)

ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.

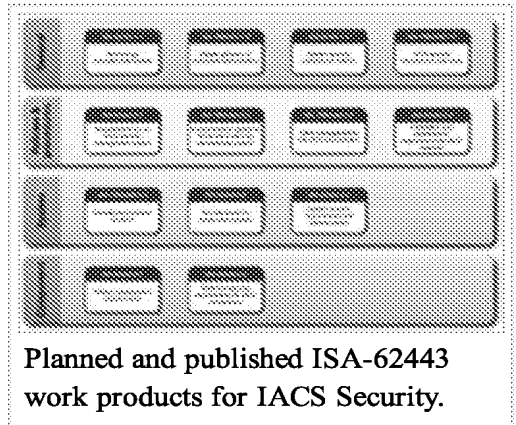
These documents were originally referred to as **ANSI/ISA-99** or **ISA99** standards, as they were created by the International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) documents. In 2010, they were renumbered to be the **ANSI/ISA-62443** series. This change was intended to align the ISA and ANSI document numbering with the corresponding International Electrotechnical Commission (IEC) standards.

All ISA work products are now numbered using the convention "ISA-62443-x-y" and previous ISA99 nomenclature is maintained for continuity purposes only. Corresponding IEC documents are referenced as "IEC 62443-x-y". The approved IEC and ISA versions are generally identical for all functional purposes.

ISA99 remains the name of the Industrial Automation and Control System Security Committee of the ISA. Since 2002, the committee has been developing a multi-part series of standards and technical reports on the subject. These work products are then submitted to the ISA approval and publishing under ANSI. They are also submitted to IEC for review and approval as standards and specifications in the IEC 62443 series.

All ISA-62443 standards and technical reports are organized into four general categories called **General, Policies and Procedures, System, and Component**.

1. The first (top) category includes common or foundational information such as concepts, models and terminology. Also included are work products that describe security metrics and security life cycles for IACS.
2. The second category of work products targets the Asset Owner. These address various aspects of creating and maintaining an effective IACS security program.
3. The third category includes work products that describe system design guidance and requirements for the secure integration of control systems. Core in this is the zone and conduit design model.
4. The fourth category includes work products that describe the specific product development and technical requirements of control system products. This is primarily intended for control product vendors, but can be used by integrator and asset owners for to assist in the procurement of secure products.



The planned and published ISA-62443 documents are as follows:

- **Group 1: General**

- **ISA-62443-1-1** (http://www.isa.org/Template.cfm?Section=Shop_ISA&Template=/Ecommerce/ProductDisplay.cfm&Productid=9661) (**IEC/TS 62443-1-1** (http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/43215)) (formerly referred to as "ISA-99 Part 1") was originally published as ISA standard ANSI/ISA-99.00.01-2007, as well as an IEC technical specification IEC/TS 62443-1-1. The ISA99 committee is currently revising it to make it align with other documents in the series, and to clarify normative content.
- **ISA-TR62443-1-2 (IEC 62443-1-2)** is a master glossary of terms used by the ISA99 committee. This document is a working draft, but the content is available on the ISA99 committee Wiki (<http://isa99.isa.org/ISA99%20Wiki/Master-Glossary.aspx>).
- **ISA-62443-1-3 (IEC 62443-1-3)** identifies a set of compliance metrics for IACS security. This document is currently under development and the committee will be releasing a draft for comment in 2013.
- **ISA-62443-1-4 (IEC/TS 62443-1-4)** defines the IACS security life cycle and use case. This work product has been proposed as part of the series, but as of January 2013 development had not yet started.

- **Group 2: Policy and Procedure**

- **ISA-62443-2-1** (<http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=10243>) (**IEC 62443-2-1** (http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/46312)) (formerly referred to as "ANSI/ISA 99.02.01-2009 or ISA-99 Part 2") addresses how to establish an IACS security program. This standard is approved and published the IEC as IEC 62443-2-1. It now being revised to permit closer alignment with the ISO 27000 series of standards.
- **ISA-62443-2-2 (IEC 62443-2-2)** addresses how to operate an IACS security program. This standard is currently under development.
- **ISA-TR62443-2-3** (<http://isa99.isa.org/ISA99%20Wiki/WG6.aspx>) (**IEC/TR 62443-2-3**) is a technical report on the subject of patch management in IACS environments. This report is currently under development.
- **ISA-62443-2-4 (IEC 62443-2-4** (http://www.iec.ch/dyn/www/f?p=103:38:0::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_LANG_ID,FSP_PROJECT:1250,23,25,IEC%2062443-2-4%20Ed.%201.0)) focuses on the certification of IACS supplier security policies and practices. This document was adopted from the WIB organization and is now a working product of the IEC TC65/WG10 committee. The proposed ISA version will be a U.S.

national publication of the IEC standard.

- **Group 3: System Integrator**

- **ISA-TR62443-3-1** (<http://www.isa.org/Template.cfm?Section=Standards&template=/Ecommerce/ProductDisplay.cfm&ProductID=9665>) (IEC/TR 62443-3-1) is a technical report on the subject of suitable technologies for IACS security. This report is approved and published as ANSI/ISA-TR99.00.01-2007 and is now being revised.
- **ISA-62443-3-2 (IEC 62443-3-2)** addresses how to define security assurance levels using the zones and conduits concept. This standard is currently under development.
- **ISA-62443-3-3** (<http://www.isa.org/Template.cfm?Section=Standards&Template=/Ecommerce/ProductDisplay.cfm&ProductID=13420>) (IEC 62443-3-3 (http://webstore.iec.ch/Webstore/webstore.nsf/ArtNum_PK/48406)) defines detailed technical requirements for IACS security. This standard has been published as ANSI/ISA-62443-3-3 (99.03.03)-2013. It was previously numbered as ISA-99.03.03.

- **Group 4: Component Provider**

- **ISA-62443-4-1 (IEC 62443-4-1)** addresses the requirements for the development of secure IACS products and solutions. This standard is currently under development.
- **ISA-62443-4-2 (IEC 62443-4-2)** series address detailed technical requirements for IACS components level. This standard is currently under development.

More information about the activities and plans of the ISA99 committee is available on the ISA99 committee Wiki site (<http://isa99.isa.org/ISA99%20Wiki/Home.aspx>). For more information on the activities of the IEC TC65/WG10 committee see the IEC TC65 site (http://www.iec.ch/dyn/www/f?p=103:7:0:::FSP_ORG_ID,FSP_LANG_ID:1250,25).

IEC 62443 Conformity Assessment Program

The ISA Security Compliance Institute (ISCI) www.isasecure.org (<http://www.isasecure.org>) operates the first conformity assessment scheme for IEC 62443 IACS cybersecurity standards. This program certifies Commercial Off-the-shelf (COTS) IACS products and systems, addressing securing the IACS supply chain.

Certification Offerings Two COTS product certifications are available under the ISASecure® brand: ISASecure-EDSA (Embedded Device Security Assurance) certifying IACS products to the IEC 62443-4-2 IACS cybersecurity standard and ISASecure-SSA (System Security Assurance), certifying IACS systems to the IEC 62443-3-3 IACS cybersecurity standard.

A third certification, SDLA (Secure Development Lifecycle Assurance) is available which certifies IACS development organizations to the IEC 62443-4-1 cybersecurity standard, providing assurances that a supplier organization has institutionalized cybersecurity into their product development practices.

ISO 17065 and Global Accreditation The ISASecure 62443 conformity assessment scheme is an ISO 17065 program whose labs (certification bodies or CB) are independently accredited by ANSI/ANAB, JAB and other global ISO 17011 accreditation bodies (AB). The certification labs must also meet ISO 17025 lab accreditation requirements to ensure consistent application of certification requirements and recognized tools.

Through Mutual Recognition Arrangements (MRA) with IAF, ILAC and others, the accreditation of the ISASecure labs by the ISO 17011 accreditation bodies ensures that certificates issued by any of the ISASecure labs are globally recognized.

Test Tool Recognition The ISASecure scheme includes a process for recognizing test tools to ensure the tools meet functional requirements necessary and sufficient to execute all required product tests and that test results will be consistent among the recognized tools.

Chemicals, Oil and Gas Industries ISCI development processes include maintenance policies to ensure that the ISASecure certifications remain in alignment with the IEC 62443 standards as they evolve. While the IEC 62443 standards are designed to horizontally address technical cybersecurity requirements of a cross-section of process industries, the ISASecure scheme's certification requirements have been vetted by representatives from the chemical and oil and gas industries and are reflective of their cybersecurity needs.

IASME

IASME is a UK-based standard for information assurance at small-to-medium enterprises (SMEs).^[10] It provides criteria and certification for small-to-medium business cybersecurity readiness. It also allows small to medium business to provide potential and existing customers and clients with an accredited measurement of the cybersecurity posture of the enterprise and its protection of personal/business data.

IASME was established to enable businesses with capitalization of 1.2 billion pounds or less (1.5 billion Euros; 2 billion US dollars) to achieve an accreditation similar to ISO 27001 but with reduced complexity, cost, and administrative overhead (specifically focused on SME in recognition that it is difficult for small cap businesses to achieve and maintain ISO 27001).

The cost of the certification is progressively graduated based upon the employee population of the SME (e.g., 10 & fewer, 11 to 25, 26 - 100, 101 - 250 employees); the certification can be based upon a self-assessment with an IASME questionnaire or by a third-party professional assessor. Some insurance companies reduce premiums for cybersecurity related coverage based upon the IASME certification.

See also

- 201 CMR 17.00 (Massachusetts Standards for the Protection of Personal Information)
- BS 7799
- Common Criteria
- Computer security
- Computer Security Policy
- Information security
- Information assurance
- ISO/IEC 27002
- IT Baseline Protection Catalogs
- North American Electric Reliability Corporation (NERC)
- National Institute of Standards and Technology (NIST)
- Payment Card Industry Data Security Standard
- Privacy engineering
- *Standard of Good Practice*
- Semantic service-oriented architecture (SSOA)
- ISA-99 Security for Industrial Automation and Control Systems
- Control system security
- Information security indicators

Notes

1. "Guidelines for Smart Grid Cyber Security" (PDF). National Institute of Standards and Technology. 2010-08-01. Retrieved 2014-03-30.
2. <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136>
3. <https://portal.etsi.org/tb.aspx?tbid=824&SubTB=824>
4. http://fsi.stanford.edu/research/consortium_for_research_on_information_security_and_policy
5. "NIST Cybersecurity Framework Adoption Hampered By Costs, Survey Finds". Retrieved 2016-08-02.
6. <https://portal.etsi.org/TBSiteMap/CYBER/CyberToR.aspx>
7. http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=45906
8. [1] (http://eval.symantec.com/mktginfo/enterprise/fact_sheets/b-datasheet_css_nerc_ferc.10-2008.14566044-1.en-us.pdf) Symantec Control Compliance Suite - NERC and FERC Regulation Subsection: History of NERC Standards
9. "NIST Cybersecurity Framework". Retrieved 2016-08-02.
10. <http://www.iasme.co.uk>

References

1. ^ Department of Homeland Security, A Comparison of Cyber Security Standards Developed by the Oil and Gas Segment. (November 5, 2004)
2. ^ Guttman, M., Swanson, M., National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce., Generally Accepted Principles and Practices for Securing Information Technology Systems (800-14). (September 1996)
3. ^ National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce., An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12.
4. ^ Swanson, M., National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce., Security Self-Assessment Guide for Information Technology Systems (800-26).
5. ^ Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A.; National Institute of Standards and Technology; U.S. Department of Commerce., Guide to Industrial Control Systems (ICS) Security (800-82).
6. ^ The North American Electric Reliability Council (NERC). <http://www.nerc.com>. Retrieved November 12, 2005.

External links

- ISA99 info (<http://www.isa.org/isa99>)
- NERC Standards (see CIP 002-009) (<http://www.nerc.com/page.php?cid=2%7C20>)
- Securing Cyberspace-Media (<http://hsgac.senate.gov/index.cfm?Fuseaction=Hearings.Detail&HearingID=261>)
- Presentation by Professor William Sanders, University of Illinois (<http://media.cs.uiuc.edu/DCS/2007-08/ETSI-2008-02-27.asx>)
- Global Cybersecurity Policy Conference (<http://www.stevens.edu/cyberpolicy/>)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Cyber_security_standards&oldid=742414319"

Categories: Computer security standards | Cyberwarfare | Computer security procedures

- This page was last modified on 3 October 2016, at 15:29.
- Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

HTTPS

From Wikipedia, the free encyclopedia

HTTPS (also called **HTTP over TLS**,^{[1][2]} **HTTP over SSL**,^[3] and **HTTP Secure**^{[4][5]}) is a protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.

In its popular deployment on the internet, HTTPS provides authentication of the website and associated web server with which one is communicating, which protects against man-in-the-middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with or forging the contents of the communication.^[6] In practice, this provides a reasonable guarantee that one is communicating with precisely the website that one intended to communicate with (as opposed to an impostor), as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party.

Historically, HTTPS connections were primarily used for payment transactions on the World Wide Web, e-mail and for sensitive transactions in corporate information systems. In the late 2000s and early 2010s, HTTPS began to see widespread use for protecting page authenticity on all types of websites, securing accounts and keeping user communications, identity and web browsing private.

Contents

- 1 Overview
 - 1.1 Usage in websites
 - 1.2 Browser integration
- 2 Security
- 3 Technical
 - 3.1 Difference from HTTP
 - 3.2 Network layers
 - 3.3 Server setup
 - 3.3.1 Acquiring certificates
 - 3.3.2 Use as access control
 - 3.3.3 In case of compromised secret (private) key
 - 3.4 Limitations
- 4 History
- 5 See also
- 6 References
- 7 External links

Overview

The *HTTPS* uniform resource identifier (URI) scheme has identical syntax to the standard HTTP scheme, aside from its scheme token. However, HTTPS signals the browser to use an added encryption layer of SSL/TLS to protect the traffic. SSL/TLS is especially suited for HTTP, since it can provide

some protection even if only one side of the communication is authenticated. This is the case with HTTP transactions over the Internet, where typically only the server is authenticated (by the client examining the server's certificate).

HTTPS creates a secure channel over an insecure network. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided that adequate cipher suites are used and that the server certificate is verified and trusted.

Because HTTPS piggybacks HTTP entirely on top of TLS, the entirety of the underlying HTTP protocol can be encrypted. This includes the request URL (which particular web page was requested), query parameters, headers, and cookies (which often contain identity information about the user). However, because host (website) addresses and port numbers are necessarily part of the underlying TCP/IP protocols, HTTPS cannot protect their disclosure. In practice this means that even on a correctly configured web server, eavesdroppers can infer the IP address and port number of the web server (sometimes even the domain name e.g. `www.example.org`, but not the rest of the URL) that one is communicating with, as well as the amount (data transferred) and duration (length of session) of the communication, though not the content of the communication.^[6]

Web browsers know how to trust HTTPS websites based on certificate authorities that come pre-installed in their software. Certificate authorities (such as Symantec, Comodo, GoDaddy and GlobalSign) are in this way being trusted by web browser creators to provide valid certificates. Therefore, a user should trust an HTTPS connection to a website if and only if all of the following are true:

- The user trusts that the browser software correctly implements HTTPS with correctly pre-installed certificate authorities.
- The user trusts the certificate authority to vouch only for legitimate websites.
- The website provides a valid certificate, which means it was signed by a trusted authority.
- The certificate correctly identifies the website (e.g., when the browser visits "`https://example.com`", the received certificate is properly for "`example.com`" and not some other entity).
- The user trusts that the protocol's encryption layer (SSL/TLS) is sufficiently secure against eavesdroppers.

HTTPS is especially important over insecure networks (such as public Wi-Fi access points), as anyone on the same local network can packet-sniff and discover sensitive information not protected by HTTPS. Additionally, many free to use and even paid for WLAN networks engage in packet injection in order to serve their own ads on webpages. However, this can be exploited maliciously in many ways, such as injecting malware onto webpages and stealing users' private information.^[7]

HTTPS is also very important for connections over the Tor anonymity network, as malicious Tor nodes can damage or alter the contents passing through them in an insecure fashion and inject malware into the connection. This is one reason why the Electronic Frontier Foundation and the Tor project started the development of HTTPS Everywhere,^[6] which is included in the Tor Browser Bundle.^[8]

As more information is revealed about global mass surveillance and criminals stealing personal information, the use of HTTPS security on all websites is becoming increasingly important regardless of the type of Internet connection being used.^{[9][10]} While metadata about individual pages that a user visits



Logo of the networking protocol
https and the www letters

is not sensitive, when combined together, they can reveal a lot about the user and compromise the user's privacy.^{[2][11][12]}

Deploying HTTPS also allows the use of HTTP/2 (or its predecessor, the now-deprecated protocol SPDY), that are new generations of HTTP, designed to reduce page load times and latency.

It is recommended to use HTTP Strict Transport Security (HSTS) with HTTPS to protect users from man-in-the-middle attacks, especially SSL stripping.^{[12][13]}

HTTPS should not be confused with the little-used Secure HTTP (S-HTTP) specified in RFC 2660.

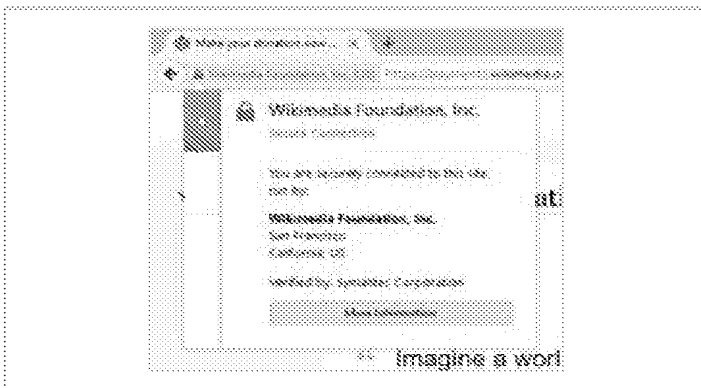
Usage in websites

As of June 2016, 10.2% of Alexa top 1,000,000 websites use HTTPS as default,^[14] 43.1% of the Internet's 141,387 most popular websites have a secure implementation of HTTPS,^[15] and 45% of page loads (measured by Firefox Telemetry) use HTTPS.^[16]

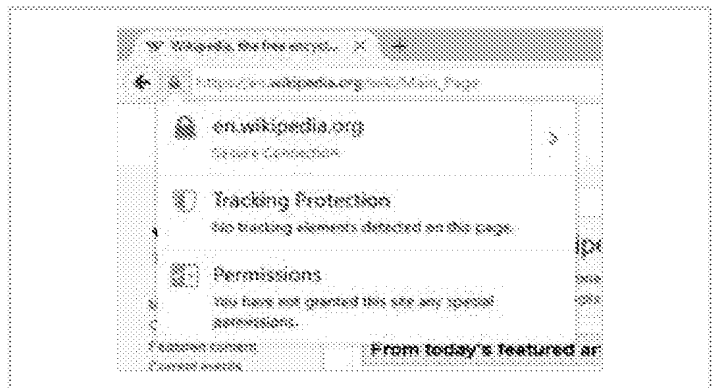
Browser integration

Most browsers display a warning if they receive an invalid certificate. Older browsers, when connecting to a site with an invalid certificate, would present the user with a dialog box asking whether they wanted to continue. Newer browsers display a warning across the entire window. Newer browsers also prominently display the site's security information in the address bar. Extended validation certificates turn the address bar green in newer browsers. Most browsers also display a warning to the user when visiting a site that contains a mixture of encrypted and unencrypted content.

Comparison between different kinds of SSL/TLS certificates (Using Firefox as an example)



Many web browsers, including Firefox (shown here), use the address bar to tell the user that their connection is secure, often by coloring the background.



When accessing a site only with a common certificate, the address bar of Firefox turns green. For some other browsers, a "lock" sign may appear.



Most web browsers alert the user when visiting sites that have invalid security certificates.

Firefox uses HTTPS for Google searches as of version 14,^[17] to "shield our users from network infrastructure that may be gathering data about the users or modifying/censoring their search results".^[18]

The Electronic Frontier Foundation, opining that "In an ideal world, every web request could be defaulted to HTTPS", has provided an add-on called HTTPS Everywhere for Mozilla Firefox that enables HTTPS by default for hundreds of frequently used websites. A beta version of this plugin is also available for Google Chrome and Chromium.^{[19][20]}

Security

The security of HTTPS is that of the underlying TLS, which typically uses long-term public and private keys to generate a short-term session key, which is then used to encrypt the data flow between client and server. X.509 certificates are used to authenticate the server (and sometimes the client as well). As a consequence, certificate authorities and public key certificates are necessary to verify the relation between the certificate and its owner, as well as to generate, sign, and administer the validity of certificates. While this can be more beneficial than verifying the identities via a web of trust, the 2013 mass surveillance disclosures drew attention to certificate authorities as a potential weak point allowing man-in-the-middle attacks.^{[21][22]} An important property in this context is forward secrecy, which ensures that encrypted communications recorded in the past cannot be retrieved and decrypted should long-term secret keys or passwords be compromised in the future. Not all web servers provide forward secrecy.^[23]

A site must be completely hosted over HTTPS, without having part of its contents loaded over HTTP – for example, having scripts loaded insecurely – or the user will be vulnerable to some attacks and surveillance. Also having only a certain page that contains sensitive information (such as a log-in page) of a website loaded over HTTPS, while having the rest of the website loaded over plain HTTP, will expose the user to attacks. On a site that has sensitive information somewhere on it, every time that site is accessed with HTTP instead of HTTPS, the user and the session will get exposed. Similarly, cookies on a site served through HTTPS have to have the secure attribute enabled.^[12]

Technical

Difference from HTTP

HTTPS URLs begin with "https://" and use port 443 by default, whereas HTTP URLs begin with "http://" and use port 80 by default.

HTTP is not encrypted and is vulnerable to man-in-the-middle and eavesdropping attacks, which can let attackers gain access to website accounts and sensitive information, and modify webpages to inject malware or advertisements. HTTPS is designed to withstand such attacks and is considered secure against them (with the exception of older, deprecated versions of SSL).

Network layers

HTTP operates at the highest layer of the TCP/IP model, the Application layer; as does the TLS security protocol (operating as a lower sublayer of the same layer), which encrypts an HTTP message prior to transmission and decrypts a message upon arrival. Strictly speaking, HTTPS is not a separate protocol, but refers to use of ordinary HTTP over an encrypted SSL/TLS connection.

Everything in the HTTPS message is encrypted, including the headers, and the request/response load. With the exception of the possible CCA cryptographic attack described in the limitations section below, the attacker can only know that a connection is taking place between the two parties and their domain names and IP addresses.

Server setup

To prepare a web server to accept HTTPS connections, the administrator must create a public key certificate for the web server. This certificate must be signed by a trusted certificate authority for the web browser to accept it without warning. The authority certifies that the certificate holder is the operator of the web server that presents it. Web browsers are generally distributed with a list of signing certificates of major certificate authorities so that they can verify certificates signed by them.

Acquiring certificates

Authoritatively signed certificates may be free^{[24][25]} or cost between 8 USD^[26] and 70 USD^[27] per year (in 2012–2014).

Organizations may also run their own certificate authority, particularly if they are responsible for setting up browsers to access their own sites (for example, sites on a company intranet, or major universities). They can easily add copies of their own signing certificate to the trusted certificates distributed with the browser.

There also exists a peer-to-peer certificate authority, CACert. However, it is not included in the trusted root certificates of many popular browsers (e.g. Firefox, Chrome, Internet Explorer), which may cause warning messages to be displayed to end users.

Let's Encrypt, launched in April 2016,^[28] provides free and automated SSL/TLS certificates to websites.^[29] According to the Electronic Frontier Foundation, "Let's Encrypt" will make switching from HTTP to HTTPS "as easy as issuing one command, or clicking one button."^[30]

Use as access control

The system can also be used for client authentication in order to limit access to a web server to authorized users. To do this, the site administrator typically creates a certificate for each user, a certificate that is loaded into their browser. Normally, that contains the name and e-mail address of the authorized user and is automatically checked by the server on each reconnect to verify the user's identity, potentially without even entering a password.

In case of compromised secret (private) key

An important property in this context is perfect forward secrecy (PFS). Possessing one of the long-term asymmetric secret keys used to establish an HTTPS session should not make it easier to derive the short-term session key to then decrypt the conversation, even at a later time. Diffie–Hellman key exchange (DHE) and Elliptic curve Diffie–Hellman key exchange (ECDHE) are in 2013 the only ones known to have that property. Only 30% of Firefox, Opera, and Chromium Browser sessions use it, and nearly 0% of Apple's Safari and Microsoft Internet Explorer sessions.^[23] Among the larger internet providers, only Google supports PFS since 2011 (State of September 2013).

A certificate may be revoked before it expires, for example because the secrecy of the private key has been compromised. Newer versions of popular browsers such as Firefox,^[31] Opera,^[32] and Internet Explorer on Windows Vista^[33] implement the Online Certificate Status Protocol (OCSP) to verify that this is not the case. The browser sends the certificate's serial number to the certificate authority or its delegate via OCSP and the authority responds, telling the browser whether or not the certificate is still valid.^[34]

Limitations

SSL/TLS comes in two options, simple and mutual. The mutual version is more secure, but requires the user to install a personal client certificate into their web browser in order to authenticate themselves.^[35]

Whether the strategy is simple or mutual, the level of protection strongly depends on the correctness of the implementation of the web browser and the server software and the actual cryptographic algorithms supported.

SSL/TLS does not prevent the entire site from being indexed using a web crawler, and in some cases the URI of the encrypted resource can be inferred by knowing only the intercepted request/response size.^[36] This allows an attacker to have access to the plaintext (the publicly available static content), and the encrypted text (the encrypted version of the static content), permitting a cryptographic attack.

Because TLS operates below HTTP and has no knowledge of higher-level protocols, TLS servers can only strictly present one certificate for a particular IP/port combination.^[37] This means that, in most cases, it is not feasible to use name-based virtual hosting with HTTPS. A solution called Server Name Indication (SNI) exists, which sends the hostname to the server before encrypting the connection, although many older browsers do not support this extension. Support for SNI is available since Firefox 2, Opera 8, Safari 2.1, Google Chrome 6, and Internet Explorer 7 on Windows Vista.^{[38][39][40]}

From an architectural point of view:

1. An SSL/TLS connection is managed by the first front machine that initiates the TLS connection. If, for any reasons (routing, traffic optimization, etc.), this front machine is not the application server and it has to decipher data, solutions have to be found to propagate user authentication information or certificate to the application server, which needs to know who is going to be

connected.

2. For SSL/TLS with mutual authentication, the SSL/TLS session is managed by the first server that initiates the connection. In situations where encryption has to be propagated along chained servers, session timeout management becomes extremely tricky to implement.
3. With mutual SSL/TLS, security is maximal, but on the client-side, there is no way to properly end the SSL/TLS connection and disconnect the user except by waiting for the server session to expire or closing all related client applications.

A sophisticated type of man-in-the-middle attack called SSL stripping was presented at the Blackhat Conference 2009. This type of attack defeats the security provided by HTTPS by changing the https: link into an http: link, taking advantage of the fact that few Internet users actually type "https" into their browser interface: they get to a secure site by clicking on a link, and thus are fooled into thinking that they are using HTTPS when in fact they are using HTTP. The attacker then communicates in clear with the client.^[41] This prompted the development of a countermeasure in HTTP called HTTP Strict Transport Security.

HTTPS has been shown vulnerable to a range of traffic analysis attacks. Traffic analysis attacks are a type of side-channel attack that relies on variations in the timing and size of traffic in order to infer properties about the encrypted traffic itself. Traffic analysis is possible because SSL/TLS encryption changes the contents of traffic, but has minimal impact on the size and timing of traffic. In May 2010, a research paper by researchers from Microsoft Research and Indiana University discovered that detailed sensitive user data can be inferred from side channels such as packet sizes. More specifically, the researchers found that an eavesdropper can infer the illnesses/medications/surgeries of the user, his/her family income and investment secrets, despite HTTPS protection in several high-profile, top-of-the-line web applications in healthcare, taxation, investment and web search.^[42] Although this work demonstrated vulnerability of HTTPS to traffic analysis, the approach presented by the authors required manual analysis and focused specifically on web applications protected by HTTPS.

In June 2014, a team of researchers at UC Berkeley and Intel led by Brad Miller (<http://bradmiller.io>) demonstrated a generalized approach to HTTPS traffic analysis based on machine learning.^{[43][44]} The researchers demonstrated that the attack applied to a range of websites, including Mayo Clinic, Planned Parenthood and Youtube.^[45] The attack assumes that the attacker is able to visit the same webpages as the victim to gather network traffic which serves as training data. The attacker is then able to identify similarities in the packet sizes and orderings between the victim traffic and the training data traffic which frequently allow the attacker to infer the exact page the victim is visiting. For example, this attack could be used to determine whether a user browsing the Planned Parenthood website is looking for information about preventative health screening or an abortion. Note that the attack can not be used to discover user specific values embedded in a webpage. For example, many banks offer web interfaces which allow users to view account balances. While the attacker would be able to discover that the user was viewing an account balance page, they would be unable to learn the user's exact account balance or account number.

History

Netscape Communications created HTTPS in 1994 for its Netscape Navigator web browser.^[46] Originally, HTTPS was used with the SSL protocol. As SSL evolved into Transport Layer Security (TLS), the current version of HTTPS was formally specified by RFC 2818 in May 2000.

See also

- Bullrun (decryption program) – a secret anti-encryption program run by the U.S. National Security Agency
- Computer security
- curl-loader
- Diameter protocol
- HTTPsec
- Moxie Marlinspike
- Opportunistic encryption
- Stunnel

References

1. Network Working Group (May 2000). "HTTP Over TLS". The Internet Engineering Task Force. Retrieved February 27, 2015.
2. "HTTPS as a ranking signal". *Google Webmaster Central Blog*. Google Inc. August 6, 2014. Retrieved February 27, 2015. "You can make your site secure with HTTPS (Hypertext Transfer Protocol Secure) [...]"
3. "Enabling HTTP Over SSL". Adobe Systems Incorporated. Retrieved February 27, 2015.
4. "Secure your site with HTTPS". *Google Support*. Google, Inc. Retrieved February 27, 2015.
5. "What is HTTPS?". Comodo CA Limited. Retrieved February 27, 2015. "Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP [...]"
6. "HTTPS Everywhere FAQ". Retrieved 3 May 2012.
7. "Hotel Wifi JavaScript Injection". Retrieved 24 July 2012.
8. The Tor Project, Inc. "Tor". *torproject.org*.
9. Konigsburg, Eitan; Pant, Rajiv; Kvochko, Elena (November 13, 2014). "Embracing HTTPS". The New York Times. Retrieved February 27, 2015.
10. Gallagher, Kevin (September 12, 2014). "Fifteen Months After the NSA Revelations, Why Aren't More News Organizations Using HTTPS?". Freedom of the Press Foundation. Retrieved February 27, 2015.
11. Grigorik, Ilya; Far, Pierre (June 26, 2014). "Google I/O 2014 - HTTPS Everywhere". Google Developers. Retrieved February 27, 2015.
12. "How to Deploy HTTPS Correctly". Retrieved 13 June 2012.
13. "HTTP Strict Transport Security". *Mozilla Developer Network*.
14. "HTTPS usage statistics on top websites". statoperator. Retrieved 2016-06-28.
15. "SSL Pulse". Trustworthy Internet Movement. 2015-10-03. Retrieved 2015-10-19.
16. Aas, Josh (22 June 2016). "Progress Towards 100% HTTPS, June 2016". Lets Encrypt. Retrieved 23 July 2016.
17. "Firefox 14.0.1 Release Notes". Retrieved 24 July 2012.
18. "Firefox Rolling Out HTTPS Google search". Retrieved 24 July 2012.
19. Peter Eckersley: Encrypt the Web with the HTTPS Everywhere Firefox Extension (<https://www.eff.org/deeplinks/2010/06/encrypt-web-https-everywhere-firefox-extension>) EFF blog, 17 June 2010
20. HTTPS Everywhere (<https://www.eff.org/https-everywhere>) EFF projects
21. Law Enforcement Appliance Subverts SSL (<https://www.wired.com/threatlevel/2010/03/packet-forensics/>), Wired, 2010-04-03.
22. New Research Suggests That Governments May Fake SSL Certificates (<https://www.eff.org/deeplinks/2010/03/researchers-reveal-likelihood-governments-fake-ssl>), EFF, 2010-03-24.
23. SSL: Intercepted today, decrypted tomorrow (<https://news.netcraft.com/archives/2013/06/25/ssl-intercepted-to-day-decrypted-tomorrow.html>), Netcraft, 2013-06-25.
24. "Free SSL Certificates from a Free Certificate Authority". sslshopper.com. Retrieved 2009-10-24.
25. Justin Fielding (2006-07-16). "Secure Outlook Web Access with (free) SSL: Part 1". TechRepublic. Retrieved 2009-10-24.
26. "Namecheap.com SSL Services". namecheap. Retrieved 30 Jan 2012.
27. "Secure Site Pro with SSL Certificate". Retrieved August 23, 2014.
28. Catalin Cimpanu. "Let's Encrypt Launched Today, Currently Protects 3.8 Million Domains". Softpedia News. Retrieved April 12, 2016.
29. Kerner, Sean Michael (November 18, 2014). "Let's Encrypt Effort Aims to Improve Internet Security". *eWeek.com*. Quinstreet Enterprise. Retrieved February 27, 2015.

30. Eckersley, Peter (November 18, 2014). "Launching in 2015: A Certificate Authority to Encrypt the Entire Web". Electronic Frontier Foundation. Retrieved February 27, 2015.
31. "Mozilla Firefox Privacy Policy". Mozilla Foundation. 27 April 2009. Retrieved 13 May 2009.
32. "Opera 8 launched on FTP". Softpedia. 19 April 2005. Retrieved 13 May 2009.
33. Lawrence, Eric (31 January 2006). "HTTPS Security Improvements in Internet Explorer 7". MSDN. Retrieved 13 May 2009.
34. Myers, M; Ankney, R; Malpani, A; Galperin, S; Adams, C (June 1999). "Online Certificate Status Protocol – OCSP". Internet Engineering Task Force. Retrieved 13 May 2009.
35. "Manage client certificates on Chrome devices - Chrome for business and education Help". *support.google.com*. Retrieved 2016-10-13.
36. Pusep, Stanislaw (31 July 2008). "The Pirate Bay un-SSL". Retrieved 6 March 2009.
37. "SSL/TLS Strong Encryption: FAQ". *apache.org*.
38. Lawrence, Eric (22 October 2005). "Upcoming HTTPS Improvements in Internet Explorer 7 Beta 2". Microsoft. Retrieved 12 May 2009.
39. "Server Name Indication (SNI)". *inside aebrahim's head*.
40. Pierre, Julien. "Browser support for TLS server name indication" (2001-12-19). *Bugzilla*. Mozilla Foundation. Retrieved 2010-12-15.
41. "sslstrip". Retrieved 2011-11-26.
42. Shuo Chen; Rui Wang; XiaoFeng Wang; Kehuan Zhang (May 2010). "Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow" (PDF). IEEE Symposium on Security & Privacy 2010.
43. "Statistical Tricks Extract Sensitive Data from Encrypted Communications". MIT Technology Review. 2014-06-19.
44. "Researchers Use Big Data to Get Around Encryption". The Wall Street Journal. 2014-06-23.
45. Brad Miller; Ling Huang; Anthony D. Joseph; J.D. Tygar. "I Know Why You Went to the Clinic: Risks and Realization of HTTPS Traffic Analysis" (PDF).
46. Walls, Colin (2005). *Embedded software*. Newnes. p. 344. ISBN 0-7506-7954-9.

External links

- RFC 2818: HTTP Over TLS (<https://tools.ietf.org/html/rfc2818>)
- Hacking HTTPS by man-in-the-middle attack (<http://greyhatsspeak.blogspot.in/2013/10/mitm-against-https-sites.html>)
- RFC 5246: The Transport Layer Security Protocol 1.2 (<https://tools.ietf.org/html/rfc5246>)
- SSL 3.0 Specification (<https://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00>) (IETF)
- HTTPS Error: Your connection is not private (<https://usefulpcguide.com/16666/your-connection-is-not-private/>)



Wikimedia Commons has media related to **HTTPS**.

Retrieved from "<https://en.wikipedia.org/w/index.php?title=HTTPS&oldid=748533850>"

Categories: Hypertext Transfer Protocol | Cryptographic protocols | Secure communication | URI schemes | Transport Layer Security

- This page was last modified on 8 November 2016, at 18:26.
- Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Hypervisor

From Wikipedia, the free encyclopedia

A **hypervisor** or **virtual machine monitor (VMM)** is a piece of computer software, firmware or hardware that creates and runs virtual machines. A computer on which a hypervisor runs one or more virtual machines is called a *host machine*, and each virtual machine is called a *guest machine*. The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources: for example, Linux, Windows, and OS X instances can all run on a single physical x86 machine. This contrasts with operating-system-level virtualization, where all instances (usually called *containers*) must share a single kernel, though the guest operating systems can differ in user space, such as different Linux distributions with the same kernel.

The term *hypervisor* is a variant of *supervisor*, a traditional term for the kernel of an operating system: the hypervisor is the supervisor of the supervisor,^[1] with *hyper-* used as a stronger variant of *super-*.^[a] The term dates to circa 1970;^[2] in the earlier CP/CMS (1967) system the term *Control Program* was used instead.

Contents

- 1 Classification
- 2 Mainframe origins
- 3 Operating system support
- 4 x86 systems
- 5 Embedded systems
- 6 Security implications
- 7 Notes
- 8 References
- 9 External links

Classification

In their 1974 article, *Formal Requirements for Virtualizable Third Generation Architectures*, Gerald J. Popek and Robert P. Goldberg classified two types of hypervisor:^[3]

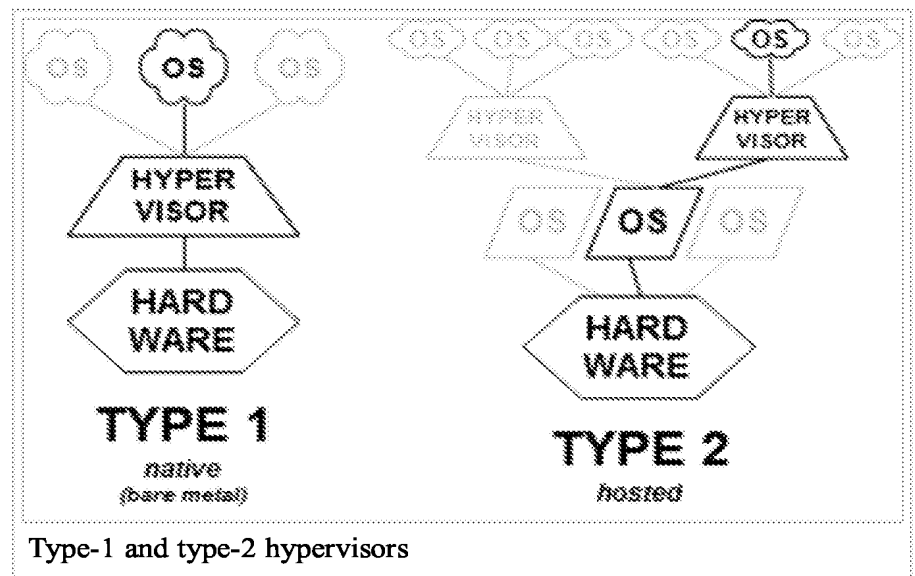
Type-1, native or bare-metal hypervisors

These hypervisors run directly on the host's hardware to control the hardware and to manage guest operating systems. For this reason, they are sometimes called bare metal hypervisors. The first hypervisors, which IBM developed in the 1960s, were native hypervisors.^[4] These included the test software SIMMON and the CP/CMS operating system (the predecessor of IBM's z/VM). Modern equivalents include Oracle VM Server for SPARC, Oracle VM Server for x86, the Citrix XenServer, Microsoft Hyper-V and VMware ESX/ESXi.

Type-2 or hosted hypervisors

These hypervisors run on a conventional operating system just as other computer programs do. A guest operating system runs as a process on the host. Type-2 hypervisors abstract guest operating systems from the host operating system. VMware Workstation, VMware Player, VirtualBox, Parallels Desktop for Mac and QEMU are examples of type-2 hypervisors.

However, the distinction between these two types is not necessarily clear. Linux's Kernel-based Virtual Machine (KVM) and FreeBSD's bhyve are kernel modules^[5] that effectively convert the host operating system to a type-1 hypervisor.^[6] At the same time, since Linux distributions and FreeBSD are still general-purpose operating systems, with other applications competing for VM resources, KVM and bhyve can also be categorized as type-2 hypervisors.^[7]



Type-1 and type-2 hypervisors

Mainframe origins

The first hypervisors providing full virtualization were the test tool SIMMON and IBM's one-off research CP-40 system, which began production use in January 1967, and became the first version of IBM's CP/CMS operating system. CP-40 ran on a S/360-40 that was modified at the IBM Cambridge Scientific Center to support Dynamic Address Translation, a key feature that allowed virtualization. Prior to this time, computer hardware had only been virtualized enough to allow multiple user applications to run concurrently (see CTSS and IBM M44/44X). With CP-40, the hardware's *supervisor state* was virtualized as well, allowing multiple operating systems to run concurrently in separate virtual machine contexts.

Programmers soon re-implemented CP-40 (as CP-67) for the IBM System/360-67, the first production computer-system capable of full virtualization. IBM first shipped this machine in 1966; it included page-translation-table hardware for virtual memory, and other techniques that allowed a full virtualization of all kernel tasks, including I/O and interrupt handling. (Note that its "official" operating system, the ill-fated TSS/360, did not employ full virtualization.) Both CP-40 and CP-67 began production use in 1967. CP/CMS was available to IBM customers from 1968 to early 1970s, in source code form without support.

CP/CMS formed part of IBM's attempt to build robust time-sharing systems for its mainframe computers. By running multiple operating systems concurrently, the hypervisor increased system robustness and stability: Even if one operating system crashed, the others would continue working without interruption. Indeed, this even allowed beta or experimental versions of operating systems—or even of new hardware^[8]—to be deployed and debugged, without jeopardizing the stable main production system, and without requiring costly additional development systems.

IBM announced its System/370 series in 1970 without any virtualization features, but added virtual memory support in the August 1972 Advanced Function announcement. Virtualization has been featured in all successor systems (all modern-day IBM mainframes, such as the zSeries line, retain backward compatibility with the 1960s-era IBM S/360 line) The 1972 announcement also included VM/370, a reimplement of CP/CMS for the S/370. Unlike CP/CMS, IBM provided support for this version (though it was still distributed in source code form for several releases). VM stands for *Virtual Machine*, emphasizing that all, and not just some, of the hardware interfaces are virtualized. Both VM and CP/CMS enjoyed early acceptance and rapid development by universities, corporate users, and time-sharing vendors, as well as within IBM. Users played an active role in ongoing development,

anticipating trends seen in modern open source projects. However, in a series of disputed and bitter battles, time-sharing lost out to batch processing through IBM political infighting, and VM remained IBM's "other" mainframe operating system for decades, losing to MVS. It enjoyed a resurgence of popularity and support from 2000 as the z/VM product, for example as the platform for Linux for zSeries.

As mentioned above, the VM control program includes a *hypervisor-call* handler that intercepts DIAG ("Diagnose") instructions used within a virtual machine. This provides fast-path non-virtualized execution of file-system access and other operations (DIAG is a model-dependent privileged instruction, not used in normal programming, and thus is not virtualized. It is therefore available for use as a signal to the "host" operating system). When first implemented in CP/CMS release 3.1, this use of DIAG provided an operating system interface that was analogous to the System/360 Supervisor Call instruction (SVC), but that did not require altering or extending the system's virtualization of SVC.

In 1985 IBM introduced the PR/SM hypervisor to manage logical partitions (LPAR).

Operating system support

Several factors led to a resurgence around 2005 in the use of virtualization technology among Unix, Linux, and other Unix-like operating systems:^[9]

- Expanding hardware capabilities, allowing each single machine to do more simultaneous work
- Efforts to control costs and to simplify management through consolidation of servers
- The need to control large multiprocessor and cluster installations, for example in server farms and render farms
- The improved security, reliability, and device independence possible from hypervisor architectures
- The ability to run complex, OS-dependent applications in different hardware or OS environments

Major Unix vendors, including Sun Microsystems, HP, IBM, and SGI, have been selling virtualized hardware since before 2000. These have generally been large, expensive systems (in the multimillion-dollar range at the high end), although virtualization has also been available on some low- and mid-range systems, such as IBM's pSeries servers, Sun/Oracle's T-series CoolThreads servers and HP Superdome series machines.

Although Solaris has always been the only guest domain OS officially supported by Sun/Oracle on their Logical Domains hypervisor, as of late 2006, Linux (Ubuntu and Gentoo), and FreeBSD have been ported to run on top of the hypervisor (and can all run simultaneously on the same processor, as fully virtualized independent guest OSes). Wind River "Carrier Grade Linux" also runs on Sun's Hypervisor.^[10] Full virtualization on SPARC processors proved straightforward: since its inception in the mid-1980s Sun deliberately kept the SPARC architecture clean of artifacts that would have impeded virtualization. (Compare with virtualization on x86 processors below.)^[11]

HP calls its technology to host multiple OS technology on its Itanium powered systems "Integrity Virtual Machines" (Integrity VM). Itanium can run HP-UX, Linux, Windows and OpenVMS. Except for OpenVMS, to be supported in a later release, these environments are also supported as virtual servers on HP's Integrity VM platform. The HP-UX operating system hosts the Integrity VM hypervisor layer that allows for many important features of HP-UX to be taken advantage of and provides major differentiation between this platform and other commodity platforms - such as processor hotswap, memory hotswap, and dynamic kernel updates without system reboot. While it heavily leverages HP-UX, the Integrity VM hypervisor is really a hybrid that runs on bare-metal while guests are executing. Running normal HP-UX applications on an Integrity VM host is heavily discouraged, because Integrity

VM implements its own memory management, scheduling and I/O policies that are tuned for virtual machines and are not as effective for normal applications. HP also provides more rigid partitioning of their Integrity and HP9000 systems by way of VPAR and nPar technology, the former offering shared resource partitioning and the latter offering complete I/O and processing isolation. The flexibility of virtual server environment (VSE) has given way to its use more frequently in newer deployments.

IBM provides virtualization partition technology known as logical partitioning (LPAR) on System/390, zSeries, pSeries and iSeries systems. For IBM's Power Systems, the Power Hypervisor (PowerVM) functions as a native (bare-metal) hypervisor in firmware and provides isolation between LPARs. Processor capacity is provided to LPARs in either a dedicated fashion or on an entitlement basis where unused capacity is harvested and can be re-allocated to busy workloads. Groups of LPARs can have their processor capacity managed as if they were in a "pool" - IBM refers to this capability as Multiple Shared-Processor Pools (MSPPs) and implements it in servers with the POWER6 processor. LPAR and MSPP capacity allocations can be dynamically changed. Memory is allocated to each LPAR (at LPAR initiation or dynamically) and is address-controlled by the POWER Hypervisor. For real-mode addressing by operating systems (AIX, Linux, IBM i), the POWER processors (POWER4 onwards) have designed virtualization capabilities where a hardware address-offset is evaluated with the OS address-offset to arrive at the physical memory address. Input/Output (I/O) adapters can be exclusively "owned" by LPARs or shared by LPARs through an appliance partition known as the Virtual I/O Server (VIOS). The Power Hypervisor provides for high levels of reliability, availability and serviceability (RAS) by facilitating hot add/replace of many parts (model dependent: processors, memory, I/O adapters, blowers, power units, disks, system controllers, etc.)

Similar trends have occurred with x86/x86-64 server platforms, where open-source projects such as Xen have led virtualization efforts. These include hypervisors built on Linux and Solaris kernels as well as custom kernels. Since these technologies span from large systems down to desktops, they are described in the next section.

x86 systems

Starting in 2005, CPU vendors have added hardware virtualization assistance to their products, for example: Intel VT-x (codenamed Vanderpool) and AMD-V (codenamed Pacifica).

An alternative approach requires modifying the guest operating-system to make system calls to the hypervisor, rather than executing machine I/O instructions that the hypervisor simulates. This is called paravirtualization in Xen, a "hypercall" in Parallels Workstation, and a "DIAGNOSE code" in IBM's VM. All are really the same thing, a system call to the hypervisor below. Some microkernels such as Mach and L4 are flexible enough such that "paravirtualization" of guest operating systems is possible.

Embedded systems

Embedded hypervisors, targeting embedded systems and certain real-time operating system (RTOS) environments, are designed with different requirements when compared to desktop and enterprise systems, including robustness, security and real-time capabilities. The resource-constrained nature of many embedded systems, especially battery-powered mobile systems, imposes a further requirement for small memory-size and low overhead. Finally, in contrast to the ubiquity of the x86 architecture in the PC world, the embedded world uses a wider variety of architectures and less standardized environments. Support for virtualization requires memory protection (in the form of a memory management unit or at

least a memory protection unit) and a distinction between user mode and privileged mode, which rules out most microcontrollers. This still leaves x86, MIPS, ARM and PowerPC as widely deployed architectures on medium- to high-end embedded systems.^[12]

As manufacturers of embedded systems usually have the source code to their operating systems, they have less need for full virtualization in this space. Instead, the performance advantages of paravirtualization make this usually the virtualization technology of choice. Nevertheless, ARM and MIPS have recently added full virtualization support as an IP option and has included it in their latest high-end processors and architecture versions, such as ARM Cortex-A15 MPCore and ARMv8 EL2.

Other differences between virtualization in server/desktop and embedded environments include requirements for efficient sharing of resources across virtual machines, high-bandwidth, low-latency inter-VM communication, a global view of scheduling and power management, and fine-grained control of information flows.^[13]

Security implications

The use of hypervisor technology by malware and rootkits installing themselves as a hypervisor below the operating system, known as *hyperjacking*, can make them more difficult to detect because the malware could intercept any operations of the operating system (such as someone entering a password) without the anti-malware software necessarily detecting it (since the malware runs below the entire operating system). Implementation of the concept has allegedly occurred in the SubVirt laboratory rootkit (developed jointly by Microsoft and University of Michigan researchers^[14]) as well as in the Blue Pill malware package. However, such assertions have been disputed by others who claim that it would be possible to detect the presence of a hypervisor-based rootkit.^[15]

In 2009, researchers from Microsoft and North Carolina State University demonstrated a hypervisor-layer anti-rootkit called Hooksafe that can provide generic protection against kernel-mode rootkits.^[16]

Notes

- a. *super-* is from Latin, meaning "above", while *hyper-* is from the cognate term in Ancient Greek, also meaning "above".

References

1. Bernard Golden (2011). *Virtualization For Dummies*. p. 54.
2. "How did the term "hypervisor" come into use?"
3. Popek, Gerald J.; Goldberg, Robert P. (1974). "Formal requirements for virtualizable third generation architectures". *Communications of the ACM*. 17 (7): 412–421. doi:10.1145/361011.361073. Retrieved 2015-03-01.
4. Meier, Shannon (2008). "IBM Systems Virtualization: Servers, Storage, and Software" (PDF). pp. 2, 15, 20. Retrieved 2015-12-22.
5. Dexter, Michael. "Hands-on bhyve". *CallForTesting.org*. Retrieved 2013-09-24.
6. Graziano, Charles (2011). "A performance analysis of Xen and KVM hypervisors for hosting the Xen Worlds Project". *Graduate Theses and Dissertations*. Iowa State University. Retrieved 2013-01-29.
7. Pariseau, Beth (15 April 2011). "KVM reignites Type 1 vs. Type 2 hypervisor debate". *SearchServerVirtualization*. TechTarget. Retrieved 2013-01-29.
8. See History of CP/CMS for virtual-hardware simulation in the development of the System/370
9. Loftus, Jack (19 December 2005). "Xen virtualization quickly becoming open source 'killer app'". *TechTarget*. Retrieved 26 October 2015.

10. "Wind River To Support Sun's Breakthrough UltraSPARC T1 Multithreaded Next-Generation Processor". *Wind River Newsroom* (Press release). Alameda, California. 1 November 2006. Retrieved 26 October 2015.
11. Fritsch, Lothar; Husseiki, Rani; Alkassar, Ammar. Complementary and Alternative Technologies to Trusted Computing (TC-Erg./-A.), Part 1, A study on behalf of the German Federal Office for Information Security (BSI) (PDF) (Report).
12. Strobl, Marius (2013). *Virtualization for Reliable Embedded Systems*. Munich: GRIN Publishing GmbH. pp. 5–6. ISBN 978-3-656-49071-5. Retrieved 2015-03-07.
13. Gernot Heiser (April 2008). "The role of virtualization in embedded systems". *Proc. 1st Workshop on Isolation and Integration in Embedded Systems (IIES'08)*. pp. 11–16.
14. "SubVirt: Implementing malware with virtual machines" (PDF). University of Michigan, Microsoft. 2006-04-03. Retrieved 2008-09-15.
15. "Debunking Blue Pill myth". Virtualization.info. Retrieved 2010-12-10.
16. Wang, Zhi; Jiang, Xuxian; Cui, Weidong; Ning, Peng (11 August 2009). "Countering Kernel Rootkits with Lightweight Hook Protection" (PDF). *Proceedings of the 16th ACM Conference on Computer and Communications Security*. CCS '09. Chicago, Illinois, USA: ACM. doi:10.1145/1653662.1653728. ISBN 978-1-60558-894-0. Retrieved 2009-11-11.

External links

- Hypervisors and Virtual Machines: Implementation Insights on the x86 Architecture (<https://www.usenix.org/system/files/login/articles/105498-Revelle.pdf>)
- A Performance Comparison of Hypervisors (http://www.citd.ernet.in/misc/cloud/hypervisor_performance.pdf), VMware



Wikimedia Commons has media related to ***Hypervisor***.

Retrieved from "<https://en.wikipedia.org/w/index.php?title=Hypervisor&oldid=744915197>"

Categories: Servers (computing) ‌ Virtualization software

-
- This page was last modified on 18 October 2016, at 06:40.
 - Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Internet Protocol

From Wikipedia, the free encyclopedia

The **Internet Protocol (IP)** is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

Historically, IP was the connectionless datagram service in the original *Transmission Control Program* introduced by Vint Cerf and Bob Kahn in 1974; the other being the connection-oriented Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.

The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6).

Contents

- 1 Function
 - 1.1 Datagram construction
 - 1.2 IP addressing and routing
- 2 Version history
- 3 Reliability
- 4 Link capacity and capability
- 5 Security
- 6 See also
- 7 References
- 8 External links

Function

The Internet Protocol is responsible for addressing hosts and for routing datagrams (packets) from a source host to a destination host across one or more IP networks. For this purpose, the Internet Protocol defines the format of packets and provides an addressing system that has two functions: Identifying hosts and providing a logical location service.

Datagram construction

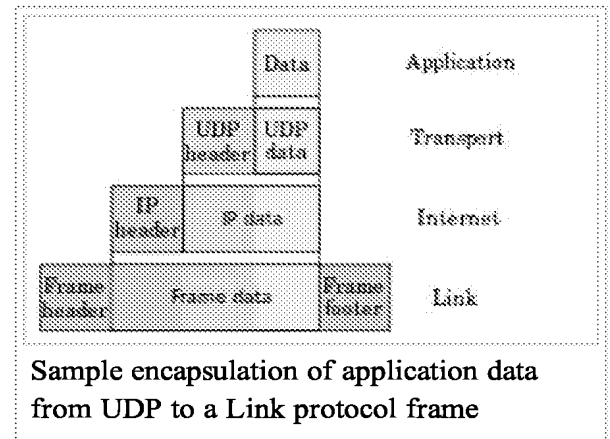
Each datagram has two components: a header and a payload. The IP header is tagged with the source IP address, the destination IP address, and other meta-data needed to route and deliver the datagram. The payload is the data that is transported. This method of nesting the data payload in a packet with a header is called encapsulation.

IP addressing and routing

IP addressing entails the assignment of IP addresses and associated parameters to host interfaces. The address space is divided into networks and subnetworks, involving the designation of network or routing prefixes. IP routing is performed by all hosts, as well as routers, whose main function is to transport packets across network boundaries. Routers communicate with one another via specially designed routing protocols, either interior gateway protocols or exterior gateway protocols, as needed for the topology of the network.

IP routing is also common in local networks. For example, many Ethernet switches support IP multicast operations.^[1]

These switches use IP addresses and Internet Group Management Protocol to control multicast routing but use MAC addresses for the actual routing.



Version history

The versions currently relevant are IPv4 and IPv6.

In May 1974, the Institute of Electrical and Electronic Engineers (IEEE) published a paper entitled "A Protocol for Packet Network Intercommunication".^[2] The paper's authors, Vint Cerf and Bob Kahn, described an internetworking protocol for sharing resources using packet switching among network nodes. A central control component of this model was the "Transmission Control Program" that incorporated both connection-oriented links and datagram services between hosts. The monolithic Transmission Control Program was later divided into a modular architecture consisting of the Transmission Control Protocol and User Datagram Protocol at the transport layer and the Internet Protocol at the network layer. The model became known as the *Department of Defense (DoD) Internet Model* and *Internet protocol suite*, and informally as *TCP/IP*.

IP versions 0 to 3 were experimental versions, used between 1977 and 1979. The following Internet Experiment Note (IEN) documents describe versions of the Internet Protocol prior to the modern version of IPv4:

- IEN 2 (<http://www.rfc-editor.org/ien/ien2.txt>) (*Comments on Internet Protocol and TCP*), dated August 1977 describes the need to separate the TCP and Internet Protocol functionalities (which were previously combined.) It proposes the first version of the IP header, using 0 for the version field.
- IEN 26 (<http://www.rfc-editor.org/ien/ien26.pdf>) (*A Proposed New Internet Header Format*), dated February 1978 describes a version of the IP header that uses a 1-bit version field.
- IEN 28 (<http://www.rfc-editor.org/ien/ien28.pdf>) (*Draft Internetwork Protocol Description Version 2*), dated February 1978 describes IPv2.
- IEN 41 (<http://www.rfc-editor.org/ien/ien41.pdf>) (*Internetwork Protocol Specification Version 4*), dated June 1978 describes the first protocol to be called IPv4. The IP header is different from the modern IPv4 header.
- IEN 44 (<http://www.rfc-editor.org/ien/ien44.pdf>) (*Latest Header Formats*), dated June 1978 describes another version of IPv4, also with a header different from the modern IPv4 header.
- IEN 54 (<http://www.rfc-editor.org/ien/ien54.pdf>) (*Internetwork Protocol Specification Version 4*), dated September 1978 is the first description of IPv4 using the header that would be standardized in RFC 760.

The dominant internetworking protocol in the Internet Layer in use today is IPv4; the number 4 is the protocol version number carried in every IP datagram. IPv4 is described in RFC 791 (1981).

Version 5 was used by the Internet Stream Protocol, an experimental streaming protocol.

The successor to IPv4 is IPv6. Its most prominent difference from version 4 is the size of the addresses. While IPv4 uses 32 bits for addressing, yielding c. 4.3 billion (4.3×10^9) addresses, IPv6 uses 128-bit addresses providing ca. 340 undecillion, or 3.4×10^{38} addresses. Although adoption of IPv6 has been slow, as of June 2008, all United States government systems have demonstrated basic infrastructure support for IPv6.^[3] IPv6 was a result of several years of experimentation and dialog during which various protocol models were proposed, such as TP/IX (RFC 1475), PIP (RFC 1621) and TUBA (TCP and UDP with Bigger Addresses, RFC 1347).

The assignment of the new protocol as IPv6 was uncertain until due diligence revealed that IPv6 had not yet been used previously.^[4] Other protocol proposals named *IPv9* and *IPv8* briefly surfaced, but had no affiliation with any international standards body, and have had no support.^[5]

On April 1, 1994, the IETF published an April Fool's Day joke about IPv9.^[6]

Reliability

The design of the Internet protocols is based on the end-to-end principle. The network infrastructure is considered inherently unreliable at any single network element or transmission medium and is dynamic in terms of availability of links and nodes. No central monitoring or performance measurement facility exists that tracks or maintains the state of the network. For the benefit of reducing network complexity, the intelligence in the network is purposely located in the end nodes.

As a consequence of this design, the Internet Protocol only provides best-effort delivery and its service is characterized as unreliable. In network architectural language, it is a connectionless protocol, in contrast to connection-oriented communication. Various error conditions may occur, such as data corruption, packet loss, duplication and out-of-order delivery. Because routing is dynamic, meaning every packet is treated independently, and because the network maintains no state based on the path of prior packets, different packets may be routed to the same destination via different paths, resulting in out-of-order sequencing at the receiver.

IPv4 provides safeguards to ensure that the IP packet header is error-free. A routing node calculates a checksum for a packet. If the checksum is bad, the routing node discards the packet. Although the Internet Control Message Protocol (ICMP) allows such notification, the routing node is not required to notify either end node of these errors. By contrast, in order to increase performance, and since current link layer technology is assumed to provide sufficient error detection,^[7] the IPv6 header has no checksum to protect it.^[8]

All error conditions in the network must be detected and compensated by the end nodes of a transmission. The upper layer protocols of the internet protocol suite are responsible for resolving reliability issues. For example, a host may buffer network data to ensure correct ordering before the data is delivered to an application.

Link capacity and capability

The dynamic nature of the Internet and the diversity of its components provide no guarantee that any particular path is actually capable of, or suitable for, performing the data transmission requested, even if the path is available and reliable. One of the technical constraints is the size of data packets allowed on a given link. An application must assure that it uses proper transmission characteristics. Some of this responsibility lies also in the upper layer protocols. Facilities exist to examine the maximum transmission unit (MTU) size of the local link and Path MTU Discovery can be used for the entire projected path to the destination. The IPv4 internetworking layer has the capability to automatically fragment the original datagram into smaller units for transmission. In this case, IP provides re-ordering of fragments delivered out of order.^[9]

The Transmission Control Protocol (TCP) is an example of a protocol that adjusts its segment size to be smaller than the MTU. The User Datagram Protocol (UDP) and the Internet Control Message Protocol (ICMP) disregard MTU size, thereby forcing IP to fragment oversized datagrams.^[10]

An IPv6 network does not perform fragmentation or reassembly, and as per the end-to-end principle, requires end stations and higher-layer protocols to avoid exceeding the network's MTU.^[11]

Security

During the design phase of the ARPANET and the early Internet, the security aspects and needs of a public, international network could not be adequately anticipated. Consequently, many Internet protocols exhibited vulnerabilities highlighted by network attacks and later security assessments. In 2008, a thorough security assessment and proposed mitigation of problems was published.^[12] The Internet Engineering Task Force (IETF) has been pursuing further studies.^[13]

See also

- List of IP protocol numbers
- Next-generation network
- IP forwarding algorithm

References

1. Netgear ProSafe XSM7224S reference manual
2. Vinton G. Cerf, Robert E. Kahn, "A Protocol for Packet Network Intercommunication", IEEE Transactions on Communications, Vol. 22, No. 5, May 1974 pp. 637–648
3. CIO council adds to IPv6 transition primer (http://www.gcn.com/print/25_16/41051-1.html), gcn.com
4. Mulligan, Geoff. "It was almost IPv7". *O'Reilly*. O'Reilly Media. Retrieved 4 July 2015.
5. Leyden, John (6 July 2004). "China disowns IPv9 hype". *theregister.co.uk*. The Register. Retrieved 4 May 2014.
6. RFC 1606: *A Historical Perspective On The Usage Of IP Version 9*. April 1, 1994.
7. RFC 1726 section 6.2
8. RFC 2460
9. Siyan, Karanjit. *Inside TCP/IP*, New Riders Publishing, 1997. ISBN 1-56205-714-6
10. Parker, Don (2 November 2010). "Basic Journey of a Packet". *symantec.com*. Symantec. Retrieved 4 May 2014.
11. Bill Cervený (2011-07-25). "IPv6 Fragmentation". Arbor Networks. Retrieved 2016-09-10.
12. Security Assessment of the Internet Protocol (IP)(archived version) (<http://web.archive.org/web/20100211145721/http://www.cpni.gov.uk/Docs/InternetProtocol.pdf>)
13. Security Assessment of the Internet Protocol version 4 (IPv4) (<http://tools.ietf.org/html/draft-ietf-opsec-ip-security>)

External links

- Internet Protocol (<https://www.dmoz.org/Computers/Internet/Protocols>) at DMOZ
- RFC 791
- Data Communication Lectures of Manfred Lindner – Part IP Technology Fundamentals (https://www.ict.tuwien.ac.at/lva/384.081/datacom/09-IP_Technology_v6-1_handout.pdf)
- Data Communication Lectures of Manfred Lindner – Part IP Routing Fundamentals (https://www.ict.tuwien.ac.at/lva/384.081/datacom/10-IP_Routing_v6-1_handout.pdf)



Look up ***internet protocol*** in Wiktionary, the free dictionary.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Internet_Protocol&oldid=749645187"

Categories: Internet layer protocols

-
- This page was last modified on 15 November 2016, at 13:47.
 - Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Multiprotocol Label Switching

From Wikipedia, the free encyclopedia

Multiprotocol Label Switching (MPLS) is a type of data-carrying technique for high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (*paths*) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols, hence its name "multiprotocol". MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL.

Contents

- 1 Role and functioning
- 2 History
- 3 Operation
 - 3.1 Label switch router
 - 3.2 Label edge router
 - 3.3 Provider router
 - 3.4 Label Distribution Protocol
 - 3.5 Label-switched paths
 - 3.6 Routing
 - 3.6.1 Label-switched path
 - 3.7 Installing and removing paths
 - 3.8 Multicast addressing
- 4 Relationship to Internet Protocol
 - 4.1 MPLS local protection (fast reroute)
- 5 Comparisons
 - 5.1 Frame Relay
 - 5.2 ATM
- 6 Deployment
- 7 Evolution
- 8 Competitor protocols
- 9 See also
- 10 Notes
- 11 References
- 12 Further reading
- 13 External links

Role and functioning

MPLS is a scalable, protocol-independent transport. In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport medium, using any protocol. The primary benefit is to eliminate dependence on a particular OSI model data link layer (layer 2) technology, such as Asynchronous Transfer Mode (ATM), Frame Relay, Synchronous Optical Networking (SONET) or Ethernet, and eliminate the need for multiple layer-2 networks to satisfy different types of traffic. MPLS belongs to the family of packet-switched networks.

MPLS operates at a layer that is generally considered to lie between traditional definitions of OSI Layer 2 (data link layer) and Layer 3 (network layer), and thus is often referred to as a *layer 2.5* protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET, and Ethernet frames.

A number of different technologies were previously deployed with essentially identical goals, such as Frame Relay and ATM. Frame Relay and ATM use "labels" to move frames or cells throughout a network. The header of the Frame Relay frame and the ATM cell refers to the virtual circuit that the frame or cell resides on. The similarity between Frame Relay, ATM, and MPLS is that at each hop throughout the network, the "label" value in the header is changed. This is different

from the forwarding of IP packets.^[1] MPLS technologies have evolved with the strengths and weaknesses of ATM in mind. Many network engineers agree that ATM should be replaced with a protocol that requires less overhead, while providing connection-oriented services for variable-length frames. MPLS is currently replacing some of these technologies in the marketplace. It is highly possible that MPLS will completely replace these technologies in the future, thus aligning these technologies with current and future technology needs.^[2]

In particular, MPLS dispenses with the cell-switching and signaling-protocol baggage of ATM. MPLS recognizes that small ATM cells are not needed in the core of modern networks, since modern optical networks are so fast (as of 2015, at 100 Gbit/s and beyond) that even full-length 1500 byte packets do not incur significant real-time queuing delays (the need to reduce such delays — *e.g.*, to support voice traffic — was the motivation for the cell nature of ATM).

At the same time, MPLS attempts to preserve the traffic engineering (TE) and out-of-band control that made Frame Relay and ATM attractive for deploying large-scale networks.

While the traffic management benefits of migrating to MPLS are quite valuable (better reliability, increased performance), there is a significant loss of visibility and access into the MPLS cloud for IT departments.

History

- 1994: Toshiba presented Cell Switch Router (CSR) ideas to IETF BOF
- 1996: Ipsilon, Cisco and IBM announced label switching plans
- 1997: Formation of the IETF MPLS working group
- 1999: First MPLS VPN (L3VPN) and TE deployments
- 2000: MPLS traffic engineering
- 2001: First MPLS Request for Comments (RFCs) released
- 2002: AToM (L2VPN)
- 2004: GMPLS; Large scale L3VPN
- 2006: Large scale TE
- 2007: Large scale L2VPN
- 2009: Label Switching Multicast
- 2011: MPLS transport profile

In 1996 a group from Ipsilon Networks proposed a "flow management protocol".^[3] Their "IP Switching" technology, which was defined only to work over ATM, did not achieve market dominance. Cisco Systems introduced a related proposal, not restricted to ATM transmission, called "Tag Switching".^[4] It was a Cisco proprietary proposal, and was renamed "Label Switching". It was handed over to the Internet Engineering Task Force (IETF) for open standardization. The IETF work involved proposals from other vendors, and development of a consensus protocol that combined features from several vendors' work.

One original motivation was to allow the creation of simple high-speed switches, since for a significant length of time it was impossible to forward IP packets entirely in hardware. However, advances in VLSI have made such devices possible. Therefore, the advantages of MPLS primarily revolve around the ability to support multiple service models and perform traffic management. MPLS also offers a robust recovery framework^[5] that goes beyond the simple protection rings of synchronous optical networking (SONET/SDH).

Operation

MPLS works by prefixing packets with an MPLS header, containing one or more labels. This is called a label stack. Each entry in the label stack contains four fields:

- A 20-bit label value. A label with the value of 1 represents the router alert label.
- a 3-bit *Traffic Class* field for QoS (quality of service) priority and ECN (Explicit Congestion Notification). Prior to 2009 this field was called EXP.^[6]
- a 1-bit *bottom of stack* flag. If this is set, it signifies that the current label is the last in the stack.
- an 8-bit TTL (time to live) field.

MPLS Label

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Label																				TC: Traffic Class (QoS and ECN)	S: Bottom- of- Stack	TTL: Time-to-Live									

These MPLS-labeled packets are switched after a label lookup/switch instead of a lookup into the IP table. As mentioned above, when MPLS was conceived, label lookup and label switching were faster than a routing table or RIB (Routing Information Base) lookup because they could take place directly within the switched fabric and not the CPU.

The presence of such a label, however, has to be indicated to the router/switch. In the case of Ethernet frames this is done through the use of EtherType values 0x8847 and 0x8848, for unicast and multicast connections respectively.^[7]

Label switch router

An MPLS router that performs routing based only on the label is called a **label switch router (LSR)** or **transit router**. This is a type of router located in the middle of an MPLS network. It is responsible for switching the labels used to route packets.

When an LSR receives a packet, it uses the label included in the packet header as an index to determine the next hop on the label-switched path (LSP) and a corresponding label for the packet from a lookup table. The old label is then removed from the header and replaced with the new label before the packet is routed forward.

Label edge router

A label edge router (LER, also known as edge LSR) is a router that operates at the edge of an MPLS network and acts as the entry and exit points for the network. LERs *push* an MPLS label onto an incoming packet^[note 1] and *pop* it off an outgoing packet. Alternatively, under penultimate hop popping this function may instead be performed by the LSR directly connected to the LER.

When forwarding an IP datagram into the MPLS domain, an LER uses routing information to determine the appropriate label to be affixed, labels the packet accordingly, and then forwards the labelled packet into the MPLS domain. Likewise, upon receiving a labelled packet which is destined to exit the MPLS domain, the LER strips off the label and forwards the resulting IP packet using normal IP forwarding rules.

Provider router

In the specific context of an MPLS-based virtual private network (VPN), LERs that function as ingress and/or egress routers to the VPN are often called PE (Provider Edge) routers. Devices that function only as transit routers are similarly called P (Provider) routers.^[8] The job of a P router is significantly easier than that of a PE router, so they can be less complex and may be more dependable because of this.

Label Distribution Protocol

Labels are distributed between LERs and LSRs using the Label Distribution Protocol (LDP).^[9] LSRs in an MPLS network regularly exchange label and reachability information with each other using standardized procedures in order to build a complete picture of the network they can then use to forward packets.

Label-switched paths

Label-switched paths (LSPs) are established by the network operator for a variety of purposes, such as to create network-based IP virtual private networks or to route traffic along specified paths through the network. In many respects, LSPs are not different from permanent virtual circuits (PVCs) in ATM or Frame Relay networks, except that they are not dependent on a particular layer-2 technology.

Routing

When an unlabeled packet enters the ingress router and needs to be passed on to an MPLS tunnel, the router first determines the forwarding equivalence class (FEC) for the packet and then inserts one or more labels in the packet's newly created MPLS header. The packet is then passed on to the next hop router for this tunnel.

The MPLS Header is added between the network layer header and link layer header of the OSI model.^[10]

When a labeled packet is received by an MPLS router, the topmost label is examined. Based on the contents of the label a *swap*, *push* (*impose*) or *pop* (*dispose*) operation is performed on the packet's label stack. Routers can have prebuilt lookup tables that tell them which kind of operation to do based on the topmost label of the incoming packet so they can process the packet very quickly.

- In a *swap* operation the label is swapped with a new label, and the packet is forwarded along the path associated with the new label.
- In a *push* operation a new label is pushed on top of the existing label, effectively "encapsulating" the packet in another layer of MPLS. This allows hierarchical routing of MPLS packets. Notably, this is used by MPLS VPNs.
- In a *pop* operation the label is removed from the packet, which may reveal an inner label below. This process is called "decapsulation". If the popped label was the last on the label stack, the packet "leaves" the MPLS tunnel. This is usually done by the egress router, but see Penultimate Hop Popping (PHP) below.

During these operations, the contents of the packet below the MPLS Label stack are not examined. Indeed, transit routers typically need only to examine the topmost label on the stack. The forwarding of the packet is done based on the contents of the labels, which allows "protocol-independent packet forwarding" that does not need to look at a protocol-dependent routing table and avoids the expensive IP longest prefix match at each hop.

At the egress router, when the last label has been popped, only the payload remains. This can be an IP packet, or any of a number of other kinds of payload packet. The egress router must therefore have routing information for the packet's payload, since it must forward it without the help of label lookup tables. An MPLS transit router has no such requirement.

In some special cases, the last label can also be popped off at the penultimate hop (the hop before the egress router). This is called penultimate hop popping (PHP). This may be interesting in cases where the egress router has lots of packets leaving MPLS tunnels, and thus spends inordinate amounts of CPU time on this. By using PHP, transit routers connected directly to this egress router effectively offload it, by popping the last label themselves.

Label-switched path

A label-switched path (LSP) is a path through an MPLS network, set up by a signaling protocol such as LDP, RSVP-TE, BGP or CR-LDP. The path is set up based on criteria in the FEC.

The path begins at a label edge router (LER), which makes a decision on which label to prefix to a packet, based on the appropriate FEC. It then forwards the packet along to the next router in the path, which swaps the packet's outer label for another label, and forwards it to the next router. The last router in the path removes the label from the packet and forwards the packet based on the header of its next layer, for example IPv4. Due to the forwarding of packets through an LSP being opaque to higher network layers, an LSP is also sometimes referred to as an MPLS tunnel.

The router which first prefixes the MPLS header to a packet is called an ingress router. The last router in an LSP, which pops the label from the packet, is called an egress router. Routers in between, which need only swap labels, are called transit routers or label switch routers (LSRs).

Note that LSPs are unidirectional; they enable a packet to be label switched through the MPLS network from one endpoint to another. Since bidirectional communication is typically desired, the aforementioned dynamic signaling protocols can set up an LSP in the other direction to compensate for this.

When protection is considered, LSPs could be categorized as primary (working), secondary (backup) and tertiary (LSP of last resort). As described above, LSPs are normally P2P (point to point). A new concept of LSPs, which are known as P2MP (point to multi-point), was introduced recently. These are mainly used for multicasting purposes.

The hub&spoke multipoint LSP is also introduced by IETF, short as HSMP LSP. HSMP LSP is mainly used for multicast, time synchronization and other purpose.

Installing and removing paths

There are two standardized protocols for managing MPLS paths: the Label Distribution Protocol (LDP) and RSVP-TE, an extension of the Resource Reservation Protocol (RSVP) for traffic engineering.^{[11][12]} Furthermore, there exist extensions of the Border Gateway Protocol (BGP) that can be used to manage an MPLS path.^{[8][13][14]}

An MPLS header does not identify the type of data carried inside the MPLS path. If one wants to carry two different types of traffic between the same two routers, with different treatment by the core routers for each type, one has to establish a separate MPLS path for each type of traffic.

Multicast addressing

Multicast was for the most part an after-thought in MPLS design. It was introduced by point-to-multipoint RSVP-TE.^[15] It was driven by service provider requirements to transport broadband video over MPLS. Since the inception of RFC 4875 there has been tremendous surge in interest and deployment of MPLS multicast and this has led to several new developments both in the IETF and in shipping products.

The hub&spoke multipoint LSP is also introduced by IETF, short as HSMP LSP. HSMP LSP is mainly used for multicast, time synchronization and other purpose.

Relationship to Internet Protocol

MPLS works in conjunction with the Internet Protocol (IP) and its routing protocols, such as the Interior Gateway Protocol (IGP). MPLS LSPs provide dynamic, transparent virtual networks with support for traffic engineering, the ability to transport layer-3 (IP) VPNs with overlapping address spaces, and support for layer-2 pseudowires using Pseudowire Emulation Edge-to-Edge (PWE3)^[16] that are capable of transporting a variety of transport payloads (IPv4, IPv6, ATM, Frame Relay, etc.). MPLS-capable devices are referred to as LSRs. The paths an LSR knows can be defined using explicit hop-by-hop configuration, or are dynamically routed by the constrained shortest path first (CSPF) algorithm, or are configured as a loose route that avoids a particular IP address or that is partly explicit and partly dynamic.

In a pure IP network, the shortest path to a destination is chosen even when the path becomes congested. Meanwhile, in an IP network with MPLS Traffic Engineering CSPF routing, constraints such as the RSVP bandwidth of the traversed links can also be considered, such that the shortest path with available bandwidth will be chosen. MPLS Traffic Engineering relies upon the use of TE extensions to Open Shortest Path First (OSPF) or Intermediate System To Intermediate System (IS-IS) and RSVP. In addition to the constraint of RSVP bandwidth, users can also define their own constraints by specifying link attributes and special requirements for tunnels to route (or not to route) over links with certain attributes.^[17]

For end-users the use of MPLS is not visible directly, but can be assumed when doing a traceroute: only nodes that do *full* ip routing are shown as hops in the path, thus not the MPLS nodes used in between, therefore when you see that a packet *hops* between two very distant nodes and hardly any other 'hop' is seen in that providers network (or AS) it is very likely that network uses MPLS.

MPLS local protection (fast reroute)

In the event of a network element failure when recovery mechanisms are employed at the IP layer, restoration may take several seconds which may be unacceptable for real-time applications such as VoIP.^{[18][19][20]} In contrast, MPLS local protection meets the requirements of real-time applications with recovery times comparable to those of shortest path bridging networks or SONET rings of less than 50 ms.^{[18][20][21]}

Comparisons

MPLS can make use of existing ATM network or Frame Relay infrastructure, as its labeled flows can be mapped to ATM or Frame Relay virtual-circuit identifiers, and vice versa.

Frame Relay

Frame Relay aimed to make more efficient use of existing physical resources, which allow for the underprovisioning of data services by telecommunications companies (telcos) to their customers, as clients were unlikely to be utilizing a data service 100 percent of the time. In more recent years, Frame Relay has acquired a bad reputation in some markets because of excessive bandwidth overbooking by these telcos.

Telcos often sell Frame Relay to businesses looking for a cheaper alternative to dedicated lines; its use in different geographic areas depended greatly on governmental and telecommunication companies' policies.

Many customers are likely to migrate from Frame Relay to MPLS over IP or Ethernet within the next two years, which in many cases will reduce costs and improve manageability and performance of their wide area networks.^[22]

ATM

While the underlying protocols and technologies are different, both MPLS and ATM provide a connection-oriented service for transporting data across computer networks. In both technologies, connections are signaled between endpoints, connection state is maintained at each node in the path, and encapsulation techniques are used to carry data across the connection. Excluding differences in the signaling protocols (RSVP/LDP for MPLS and PNNI:Private Network-to-Network Interface for ATM) there still remain significant differences in the behavior of the technologies.

The most significant difference is in the transport and encapsulation methods. MPLS is able to work with variable length packets while ATM transports fixed-length (53 byte) cells. Packets must be segmented, transported and re-assembled over an ATM network using an adaptation layer, which adds significant complexity and overhead to the data stream. MPLS, on the other hand, simply adds a label to the head of each packet and transmits it on the network.

Differences exist, as well, in the nature of the connections. An MPLS connection (LSP) is unidirectional—allowing data to flow in only one direction between two endpoints. Establishing two-way communications between endpoints requires a pair of LSPs to be established. Because 2 LSPs are required for connectivity, data flowing in the forward direction may use a different path from data flowing in the reverse direction. ATM point-to-point connections (virtual circuits), on the other hand, are bidirectional, allowing data to flow in both directions over the same path (Both SVC and PVC ATM connections are bidirectional. Check ITU-T I.150 3.1.3.1).

Both ATM and MPLS support tunneling of connections inside connections. MPLS uses label stacking to accomplish this while ATM uses *virtual paths*. MPLS can stack multiple labels to form tunnels within tunnels. The ATM virtual path indicator (VPI) and virtual circuit indicator (VCI) are both carried together in the cell header, limiting ATM to a single level of tunnelling.

The biggest advantage that MPLS has over ATM is that it was designed from the start to be complementary to IP. Modern routers are able to support both MPLS and IP natively across a common interface allowing network operators great flexibility in network design and operation. ATM's incompatibilities with IP require complex adaptation, making it comparatively less suitable for today's predominantly IP networks.

Deployment

MPLS is currently (as of March 2012) in use in IP-only networks and is standardized by the IETF in RFC 3031. It is deployed to connect as few as two facilities to very large deployments.

In practice, MPLS is mainly used to forward IP protocol data units (PDUs) and Virtual Private LAN Service (VPLS) Ethernet traffic. Major applications of MPLS are telecommunications traffic engineering, and MPLS VPN.

Evolution

MPLS has been originally proposed to allow high performance traffic forwarding and traffic engineering in IP networks. However it evolved in Generalized MPLS (GMPLS) to allow the creation of label-switched paths (LSPs) also in non-native IP networks, such as SONET/SDH networks and wavelength switched optical networks.

Competitor protocols

MPLS can exist in both an IPv4 and an IPv6 environment, using appropriate routing protocols. The major goal of MPLS development was the increase of routing speed. This goal is no longer relevant because of the usage of newer switching methods, such as ASIC, TCAM and CAM-based switching. Now, therefore, the main application of MPLS is to implement limited traffic engineering and layer 3 / layer 2 “service provider type” VPNs over IPv4 networks.

Besides GMPLS, the main competitors to MPLS are Shortest Path Bridging (SPB), Provider Backbone Bridges (PBB), and MPLS-TP. These also provide services such as service provider layer 2 and layer 3 VPNs. L2TPv3 has been suggested as a competitor, but has not reached any wider success. Some internet providers are offering different services to customers along with MPLS. These services mainly include National Private Lease Circuit (NPLC), ILL, IPLC etc. As an example of NPLC, consider City A and City B. An organisation has an office in each city. The organisation requires connectivity between these two offices. The ISP will have access to a PoP in each city and therefore has a link between the PoPs. To connect the offices to the PoPs, a connection via the local loop will be commissioned for each office. In this way, an NPLC is delivered.

IEEE 1355 and Spacewire are a family of simplified physical-layer standards very similar in function at the hardware level to MPLS.

See also

- Generalized Multi-Protocol Label Switching
- MPLS VPN
- Per-hop behavior
- Virtual private LAN service
- Label Information Base
- IEEE 802.1aq - Shortest Path Bridging (SPB)

Notes

1. In some applications, the packet presented to the LER already may have a label, so that the new LER pushes a second label onto the packet.

References

1. MPLS Fundamentals, By Luc De Ghein Nov 21, 2006 (ISBN 1-58705-197-4)
2. Applied Data Communications (A Business-Oriented Approach) James E. Goldman & Phillip T. Rawles, 2004 (ISBN 0-471-34640-3)
3. P. Newman; et al. (May 1996). "Ipsilon Flow Management Protocol Specification for IPv4". *RFC 1953*. IETF.
4. Y. Rekhter et al., Tag switching architecture overview (http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=650179), Proc. IEEE 82 (December 1997), 1973–1983.
5. V. Sharma; F. Hellstrand (February 2003), *RFC 3469: Framework for Multi-Protocol Label Switching (MPLS)-based Recovery*, IETF
6. L. Andersson; R. Asati (February 2009), *Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field*, IETF
7. Ivan Pepelnjak; Jim Guichard (2002), *MPLS and VPN Architectures, Volume 1*, Cisco Press, p. 27, ISBN 1587050811
8. E. Rosen; Y. Rekhter (February 2006), *RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs)*, IETF
9. B. Thomas; E. Gray (January 2001), *RFC 3037: LDP Applicability*, IETF
10. Savecall telecommunication consulting company Germany Savecall - MPLS (<http://www.savecall.de/mppls/>)
11. L. Andersson; I. Minei; B. Thomas (October 2007), *RFC 5036: LDP Specification*, IETF
12. D. Awduche; L. Berger; D. Gan; T. Li; V. Srinivasan; G. Swallow (December 2001), *RFC 3209: RSVP-TE: Extensions to RSVP for LSP Tunnels*, IETF
13. Y. Rekhter; E. Rosen (May 2001), *RFC 3107: Carrying Label Information in BGP-4*, IETF
14. Y. Rekhter; R. Aggarwal (January 2007), *RFC 4781: Graceful Restart Mechanism for BGP with MPLS*, IETF
15. R. Aggarwal; D. Papadimitriou; S. Yasukawa (May 2007), *RFC 4875: Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)*, IETF
16. S. Bryant; P. Pate (March 2005), *RFC 3985: Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture*, IETF
17. de Ghein, Luc, *MPLS Fundamentals*, pp. 249–326
18. Aslam; et al. (2005-02-02), *NPP: A Facility Based Computation Framework for Restoration Routing Using Aggregate Link Usage Information*, QoS-IP 2005 : quality of service in multiservice IP network, retrieved 2006-10-27.
19. Raza; et al., *Online routing of bandwidth guaranteed paths with local restoration using optimized aggregate usage information* (PDF), IEEE-ICC 2005, retrieved 2006-10-27.
20. Li Li; et al., *Routing bandwidth guaranteed paths with local restoration in label switched networks* (PDF), IEEE Journal on

Selected Areas in Communications, retrieved 2006-10-27.

21. Kodialam; et al., *Dynamic Routing of Locally Restorable Bandwidth Guaranteed Tunnels using Aggregated Link Usage Information* (PDF), IEEE Infocom. pp. 376–385. 2001, retrieved 2006-10-27.
22. "AT&T — Frame Relay and IP-Enabled Frame Relay Service (Product Advisor)" (http://www.researchandmarkets.com/reportinfo.asp?report_id=451078), Research and Markets, June 2007.

Further reading

- "Deploying IP and MPLS QoS for Multiservice Networks: Theory and Practice" by John Evans, Clarence Filsfils (Morgan Kaufmann, 2007, ISBN 0-12-370549-5)
- Rick Gallaher's MPLS Training Guide (ISBN 1932266003)

External links

- MPLS Working Group (<http://tools.ietf.org/wg/mpls/>), IETF.
- MPLS IP Specifications (<http://www.broadband-forum.org/technical/ipmplstechspec.php>), Broadband Forum.
- A brief history of MPLS (<http://meetings.ripe.net/ripe-39/presentations/mpls-arch/sld005.html>), RIPE

Retrieved from "https://en.wikipedia.org/w/index.php?title=Multiprotocol_Label_Switching&oldid=747041625"

Categories: MPLS networking | Internet Standards | Tunneling protocols

-
- This page was last modified on 31 October 2016, at 03:00.
 - Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Network address translation

From Wikipedia, the free encyclopedia

Network address translation (NAT) is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.^[1] The technique was originally used for ease of rerouting traffic in IP networks without readdressing every host. It has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion by sharing one Internet-routable IP address of a NAT gateway for an entire private network.

Contents

- 1 Methodology
- 2 Basic NAT
- 3 One-to-many NAT
- 4 Methods of translation
- 5 Type of NAT and NAT traversal, role of port preservation for TCP
- 6 Implementation
 - 6.1 Establishing two-way communication
 - 6.2 Telephone number extension analogy
 - 6.3 Translation of the endpoint
 - 6.4 Visibility of operation
- 7 NAT and TCP/UDP
- 8 DNAT
- 9 SNAT
- 10 Dynamic network address translation
- 11 NAT loopback
- 12 NAT in IPv6
- 13 Applications affected by NAT
- 14 Examples of NAT software
- 15 See also
- 16 References
- 17 External links

Methodology

The original use of network address translation consisted of mapping every address of one address space to a corresponding address in another space, such as when an enterprise changed Internet service providers without having a facility to announce a public route to the network. In the face of the foreseeable global IP address space exhaustion, NAT was increasingly used since the late 1990s in conjunction with IP masquerading, which is a technique that hides an entire IP address space, usually consisting of private network IP addresses (RFC 1918), behind a single IP address in another, usually public address space. I.e. the address that has to be hidden is changed into a single (public) IP address as "new" source address of the outgoing IP packet so it appears as originating not from the hidden host but from the routing device itself. Masquerading routing devices keep stateful translation tables of a certain conversation to "remember" the original source address when packets return during this conversation. The translation tables are flushed after a defined period unless new traffic refreshes their state to prevent port exhaustion and free state table resources.

The method enables communication through the router only when the conversation originates in the masqueraded network since this establishes the translation tables. For example, a web browser in the masqueraded network can browse a website outside, but a web browser outside could not browse a website hosted within the masqueraded network. However, most NAT devices today allow the network administrator to configure translation table entries for permanent use. This feature is often referred to as "static NAT" or port forwarding and allows traffic originating in the "outside" network to reach designated hosts in the masqueraded network.

Because of the popularity of this technique to conserve IPv4 address space, the term *NAT* has become virtually synonymous with the method of IP masquerading.

As network address translation modifies the IP address information in packets, it has serious consequences on the quality of Internet connectivity and requires careful attention to the details of its implementation. NAT implementations vary widely in their specific behavior in various addressing cases and their effect on network traffic. The specifics of NAT behavior is not commonly documented by vendors of equipment containing implementations.^[2]

Basic NAT

The simplest type of NAT provides a one-to-one translation of IP addresses. RFC 2663 refers to this type of NAT as *basic NAT*; it is often also called a *one-to-one NAT*. In this type of NAT, only the IP addresses, IP header checksum and any higher level checksums that include the IP address are changed. Basic NATs can be used to interconnect two IP networks that have incompatible addressing.

One-to-many NAT

The majority of NATs map multiple private hosts to one publicly exposed IP address. In a typical configuration, a local network uses one of the designated "private" IP address subnets (RFC 1918). A router on that network has a private address in that address space. The router is also connected to the Internet with a "public" address assigned by an Internet service provider. As traffic passes from the local network to the Internet, the source address in each packet is translated on the fly from a private address to the public address. The router tracks basic data about each active connection (particularly the destination address and port). When a reply returns to the router, it uses the connection tracking data it stored during the outbound phase to determine the private address on the internal network to which to forward the reply.

One of the benefits of this is that it is a practical solution to the impending exhaustion of the IPv4 address space. Even large networks can be connected to the Internet with a single IP address. The more common arrangement is having computers that require end-to-end connectivity supplied with a routable IP address, while having others that do not provide services to outside users behind NAT with only a few IP addresses used to enable Internet access.

All datagram packets on IP networks have a source IP address and a destination IP address. Typically packets passing from the private network to the public network will have their source address modified while packets passing from the public network back to the private network will have their destination address modified. More complex configurations are also possible.

To avoid ambiguity in how to translate returned packets, further modifications to the packets are required. The vast bulk of Internet traffic is TCP and UDP packets, and for these protocols the port numbers are changed so that the combination of IP address and port information on the returned packet can be unambiguously mapped to the corresponding private address and port information. RFC 2663

uses the term *network address and port translation* (NAPT) for this type of NAT. Other names include *port address translation* (PAT), *IP masquerading*, *NAT overload* and *many-to-one NAT*. This is the most common type of NAT and has become synonymous with the term NAT in common usage. This method enables communication through the router only when the conversation originates in the masqueraded network since this establishes the translation tables. For example, a web browser in the masqueraded network can browse a website outside, but a web browser outside could not browse a website hosted within the masqueraded network. However, most NAT devices today allow the network administrator to configure static translation table entries for connections from the external network to the internal masqueraded network. This feature is often referred to as *static NAT*. It may be implemented in two types: port forwarding which forwards traffic from a specific external port to an internal host on a specified port, and designation of a DMZ host which passes all traffic received on the external interface (on any port number) to an internal IP address while preserving the destination port. Both types may be available in the same NAT device.

Protocols not based on TCP and UDP require other translation techniques. Internet Control Message Protocol (ICMP) packets typically relate to an existing connection and need to be mapped using the same IP address and port mappings as established in that connection.

Hosts behind NAT-enabled routers do not have end-to-end connectivity and cannot participate in some Internet protocols. Services that require the initiation of TCP connections from the outside network, or stateless protocols such as those using UDP, can be disrupted. Unless the NAT router makes a specific effort to support such protocols, incoming packets cannot reach their destination. Some protocols can accommodate one instance of NAT between participating hosts ("passive mode" FTP, for example), sometimes with the assistance of an application-level gateway (see below), but fail when both systems are separated from the Internet by NAT. Use of NAT also complicates tunneling protocols such as IPsec because NAT modifies values in the headers which interfere with the integrity checks done by IPsec and other tunneling protocols.

End-to-end connectivity has been a core principle of the Internet, supported for example by the Internet Architecture Board. Current Internet architectural documents observe that NAT is a violation of the End-to-End Principle, but that NAT does have a valid role in careful design.^[3] There is considerably more concern with the use of IPv6 NAT, and many IPv6 architects believe IPv6 was intended to remove the need for NAT.^[4]

- Scalability - An implementation that only tracks ports can be quickly depleted by internal applications that use multiple simultaneous connections (such as an HTTP request for a web page with many embedded objects). This problem can be mitigated by tracking the destination IP address in addition to the port (thus sharing a single local port with many remote hosts), at the expense of implementation complexity and CPU/memory resources of the translation device.
- Firewall complexity - Because the internal addresses are all disguised behind one publicly accessible address, it is impossible for external hosts to initiate a connection to a particular internal host without special configuration on the firewall to forward connections to a particular port. Applications such as VOIP, videoconferencing, and other peer-to-peer applications must use NAT traversal techniques to function.

IEEE^[5] Reverse Address and Port Translation (RAPT, or RAT) allows a host whose real IP address is changing from time to time to remain reachable as a server via a fixed home IP address. In principle, this should allow setting up servers on DHCP-run networks. While not a perfect mobility solution, RAPT together with upcoming protocols like DHCP-DDNS, it may end up becoming another useful tool in the network admin's arsenal.

Cisco *RAPT* implementation is port address translation (PAT) or NAT overloading, and maps multiple private IP addresses to a single public IP address. Multiple addresses can be mapped to a single address because each private address is tracked by a port number. PAT uses unique source port numbers on the inside global IP address to distinguish between translations. The port numbers are 16-bit integers. The total number of internal addresses that can be translated to one external address could theoretically be as high as 65,536 per IP address. Realistically, the number of ports that can be assigned a single IP address is around 4000. PAT attempts to preserve the original source port. If this source port is already used, PAT assigns the first available port number starting from the beginning of the appropriate port group 0-511, 512-1023, or 1024-65535. When there are no more ports available and there is more than one external IP address configured, PAT moves to the next IP address to try to allocate the original source port again. This process continues until it runs out of available ports and external IP addresses.

Mapping of Address and Port is a Cisco proposal which combines A+P port address translation with tunneling of the IPv4 packets over an ISP provider's internal IPv6 network. In effect, it is an (almost) stateless alternative to Carrier Grade NAT and DS-Lite that pushes the IPv4 IP address/port translation function (and therefore the maintenance of NAT state) entirely into the existing customer premises equipment NAT implementation. Thus avoiding the NAT444 and statefulness problems of Carrier Grade NAT, and also provides a transition mechanism for the deployment of native IPv6 at the same time with very little added complexity.

Methods of translation

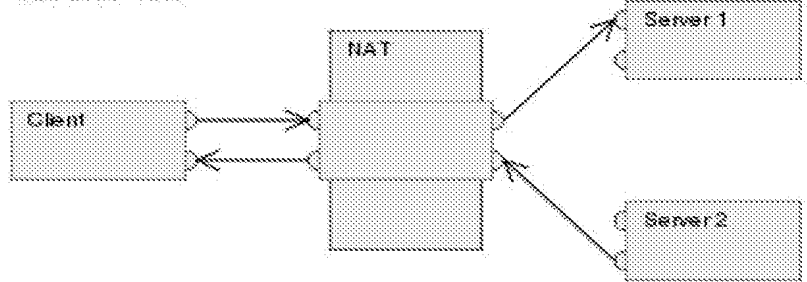
There are several ways of implementing network address and port translation. In some application protocols that use IP address information, the application running on a node in the masqueraded network needs to determine the external address of the NAT, i.e., the address that its communication peers detect, and, furthermore, often needs to examine and categorize the type of mapping in use. Usually this is done because it is desired to set up a direct communications path (either to save the cost of taking the data via a server or to improve performance) between two clients both of which are behind separate NATs.

For this purpose, the Simple traversal of UDP over NATs (STUN) protocol was developed (RFC 3489, March 2003). It classified NAT implementation as *full-cone NAT*, *(address) restricted-cone NAT*, *port-restricted cone NAT* or *symmetric NAT* and proposed a methodology for testing a device accordingly. However, these procedures have since been deprecated from standards status, as the methods are inadequate to correctly assess many devices. New methods have been standardized in RFC 5389 (October 2008) and the STUN acronym now represents the new title of the specification: *Session Traversal Utilities for NAT*.

Full-cone NAT, also known as *one-to-one NAT*

- Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort are sent through eAddr:ePort.
- Any external host can send packets to iAddr:iPort by sending packets to eAddr:ePort.

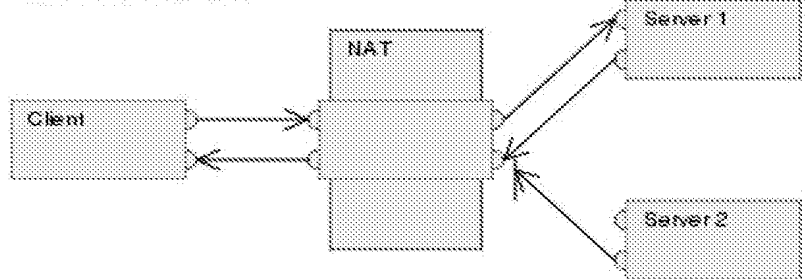
"Full Cone" NAT



(Address)-restricted-cone NAT

- Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort are sent through eAddr:ePort.
- An external host (*hAddr:any*) can send packets to iAddr:iPort by sending packets to eAddr:ePort only if iAddr:iPort has previously sent a packet to hAddr:any. "Any" means the port number doesn't matter.

"Restricted Cone" NAT

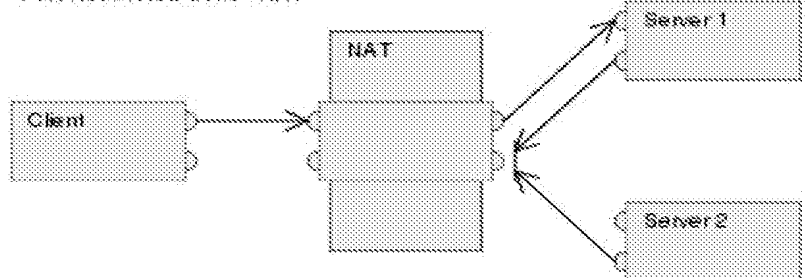


Port-restricted cone NAT

Like an address restricted cone NAT, but the restriction includes port numbers.

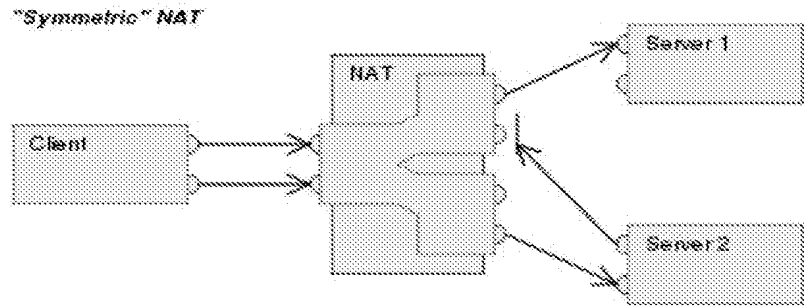
- Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort are sent through eAddr:ePort.
- An external host (*hAddr:hPort*) can send packets to iAddr:iPort by sending packets to eAddr:ePort only if iAddr:iPort has previously sent a packet to hAddr:hPort.

"Port Restricted Cone" NAT



Symmetric NAT

- Each request from the same internal IP address and port to a specific destination IP address and port is mapped to a unique external source IP address and port; if the same internal host sends a packet even with the same source address and port but to a different destination, a different mapping is used.
- Only an external host that receives a packet from an internal host can send a packet back.



This terminology has been the source of much confusion, as it has proven inadequate at describing real-life NAT behavior.^[2] Many NAT implementations combine these types, and it is, therefore, better to refer to specific individual NAT behaviors instead of using the Cone/Symmetric terminology. Especially, most NATs combine *symmetric NAT* for outgoing connections with *static port mapping*, where incoming packets addressed to the external address and port are redirected to a specific internal address and port. Some products can redirect packets to several internal hosts, *e.g.*, to divide the load between a few servers. However, this introduces problems with more sophisticated communications that have many interconnected packets, and thus is rarely used.

Type of NAT and NAT traversal, role of port preservation for TCP

The NAT traversal problem arises when two peers behind distinct NAT try to communicate. One way to solve this problem is to use port forwarding, another way is to use various NAT traversal techniques. The most popular technique for TCP NAT traversal is TCP hole punching, which requires the NAT to follow the *port preservation* design for TCP, as explained below.

Many NAT implementations follow the *port preservation* design for TCP: for a given outgoing TCP communication, they use the same values as internal and external port numbers. NAT *port preservation* for outgoing TCP connections is crucial for TCP NAT traversal, because as TCP requires that one port can only be used for one communication at a time, programs bind distinct TCP sockets to ephemeral ports for each TCP communication, rendering NAT port prediction impossible for TCP.^[2]

On the other hand, for UDP, NATs do not need to have *port preservation*. Indeed, multiple UDP communications (each with a distinct endpoint) can occur on the same source port, and applications usually reuse the same UDP socket to send packets to distinct hosts. This makes port prediction straightforward, as it is the same source port for each packet.

Furthermore, *port preservation* in NAT for TCP allows P2P protocols to offer less complexity and less latency because there is no need to use a third party (like STUN) to discover the NAT port since the application itself already knows the NAT port.^{[2][6]}

However, if two internal hosts attempt to communicate with the same external host using the same port number, the external port number used by the second host is chosen at random. Such NAT is sometimes perceived as (*address*) *restricted cone NAT* and other times as *symmetric NAT*.

Recent studies have shown that roughly 70% of clients in P2P networks employ some form of NAT.^[7]

Implementation

Establishing two-way communication

Every TCP and UDP packet contains a source IP address and source port number as well as a destination IP address and destination port number. The IP address/port number pair forms a socket. In particular, the source IP address and source port number form the source socket.

For publicly accessible services such as web servers and mail servers the port number is important. For example, port 80 connects to the web server software and port 25 to a mail server's SMTP daemon. The IP address of a public server is also important, similar in global uniqueness to a postal address or telephone number. Both IP address and port number must be correctly known by all hosts wishing to successfully communicate.

Private IP addresses as described in RFC 1918 are significant only on private networks where they are used, which is also true for host ports. Ports are unique endpoints of communication on a host, so a connection through the NAT device is maintained by the combined mapping of port and IP address.

PAT (Port Address Translation) resolves conflicts that would arise through two different hosts using the same source port number to establish unique connections at the same time.

Telephone number extension analogy

A NAT device is similar to a phone system at an office that has one public telephone number and multiple extensions. Outbound phone calls made from the office all appear to come from the same telephone number. However, an incoming call that does not specify an extension cannot be transferred to an individual inside the office. In this scenario, the office is a private LAN, the main phone number is the public IP address, and the individual extensions are unique port numbers.^[8]

Translation of the endpoint

With NAT, all communications sent to external hosts actually contain the *external* IP address and port information of the NAT device instead of internal host IP addresses or port numbers.

- When a computer on the private (internal) network sends an IPv4 packet to the external network, the NAT device replaces the internal IP address in the source field of the packet header (*sender's address*) with the external IP address of the NAT device. PAT may then assign the connection a port number from a pool of available ports, inserting this port number in the source port field (much like the *post office box number*), and forwards the packet to the external network. The NAT device then makes an entry in a translation table containing the internal IP address, original source port, and the translated source port. Subsequent packets from the same connection are translated to the same port number.
- The computer receiving a packet that has undergone NAT establishes a connection to the port and IP address specified in the altered packet, oblivious to the fact that the supplied address is being translated (analogous to using a *post office box number*).

- A packet coming from the external network is mapped to a corresponding internal IP address and port number from the translation table, replacing the external IP address and port number in the incoming packet header (similar to the translation from *post office box number* to *street address*). The packet is then forwarded over the inside network. Otherwise, if the destination port number of the incoming packet is not found in the translation table, the packet is dropped or rejected because the PAT device doesn't know where to send it.

NAT only translates IP addresses and ports of its internal hosts, hiding the true endpoint of an internal host on a private network.

Visibility of operation

NAT operation is typically transparent to both the internal and external hosts.

Typically the internal host is aware of the true IP address and TCP or UDP port of the external host. Typically the NAT device may function as the default gateway for the internal host. However the external host is only aware of the public IP address for the NAT device and the particular port being used to communicate on behalf of a specific internal host.

NAT and TCP/UDP

"Pure NAT", operating on IP alone, may or may not correctly parse protocols that are totally concerned with IP information, such as ICMP, depending on whether the payload is interpreted by a host on the "inside" or "outside" of translation. As soon as the protocol stack is traversed, even with such basic protocols as TCP and UDP, the protocols will break unless NAT takes action beyond the network layer.

IP packets have a checksum in each packet header, which provides error detection only for the header. IP datagrams may become fragmented and it is necessary for a NAT to reassemble these fragments to allow correct recalculation of higher-level checksums and correct tracking of which packets belong to which connection.

The major transport layer protocols, TCP and UDP, have a checksum that covers all the data they carry, as well as the TCP/UDP header, plus a "pseudo-header" that contains the source and destination IP addresses of the packet carrying the TCP/UDP header. For an originating NAT to pass TCP or UDP successfully, it must recompute the TCP/UDP header checksum based on the translated IP addresses, not the original ones, and put that checksum into the TCP/UDP header of the first packet of the fragmented set of packets. The receiving NAT must recompute the IP checksum on every packet it passes to the destination host, and also recognize and recompute the TCP/UDP header using the retranslated addresses and pseudo-header. This is not a completely solved problem. One solution is for the receiving NAT to reassemble the entire segment and then recompute a checksum calculated across all packets.

The originating host may perform Maximum transmission unit (MTU) path discovery to determine the packet size that can be transmitted without fragmentation, and then set the *don't fragment* (DF) bit in the appropriate packet header field. Of course, this is only a one-way solution, because the responding host can send packets of any size, which may be fragmented before reaching the NAT.

DNAT

Destination network address translation (DNAT) is a technique for transparently changing the destination IP address of an end route packet and performing the inverse function for any replies. Any router situated between two endpoints can perform this transformation of the packet.

DNAT is commonly used to publish a service located in a private network on a publicly accessible IP address. This use of DNAT is also called port forwarding, or DMZ when used on an entire server, which becomes exposed to the WAN, becoming analogous to an undefended military demilitarised zone (DMZ).

SNAT

The meaning of the term *SNAT* varies by vendor. Many vendors have proprietary definitions for *SNAT*:

- *source NAT* is the common expansion, as the counterpart of *destination NAT* (DNAT)
- *stateful NAT* is used by Cisco Systems
- *static NAT* is used by WatchGuard
- *secure NAT* is used by F5 Networks and by Microsoft (in regard to the ISA Server)

Microsoft's Secure network address translation (SNAT) is part of Microsoft's Internet Security and Acceleration Server and is an extension to the NAT driver built into Microsoft Windows Server. It provides connection tracking and filtering for the additional network connections needed for the FTP, ICMP, H.323, and PPTP protocols as well as the ability to configure a transparent HTTP proxy server.

Dynamic network address translation

Dynamic NAT, just like static NAT, is not common in smaller networks but is found within larger corporations with complex networks. The way dynamic NAT differs from static NAT is that where static NAT provides a one-to-one internal to public static IP address mapping, dynamic NAT doesn't make the mapping to the public IP address static and usually uses a group of available public IP addresses.

NAT loopback

NAT loopback, also known as *NAT hairpinning* or *NAT reflection*,^[9] is a feature in many consumer routers^[10] which permits the access of a service via the public IP address from inside the local network. This eliminates the need for using separate domain name resolution for hosts inside the network than for the public network for a website, for example.

The following describes an example network:

- Public address: 203.0.113.1. This is the address of the WAN interface on the router.
- Internal address of router: 192.168.1.1
- Address of the server: 192.168.1.2
- Address of a local computer: 192.168.1.100

If a packet is sent to the public address by a computer at 192.168.1.100, the packet would normally be routed to the default gateway (the router), unless an explicit route is set in the computer's routing tables. A router with the NAT loopback feature detects that 203.0.113.1 is the address of its WAN interface, and treats the packet as if coming from that interface. It determines the destination for that packet, based on DNAT (port forwarding) rules for the destination. If the data were sent to port 80 and a DNAT rule exists for port 80 directed to 192.168.1.2, then the host at that address receives the packet.

If no applicable DNAT rule is available, the router drops the packet. An ICMP Destination Unreachable reply may be sent. If any DNAT rules were present, address translation is still in effect; the router still rewrites the source IP address in the packet. The local computer (192.168.1.100) sends the packet as

coming from 192.168.1.100, but the server (192.168.1.2) receives it as coming from 203.0.113.1. When the server replies, the process is identical as for an external sender. Thus, two-way communication is possible between hosts inside the LAN network via the public IP address.

NAT in IPv6

Network address translation is not commonly used in IPv6, because one of the design goals of IPv6 is to restore end-to-end network connectivity.^[11] NAT loopback is not commonly needed. Although still possible, the large addressing space of IPv6 obviates the need to conserve addresses and every device can be given a unique globally routable address. That being said, using unique local addresses in combination with network prefix translation can achieve similar results.

Applications affected by NAT

Some Application Layer protocols (such as FTP and SIP) send explicit network addresses within their application data. FTP in active mode, for example, uses separate connections for control traffic (commands) and for data traffic (file contents). When requesting a file transfer, the host making the request identifies the corresponding data connection by its network layer and transport layer addresses. If the host making the request lies behind a simple NAT firewall, the translation of the IP address and/or TCP port number makes the information received by the server invalid. The Session Initiation Protocol (SIP) controls many Voice over IP (VoIP) calls, and suffers the same problem. SIP and SDP may use multiple ports to set up a connection and transmit voice stream via RTP. IP addresses and port numbers are encoded in the payload data and must be known prior to the traversal of NATs. Without special techniques, such as STUN, NAT behavior is unpredictable and communications may fail.

Application Layer Gateway (ALG) software or hardware may correct these problems. An ALG software module running on a NAT firewall device updates any payload data made invalid by address translation. ALGs obviously need to understand the higher-layer protocol that they need to fix, and so each protocol with this problem requires a separate ALG. For example, on many Linux systems, there are kernel modules called *connection trackers* which serve to implement ALGs. However, ALG does not work if the control channel is encrypted (e.g. FTPS).

Another possible solution to this problem is to use NAT traversal techniques using protocols such as STUN or ICE, or proprietary approaches in a session border controller. NAT traversal is possible in both TCP- and UDP-based applications, but the UDP-based technique is simpler, more widely understood, and more compatible with legacy NATs. In either case, the high level protocol must be designed with NAT traversal in mind, and it does not work reliably across symmetric NATs or other poorly behaved legacy NATs.

Other possibilities are UPnP Internet Gateway Device Protocol, NAT-PMP (NAT Port Mapping Protocol), or Port Control Protocol (PCP),^[12] but these require the NAT device to implement that protocol.

Most traditional client-server protocols (FTP being the main exception), however, do not send layer 3 contact information and therefore do not require any special treatment by NATs. In fact, avoiding NAT complications is practically a requirement when designing new higher-layer protocols today (e.g. the use of SFTP instead of FTP).

NATs can also cause problems where IPsec encryption is applied and in cases where multiple devices such as SIP phones are located behind a NAT. Phones which encrypt their signaling with IPsec encapsulate the port information within an encrypted packet, meaning that NA(P)T devices cannot access and translate the port. In these cases the NA(P)T devices revert to simple NAT operation. This means that all traffic returning to the NAT is mapped onto one client causing service to more than one client "behind" the NAT to fail. There are a couple of solutions to this problem: one is to use TLS, which operates at level 4 in the OSI Reference Model and therefore does not mask the port number; another is to encapsulate the IPsec within UDP - the latter being the solution chosen by TISPAN to achieve secure NAT traversal, or a NAT with "IPsec Passthru" support.

Interactive Connectivity Establishment is a NAT traversal technique which does not rely on ALG support.

The DNS protocol vulnerability announced by Dan Kaminsky on July 8, 2008 is indirectly affected by NAT port mapping. To avoid DNS server cache poisoning, it is highly desirable not to translate UDP source port numbers of outgoing DNS requests from a DNS server which is behind a firewall that implements NAT. The recommended work-around for the DNS vulnerability is to make all caching DNS servers use randomized UDP source ports. If the NAT function de-randomizes the UDP source ports, the DNS server becomes vulnerable.

Examples of NAT software

- Internet Connection Sharing (ICS): NAT & DHCP implementation included with Windows desktop operating systems
- IPFilter: included with (Open)Solaris, FreeBSD and NetBSD, available for many other Unix-like operating systems
- ipfirewall (ipfw): FreeBSD-native packet filter
- Netfilter with iptables/nftables: the Linux packet filter
- NPF: NetBSD-native Packet Filter
- PF: OpenBSD-native Packet Filter
- Routing and Remote Access Service: routing implementation included with Windows Server operating systems
- WinGate: third-party routing implementation for Windows

See also

- Anything In Anything (AYIYA) — IPv6 over IPv4 UDP, thus working IPv6 tunneling over most NATs
- Gateway (telecommunications)
- Internet Gateway Device Protocol (IGD) — UPnP NAT-traversal method
- Middlebox
- Port triggering
- Hairpinning
- Subnetwork
- Port (computer networking)
- Teredo tunneling — NAT traversal using IPv6

References

1. *Network Protocols Handbook* (2 ed.). Javvin Technologies Inc. 2005. p. 27. ISBN 9780974094526. Retrieved

2014-09-16.

2. François Audet; and Cullen Jennings (January 2007). "RFC 4787 Network Address Translation (NAT) Behavioral Requirements for Unicast UDP" (text). IETF. Retrieved 2007-08-29.
3. R. Bush; and D. Meyer; RFC 3439, *Some Internet Architectural Guidelines and Philosophy* (<http://www.ietf.org/rfc/rfc3439.txt>), December 2002
4. G. Van de Velde *et al.*; RFC 4864, *Local Network Protection for IPv6* (<http://tools.ietf.org/rfc/rfc4864.txt>), May 2007
5. ieeexplore.ieee.org (<http://ieeexplore.ieee.org/iel4/6056/16183/00749275.pdf>)
6. "Characterization and Measurement of TCP Traversal through NATs and Firewalls". December 2006.
7. "Illuminating the shadows: Opportunistic network and web measurement". December 2006.
8. "The Audio over IP Instant Expert Guide" (PDF). Tieline. January 2010. Retrieved 2011-08-19.
9. superuser.com (<http://superuser.com/a/362901/121343>)
10. "NAT Loopback Routers - OpenSim". [Opensimulator.org](http://opensimulator.org). 2013-10-21. Retrieved 2014-02-21.
11. Iljitsch van Beijnum (2008-07-23). "After staunch resistance, NAT may come to IPv6 after all". *Ars Technica*. Retrieved 2014-04-24.
12. RFC 6887, *Port Control Protocol (PCP)*, Wing, Cheshire, Boucadair, Penno & Selkirk (April 2013)

External links

- NAT-Traversal Test and results (<http://nattest.net.in.tum.de>)
- Characterization of different TCP NATs (<http://nutss.net/pub/imc05-tcpnat/>) – Paper discussing the different types of NAT
- Anatomy: A Look Inside Network Address Translators – Volume 7, Issue 3, September 2004 (http://www.cisco.com/en/US/about/ac123/ac147/archived_issues/ipj_7-3/anatomy.html)
- Jeff Tyson, HowStuffWorks: *How Network Address Translation Works* (<http://computer.howstuffworks.com/nat.htm/printable>)
- Routing with NAT (<http://publib.boulder.ibm.com/infocenter/iseriess/v5r3/index.jsp?topic=/rzajw/rzajwstatic.htm>) (Part of the documentation for the IBM iSeries)
- Network Address Translation (NAT) FAQ (<http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html>) – Cisco Systems

Retrieved from "https://en.wikipedia.org/w/index.php?title=Network_address_translation&oldid=745485744"

Categories: Network address translation | Internet architecture

-
- This page was last modified on 21 October 2016, at 11:46.
 - Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Security-focused operating system

From Wikipedia, the free encyclopedia

This is a list of operating systems with a sharp security focus. Here, "security-focused" means that the project is devoted to increasing the security as a major goal. As such, something may be secure without being "security-focused." For example, almost all of the operating systems mentioned here are faced with security bug fixes in their lifetime; however, they all strive consistently to approach all generic security flaws inherent in their design with new ideas in an attempt to create a secure computing environment. Security-focused does not mean security-evaluated operating system, which refers to operating systems that have achieved certification from an external security-auditing organization. An operating system that provides sufficient support for multilevel security and evidence of correctness to meet a particular set of government requirements is called a "trusted operating system".

The list is alphabetical and does not imply a ranking.

Contents

- 1 BSD
 - 1.1 Anonym.OS
 - 1.2 OpenBSD
 - 1.3 TrustedBSD
 - 1.4 HardenedBSD
- 2 Linux
 - 2.1 Alpine Linux
 - 2.2 Annvix
 - 2.3 BlackArch Linux
 - 2.4 CopperheadOS
 - 2.5 Debian
 - 2.6 EnGarde Secure Linux
 - 2.7 Fedora
 - 2.8 Hardened Gentoo
 - 2.9 Hardened Linux
 - 2.10 Immunix
 - 2.11 Kali Linux
 - 2.12 Mempo
 - 2.13 Openwall Project
 - 2.14 Parrot Security OS
 - 2.15 Pentoo Project
 - 2.16 Qubes OS
 - 2.17 Replicant
 - 2.18 Red Hat Enterprise Linux
 - 2.19 Subgraph OS
 - 2.20 Tails (The Amnesic Incognito Live System)
 - 2.21 Tin Hat
 - 2.22 Ubuntu Privacy Remix
 - 2.23 Whonix (anonymous operating system)
 - 2.24 IprediaOS
 - 2.25 Liberté Linux
 - 2.26 Security Onion
- 3 Solaris

- 3.1 Trusted Solaris
- 3.2 Solaris 10 and trusted functionality
- 4 Object-capability systems
- 5 See also
- 6 References
- 7 External links

BSD

BSD is a family of Unix variants derived from a code base originating at the University of California, Berkeley. All derived BSD operating systems are released under the terms of a BSD-style license. There are several BSD variants, with only one being heavily focused on security.

Anonym.OS

Anonym.OS was a Live CD operating system based on OpenBSD 3.8 with strong encryption and anonymization tools. The goal of the project was to provide secure, anonymous web browsing access to everyday users.^[1] The project was discontinued after the release of Beta 4 (2006).

OpenBSD

OpenBSD is an open source BSD operating system that is known to be concerned heavily with security. The project has completed rigorous manual reviews of the code and addressed issues most systems have not.^[2] OpenBSD also supplies an executable space protection scheme known as W^X (memory is writeable xor executable), as well as a ProPolice compiled executable base. OpenBSD became the first mainstream operating system to support partial ASLR and to activate it by default, ASLR support was completed in 2008 when it added support for position-independent executable (PIE) binaries.

TrustedBSD

TrustedBSD is a sub-project of FreeBSD designed to add trusted operating system extensions, targeting the Common Criteria for Information Technology Security Evaluation (see also Orange Book). Its main focuses are working on access control lists, event auditing, extended attributes, mandatory access controls, and fine-grained capabilities. Since access control lists are known to be confronted with the confused deputy problem, capabilities are a different way to avoid this issue. As part of the TrustedBSD project, there is also a port of NSA's FLASK/TE implementation to run on FreeBSD. Many of these trusted extensions have been integrated into the main FreeBSD branch starting at 5.x.

HardenedBSD

HardenedBSD is a forked project from FreeBSD,^[3] that brings low level security enhancements to the FreeBSD project, by aiming "to continuously implement kernel and userland hardening features, such as Address Space Layout Randomization (ASLR), mprotect hardening, Position Independent Executable (PIE) support, and PTrace hardening, among other features."^{[4][5]} Together with TrustedBSD, the HardenedBSD project resembles Trusted Solaris, a precursor that provided further security enhancements to the Solaris operating system. These early enhancements found their way into security features across a number of different operating systems, mostly Unix-like ones.

Linux

The Linux kernel provides among other security features, the Linux Security Module (LSM), officially integrated with the mainline Linux kernel since 2003. However, there have been specialized distributions and projects that attempt to make Linux more secure in general or for particular scenarios.

Alpine Linux

Alpine Linux is a lightweight musl and BusyBox-based distribution. It uses PaX and grsecurity patches in the default kernel and compiles all packages with stack-smashing protection. Version 3.0 was released June 4, 2014.

Annvix

Annvix originally was forked from Mandriva to provide a security-focused server distribution that employs ProPolice protection, hardened configuration, and a small footprint. There were plans to include full support for the RSBAC mandatory access control system. However, Annvix is dormant, with the last version being released on December 30, 2007.

BlackArch Linux

BlackArch is a distribution in its own right, or you can add its Arch Linux *unofficial* repo to an existing installation. BlackArch is oriented around penetration testing and security research. It offers over 1350 tools organized by category, for security and forensic specialists. It has the live-DVD feature and several lightweight window managers.^[6]

CopperheadOS

CopperheadOS is a hardened free and open-source operating system based on the Android mobile platform, which uses an unofficial port of PaX.^{[7][8][9]}

Debian

The "Securing Debian Manual"^[10] contains information for Debian administrators. Debian includes support for SELinux^[11] since version 5.0, as well as AppArmor and Tomoyo. See also Debian Security information and policy.

EnGarde Secure Linux

EnGarde Secure Linux is a secure platform designed for servers. It has had a browser-based tool for MAC using SELinux since 2003. Additionally, it can be accompanied with Web, DNS, and email enterprise applications, specifically focusing on security without any unnecessary software. The community platform of EnGarde Secure Linux is the bleeding-edge version freely available for download.

Fedora

Fedora is a free, Red Hat-sponsored community-developed Linux distribution. Fedora is a mainstream distribution that makes significant efforts to improve security.^[12] As a consequence, it has a fully integrated SELinux MAC and fine-grained executable memory permission system (Exec Shield) and all binaries compiled with GCC's standard stack-smashing protection, as well as focusing on getting security updates into the system in a timely manner.

Hardened Gentoo

Hardened Gentoo is a sub-project of the Gentoo Linux project. Hardened Gentoo offers a ProPolice protected and position-independent executable base using exactly the same package tree as Gentoo. Executable space protection in Hardened Gentoo is handled by PaX. The Hardened Gentoo project is an extremely modular project, and also provides subprojects to integrate other intrusion-detection and mandatory access control systems into Gentoo. All of these can be optionally installed in any combination, with or without PaX and a ProPolice base.

Hardened Linux

Hardened Linux is a small distribution for firewalls, intrusion detection systems, VPN-gateways and authentication jobs that is still under heavy development. It includes grsecurity, PaX, and GCC stack smashing protection.

Immunix

Immunix was a commercial distribution of Linux focused heavily on security. They supplied many systems of their own making, including StackGuard; cryptographic signing of executables; race condition patches; and format string exploit guarding code. Immunix traditionally releases older versions of their distribution free for non-commercial use. The Immunix distribution itself is licensed under two licenses: The Immunix commercial and non-commercial licenses. Many tools within are GPL, however; as is the kernel.

Kali Linux

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing, formerly known as Backtrack.

Mempo

Mempo^[13] is a privacy-focused derivative of Debian and aims to provide the "most secure and yet comfortable out-of-the-box Desktop and Server" operating system. Among others, Mempo also relies on the Freenet and Tor.

Openwall Project

Solar Designer's Openwall Project (Owl) was the first distribution to have a non-executable userspace stack, /tmp race condition protection, and access control restrictions to /proc data, by way of a kernel patch. It also features a per-user tmp directory via the pam_mktemp PAM module, and supports Blowfish password encryption.

Parrot Security OS

Parrot Security OS is a Cloud oriented GNU/Linux distribution based on Debian and designed to perform security and penetration tests, do forensic analysis, or act in anonymity. It uses the MATE Desktop Environment, Linux Kernel 4.6 or higher and it is available as a live lightweight installable ISO image for 32-bit, 64-bit and ARM processors with forensic options at boot, optimizations for programmers, and new custom pentesting tools.

Pentoo Project

Pentoo Penetration Testing Overlay and Livecd is a live CD and Live USB designed for penetration testing and security assessment. Based on Gentoo Linux, Pentoo is provided both as 32-bit and 64-bit installable live cd. Pentoo also is available as an overlay for an existing Gentoo installation. It features packet injection patched wifi drivers, GPGPU cracking software, and lots of tools for penetration testing and security assessment. The Pentoo kernel includes grsecurity and PAX hardening and extra patches – with binaries compiled from a hardened toolchain with the latest nightly versions of some tools available.

Qubes OS

Qubes OS is a Linux distribution based around the Xen hypervisor that allows to group programs into a number of isolated sandboxes (virtual machines) to provide security. Windows for programs running within these sandboxes ("security domains") can be color coded for easy recognition. The security domains are configurable, they can be transient (changes to the file system will not be preserved), and their network connection can be routed through special virtual machines (for example one that only provides Tor networking). The operating system provides secure mechanisms for copy and paste and for copying files between the security domains.^[14]

Replicant

Replicant is a free and open-source operating system based on the Android mobile platform, which aims to replace all proprietary Android components with their free software counterparts. It is available for several smartphones and tablet computers.^{[15][16][17][18]}

In March 2014, the Replicant project announced the discovery of a backdoor present in a wide range of Samsung Galaxy products that allows the baseband processor to read and write the device's storage,^{[19][20]} sometimes with normal user privileges and sometimes as the root user, depending on device model.^[21] It is unknown whether Samsung's proprietary firmware for the radio chip can be remotely instructed to use these access features and, whether the vulnerability was introduced with legitimate uses in mind.

Red Hat Enterprise Linux

Red Hat Enterprise Linux offers the same security benefits as Fedora with the additional support of back-porting security fixes to the released versions of the packages (particularly the kernel) so the sys-admin does not have to perform a significant (and risky) upgrade to get a security fix.

Subgraph OS

Subgraph OS is a Linux-based operating system designed to be resistant to surveillance and interference by sophisticated adversaries over the Internet. Subgraph OS is designed with features which aim to reduce the attack surface of the operating system, and increase the difficulty required to carry out certain

classes of attack. This is accomplished through system hardening and a proactive, ongoing focus on security and attack resistance. Subgraph OS also places emphasis on ensuring the integrity of installed software packages through deterministic compilation.

Subgraph OS features a kernel hardened with the Grsecurity and PaX patchset, Linux namespaces, and Xpra for application containment, mandatory file system encryption using LUKS, resistance to cold boot attacks, and is configured by default to isolate network communications for installed applications to independent circuits on the Tor anonymity network.

Tails (The Amnesic Incognito Live System)

Tails or The Amnesic Incognito Live System is a Linux distribution aimed at preserving privacy and anonymity. It is the next iteration of development on the Incognito Linux distribution. It is based on Debian, with all outgoing connections forced to go through Tor and optionally I2P. Direct (non-anonymous) connections are blocked. The system is designed to be booted as a live CD or USB and no trace (digital footprint) is left on local storage unless explicitly told to. The Tor Project has provided most of the financial support for development.

Tin Hat

Tin Hat Linux is derived from Hardened Gentoo Linux. It aims to provide a very secure, stable, and fast desktop environment that lives purely in RAM.

Ubuntu Privacy Remix

Ubuntu Privacy Remix is a distribution based on Ubuntu, focused on security.^[22]

Whonix (anonymous operating system)

Whonix is an anonymous general-purpose operating system based on VirtualBox, Debian GNU/Linux, Tor, and optionally I2P. By Whonix design, IP, and DNS leaks are impossible. Not even malware as superuser can find out the user's real IP address or location, because Whonix consists of two (virtual) machines. One machine solely runs Tor and acts as a gateway, called Whonix-Gateway. The other machine, called Whonix-Workstation, is on a completely isolated network. Only connections through Tor are possible.

IprediaOS

IprediaOS is an operating system in which all connections go through I2P.^[23] This system is notable for its use of anonymous bittorrent download,^[24] but it is known as using out-of date I2P version, so users focusing on security must update I2P before use.^[25]

Liberté Linux

Liberté Linux is a secure, reliable, lightweight and easy to use Gentoo-based LiveUSB/SD/CD Linux distribution with the primary purpose of enabling anyone to communicate safely and covertly in hostile environments. The last official release was in 2012, and seems to have been abandoned at this point.^[26]

Security Onion

Security Onion is an Ubuntu-based distribution for intrusion detection and network security monitoring. It contains tools such as Snort, Suricata, Sguil, Bro, and Xplico. ^{[27][28][29]}

Solaris

Solaris is a Unix variant created by Sun Microsystems. Solaris itself is not inherently security-focused. The major portion of the Solaris source code has been released via the OpenSolaris project, mostly under the Common Development and Distribution License. Enhancements to OpenSolaris, both security related and others, are backported to the official Solaris when Sun certifies their quality.

Trusted Solaris

Trusted Solaris is a security-focused version of the Solaris Unix operating system. Aimed primarily at the government computing sector, Trusted Solaris adds detailed auditing of all tasks, pluggable authentication, mandatory access control, additional physical authentication devices, and fine-grained access control. Trusted Solaris is Common Criteria certified. (See [1] (<https://web.archive.org/web/20041013000439/http://www.sun.com/software/security/securitycert/trustedsolaris.html>) and [2] (https://web.archive.org/web/20070312070621/http://www.sun.com/software/security/securitycert/images/TSol8_7-03CMS.jpg)) The most recent version, Trusted Solaris 8 (released 2000), received the EAL4 certification level augmented by a number of protection profiles. Telnet was vulnerable to buffer overflow exploits until patched in April 2001.^[30]

Solaris 10 and trusted functionality

Trusted Solaris functionality has now been added to the mainstream version of Solaris. In the 11/06 update to Solaris 10, the *Solaris Trusted Extensions* feature adds mandatory access control and labelled security. Introduced in the same update, the *Secure by Default Networking* feature implements less services on by default compared to most previous releases that had most services enabled. RBAC, found in both mainstream Solaris and Trusted Solaris, dramatically lessens the need for using root directly by providing a way for fine grained control over various administrative tasks.

Object-capability systems

These operating systems are all engineered around a different paradigm of security, object-capabilities, where instead of having the system deciding if an access request should be granted (usually through one or several access control lists), the bundling of authority and designation makes it impossible to request anything not legitimate.

- CapROS
- EROS
- Fiasco.OC
- KeyKOS
- seL4

See also

- Capabilities and access control lists
- Comparison of operating systems
- Damn Vulnerable Linux
- IX (operating system)
- OpenBSM
- Operating system (section Security)
- Security engineering
- Security-evaluated operating system
- Trusted operating system

References

1. Quinn Norton (January 14, 2006). "Anonyity on a Disc". Wired.com. Retrieved November 6, 2011.
2. McIntire, Tim (8 August 2006). "Take a closer look at OpenBSD". IBM. Archived from the original on January 27, 2007. Retrieved 19 February 2015.
3. "HardenedBSD – Proactive Security Project". *bsdmag.org*. HAKIN9 MEDIA SP. Z O.O. SP. K. Retrieved 12 June 2015.
4. Carlier, David (December 4, 2014). "Hardened BSD - A Proactive Security Project". *BSD Magazine*. HAKIN9 MEDIA SP. Z O.O. SP. K. **8** (10/2014 (63)). ISSN 1898-9144. Retrieved 12 June 2015.
5. Percival, Colin, Fabian Keil, delphij, mahrens, et. al. (12 June 2015). "HardenedBSD — sys/dev/xen/blkback blkback.c, sys/dev/xen/blkfront blkfront.c block.h" (4443). secure.freshbsd.org. Retrieved 12 June 2015.
6. "BlackArch Linux". Retrieved 5 Feb 2016.
7. Porup, J.M. (9 August 2016). "Copperhead OS: The startup that wants to solve Android's woeful security". *arstechnica.co.uk*. Ars Technica UK.
8. Corbet, Jonathan (17 February 2016). "CopperheadOS: Securing the Android". *lwn.net*.
9. Linder, Brad (29 March 2016). "F-Droid, Copperhead, Guardian Project partner to create a security-focused, Android-based ecosystem". *liliputing.com*.
10. "Securing Debian Manual". *debian.org*. Retrieved 19 April 2015.
11. "SELinux". *debian.org*. Retrieved 19 April 2015.
12. "SELinux: бронезилет для корпоративного пингвина" [SELinux: bullet-proof vest for corporate penguin] (in Russian). 6 September 2011. Retrieved 26 October 2011.
13. Mempo (<https://rawgit.com/mempo/mempo-websites/master/mempo-main/html/index.html>)
14. "Redirecting...". *qubes-os.org*. Retrieved 19 April 2015.
15. "Overview - Replicant". Redmine.replicant.us. Retrieved 2013-09-30.
16. Paul Kocialkowski (February 4, 2012). "WikiStart – Replicant". Redmine.replicant.us. Retrieved 2013-09-30.
17. "Android and Users' Freedom - GNU Project - Free Software Foundation". Gnu.org. Retrieved 2013-09-30.
18. "About". Replicant project. Retrieved 2013-09-30.
19. Don Reisinger (13 March 2014). "Samsung Galaxy devices may have backdoor to user data, developer says". CNET. Retrieved 25 April 2014.
20. Michael Larabel (12 March 2014). "Replicant Developers Find Backdoor In Android Samsung Galaxy Devices". *Phoronix*. Retrieved 25 April 2014.
21. Paul Kocialkowski. "Samsung Galaxy Back-door". *Replicant Wiki*. Archived from the original on 6 April 2014. Retrieved 25 April 2014.
22. Grey One. "Linux Distributions Built For Anonymity". *GreyCoder*. Retrieved 19 April 2015.
23. "Ipredia". *ipredia.org*. Retrieved 19 April 2015.
24. "IprediaOS". *ipredia.org/os*. Retrieved 19 May 2015.
25. "IprediaI2P-out-of-date". reddit.com/r/i2p/comments/2hcbhl/anyone_else_here_use_iprediaos/. Retrieved 19 May 2015.
26. "DE(E)SU - Liberté Linux". *dee.su*. Retrieved 19 April 2015.
27. Security Onion (<https://securityonion.net/>) (official website).
28. Security Onion Wiki (<http://sourceforge.net/p/security-onion/wiki/Home/>) (on SourceForge).
29. Security Onion Solutions: Tools (<https://github.com/Security-Onion-Solutions/security-onion/wiki/Tools>) (on GitHub).
30. "Sun Patch: Trusted Solaris 8 4/01: in.telnet patch". 4 October 2002. Retrieved 13 August 2012. "4734086 in.telnetd vulnerable to buffer overflow ?? (Solaris bug 4483514)"

External links

- AIX (<http://www-03.ibm.com/systems/power/software/aix/>)
- OpenBSD (<http://www.openbsd.org>)
- Hardened Linux (<http://hardenedlinux.sourceforge.net/>)
- Qubes (<http://qubes-os.org/Architecture.html>)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Security-

focused_operating_system&oldid=742900056"

Categories: [Operating system security](#) [Operating system technology](#) [Security](#)

- This page was last modified on 6 October 2016, at 14:26.
- Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Virtual desktop

From Wikipedia, the free encyclopedia

In computing, a **virtual desktop** is a term used with respect to user interfaces, usually within the WIMP paradigm, to describe ways in which the virtual space of a computer's desktop environment is expanded beyond the physical limits of the screen's display area through the use of software. This compensates for a limited desktop area and can also be helpful in reducing clutter. There are two major approaches to expanding the virtual area of the screen. Switchable virtual desktops allow the user to make virtual copies of their desktop view-port and switch between them, with open windows existing on single virtual desktops. Another approach is to expand the size of a single virtual screen beyond the size of the physical viewing device. Typically, scrolling/panning a subsection of the virtual desktop into view is used to navigate an oversized virtual desktop.

Contents

- 1 Overview
 - 1.1 Switching desktops
 - 1.2 Oversized Desktops
- 2 Implementation
 - 2.1 Amiga
 - 2.2 X Window System (Unix and Unix-like)
 - 2.3 OS/2
 - 2.4 Windows
 - 2.5 Mac OS
 - 2.6 BeOS
- 3 References
- 4 External links

Overview

Switching desktops

Switchable desktops were designed and implemented at Xerox PARC as "Rooms" by Austin Henderson and Stuart Card in 1986^[1] and (unknowingly to the authors until their publication) was conceptually similar to earlier work by Patrick Peter Chan in 1984. This work was covered by a US patent.^[2]

Switchable desktops were introduced to a much larger audience by Tom LaStrange in swm (the Solbourne Window Manager, for the X Window System) in 1989. ("Virtual Desktop" was originally a trademark of Solbourne Computer.)^[3] Rather than simply being placed at an x, y position on the computer's display, windows of running applications are then placed at x, y positions on a given virtual desktop "context". They are then only accessible to the user if that particular context is enabled. A



Virtual desktops rendered as the faces of a cube.

In this example a Unix-like operating system is using the X windowing system and the Compiz cube plugin to decorate the KDE desktop environment.

switching desktop provides a pager for the user to switch between "contexts", or pages of screen space, only one of which can be displayed on the computer's display at any given time. Several X window managers provide switching desktops.

Oversized Desktops

Other kinds of virtual desktop environments do not offer discrete virtual screens, but instead make it possible to pan around a desktop that is larger than the available hardware is capable of displaying. This facility is sometimes referred to as panning, scrolling desktops or view-port. For example, if a graphics card has a maximum resolution that is higher than the monitor's display resolution, the virtual desktop manager may allow windows to be placed "off the edge" of the screen. The user can then scroll to them by moving the mouse pointer to the edge of the display. The visible part of the larger virtual screen is called a viewport.

Implementation

Virtual desktop managers are available for most graphical user interface operating systems and offer various features, such as placing different wallpapers for each virtual desktop and use of hotkeys or other convenient methods to allow the user to switch amongst the different screens.

Amiga

The first platform to implement multiple desktop display as a hardware feature was Amiga 1000, released in 1985. The Amiga moved on to succeed in the consumer and video production market. All Amigas supported multiple in-memory screens displayed concurrently via the use of the graphics co-processor, AKA the "Copper". The Copper was a simple processor that could wait for a screen position and write to hardware registers. Using the GUI implemented in system ROM API's, programs could transparently display multiple independent screens, from non-consecutive memory, without moving the memory. This hardware-based scrolling does not use blitting, but something more like what is sometimes called hardware panning. The video output is simply told (once, or many times) where to display (scanline) and from what screen memory address. A screen can move to any position, or display any portion, by modifying the wait, or fetch position. Typically a single byte value. The Copperlist did need to be sorted in vertical and horizontal wait position in order to function. Note: See <http://www.faqs.org/faqs/amiga/books/> for a list of reference material.

Each desktop or 'screen' could have its own colour depth (number of available colours) and resolution, including use of interlacing. The display chipset ('graphics card' on a PC) could switch between these desktop modes on the fly, and during the drawing of a single screen, usually with three pixel deep line between each desktop shown on the screen. However, if one interlaced (flickering) desktop was displayed, all desktops onscreen would be similarly affected.

This also allowed the OS to seamlessly mix "Full Screen" and Windowed "desktop"-style applications in a single environment.

Some programs, VWorlds (an astronomy simulator) being an example, used the multiple desktops feature to overlay a set of controls over the main display screen. The controls could then be dragged up and down in order to show more or less of the main display.

X Window System (Unix and Unix-like)

Almost all Unix and Unix-like systems use the X Window System to provide their windowing environment.

The X Window System is unique in that the decoration, placement, and management of windows are handled by a separate, replaceable program known as a window manager. This separation allowed third-party developers to introduce a host of different window manager features, resulting in the early development of virtual desktop capabilities in X. The first implementation of virtual desktops for Unix was vtwm in 1990. Many of today's X window managers now include virtual desktop capabilities.



Dynamic virtual desktops in GNOME Shell. Workspaces are automatically added or deleted as the existing ones are respectively consumed or freed.

Configurations range from as few as two virtual desktops to several hundred. The most popular desktop environments, GNOME and KDE, use multiple virtual desktops (two or four by default) called workspaces. Some window managers, like FVWM, offer separate "desks" that allow the user to organize applications even further. For example, a user may have separate desks labeled "Work" and "Home", with the same programs running on both desks, but fulfilling different functions. Some window managers such as dwm and Sawfish support "tagging" where applications can be configured to always launch on a particular desktop, supporting automatic organization and easy navigation.

OS/2

IBM's personal computer OS/2 operating system included multiple desktops (up to 4 natively) in the OS/2 Warp 4 release in 1996. This functionality has also been provided by the open source XWorkplace project, with support for up to 100 virtual desktops. (A somewhat limited functionality version of XWorkplace is bundled with eComStation as eWorkplace, which includes this same functionality.)

Windows

Until Windows 10, Microsoft Windows did not implement virtual desktops natively in a user-accessible way. There are objects in the architecture of Windows known as "desktop objects" that are used to implement separate screens for logon and the secure desktop sequence (**Ctrl** + **Alt** + **Delete**). There is no native and easy way for users to create their own desktops or populate them with programs.^[4] However, there are many third-party (e. g. VirtuaWin, Dexpot and others) and some partially supported Microsoft products that implement virtual desktops to varying degrees of completeness.

Microsoft offers a utility called Desktops (<http://technet.microsoft.com/en-us/sysinternals/cc817881.aspx>) which allows users running Windows XP or Windows Server 2003 or later operating systems to run applications on up to 4 virtual desktops. Unlike nearly all other virtual desktop solutions for Windows, this utility actually uses native "desktop objects," as discussed above. Because of this, it does not offer the ability to move programs between desktops, or in fact to stop using virtual desktops at all, short of logging off,^[5] and Windows Aero only works on the primary desktop object.



Virtual desktop in Windows 10 showing two open apps in the same desktop, with a thumbnail showing another desktop

Microsoft had previously provided a Virtual Desktop PowerToy for Windows XP, which simulates many desktops with the more common method of hiding and showing windows in groups, each group being a different desktop. However, the functionality provided is less comprehensive than that of many other virtual desktop solutions (e. g. maintain a window in a given desktop even when its application bar button flashes, etc.). As with all virtual desktop utilities that work by hiding and showing windows, application compatibility problems are common, because application developers do not expect virtual desktops to be in use on the Windows platform.

Historically, software packaged with some video card drivers provided virtual desktop functionality, such as in Nvidia's nView product (this product has been discontinued for GeForce card owners since Vista). Some of these programs provide eye-candy features similar to those available on Compiz.

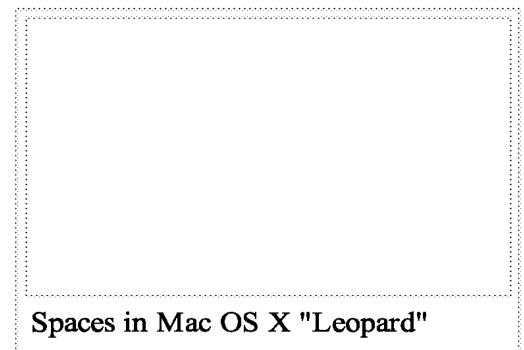
Many desktop shell replacements for Windows, including LiteStep, bblean, GeoShell, SharpE, Emerge Desktop and others, also support virtual desktops via optional modules.

Windows 10 offers virtual desktops through a system known as "Task View".^{[6][7]}

Mac OS

Beginning with version 10.5 "Leopard" in late 2007, Mac OS X has shipped with native virtual desktop support, called Spaces, which allows up to 16 virtual desktops. It allows the user to associate applications with a particular "Space". As of Mac OS X 10.7 "Lion", this functionality has been moved into Mission Control.

Scrolling desktops were made available to Macintosh users by a 3rd party extension called Stepping Out created by Wes Boyd (the future founder of Berkeley Systems) in 1986. The code for this extension was integrated by Apple into a later version of the Mac OS, although the ability to create virtual desktops larger than the screen was removed. The code was used instead as an assist for visually impaired users to zoom into portions of the desktop and view them as larger, more easily discerned images.



BeOS

BeOS includes an implementation of virtual desktops called "Workspaces". Up to 32 different Workspaces are supported.

References

1. D. Austin Henderson, Jr., Stuart Card (1986) Rooms: the use of multiple virtual workspaces to reduce space contention in a window-based graphical user interface (<http://portal.acm.org/citation.cfm?id=24056&coll=portal&dl=ACM&CFID=23778768&CFTOKEN=77139655>) ACM Transactions on Graphics
2. User interface with multiple workspaces for sharing display system objects ([http://patft.uspto.gov/netacgi/nph-Parser?u=%2Fnetacgi/nph-Parser&f=US&d=FULL&s1=5533183.PN.&OS=PN/5533183&RS=PN/5533183](http://patft.uspto.gov/netacgi/nph-Parser?u=%2Fnetacgi/nph-Parser?u=%2Fnetacgi/nph-Parser&f=US&d=FULL&s1=5533183.PN.&OS=PN/5533183&RS=PN/5533183)), US Patent 5,533,183
3. Thomas E. LaStrange (1990) swm: An X window manager shell (<http://www.lastrange.com/work/swm.pdf>). USENIX Summer.
4. "Desktops." Windows Dev Center. 27 Mar 2012 21:35 EST. <http://msdn.microsoft.com/en-us/library/windows/desktop/ms682573.aspx>
5. "Desktops." Windows Sysinternals, Microsoft TechNet. 17 Oct 2010 11:07 AM EDT. <http://technet.microsoft.com/en-us/sysinternals/cc817881.aspx>

6. "Microsoft Unveils Windows 10 with New Start Menu". *Tom's Guide*. Retrieved 30 September 2014.
7. "Windows 10 is the official name for Microsoft's next version of Windows". *The Verge*. Retrieved 30 September 2014.

External links

- Ars Technica: "The Micro-AmigaOne and Amiga OS4 Developer Prerelease" (<http://arstechnica.com/reviews/os/amiga.ars/3>) (Update 1), By Jeremy Reimer, Monday January 17, 2005 ("Desktop and drawers" section).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Virtual_desktop&oldid=729833826"

Categories: Graphical user interfaces | User interface techniques

- This page was last modified on 14 July 2016, at 21:35.
- Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Virtual private network

From Wikipedia, the free encyclopedia

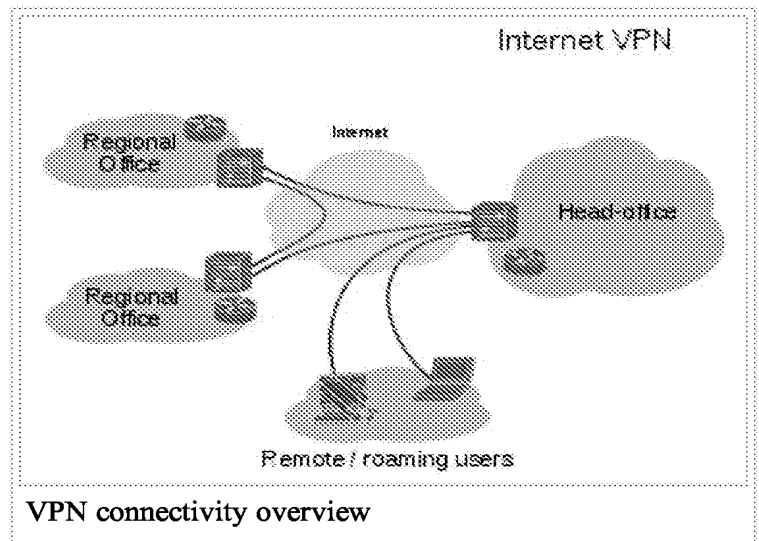
A **virtual private network (VPN)** extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.^[1]

VPNs may allow employees to securely access a corporate intranet while located outside the office. They are used to securely connect geographically separated offices of an organization, creating one cohesive network.

Individual Internet users may secure their wireless transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers for the purpose of protecting personal identity and location. However, some Internet sites block access to known VPN technology to prevent the circumvention of their geo-restrictions.

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.^[2]

Traditional VPNs are characterized by a point-to-point topology, and they do not tend to support or connect broadcast domains, so services such as Microsoft Windows NetBIOS may not be fully supported or work as they would on a local area network (LAN). Designers have developed VPN variants, such as Virtual Private LAN Service (VPLS), and layer-2 tunneling protocols, to overcome this limitation.



Contents

- 1 Types
- 2 Security mechanisms
 - 2.1 Authentication
- 3 Routing
 - 3.1 Provider-provisioned VPN building-blocks
- 4 User-visible PPVPN services
 - 4.1 OSI Layer 2 services
 - 4.2 OSI Layer 3 PPVPN architectures
 - 4.3 Unencrypted tunnels
- 5 Trusted delivery networks
- 6 VPNs in mobile environments
- 7 VPN on routers
- 8 Networking limitations

- 9 See also
- 10 Further reading
- 11 References

Types

Early data networks allowed VPN-style remote connectivity through dial-up modem or through leased line connections utilizing Frame Relay and Asynchronous Transfer Mode (ATM) virtual circuits, provisioned through a network owned and operated by telecommunication carriers. These networks are not considered true VPNs because they passively secure the data being transmitted by the creation of logical data streams.^[3] They have been replaced by VPNs based on IP and IP/Multi-protocol Label Switching (MPLS) Networks, due to significant cost-reductions and increased bandwidth^[4] provided by new technologies such as Digital Subscriber Line (DSL)^[5] and fiber-optic networks.

VPNs can be either remote-access (connecting a computer to a network) or site-to-site (connecting two networks). In a corporate setting, remote-access VPNs allow employees to access their company's intranet from home or while travelling outside the office, and site-to-site VPNs allow employees in geographically disparate offices to share one cohesive virtual network. A VPN can also be used to interconnect two similar networks over a dissimilar middle network; for example, two IPv6 networks over an IPv4 network.^[6]

VPN systems may be classified by:

- The protocols used to tunnel the traffic
- The tunnel's termination point location, e.g., on the customer edge or network-provider edge
- The type of topology of connections, such as site-to-site or network-to-network
- The levels of security provided
- The OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity
- The number of simultaneous connections

Security mechanisms

VPNs cannot make online connections completely anonymous, but they can usually increase privacy and security. To prevent disclosure of private information, VPNs typically allow only authenticated remote access using tunneling protocols and encryption techniques.

The VPN security model provides:

- Confidentiality such that even if the network traffic is sniffed at the packet level (see network sniffer and Deep packet inspection), an attacker would only see encrypted data
- Sender authentication to prevent unauthorized users from accessing the VPN
- Message integrity to detect any instances of tampering with transmitted messages

Secure VPN protocols include the following:

- Internet Protocol Security (IPsec) as initially developed by the Internet Engineering Task Force (IETF) for IPv6, which was required in all standards-compliant implementations of IPv6 before RFC 6434 made it only a recommendation.^[7] This standards-based security protocol is also widely used with IPv4 and the Layer 2 Tunneling Protocol. Its design meets most security goals:

authentication, integrity, and confidentiality. IPsec uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.

- Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic (as it does in the OpenVPN project and SoftEther VPN project^[8]) or secure an individual connection. A number of vendors provide remote-access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.
- Datagram Transport Layer Security (DTLS) – used in Cisco AnyConnect VPN and in OpenConnect VPN^[9] to solve the issues SSL/TLS has with tunneling over UDP.
- Microsoft Point-to-Point Encryption (MPPE) works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.
- Microsoft Secure Socket Tunneling Protocol (SSTP) tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL 3.0 channel. (SSTP was introduced in Windows Server 2008 and in Windows Vista Service Pack 1.)
- Multi Path Virtual Private Network (MPVPN). Ragula Systems Development Company owns the registered trademark "MPVPN".^[10]
- Secure Shell (SSH) VPN – OpenSSH offers VPN tunneling (distinct from port forwarding) to secure remote connections to a network or to inter-network links. OpenSSH server provides a limited number of concurrent tunnels. The VPN feature itself does not support personal authentication.^{[11][12][13]}

Authentication

Tunnel endpoints must be authenticated before secure VPN tunnels can be established. User-created remote-access VPNs may use passwords, biometrics, two-factor authentication or other cryptographic methods. Network-to-network tunnels often use passwords or digital certificates. They permanently store the key to allow the tunnel to establish automatically, without intervention from the administrator.

Routing

Tunneling protocols can operate in a point-to-point network topology that would theoretically not be considered as a VPN, because a VPN by definition is expected to support arbitrary and changing sets of network nodes. But since most router implementations support a software-defined tunnel interface, customer-provisioned VPNs often are simply defined tunnels running conventional routing protocols.

Provider-provisioned VPN building-blocks

Depending on whether a provider-provisioned VPN (PPVPN) operates in layer 2 or layer 3, the building blocks described below may be L2 only, L3 only, or combine them both. Multi-protocol label switching (MPLS) functionality blurs the L2-L3 identity.

RFC 4026 generalized the following terms to cover L2 and L3 VPNs, but they were introduced in RFC 2547.^[14] More information on the devices below can also be found in Lewis, Cisco Press.^[15]

Customer (C) devices

A device that is within a customer's network and not directly connected to the service provider's network. C devices are not aware of the VPN.

Customer Edge device (CE)

A device at the edge of the customer's network which provides access to the PPVPN. Sometimes it's just a demarcation point between provider and customer responsibility. Other providers allow customers to configure it.

Provider edge device (PE)

A PE is a device, or set of devices, at the edge of the provider network which connects to customer networks through CE devices and presents the provider's view of the customer site. PEs are aware of the VPNs that connect through them, and maintain VPN state.

Provider device (P)

A P device operates inside the provider's core network and does not directly interface to any customer endpoint. It might, for example, provide routing for many provider-operated tunnels that belong to different customers' PPVPNs. While the P device is a key part of implementing PPVPNs, it is not itself VPN-aware and does not maintain VPN state. Its principal role is allowing the service provider to scale its PPVPN offerings, for example, by acting as an aggregation point for multiple PEs. P-to-P connections, in such a role, often are high-capacity optical links between major locations of providers.

User-visible PPVPN services

OSI Layer 2 services

Virtual LAN

A Layer 2 technique that allow for the coexistence of multiple LAN broadcast domains, interconnected via trunks using the IEEE 802.1Q trunking protocol. Other trunking protocols have been used but have become obsolete, including Inter-Switch Link (ISL), IEEE 802.10 (originally a security protocol but a subset was introduced for trunking), and ATM LAN Emulation (LANE).

Virtual private LAN service (VPLS)

Developed by Institute of Electrical and Electronics Engineers, VLANs allow multiple tagged LANs to share common trunking. VLANs frequently comprise only customer-owned facilities. Whereas VPLS as described in the above section (OSI Layer 1 services) supports emulation of both point-to-point and point-to-multipoint topologies, the method discussed here extends Layer 2 technologies such as 802.1d and 802.1q LAN trunking to run over transports such as Metro Ethernet.

As used in this context, a VPLS is a Layer 2 PPVPN, rather than a private line, emulating the full functionality of a traditional local area network (LAN). From a user standpoint, a VPLS makes it possible to interconnect several LAN segments over a packet-switched, or optical, provider core; a core transparent to the user, making the remote LAN segments behave as one single LAN.^[16]

In a VPLS, the provider network emulates a learning bridge, which optionally may include VLAN service.

Pseudo wire (PW)

PW is similar to VPLS, but it can provide different L2 protocols at both ends. Typically, its interface is a WAN protocol such as Asynchronous Transfer Mode or Frame Relay. In contrast, when aiming to provide the appearance of a LAN contiguous between two or more locations, the Virtual Private LAN service or IPLS would be appropriate.

Ethernet over IP tunneling

EtherIP (RFC 3378) (<http://tools.ietf.org/search/rfc3378>) is an Ethernet over IP tunneling protocol specification. EtherIP has only packet encapsulation mechanism. It has no confidentiality nor message integrity protection. EtherIP was introduced in the FreeBSD network stack^[17] and the SoftEther VPN^[18] server program.

IP-only LAN-like service (IPLS)

A subset of VPLS, the CE devices must have Layer 3 capabilities; the IPLS presents packets rather than frames. It may support IPv4 or IPv6.

OSI Layer 3 PPVPN architectures

This section discusses the main architectures for PPVPNs, one where the PE disambiguates duplicate addresses in a single routing instance, and the other, virtual router, in which the PE contains a virtual router instance per VPN. The former approach, and its variants, have gained the most attention.

One of the challenges of PPVPNs involves different customers using the same address space, especially the IPv4 private address space.^[19] The provider must be able to disambiguate overlapping addresses in the multiple customers' PPVPNs.

BGP/MPLS PPVPN

In the method defined by RFC 2547, BGP extensions advertise routes in the IPv4 VPN address family, which are of the form of 12-byte strings, beginning with an 8-byte Route Distinguisher (RD) and ending with a 4-byte IPv4 address. RDs disambiguate otherwise duplicate addresses in the same PE.

PEs understand the topology of each VPN, which are interconnected with MPLS tunnels, either directly or via P routers. In MPLS terminology, the P routers are Label Switch Routers without awareness of VPNs.

Virtual router PPVPN

The virtual router architecture,^{[20][21]} as opposed to BGP/MPLS techniques, requires no modification to existing routing protocols such as BGP. By the provisioning of logically independent routing domains, the customer operating a VPN is completely responsible for the address space. In the various MPLS tunnels, the different PPVPNs are disambiguated by their label, but do not need routing distinguishers.

Unencrypted tunnels

Some virtual networks may not use encryption to protect the privacy of data. While VPNs often provide security, an unencrypted overlay network does not neatly fit within the secure or trusted categorization. For example, a tunnel set up between two hosts that used Generic Routing Encapsulation (GRE) would in fact be a virtual private network, but neither secure nor trusted.^{[22][23]}

Native plaintext tunneling protocols include Layer 2 Tunneling Protocol (L2TP) when it is set up without IPsec and Point-to-Point Tunneling Protocol (PPTP) or Microsoft Point-to-Point Encryption (MPPE).^[24]

Trusted delivery networks

Trusted VPNs do not use cryptographic tunneling, and instead rely on the security of a single provider's network to protect the traffic.^[25]

- Multi-Protocol Label Switching (MPLS) often overlays VPNs, often with quality-of-service control over a trusted delivery network.
- Layer 2 Tunneling Protocol (L2TP)^[26] which is a standards-based replacement, and a compromise taking the good features from each, for two proprietary VPN protocols: Cisco's Layer 2 Forwarding (L2F)^[27] (obsolete as of 2009) and Microsoft's Point-to-Point Tunneling Protocol (PPTP).^[28]

From the security standpoint, VPNs either trust the underlying delivery network, or must enforce security with mechanisms in the VPN itself. Unless the trusted delivery network runs among physically secure sites only, both trusted and secure models need an authentication mechanism for users to gain access to the VPN.

VPNs in mobile environments

Mobile virtual private networks are used in settings where an endpoint of the VPN is not fixed to a single IP address, but instead roams across various networks such as data networks from cellular carriers or between multiple Wi-Fi access points.^[29] Mobile VPNs have been widely used in public safety, where they give law enforcement officers access to mission-critical applications, such as computer-assisted dispatch and criminal databases, while they travel between different subnets of a mobile network.^[30] They are also used in field service management and by healthcare organizations,^[31] among other industries.

Increasingly, mobile VPNs are being adopted by mobile professionals who need reliable connections.^[31] They are used for roaming seamlessly across networks and in and out of wireless coverage areas without losing application sessions or dropping the secure VPN session. A conventional VPN can not withstand such events because the network tunnel is disrupted, causing applications to disconnect, time out,^[29] or fail, or even cause the computing device itself to crash.^[31]

Instead of logically tying the endpoint of the network tunnel to the physical IP address, each tunnel is bound to a permanently associated IP address at the device. The mobile VPN software handles the necessary network authentication and maintains the network sessions in a manner transparent to the application and the user.^[29] The Host Identity Protocol (HIP), under study by the Internet Engineering Task Force, is designed to support mobility of hosts by separating the role of IP addresses for host identification from their locator functionality in an IP network. With HIP a mobile host maintains its logical connections established via the host identity identifier while associating with different IP addresses when roaming between access networks.

VPN on routers

With the increasing use of VPNs, many have started deploying VPN connectivity on routers for additional security and encryption of data transmission by using various cryptographic techniques.^[32] Setting up VPN support on a router and establishing a VPN allows any networked device to have access to the entire network—all devices look like local devices with local addresses. Supported devices are not restricted to those capable of running a VPN client.^[33]

Many router manufacturers, including Asus, Cisco, Draytek,^[33] Linksys, Netgear, and Yamaha, supply routers with built-in VPN clients. Some use open-source firmware such as DD-WRT, OpenWRT and Tomato, in order to support additional protocols such as OpenVPN.

Setting up VPN services on a router requires a deep knowledge of network security and careful installation. Minor misconfiguration of VPN connections can leave the network vulnerable. Performance will vary depending on the ISP.

Networking limitations

One major limitation of traditional VPNs is that they are point-to-point, and do not tend to support or connect broadcast domains. Therefore, communication, software, and networking, which are based on layer 2 and broadcast packets, such as NetBIOS used in Windows networking, may not be fully supported or work exactly as they would on a real LAN. Variants on VPN, such as Virtual Private LAN Service (VPLS), and layer 2 tunneling protocols, are designed to overcome this limitation.

See also

- Anonymizer
- Dynamic Multipoint Virtual Private Network
- Geo-blocking
- Internet privacy
- Mediated VPN
- OpenVPN
- Opportunistic encryption
- Split tunneling
- Tinc (protocol)
- UT-VPN
- Virtual Private LAN Service
- Virtual private server
- VPNBook

Further reading

- Kelly, Sean (August 2001). "Necessity is the mother of VPN invention". *Communication News*: 26–28. ISSN 0010-3632. Archived from the original on 2001-12-17.

References

1. Mason, Andrew G. (2002). *Cisco Secure Virtual Private Network*. Cisco Press. p. 7.
2. Microsoft Technet. "Virtual Private Networking: An Overview".
3. Cisco Systems, et al. *Internet working Technologies Handbook, Third Edition*. Cisco Press, 2000, p. 232.
4. Lewis, Mark. *Comparing, Designing. And Deploying VPNs*. Cisco Press, 2006, p. 5
5. International Engineering Consortium. *Digital Subscriber Line 2001*. Intl. Engineering Consortium, 2001, p. 40.
6. Technet Lab. "IPv6 traffic over VPN connections".
7. RFC 6434, "IPv6 Node Requirements", E. Jankiewicz, J. Loughney, T. Narten (December 2011)
8. SoftEther VPN: Using HTTPS Protocol to Establish VPN Tunnels (http://www.softether.org/1-features/1._Ultimate_Powerful_VPN_Connectivity#SoftEther_VPN's_Solution:_Using_HTTPS_Protocol_to_Establish_VPN_Tunnels)

9. "OpenConnect". Retrieved 2013-04-08. "OpenConnect is a client for Cisco's AnyConnect SSL VPN [...] OpenConnect is not officially supported by, or associated in any way with, Cisco Systems. It just happens to interoperate with their equipment."
10. Trademark Applications and Registrations Retrieval (TARR) (<http://tarr.uspto.gov/servlet/tarr?regser=serial&entry=78063238&action=Request+Status>)
11. OpenBSD ssh manual page, VPN section (<http://www.openbsd.org/cgi-bin/man.cgi?query=ssh#SSH-BASED+VIRTUAL>)
12. Unix Toolbox section on SSH VPN (<http://cb.vu/unixtoolbox.xhtml#vpn>)
13. Ubuntu SSH VPN how-to (https://help.ubuntu.com/community/SSH_VPN)
14. E. Rosen & Y. Rekhter (March 1999). "RFC 2547 BGP/MPLS VPNs". Internet Engineering Task Force (IETF).
15. Lewis, Mark (2006). *Comparing, designing, and deploying VPNs* (1st print. ed.). Indianapolis, Ind.: Cisco Press. pp. 5–6. ISBN 1587051796.
16. *Ethernet Bridging (OpenVPN)*
17. Glyn M Burton: RFC 3378 EtherIP with FreeBSD (<http://www.modiford.com/menu-computing/4-open-source/9-rfc-3378-etherip-with-freebsd>), 03 February 2011
18. net-security.org news: Multi-protocol SoftEther VPN becomes open source (<http://www.net-security.org/secworld.php?id=16171>), January 2014
19. Address Allocation for Private Internets (<http://www.ietf.org/rfc/rfc1918.txt>), RFC 1918, Y. Rekhter *et al.*, February 1996
20. RFC 2917, *A Core MPLS IP VPN Architecture*
21. RFC 2918, E. Chen (September 2000)
22. "Overview of Provider Provisioned Virtual Private Networks (PPVPN)". Secure Thoughts. Retrieved 29 August 2016.
23. RFC 1702: Generic Routing Encapsulation over IPv4 networks. October 1994.
24. IETF (1999), RFC 2661, Layer Two Tunneling Protocol "L2TP"
25. Cisco Systems, Inc. (2004). *Internetworking Technologies Handbook*. Networking Technology Series (4 ed.). Cisco Press. p. 233. ISBN 9781587051197. Retrieved 2013-02-15. "[...] VPNs using dedicated circuits, such as Frame Relay [...] are sometimes called *trusted VPNs*, because customers trust that the network facilities operated by the service providers will not be compromised."
26. Layer Two Tunneling Protocol "L2TP" (<http://www.ietf.org/rfc/rfc2661.txt>), RFC 2661, W. Townsley *et al.*, August 1999
27. IP Based Virtual Private Networks (<http://www.ietf.org/rfc/rfc2341.txt>), RFC 2341, A. Valencia *et al.*, May 1998
28. Point-to-Point Tunneling Protocol (PPTP) (<http://www.ietf.org/rfc/rfc2637.txt>), RFC 2637, K. Hamzeh *et al.*, July 1999
29. Phifer, Lisa. "Mobile VPN: Closing the Gap" (http://searchmobilecomputing.techtarget.com/tip/0,289483,sid40_gci1210989_mem1,00.html), *SearchMobileComputing.com*, July 16, 2006.
30. Willett, Andy. "Solving the Computing Challenges of Mobile Officers" ([http://www.officer.com/print/Law-Enforcement-Technology/Solving-the-Computing-Challenges-of-Mobile-Officers/1\\$30992](http://www.officer.com/print/Law-Enforcement-Technology/Solving-the-Computing-Challenges-of-Mobile-Officers/1$30992)), *www.officer.com*, May, 2006.
31. Cheng, Roger. "Lost Connections" (<http://online.wsj.com/article/SB119717610996418467.html>), *The Wall Street Journal*, December 11, 2007.
32. "Encryption and Security Protocols in a VPN". Retrieved 2015-09-23.
33. "VPN". *Draytek*. Retrieved 19 October 2016.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Virtual_private_network&oldid=748830361"

Categories: Network architecture | Computer network security | Internet privacy | Crypto-anarchism | Virtual private networks

-
- This page was last modified on 10 November 2016, at 17:11.
 - Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a

registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Electronic Acknowledgement Receipt

EFS ID:	34447972
Application Number:	16141378
International Application Number:	
Confirmation Number:	2440
Title of Invention:	NETWORK ISOLATION WITH CLOUD NETWORKS
First Named Inventor/Applicant Name:	Glenn Coleman
Customer Number:	158266
Filer:	Benjamin S. Chalfin/MELISSA OVERLINE
Filer Authorized By:	Benjamin S. Chalfin
Attorney Docket Number:	LCOM_ENT_CLOUD_US01
Receipt Date:	30-NOV-2018
Filing Date:	25-SEP-2018
Time Stamp:	12:56:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	LCOM_ENT_CLOUD_US01_AS_ FILED_IDS_TRANS.pdf	104101 0f84affbce049c5afa0ea2417f41ad347d38a c4	no	3

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	LCOM_ENT_CLOUD_US01_AS_FILED_IDS_1449.pdf	134954	no	2
			30bf9eb219466e18cf3da229c668dbaec37084bf		
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	Barnet_PraktikumPoZaschiteSe ti_2006_4pp.pdf	1463807	no	4
			06a8f6293780f99f5b20e846b12afb1a817a1513		
Warnings:					
Information:					
4	Non Patent Literature	Burnett_HowISecured_September2006_4pp.pdf	3101446	no	4
			09f01614389f06083818eb98d1dfadaa7e64a0bb		
Warnings:					
Information:					
5	Non Patent Literature	Laverick_HypervisorManagementandOptimization_2010_13pp.pdf	1756069	no	13
			6f30c9897fb3e8cc61accbf5bc9d9b28092b3d57		
Warnings:					
Information:					
6	Non Patent Literature	Li_ASscalableandSecureArchitecture_October2010_6pp.pdf	3626215	no	6
			740340bd021e5096e2c0450b450362b7752757ef		
Warnings:					
Information:					
7	Non Patent Literature	Reuben_ASurveyOnVirtual_October2007_5pp.pdf	166324	no	5
			2e25bae99cc76806ec95d0a838768294b776dfc0		
Warnings:					
Information:					
8	Foreign Reference	RU_2406138.pdf	610079	no	17
			f49a1d801e96e03b3c5f9bd46ef54a2fdc9d389f		
Warnings:					
Information:					
IBM - Ex. 1002-Part 1 of 10, Page 243					

9	Non Patent Literature	Villeneuve_CommandAndControl_October2010_3pp.pdf	568743	no	3
			0dd5a8cc485426b990fe8fa4d32f6c866c84088a		
Warnings:					
Information:					
10	Non Patent Literature	Wikipedia_ComputerNetwork_December2010_19pp.pdf	338914	no	19
			efee49dfae56aa0b62dbb4e921040f66e352fb01		
Warnings:					
Information:					
11	Non Patent Literature	Wikipedia_ComputerSecurity_December2010_27pp.pdf	11144077	no	27
			675376025595267e34c7f5ec69cb66f74c49f508		
Warnings:					
Information:					
12	Non Patent Literature	Wikipedia_CyberSecurityStandards_December2010_9pp.pdf	3357214	no	9
			3aa5722510ff7788c1783b5d4959fcb0561eef44		
Warnings:					
Information:					
13	Non Patent Literature	Wikipedia_HTTPSecure_December2010_9pp.pdf	3462519	no	9
			91fc24dd223f426a04b2dfe5a166caf2022b9519		
Warnings:					
Information:					
14	Non Patent Literature	Wikipedia_Hypervisor_December2010_6pp.pdf	2644963	no	6
			c8488a9c05b02159ce31bbaab4546c4c168b80e1		
Warnings:					
Information:					
15	Non Patent Literature	Wikipedia_InternetProtocol_December2010_5pp.pdf	1722989	no	5
			4e335148d0f22707bc6fb77e2cf0660c33ce57ab		
Warnings:					
Information:					

16	Non Patent Literature	Wikipedia_MultiprotocolLabel_December2010_8pp.pdf	3623978	no	8
			980585c6659b1c0b07f81ff64bddffd6a44c0673		
Warnings:					
Information:					
17	Non Patent Literature	Wikipedia_NetworkAddress_December2010_12pp.pdf	4552887	no	12
			e30c024a04a3be41b6d9142d77b12fad61bb2f		
Warnings:					
Information:					
18	Non Patent Literature	Wikipedia_SecurityFocused_December2010_9pp.pdf	2924141	no	9
			843da85fbc967faee5a2990d59154a079211da32		
Warnings:					
Information:					
19	Non Patent Literature	Wikipedia_VirtualDesktop_December2010_5pp.pdf	1734750	no	5
			703a750edb76d6e5e40f3939e30d463ce9b684f5		
Warnings:					
Information:					
20	Non Patent Literature	Wikipedia_VirtualPrivate_December2010_9pp.pdf	3017235	no	9
			a5123ca641ac98777f0c9ed4eaa4855a20c926de		
Warnings:					
Information:					
Total Files Size (in bytes):			50055405		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**In Re Application of:****L3 Technologies, Inc.****Confirmation No.: 2440****Application No.: 16/141,378****Group Art Unit: 2491****Filing Date: September 25, 2018****Examiner: PATEL, ASHOKKUMAR B****For: NETWORK ISOLATION WITH CLOUD NETWORKS**

Filed Via EFS

INFORMATION DISCLOSURE STATEMENT

Pursuant to 37 CFR § 1.56 and in accordance with 37 CFR §§ 1.97-1.98, information relating to the above-identified application is hereby disclosed. Inclusion of information in this statement is not to be construed as an admission that this information is material as that term is defined in 37 CFR § 1.56(b).

☒ **IDS Filed Under 37 CFR 1.97(b)**

In accordance with § 1.97(b), since this Information Disclosure Statement is being filed either within three months of the filing date of the above-identified application, within three months of the date of entry into the national stage of the above identified application as set forth in § 1.491, before the mailing date of a first Office Action on the merits of the above-identified application, or before the mailing date of a first Office Action after the filing of request for continued examination under § 1.114, no additional fee is required.

☐ **IDS filed Under 37 CFR 1.97(c)**

In accordance with § 1.97(c), this Information Disclosure Statement is being filed after the period set forth in § 1.97(b) above but before the mailing date of either a Final Action under § 1.116 or a Notice of Allowance under § 1.311, or before an action that otherwise closes prosecution in the application, therefore:

- ☐ Certification in Accordance with § 1.97(e) is attached; or
- ☐ The fee of **\$240.00** as set forth in § 1.17(p) is attached.

☐ **IDS filed Under 37 CFR 1.97(d)**

In accordance with § 1.97(d), this Information Disclosure Statement is being filed after the mailing date of either a Final Action under § 1.113 or a Notice of Allowance under § 1.311 but before, or simultaneously with, the payment of the Issue Fee, therefore included are: Certification in Accordance with § 1.97(e); and the submission fee of **\$240.00** as set forth in § 1.17(p).

CONTENT OF IDS PURSUANT TO 37 CFR 1.98

☒ Copies of reference numbers 01-17 listed on the attached Form PTO-1449 are not required to be submitted pursuant to 37 CFR § 1.98(a)(2)(ii).

☒ Copies of reference numbers 18-35 listed on the attached Form PTO-1449 are enclosed herewith.

☐ Copies of reference numbers are not being submitted because they were previously cited by or submitted to the U.S. Patent and Trademark Office in patent application number , filed for which a claim for priority under 35 U.S.C. § 120 has been made in the instant application.

☐ The month of publication for reference numbers is not available. However, the year of publication for these references is sufficiently earlier than the effective US filing date and any foreign priority date so that the particular month of publication is not in issue pursuant to 37 CFR § 1.98(b).

REFERENCES IN A LANGUAGE OTHER THAN ENGLISH

☐ The following documents are not in the English language. Accordingly, a concise explanation of the relevance of the document was incorporated in the specification passages identified below, the document was identified in a foreign communication as identified below or an English language counterpart application has been provided as indicated below.

Foreign Language Document	Cite No.	Pages of Reference in Specification or Relevance of Document

Foreign Language Document	Cite No.	English Language Counterpart	Cite No.

☐ **CERTIFICATION IN ACCORDANCE WITH § 1.97(e)**

I hereby certify that:

- ☐ Each item of information contained in this information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this information disclosure statement.
- ☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in this information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of this information disclosure statement.

Please charge any deficiency or credit any overpayment to Deposit Account No. 50-5519.

Date: November 30, 2018

/Benjamin Chalfin/
Benjamin Chalfin
Registration No. 74,181

CONDO ROCCIA KOPTIW LLP
1800 JFK BOULEVARD
SUITE 1700
PHILADELPHIA, PA 19103
Telephone: (215) 558-5740



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/141,378	09/25/2018	Glenn Coleman	LCOM_ENT_CLOUD_US01

CONFIRMATION NO. 2440

158266
Condo Roccia Koptiw LLP
1800 JFK Boulevard
Suite 1700
Philadelphia, PA 19103

PUBLICATION NOTICE



OC000000106952466

Title:NETWORK ISOLATION WITH CLOUD NETWORKS

Publication No.US-2019-0097970-A1

Publication Date:03/28/2019

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <https://portal.uspto.gov/pair/PublicPair>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/141,378	09/25/2018	Glenn Coleman	LCOM_ENT_CLOUD_US01	2440
158266	7590	05/21/2020	EXAMINER	
Condo Roccia Koptiw LLP			KORSAK, OLEG	
1800 JFK Boulevard				
Suite 1700				
Philadelphia, PA 19103				
			ART UNIT	PAPER NUMBER
			2492	
			MAIL DATE	DELIVERY MODE
			05/21/2020	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

This communication is responsive to the application # 16/141,378 filed on September 25, 2018. Claims 1-20 are pending and are directed toward NETWORK ISOLATION WITH CLOUD NETWORKS.

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(b):

(b) **CONCLUSION.**—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 5-7 and 12 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention. Claims 5-7 are indefinite, because limitation “to determine whether to send web traffic to the local network-based proxy server or the Internet-based proxy server” requires at least 2

Art Unit: 2492

proxy servers, and only at least one is claimed in claim 4. Claim 12 is indefinite because it essentially claims that “1”=“2”.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a)(1) the claimed invention was patented, described in a printed publication, or in public use, on sale or otherwise available to the public before the effective filing date of the claimed invention.

Claims 1, 2, 4-9 and 19 are rejected under 35 U.S.C. 102(a)(1) as being unpatentable over Hoy et al. (US 2013/0318594 Pub. Date: Nov. 28, 2013), hereinafter referred to as Hoy.

As per **claim 1**, Hoy teaches a host computer system comprising a processor and memory (*A host computer supports a virtual guest system running thereon. Hoy, ABSTRACT*), the processor configured to:

implement a workspace, wherein the workspace is configured to enable operation of a first set of one or more applications or processes via a first memory space (*a computerized work station comprises a computer operatively connected with one or more user-accessible data entry devices, a display device viewable by the user, and computer-accessible data storage providing for the computer an operating system and one or more applications programs that run on said operating system, and supporting a virtual computer system operating on the computer. Hoy, [0022]*);

implement an isolated computing environment, the isolated computing environment being configured to enable operation of a second set of one or more applications or processes via a second memory space, wherein the isolated computing environment is configured to access an Internet-based cloud service via at least one application of the second set of applications (*Also*

Art Unit: 2492

operating on the host computer is a hypervisor system that creates a virtual machine environment that is separate from the host computer's operating system. This virtual machine has a virtual guest operating system on which a modified browser is run. The browser is activated by a desk-top shortcut or application on the host system that allows the user to link to the isolated Internet access of the virtual guest system by launching the virtual guest web browser, which operates transparently to the user in the virtual guest system. Hoy, [0026]);

isolate the isolated computing environment from the workspace using an internal isolation firewall (According to an aspect of the invention, this is accomplished by providing a host computer that is surrounded by a host based firewall. Hoy, [0025]); and

communicate with at least one proxy server in order to access the Internet-based cloud service (Proxy content filter 4 may optionally be used to screen undesirable or inappropriate incoming or outgoing data, as above. Hoy, [0073]), wherein the isolated computing environment is configured to authenticate with an authentication device in order to allow communication between the at least one application and the Internet-based cloud service (To allow for this, the firewall 11 around the host OS 17 selectively enables the host OS 17 to access the Internet directly through ports 80 or 443, which are otherwise disabled, provided that the websites being accessed are on a whitelist of predetermined trusted sites with which the host OS 17 is permitted to communicate with. Hoy, [0057]).

As per **claim 2**, Hoy teaches the system of claim 1, wherein the processor is configured to access the Internet-based cloud service via one or more of a local area network (LAN), a wide area network (WAN), a cellular network, a Wi-Fi network, a digital subscribers line (DSL) network, a cloud computing network, a data center, or a satellite network (*The home system, when the host is "home" on the trusted LAN network, is allowed by the HBFW to communicate to*

other LAN resources as well as any whitelisted sites outside the LAN on the Internet. Hoy, [0062]).

As per **claim 4**, Hoy teaches the system of claim 1, wherein the processor is configured to select the at least one proxy server from a plurality of candidate proxy servers, the plurality of proxy servers comprising at least one Internet-based proxy server or at least one local network-based proxy server (*A proxy/web-content filter 4 is connected with and cooperates with the firewall hardware 3 to control the type of data permitted to pass from the Internet 5 into the local system 1, filtering e.g., pornographic material or data not intended for the system 1, and also blocks communications from users on the LAN trying to reach disallowed sites, e.g., requests to access www.onlinecasino.com. Hoy, [0038]).*

As per **claim 5**, Hoy teaches the system of claim 4, wherein the processor is configured to determine whether to send web traffic to the local network-based proxy server or the Internet-based proxy server based on a location of the host computer system (*Proxy content filter 4 may optionally be used to screen undesirable or inappropriate incoming or outgoing data, Hoy, [0073]).*

As per **claim 6**, Hoy teaches the system of claim 4, wherein the processor is configured to determine whether to send web traffic to the local network-based proxy server or the Internet-based proxy server based on an identity of a network to which the host computer system is connected (*Proxy content filter 4 may optionally be used to screen undesirable or inappropriate incoming or outgoing data, Hoy, [0073]).*

As per **claim 7**, Hoy teaches the system of claim 4, wherein the processor is configured to determine whether to send web traffic to the local network-based proxy server or the Internet-based proxy server based on the identity of the at least one application running in the isolated

Art Unit: 2492

computing environment (*The virtual guest system 13 shows no software installed except for a browser and possibly some related supportive software, such as Adobe or Windows Media Player that cooperate with the browser when certain types of files are accessed on the Internet, and potentially an email program such as Microsoft Outlook for certain configurations. Hoy, [0048]).*

As per **claim 8**, Hoy teaches the system of claim 1, wherein the internal isolation firewall is configured to segregate the first memory space from the second memory space and is configured to enforce policies for communication between the first memory space and the second memory space (*The guest computer and the host computer communicate with each other by a limited permissible internal host-based firewall in the host system that is provided by the hypervisor or some other local program. Communications across this internal firewall between the guest system and the host system are limited to cut and paste of displayed documents or files, commands to print documents, and file transfer requested manually by the host, Hoy, [0030]).*

As per **claim 9**, Hoy teaches the system of claim 8, wherein the internal isolation firewall is further configured to prompt a user of the host computer system to allow communication between the first memory space and the second memory space (*i.e., directed intentionally by the human user of the given system. Hoy, [0030]).*

Claim 19 has limitations similar to those treated in the above rejection, and are met by the references as discussed above, and are rejected for the same reasons of anticipation as used above.

Claims 10, 11 and 14-18 are rejected under 35 U.S.C. 102(a)(1) as being unpatentable over Giura et al. (US 2015/0156203, Jun. 4, 2015), hereinafter referred to as Giura.

As per **claim 10**, Giura teaches a cloud computing system comprising:

a cloud computing network (*The network provider network 125 may include and be connected to a cloud-based network, Giura, [0024]*), the cloud computing network comprising at least one server (*The network provider network 125 may include one or more servers, such as virtual browser servers 130 and 135. Giura, [0024]*), wherein the server comprises a first set of one or more applications or processes running in a workspace and a second set of one or more applications or processes running in an isolated computing environment (*The virtual browser servers 130 and 135 may host virtual machines, such as browser virtual machines, that may be utilized to render and provide virtual browsers to the user device 102. The virtual browser server 130 may include a memory 131 that includes instructions, and a processor 132 that executes the instructions from the memory 131 to perform various operations that are performed by the virtual browser server 130. Similarly, the virtual browser server 135 may include a memory 136 that includes instructions, and a processor 137 that executes the instructions from the memory 136 to perform various operations that are performed by the virtual browser server 135. The processors 132 and 137 may be hardware, software, or a combination thereof. In certain embodiments, the virtual machines may run above a hypervisor, such as hypervisor 610, which is shown in FIG. 6. Giura, [0024]*), and the server comprises an internal firewall to isolate the workspace from the isolated computing environment (*The firewall 124 may be utilized to keep the virtual machine manager 128 and the virtual browser servers 130 and 135 separate from the rest of devices and information in the enterprise network 115. Giura, [0039]*); and

at least one proxy configured to control communication between the server and at least one Internet resource, wherein the proxy is configured to allow communication between the second set of one or more applications or processes running in the isolated computing

Art Unit: 2492

environment and the at least one Internet resource and to block communication between the first set of one or more applications or processes running in the workspace and the at least one Internet resource (*Once the request to access the resource is sent from the user device 102, the request may be received by the transparent network proxy 120. In certain embodiments, the transparent network proxy 120 may be a network proxy, a network server, a router, a gateway, a computer, a mobile device, any other suitable computing device, or a combination thereof. In one embodiment, the transparent network proxy 120 may include a proxy and a categorization service. In another embodiment, the transparent network proxy 120 may include or be connected to a malware threat prevention or detection system. Giura, [0026]*).

As per **claim 11**, Giura teaches the system of claim 10, wherein the server is configured to perform at least one processing task on behalf of a client device (*receiving, from a user device, a request to access a resource, wherein the request includes an identifier for locating the resource; determining if the resource is not trusted based on an analysis of the identifier; and forwarding, if the resource is determined to not be trusted based on the analysis of the identifier, the request to a virtual machine manager for selecting a browser virtual machine from a pool of browser virtual machines, Giura, [0009]*).

As per **claim 14**, Giura teaches the system of claim 10, further comprising a border firewall configured to segregate the cloud computing network from one or more Internet destinations (*The firewall 124 may be utilized to keep the virtual machine manager 128 and the virtual browser servers 130 and 135 separate from the rest of devices and information in the enterprise network 115. Giura, [0039]*).

As per **claim 15**, Giura teaches the system of claim 10, wherein the internal firewall is further configured to allow communication between the workspace and the isolated computing

environment on a condition that the communication is in a predetermined format (*The firewall 124 may be a software or hardware-based network security system, which monitors and controls incoming and outgoing traffic based on rules established by the firewall 124. Giura, [0039]*).

As per **claim 16**, Giura teaches the system of claim 11, wherein the server is further configured to receive input data from the client device (*receiving, from a user device, a request to access a resource. Giura, [0008]*) and send one or more data communications to the client device (*Then, a stream including a rendering of the resource may be streamed from the selected browser virtual machine to the user device based on the request. Giura, [0008]*).

As per **claim 17**, Giura teaches the system of claim 11, wherein the at least one processing task performed on behalf of the client device comprises a processing task for an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS) (*The system 100 may be configured to support, but is not limited to supporting, content delivery services, cloud computing services, voice-over-internet protocol services (VoIP), software as a service (SaaS) applications, gaming applications and services, productivity applications and services, mobile applications and services, and any other computing applications and services. Giura, [0021]*).

As per **claim 18**, Giura teaches the system of claim 10, wherein the isolated computing environment is implemented using one or more of a sandboxed computing environment or a virtual machine (*securely browse unknown or suspicious URLs or destinations through the use of the transparent network proxy, virtual browser machines, and desktop virtualization technologies, Giura, [0004]*).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 3 and 20 are rejected under 35 U.S.C. 103 as being unpatentable over Hoy et al. (US 2013/0318594 Pub. Date: Nov. 28, 2013) in view of Giura et al. (US 2015/0156203, Jun. 4, 2015), hereinafter referred to as Hoy and Giura respectively.

As per **claim 3**, Hoy teaches the system of claim 1, but does **not** teach “as a Service”, Giura however teaches wherein the Internet-based cloud service comprises one or more of an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS) *(The system 100 may be configured to support, but is not limited to supporting, content delivery services, cloud computing services, voice-over-internet protocol services (VoIP), software as a service (SaaS) applications, gaming applications and services, productivity applications and services, mobile applications and services, and any other computing applications and services. Giura, [0021]).*

Hoy in view of Giura are analogous art to the claimed invention, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious to a person of ordinary skill in the art before the effective filing date of the claimed invention to modify Hoy in view of Giura. This would have been desirable because it is possible for the IT personnel to configure the system to specifically allow or whitelist other ports or websites for necessary or reasonably permitted file transfers to known entities (Hoy, [0062]).

Claim 20 has limitations similar to those treated in the above rejection, and are met by the references as discussed above, and are rejected for the same reasons of obviousness as used above.

Claim 12 is rejected under 35 U.S.C. 103 as being unpatentable over Hoy et al. (US 2013/0318594 Pub. Date: Nov. 28, 2013) in view of JAGERS (US 2017/0034174, Pub. Date: Feb. 2, 2017), hereinafter referred to as Hoy and JAGERS respectively.

As per **claim 12**, Hoy teaches the system of claim 11, but does **not** teach wherein the at least one proxy comprises a first proxy and a second proxy, and the server is configured to determine whether to send traffic to the first proxy or the second proxy, JAGERS however teaches wherein the at least one proxy comprises a first proxy and a second proxy, and the server is configured to determine whether to send traffic to the first proxy or the second proxy (*The invention provides for a method for providing access to a web server and an arrangement for performing said method. Access is provided by a first proxy server and a second proxy server on request. JAGERS, ABSTRACT*).

Hoy in view of JAGERS are analogous art to the claimed invention, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious to a person of ordinary skill in the art before the effective filing date of the claimed invention to modify Hoy in view of JAGERS. This would have been desirable because the method shown is suitable for accessing a web server which is installed on a machine, e.g. an industrial machine running on a computing unit using at least two proxy servers. The machine does not need a public IP address, access can be provided in compliance with safety requirements (JAGERS, [0038]).

Claim 13 is rejected under 35 U.S.C. 103 as being unpatentable over Hoy et al. (US 2013/0318594 Pub. Date: Nov. 28, 2013) in view of JAGERS (US 2017/0034174, Pub. Date: Feb. 2, 2017), in view of Singh et al. (US 2012/0054744, Pub. Date: Mar. 1, 2012), hereinafter referred to as Hoy, JAGERS and Singh respectively.

As per **claim 13**, Hoy in view of JAGERS teaches the system of claim 12, wherein the server is configured to determine whether to send traffic to the first proxy or the second proxy, but does **not** teach based on user-provided credentials, Singh however teaches based on user-provided credentials (*Redirection can include redirecting cookies, preferences, usage history, application settings, configurations and/or security tokens. Security tokens may include certificates, credentials, tickets and encryption keys. Thus when a URL or application access request is redirected, a required cookie or security token can be used to access a domain or other web or application content. Singh, [0152]*).

Hoy in view of JAGERS in view of Singh are analogous art to the claimed invention, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious to a person of ordinary skill in the art before the effective filing date of the claimed invention to modify Hoy in view of JAGERS in view of Singh. This would have been desirable because the method shown is suitable for accessing a web server which is installed on a machine, e.g. an industrial machine running on a computing unit using at least two proxy servers. The machine does not need a public IP address, access can be provided in compliance with safety requirements (JAGERS, [0038]), and unsecure or unsecure virtual machines 232B may be prevented from accessing resources, hardware, memory locations, and programs that secure virtual machines 232A may access. For example, a secure virtual machine 232C may be able to access one or more company resources, while the unsecure virtual machine 232B may not be allowed to access certain company resources. (Singh, [0096]).

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference

Art Unit: 2492

claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP §§ 706.02(I)(1) - 706.02(I)(3) for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claims 1-20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 10554475, and over claims 1-20 of U.S. Patent

Art Unit: 2492

No. 10558798. Although the claims at issue are not identical, they are not patentably distinct from each other because all elements of claims 1-20 of the instant application correspond to elements of claims 1-20 of the cited patents. The above claims of the present application would have been obvious over claims of the U.S. Patent No. 10554475, and over claims of U.S. Patent No. 10558798 because each element of the claims of the present application is anticipated by the claims of the U.S. Patent No. 10554475, and the claims of U.S. Patent No. 10558798 and as such are unpatentable for obviousness-type double patenting (*In re Goodman* (CAFC) 29 USPQ2D 2010 (12/3/1993)).

Claims 1-20 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claims of copending Applications No. 16/059381, 16/109275, 16/141,535, 16/138,696, 16/144,609, 16/144,761, 16/146,149, 16/142,810, 16/146,490, 16/163,796, 16/163,884, and 16/164,342. Although the claims at issue are not identical, they are not patentably distinct from each other because each element of the claims of the present application is anticipated by the claims of cited applications and as such are unpatentable for obviousness-type double patenting (*In re Goodman* (CAFC) 29 USPQ2D 2010 (12/3/1993)).

This is a provisional nonstatutory double patenting rejection because the patentably indistinct claims have not in fact been patented.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OLEG KORSACK whose telephone number is (571)270-1938. The examiner can normally be reached on 5:00 AM- 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571) 272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/OLEG KORSAK/

Primary Examiner, Art Unit 2492

<i>Notice of References Cited</i>	Application/Control No. 16/141,378		Applicant(s)/Patent Under Reexamination Coleman et al.	
	Examiner OLEG KORSAK		Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20130318594-A1	11-2013	Hoy; Robert B.	G06F21/53	726/15
*	B	US-20150156203-A1	06-2015	Giura; Paul	H04L67/02	726/4
*	C	US-20170034174-A1	02-2017	JAGERS; Stefan	H04L63/0281	1/1
*	D	US-20120054744-A1	03-2012	Singh; Manbinder Pal	G06F9/45558	718/1
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes 	Application/Control No. 16/141,378	Applicant(s)/Patent Under Reexamination Coleman et al.
	Examiner OLEG KORSAK	Art Unit 2492

CPC - Searched*		
Symbol	Date	Examiner
H04L63/0209 G06F9/45558 G06F21/53 H04L63/0236 H04L63/0281 H04L63/029 H04L63/145 H04L63/20 H04L67/10	05/19/2020	OK

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
H04L63/0209 G06F9/45558 G06F21/53 H04L63/0236 H04L63/0281 H04L63/029 H04L63/145 H04L63/20 H04L67/10	05/19/2020	OK
EAST search limited by keywords	05/19/2020	OK
GOOGLE NPL search	05/20/2020	OK

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/OLEG KORSAK/ Primary Examiner, Art Unit 2492	
--	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	39	((("L3") near3 ("TECHNOLOGIES") near3 ("INC"))).AS,AANM.	USPAT	OR	OFF	2020/05/19 05:43
L2	41	((("COLEMAN") near3 ("Glenn")) OR ((("MARTZ") near3 ("Peter"))) OR ((("MORITZ") near3 ("Kenneth"))).INV.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2020/05/19 05:44
L3	17	("20020069369" "20060070066" "20070220187" "20070260873" "20080028401" "20080201711" "20080256536" "20090172781" "20090328038" "20100138829" "20100138830" "20100223613" "20100251329" "20120023593" "7478330" "7698442" "7805516").PN.	US-PGPUB; USPAT	OR	OFF	2020/05/19 05:46
L4	83485	(H04L63/0209 G06F9/45558 G06F21/53 H04L63/0236 H04L63/0281 H04L63/029 H04L63/145 H04L63/20 H04L67/10).CPC.	US-PGPUB; USPAT	OR	OFF	2020/05/19 05:48

L5	2603	(internal NEAR2 firewall\$2)	US-PGPUB; USPAT	OR	OFF	2020/05/19 05:49
L6	2	L1 AND L5	US-PGPUB; USPAT	OR	OFF	2020/05/19 05:49
L7	13	L2 AND L5	US-PGPUB; USPAT	OR	OFF	2020/05/19 05:49
L8	0	L3 AND L5	US-PGPUB; USPAT	OR	OFF	2020/05/19 05:49
L9	866	L4 AND L5	US-PGPUB; USPAT	OR	OFF	2020/05/19 05:49
L10	1	L3 AND (protected NEAR2 memory)	US-PGPUB; USPAT	OR	OFF	2020/05/19 06:06

EAST Search History (Interference)

<This search history is empty>

5/19/2020 6:17:31 AM

C:\Users\okorsak\Documents\e-Red Folder\16\16141378 Coleman\16141378 Coleman.wsp



first proxy or the "second proxy" based on user-provided credentials.



Sign in

[All](#)
[Videos](#)
[News](#)
[Images](#)
[Shopping](#)
[More](#)
[Settings](#)
[Tools](#)

About 4,650 results (0.39 seconds)

[www.privateinternetaccess.com](#) > [helpdesk](#) > [articles](#) > [u...](#)

Understanding the Proxy Settings Feature - Knowledgebase ...

Dec 12, 2019 - The first Proxy that we provided our users the option to connect to directly ... Then fill out the username and password using your "X" credentials you ... The second Proxy connection that we provide our users is our ... Otherwise, use the Shadowsocks location closest to you based on the lowest latency.

[books.google.com](#) > [books](#)

Pro ASP.NET 2.0 in C# 2005 - Page 1206 - Google Books Result

NET and WS-Security can provide a more secure, robust approach than one an ... The first proxy class (which has the same name as the web service class) is the same as the ... The second proxy class has the suffix WSE appended to its class name. ... with your credentials using a single code statement: // Create the proxy.

Mario Szpuszta, Matthew MacDonald - 2006 - Computers

[books.google.com](#) > [books](#)

Pro ASP.NET 2.0 in C# 2005, Special Edition

NET and WS-Security can provide a more secure, robust approach than one an ... The first proxy class (which has the same name as the web service class) is the same as the ... The second proxy class has the suffix WSE appended to its class name ... with your credentials using a single code statement: // Create the proxy

Mario Szpuszta, Matthew MacDonald - 2007 - Computers

[books.google.com](#) > [books](#)

Pro ASP.NET 2.0 in VB 2005, Special Edition

The first proxy class (which has the same name as the web service class) is the same ... The second proxy class has the suffix WSE appended to its class name. ... so that it uses the EmployeeServiceWse proxy Provided you've taken those steps, you ... With your credentials using a single code statement: Create the proxy.

Laurence Moroney, Matthew MacDonald - 2007 - Computers

[success.thousandeyes.com](#) > [PublicArticlePage](#)

Configuring an Enterprise Agent to use a proxy server ...

Jul 1, 2019 - This article provides background information on web proxy servers, and steps to ... the Internet should first read the ThousandEyes Knowledge Base article ... and port number, and (if required) user credentials, are called explicit proxies. ... If so, a second proxy IP address (or hostname) and port is required.

[www.websense.com](#) > [deployou](#) > [dic_wsg_deploy_spec](#)

Special Content Gateway deployment scenarios - Forcepoint

A highly available Web proxy provides continuous, reliable system operation. Minimizing system downtime increases user access and productivity. ... The configuration can be accomplished manually, or via a PAC file or a WPAD server. ... A second proxy, the standby, assumes the virtual IP address and handles network ...

[tools.ietf.org](#) > [html](#) > [draft-khartabil-sip-auth-analysis-00](#)

draft-khartabil-sip-auth-analysis-00 - Analysis: HTTP ...

The Session Initiation Protocol (SIP) [1] provides a stateless, challenge-based mechanism ... i.e. the first proxy challenges, user provide correct authentication. ... how does the second proxy know that the credentials in the request are not for it?

[github.com](#) > [microsoft](#) > [vscode](#) > [issues](#)

Help Wanted: Proxy testing - Issue #18103 - microsoft/vscode ...

Jan 4, 2017 - Users behind proxies have had a tough time lately, and we want to make ... restriction, it's more efficient to use the first proxy where it's less strict ... Without providing credentials (only proxy server URL) ... Here is re-test using the Network interface given by the OS on the second proxy (the problematic one).

www.istl.org > 99-spring > article3 ▾

You Can't Get There from Here

Information concerning IP filtering, proxy servers, dissemination of passwords, web certificates ...
Early evidence of this document's success can be seen from the official ... Credential-based authentication involves providing the end user with a ... to establish a second proxy server for unique resources would mean that users ...
by D Krieb - 1999 - Cited by 17 - Related articles

www.google.com > patents

WO2015042546A1 - Web-based single sign-on with form-fill ...

Web-based single sign-on with form-fill proxy application ... Single sign-on (SSO) can provide a user with access to multiple systems and ... In some embodiments, a second proxy can receive the tunneled request and extract the ... least a portion of the credential and reformat the response based on the first interface before ...

Ad · www.oxylabs.io/ ▾

Best Proxy Provider 2020 | Residential Proxy Network

City Level Locations, In-House Rotation, Low Fail Rate And 24/7 Support. Easy To Integrate, In-House Rotation, Low Fail Rate, Uptime & Support Guaranteed. Low Latency. 100+ Worldwide Locations. 99% Uptime Guarantee. 60M+ Residential IPs. Unlimited Bandwidth.

Ad · www.luminati.io/business-proxy/free-trial ▾

Business Proxy Service | 72 Million Residential IPs

Proxy service for business. Without Luminati you will get blocked or misled! Try our proxy manager with automated rules for IP rotation or long session dedicated IPs.
Pricing · Mobile proxy IPs · IP Locations · Contact us · Rotating Backconnect IPs
Deal: 50% off Residential Plan

Ad · www.proxyway.com/ ▾

Top 3 Best Proxy Services | Best Proxy Providers For 2020

Compare The Best Residential Proxy Providers From Our List. Choose The Right One For You! Find Ideal For You. Detailed Reviews. Top Proxy Providers. Types: Residential Proxies, Shared Proxies, Private Proxy
Compare Proxy Providers · Best Residential Proxies · Proxy Market Research '20

Searches related to first proxy or the "second proxy" based on user-provided credentials.

- 🔍 pia squid proxy

🔍 what is pia proxy

🔍 connect failed unknown host pr...

🔍 pia pptp/l2tp/socks

🔍 vpn with socks5

🔍 log in to private internet access
- 🔍 net pia

🔍 pia vpn sign up

🔍 pia logging

🔍 private internet access vpn free ...

🔍 pia vpn premium account

🔍 pia india server

Fairfax County, Virginia · From your internet address · Use precise location · Learn more

Help · Send feedback · Privacy · Terms

Bibliographic Data

Application No: 16/141,378

Foreign Priority claimed: ☐ Yes ☒ No

35 USC 119 (a-d) conditions met: ☐ Yes ☒ No ☐ Met After Allowance

Verified and Acknowledged: /OLEG KORSAK/

Examiner's Signature

Initials

Title: NETWORK ISOLATION WITH CLOUD NETWORKS

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/25/2018	726	2492	LCOM_ENT_CLOUD_US01
RULE			

APPLICANTS

L3 Technologies, Inc., New York, NY, UNITED STATES

INVENTORS

Glenn Coleman Berwyn, PA, UNITED STATES

Peter Martz Marlton, NJ, UNITED STATES

Kenneth Moritz Lansdowne, PA, UNITED STATES

CONTINUING DATA

This application has PRO of 62563237 09/26/2017

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

10/16/2018

STATE OR COUNTRY

UNITED STATES

ADDRESS

Condo Roccia Koptiw LLP

1800 JFK Boulevard

Suite 1700

Philadelphia, PA 19103

UNITED STATES

FILING FEE RECEIVED

\$1,720

Substitute for 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>				Complete if Known	
				Application Number	16/141,378
				Filing Date	September 25, 2018
				First Named Inventor	Coleman, Glenn
				Art Unit	2491
Examiner Name	PATEL, ASHOKKUMAR B				
Sheet	1	of	2	Attorney Docket Number	LCOM_ENT_CLOUD_US01

U. S. PUBLICATION AND PATENT DOCUMENTS				
Examiner Initials	Cite No.	Document Number	Publication or Grant Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
		Number – Kind Code (if known)		
	1	7,478,330 B1	01-13-2009	Branson et al.
	2	7,698,442 B1	04-13-2010	Krishnamurthy et al.
	3	7,805,516 B2	09-28-2010	Kettler et al.
	4	2002/0069369 A1	06-06-2002	Tremain et al.
	5	2006/0070066 A1	03-30-2006	Grobman, Steven L.
	6	2007/0220187 A1	09-20-2007	Kates, Lawrence
	7	2007/0260873 A1	11-08-2007	Hatfalvi et al.
	8	2008/0028401 A1	01-31-2008	Geisinger, Nile Josiah
	9	2008/0201711 A1	08-21-2008	Amir Husain, Syed M.
	10	2008/0256536 A1	10-16-2008	Zhao et al.
	11	2009/0172781 A1	07-02-2009	Masuoka et al.
	12	2009/0328038 A1	12-31-2009	Yamada et al.
	13	2010/0138829 A1	06-03-2010	Hanquez et al.
	14	2010/0138830 A1	06-03-2010	Astete et al.
	15	2010/0223613 A1	09-02-2010	Schneider, James P.
	16	2010/0251329 A1	09-30-2010	Wei, Coach
	17	2012/0023593 A1	01-26-2012	Puder et al.

FOREIGN PATENT DOCUMENTS					
Examiner Initials	Cite No.	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T
		Country Code- Number - Kind Code (if known)			
	18	RU 2406138 C1	12-10-2010	Samsung Electronics Co., Ltd.	X

Examiner Signature	/OLEG KORSAK/	Date Considered	05/18/2020
--------------------	---------------	-----------------	------------

Substitute for 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>				Complete if Known	
				Application Number	16/141,378
				Filing Date	September 25, 2018
				First Named Inventor	Coleman, Glenn
				Art Unit	2491
Examiner Name	PATEL, ASHOKKUMAR B				
Sheet	2	of	2	Attorney Docket Number	LCOM_ENT_CLOUD_US01

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author, title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), Volume-issue Number(s), publisher, city and/or country where published.	T
	19	BARNET, MARK, "Praktikum Po Zashite Seti Kompanii", Windows IT Pro/RE, November-December 2006, pp. 79-81	
	20	BURNETT, MARK, "How I Secured One Company's Network", Using Log Parser, Virtualization, and A Little Psychology, September 17, 2006, 4 pages	
	21	LAVERICK, MIKE, "Hypervisor Management and Optimization for Advanced Virtualization", E-book, TechTarget, 2010, 13 pages	
	22	LI et al., "VSITE: A Scalable and Secure Architecture for Seamless L2 Enterprise Extension in the Cloud", 6th IEEE Workshop on Secure Network Protocols (NPsec), October 2010, pp. 31-36	
	23	REUBEN, JENNI SUSAN, "A Survey on Virtual Machine Security", TKK T-110.5290 Seminar on Network Security, October 11-12, 2007, 5 pages	
	24	VILLENEUVE, NART, "Command and Control in the Cloud", Malware Explorer, October 22, 2010, 3 pages	
	25	WIKIPEDIA, "Computer Networking", Available at https://en.wikipedia.org/wiki/Computer_network , December 2010, 19 pages	
	26	WIKIPEDIA, "Computer Security", Available at https://en.wikipedia.org/wiki/Computer_security , retrieved on December 2010, 27 pages	
	27	WIKIPEDIA, "Cyber Security Standards", Available at https://en.wikipedia.org/wiki/Cyber_security_standards , retrieved on December 2010, 9 pages	
	28	WIKIPEDIA, "HTTP Secure", Available at https://en.wikipedia.org/wiki/HTTPS , retrieved on December 2010, 9 pages	
	29	WIKIPEDIA, "Hypervisor", Available at https://en.wikipedia.org/wiki/Hypervisor , retrieved on December 2010, 6 pages	
	30	WIKIPEDIA, "Internet Protocol", Available at https://en.wikipedia.org/wiki/Internet_Protocol , retrieved on December 2010, 5 pages	
	31	WIKIPEDIA, "Multiprotocol Label Switching", Available at https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching , retrieved on December 2010, 8 pages	
	32	WIKIPEDIA, "Network Address Translation", Available at https://en.wikipedia.org/wiki/Network_address_translation , December 2010, 12 pages	
	33	WIKIPEDIA, "Security-Focused Operating System", Available at https://en.wikipedia.org/wiki/Security-focused_operating_system , retrieved on December 2010, 9 pages	
	34	WIKIPEDIA, "Virtual Desktop", Available at https://en.wikipedia.org/wiki/Virtual_desktop , retrieved on December 2010, 5 pages	
	35	WIKIPEDIA, "Virtual Private Network", Available at https://en.wikipedia.org/wiki/Virtual_private_network , retrieved on December 2010, 9 pages	

Examiner Signature	/OLEG KORSACK/	Date Considered	05/18/2020
--------------------	----------------	-----------------	------------

DOCKET NO.: LCOM_ENT_CLOUD_US01
Application No.: 16/141,378
Office Action Dated: May 21, 2020

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
L3 Technologies, Inc.

Confirmation No.: 2440

Application No.: 16/141,378

Group Art Unit: 2492

Filing Date: September 25, 2018

Examiner: KORSAK, OLEG

For: NETWORK ISOLATION WITH CLOUD NETWORKS

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

REPLY PURSUANT TO 37 CFR § 1.111

In response to the Official Action dated **May 21, 2020**, reconsideration is respectfully requested in view of the amendments and/or remarks as indicated below:

- ☐ **Amendments to the Specification** begin on page N/A of this paper.
- ☒ **Amendments to the Claims** are reflected in the listing of the claims which begins on page 2 of this paper.
- ☐ **Amendments to the Drawings** begin on page N/A of this paper and include an attached replacement sheet.
- ☒ **Remarks** begin on page 7 of this paper.
- ☒ The Commissioner is hereby authorized to charge any fee deficiency, charge any additional fees, or credit any overpayment of fees, associated with this application in connection with this filing, or any future filing, submitted to the U.S. Patent and Trademark Office during the pendency of this application, to Deposit Account No. 50-5519.

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A host computer system comprising ~~a processor and memory, the processor configured to:~~

a memory; and

a processor configured to:

implement a workspace, wherein the workspace is configured to enable operation of a first set of one or more applications or processes via a first memory space;

implement an isolated computing environment, the isolated computing environment using an operating system associated with the host computing system and comprising a sandboxed computing environment being configured to enable operation of a second set of one or more applications or processes via a second memory space, wherein the isolated computing environment is configured to access an Internet-based cloud service via at least one application of the second set of one or more applications or processes;

isolate the isolated computing environment from the workspace using an internal isolation firewall; and

communicate with ~~at least one~~ a proxy server in order to access the Internet-based cloud service, wherein the isolated computing environment is configured to authenticate with an authentication device in order to allow communication between the at least one application and the Internet-based cloud service.

2. (Currently Amended) The host computer system of claim 1, wherein the processor is configured to access the Internet-based cloud service via one or more of a local area network (LAN), a wide area network (WAN), a cellular network, a Wi-Fi network, a digital subscribers line (DSL) network, a cloud computing network, a data center, or a satellite network.

3. (Currently Amended) The host computer system of claim 1, wherein the Internet-based cloud service comprises one or more of an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS).
4. (Currently Amended) The host computer system of claim 1, wherein the processor is configured to select the ~~at least one~~ proxy server from a plurality of ~~candidate~~ proxy servers, the plurality of proxy servers comprising one or more of at least one an Internet-based proxy server ~~or at least one~~ or a local network-based proxy server.
5. (Currently Amended) The host computer system of claim [[4]] 1, wherein the processor is configured to determine whether to send web traffic to [[the]] a local network-based proxy server or [[the]] an Internet-based proxy server based on a location of the host computer system.
6. (Currently Amended) The host computer system of claim [[4]] 1, wherein the processor is configured to determine whether to send web traffic to [[the]] a local network-based proxy server or [[the]] an Internet-based proxy server based on an identity of a network to which the host computer system is connected.
7. (Currently Amended) The host computer system of claim [[4]] 1, wherein the processor is configured to determine whether to send web traffic to [[the]] a local network-based proxy server or [[the]] an Internet-based proxy server based on [[the]] an identity of the at least one application running in the isolated computing environment.
8. (Currently Amended) The host computer system of claim 1, wherein the internal isolation firewall is configured to segregate the first memory space from the second memory space, and wherein the processor is configured to enforce policies for communication between the first memory space and the second memory space using the internal isolation firewall.

9. (Currently Amended) The host computer system of claim 8, wherein the internal isolation firewall is further configured to generate a message to prompt a user of the host computer system, the message indicating whether to allow communication between the first memory space and the second memory space.

10. (Currently Amended) A cloud computing system comprising:
a cloud computing network, ~~the cloud computing network comprising at least one server~~
a server, wherein the server ~~comprises~~ is configured to:

implement a workspace configured to enable operation of a first set of one or more applications or processes running in a workspace and;

implement an isolated computing environment comprising a sandboxed computing environment and being configured to enable operation of a second set of one or more applications or processes running in an isolated computing environment; and

isolate the isolated computing environment from the workspace using the server
~~comprises an internal isolation firewall to isolate the workspace from the isolated computing environment;~~ and

~~at least one~~ a proxy configured to control communication between the server and ~~at least one~~ an Internet resource, wherein the proxy is configured to allow communication between the second set of one or more applications or processes running in the isolated computing environment and the ~~at least one~~ Internet resource and to block communication between the first set of one or more applications or processes running in the workspace and the ~~at least one~~ Internet resource.

11. (Currently Amended) The cloud computing system of claim 10, wherein the server is configured to perform at least one processing task on behalf of a client device.

12. (Currently Amended) The cloud computing system of claim 11, wherein the proxy is a first proxy ~~at least one proxy comprises a first proxy and a second proxy~~, and the server is configured to determine whether to send traffic to the first proxy or ~~[[the]]~~ a second proxy.

13. (Currently Amended) The cloud computing system of claim 12, wherein the server is configured to determine whether to send traffic to the first proxy or the second proxy based on user-provided credentials.

14. (Currently Amended) The cloud computing system of claim 10, further comprising a border firewall configured to segregate the cloud computing network from one or more Internet destinations.

15. (Currently Amended) The cloud computing system of claim 10, wherein the internal isolation firewall is further configured to allow communication between the workspace and the isolated computing environment on a condition that the communication is in a predetermined format.

16. (Currently Amended) The cloud computing system of claim 11, wherein the server is further configured to receive input data from the client device and send one or more data communications to the client device.

17. (Currently Amended) The cloud computing system of claim 11, wherein the at least one processing task performed on behalf of the client device comprises a processing task for an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS).

18. (Canceled)

19. (Currently Amended) A method implemented in a host computer system ~~comprising a processor and a memory~~, the method comprising:

implementing a workspace, wherein the workspace is configured to enable operation of a first set of one or more applications or processes via a first memory space;

implementing an isolated computing environment, the isolated computing environment using an operating system associated with the host computer system and comprising a sandboxed computing environment being configured to enable operation of a second set of one or more applications or processes via a second memory space, wherein the isolated computing environment is configured to access an Internet-based cloud service via at least one application of the second set of one or more applications or processes;

isolating the isolated computing environment from the workspace using an internal isolation firewall; and

communicating with ~~at least one~~ a proxy server in order to access the Internet-based cloud service, wherein the isolated computing environment is configured to authenticate with an authentication device in order to allow communication between the at least one application and the Internet-based cloud service.

20. (Original) The method of claim 19, wherein the Internet-based cloud service comprises one or more of an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS).

REMARKS

Claims 1-17, 19, and 20 are pending in the application. Claims 1-17 and 19 have been amended. Claim 18 has been canceled. No claims have been added. No new matter has been added.

Rejections of claims 5-7 and 12 under 35 U.S.C. §112

Claims 5-7 and 12 were rejected under 35 U.S.C. §112 for allegedly being indefinite. Specifically, the Office Action alleges that the phrase “to determine whether to send web traffic to the local network-based proxy server or the Internet-based proxy server” is indefinite in claims 5-7 because it is not clear whether one or two servers are to be used.¹ The Office Action also indicates that the phrase “at least one proxy comprises a first proxy and a second proxy” is indefinite in claim 12 because it is not clear whether one or two servers are to be used.²

Without conceding the propriety of rejection, claims 5-7 and 12 have been amended. Accordingly, Applicant requests reconsideration and withdrawal of the rejections.

Double Patenting Rejections

Claims 1-20 are rejected under the judicially created doctrine of obviousness-type double patenting as allegedly being obvious over claims 1-20 of U.S. Patent No. 10,554,475 and over claims 1-20 of U.S. Patent No. 10,558,798.³ Claims 1-20 are also provisionally rejected under the judicially created doctrine of obviousness-type double patenting as allegedly being obvious over claims of various co-pending applications.⁴

Applicant requests that the Examiner hold the rejection of the pending claims in abeyance until the pending claims of the present application are allowed, as the pending claims may have been or may be amended in such a way as to render this rejection meaningless. Applicant asserts

¹ Office Action dated 05/21/2020 at pages 2-3.

² *Id.*

³ Office Action dated 05/21/2020 at pages 12-14.

⁴ *Id.*

that the present request is fully responsive to the non-statutory type double patenting rejections. And Applicant retains the right to file a terminal disclaimer at a later stage of prosecution.

Rejection of independent claims 1 and 19 under 35 U.S.C. §102

Claims 1, 2, 4-9, and 19 were rejected under 35 U.S.C. §102 for allegedly being unpatentable over Hoy.⁵ Applicant disagrees.

As amended, independent claim 1 recites implementing an “isolated computing environment using an operating system associated with the hosting computing system and comprising a sandboxed computing environment....” But Hoy fails to disclose or suggest either these features for at least two reasons.

First, Hoy does not disclose “a sandbox computing environment,” as claim 1 recites. In fact, Hoy is completely silent with respect to a sandbox computing environment and does not even mention the term “sandbox.” So, Hoy cannot be said to teach or suggest implementing an “isolated computing environment using an operating system associated with the hosting computing system and comprising a sandboxed computing environment...,” as recited in claim 1.

Second, Hoy does not teach or suggest an “isolated computing environment using an operating system associated with the hosting computing system,” as claim 1 recites. In rejecting claim 1, the Office Action cited Hoy’s disclosure of “[a]lso operating on the host computer is a hypervisor system that creates a virtual machine environment that is *separate* from the host computer’s operating system [...] This virtual machine has *a virtual guest operating system* on which a modified browser is run,” and alleged that this disclosure in Hoy was equivalent to the claimed “isolated computing environment.”⁶

But the cited portion states that the virtual machine environment uses a virtual guest OS that is *not* associated with a host OS architecture. In fact, Hoy states that the virtual guest OS is separate.⁷ Thus, Hoy fails to teach or suggest implementing an “isolated computing environment

⁵ U.S. Patent No. 9,942,198.

⁶ Office Action dated 05/21/2020 at pages 3-4.

⁷ Hoy at para. [0026].

using an operating system associated with the hosting computing system and comprising a sandboxed computing environment...,” as recited in claim 1.

Accordingly, claim 1 is patentable over Hoy for at least above reasons. Because claim 19 recites features that are similar to claim 1, claim 19 is also patentable over Hoy. And at least due to their dependence on respective independent claims 1 and 19, dependent claims 2, 4-9 are also patentable over Hoy.

Rejection of independent claim 10 under 35 U.S.C. §102

Claims 10, 11, and 14-18 were rejected under 35 U.S.C. §102 for allegedly being unpatentable over Giura.⁸ Applicant disagrees.

As amended, independent claim 10 recites, a server that is configured to “implement an isolated computing environment comprising a sandboxed computing environment” and “isolate the isolated computing environment from the workspace using an internal isolation firewall.” But Giura fails to teach or suggest these two features.

First, Giura does not teach or suggest implementing “an isolated computing environment comprising a sandboxed computing environment,” as recited in claim 10. In fact, Giura is completely silent with the term sandboxed, much less “an isolated computing environment comprising a sandboxed computing environment.” So Giura cannot be said to teach or suggest implementing “an isolated computing environment comprising a sandboxed computing environment,” as recited in claim 10.

Second, Giura does not teach or suggest isolating “the isolated computing environment from the workspace using an internal isolation firewall.” Although Giura may disclose a firewall, the firewall disclosed in Giura does not isolate a computing environment from a workspace.⁹ Rather, the firewall in Giura merely separates virtual browser servers from an enterprise network.¹⁰

⁸ U.S. Patent Pub. No. 2015/0156203.

⁹ See Giura at para. [0039]; FIG. 2.

¹⁰ Giura at para. [0039]; FIG. 2.

For example, FIG. 2 of Giura shows that the firewall in Giura merely separates the virtual browser server from an enterprise network. As stated in Giura, the firewall 124 “monitors and controls incoming and outgoing traffic.”¹¹ Giura further states that “[t]he firewall 124 may be utilized to keep ... the virtual browser servers 130 and 135 **separate from the rest of devices and information in the enterprise network 115.**”¹² That is, the firewall taught in Giura separates the virtual browser servers from the enterprise network.

But separating the virtual browser servers from the enterprise network is not the equivalent of isolating “the isolated computing environment from the workspace using an internal isolation firewall,” as recited in amended claim 10. In Giura, the firewall only handles enterprise network traffic, such as incoming and outgoing enterprise network traffic related to the virtual browser servers.¹³ The firewall disclosed in Giura does not address traffic between a computing environment and a workspace.¹⁴ Nor does the firewall in Giura isolate a computing environment from a workspace. So Giura cannot be said to teach or suggest isolating “the isolated computing environment from the workspace using an internal isolation firewall,” as claim 10 recites.

Accordingly, claim 10 is patentable over Giura for at least above reasons. At least due to their dependence, dependent claims 11 and 14-17 are also patentable over Giura.

Rejection of dependent claims under 35 U.S.C. §103

Claims 3, 12, 13, and 20 were rejected under 35 U.S.C. §103 for allegedly being unpatentable over various combinations of references. At least due to above reasons and at least due to their dependence on their respective independent claims, dependent claims 3, 12, 13, and 20 are also patentable over the cited references.

¹¹ *Id.*

¹² *Id.*

¹³ Giura at para. [0039]; FIG. 2.

¹⁴ *See id.*

DOCKET NO.: LCOM_ENT_CLOUD_US01
Application No.: 16/141,378
Office Action Dated: May 21, 2020

PATENT

CONCLUSION

Applicant submits that the present application is in condition for allowance and a Notice of Allowance is requested. Examiner Korsak is invited to call Applicant's undersigned representative to discuss the application should the Examiner determine that such a discussion may advance prosecution.

Date: August 14, 2020

/Jeung Huh/
Jeung (Jacob) Huh
Registration No. 76,913

Condo Roccia Koptiw LLP
1800 JFK Blvd., Suite 1700
Philadelphia, PA 19103
Telephone: (215) 558-5740
Facsimile: (215) 558-5676

Electronic Acknowledgement Receipt

EFS ID:	40284370
Application Number:	16141378
International Application Number:	
Confirmation Number:	2440
Title of Invention:	NETWORK ISOLATION WITH CLOUD NETWORKS
First Named Inventor/Applicant Name:	Glenn Coleman
Customer Number:	158266
Filer:	Jeung Huh/melissa overline
Filer Authorized By:	Jeung Huh
Attorney Docket Number:	LCOM_ENT_CLOUD_US01
Receipt Date:	14-AUG-2020
Filing Date:	25-SEP-2018
Time Stamp:	10:21:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		LCOM_ENT_CLOUD_US01_AS_ FILED_REPLY_TO_NFOA_DATE D_05_21_20.pdf	172630 5dffa55814c2711981913a518d8e20f1fa0 0de	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	11
Warnings:			
Information:			
Total Files Size (in bytes):		172630	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>			

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 16/141,378		Filing Date 09/25/2018		☐ To be Mailed	
ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO									
APPLICATION AS FILED - PART I									
		(Column 1)	(Column 2)						
FOR		NUMBER FILED	NUMBER EXTRA		RATE (\$)		FEE (\$)		
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A		N/A				
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))		N/A	N/A		N/A				
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A		N/A				
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 = *		x \$100 =					
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 = *		x \$460 =					
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).							
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))									
* If the difference in column 1 is less than zero, enter "0" in column 2.					TOTAL				
APPLICATION AS AMENDED - PART II									
		(Column 1)		(Column 2)	(Column 3)				
AMENDMENT	08/14/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	* 19	Minus	** 20	= 0	x \$100 =		0	
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	x \$460 =		0	
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE		0	
		(Column 1)		(Column 2)	(Column 3)				
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	x \$0 =			
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x \$0 =			
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE			
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.						LIE			
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".						/DORIS M KING/			
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".									
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.									

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/141,378	09/25/2018	Glenn Coleman	LCOM_ENT_CLOUD_US01	2440
158266	7590	09/09/2020	EXAMINER	
Condo Roccia Koptiw LLP			KORSAK, OLEG	
1800 JFK Boulevard				
Suite 1700				
Philadelphia, PA 19103				
			ART UNIT	PAPER NUMBER
			2492	
			MAIL DATE	DELIVERY MODE
			09/09/2020	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

Response to Amendment

This action is in response to amendment filed August 14, 2020 for the application # 16/141,378 filed on September 25, 2018. Claims 1-17, 19 and 20 are pending and are directed toward NETWORK ISOLATION WITH CLOUD NETWORKS.

Any claim objection/rejection not repeated below is withdrawn due to Applicant's amendment.

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Response to Arguments

Applicant's arguments with regards to claims 1-17, 19 and 20 have been fully considered, but they are moot because of new grounds of rejection. Further to keep the record clear, Examiner is responding to "not associated" argument:

"is not associated" **argument** – Applicant argues that the cited portion states that the virtual machine environment uses a virtual guest OS that is not associated with a host OS architecture. In fact, Hoy states that the virtual guest OS is separate. (Hoy at para. [0026]) Thus, Hoy fails to teach or suggest implementing an "isolated computing environment using an

Art Unit: 2492

operating system associated with the hosting computing system and comprising a sandboxed computing environment..." as recited in claim 1 (REMARKS, pages 8-9).

Response: According to cited by Applicant [0026] of Hoy "The browser is activated by a desk-top shortcut or application on the host system that allows the user to link to the isolated Internet access of the virtual guest system by launching the virtual guest web browser, which operates transparently to the user in the virtual guest system." Therefore at least "isolated computing environment using an operating system associated with the hosting computing system" was explicitly and clearly disclosed by Hoy.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-17, 19 and 20 are rejected under 35 U.S.C. 103 as being unpatentable over Hoy et al. (US 2013/0318594 Pub. Date: Nov. 28, 2013) in view of Comodo (Comodo Internet Security Software Version 7.0 User Guide Version 7.0.111114, 579 pages, 2014), hereinafter referred to as Hoy and Comodo respectively.

As per **claim 1**, Hoy teaches a host computer system comprising: a memory; and a processor (*a computerized work station comprises a computer operatively connected with one or*

more user-accessible data entry devices, a display device viewable by the user, and computer-accessible data storage, Hoy, [0022]) configured to:

implement a workspace, wherein the workspace is configured to enable operation of a first set of one or more applications or processes via a first memory space (*providing for the computer an operating system and one or more applications programs that run on said operating system, Hoy, [0022]);*

implement an isolated computing environment (*and supporting a virtual computer system operating on the computer. Hoy, [0022]*), the isolated computing environment using an operating system associated with the host computing system and comprising a sandboxed computing environment being configured to enable operation of a second set of one or more applications or processes via a second memory space (*Also operating on the host computer is a hypervisor system that creates a virtual machine environment that is separate from the host computer's operating system. This virtual machine has a virtual guest operating system on which a modified browser is run. Hoy, [0026]*),

wherein the isolated computing environment is configured to access an Internet-based cloud service via at least one application of the second set of one or more applications or processes (*The browser is activated by a desk-top shortcut or application on the host system that allows the user to link to the isolated Internet access of the virtual guest system by launching the virtual guest web browser, which operates transparently to the user in the virtual guest system. Hoy, [0026]*);

isolate the isolated computing environment from the workspace using an internal isolation firewall (*this is accomplished by providing a host computer that is surrounded by a host based firewall. Hoy, [0025]*); and

communicate with a proxy server in order to access the Internet-based cloud service (*Proxy content filter 4 may optionally be used to screen undesirable or inappropriate incoming or outgoing data, as above. Hoy, [0073]*), wherein the isolated computing environment is configured to authenticate with an authentication device in order to allow communication between the at least one application and the Internet-based cloud service (*To allow for this, the firewall 11 around the host OS 17 selectively enables the host OS 17 to access the Internet directly through ports 80 or 443, which are otherwise disabled, provided that the websites being accessed are on a white list of predetermined trusted sites with which the host OS 17 is permitted to communicate with. Hoy, [0057]*).

Hoy does **not** use term “sandbox”, although teaches that “Because it is exposed to potentially malicious software as it browses the Internet, the virtual guest system browser and its virtual operating system may be a hardened version that is exceptionally resistant to corruption, or it may have enhanced anomaly detection to aid in noting when dangerous data has been encountered by the browser. The virtual guest system also has no connection whatsoever to the LAN, and cannot access any address on the LAN.” Which is essentially a definition of sandboxed environment as known in the art. To exclude any doubt a secondary reference by Comodo is provided, which explicitly teaches a sandboxed computing environment (*An innovative sandboxed environment to run programs and browse the Internet isolated from your real computer. Comodo, page 10*). Comodo also explicitly teaches an Internet-based cloud service (*Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Comodo, page 553. See also Comodo Cloud - online file storage service. Backup your files to a*

highly secure online storage which can also be mounted as a virtual drive in your system.

Comodo, page 466)

Hoy in view of Comodo are analogous art to the claimed invention, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious to a person of ordinary skill in the art before the effective filing date of the claimed invention to modify Hoy in view of Comodo. This would have been desirable Applications and browsers running inside the virtual desktop leave no cookies or history behind on your real system, making it an extremely secure environment for Internet banking and online shopping (Comodo, pages 10-11).

As per **claim 2**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the processor is configured to access the Internet-based cloud service via one or more of a local area network (LAN), a wide area network (WAN), a cellular network, a Wi-Fi network, a digital subscribers line (DSL) network, a cloud computing network, a data center, or a satellite network (*The home system, when the host is "home" on the trusted LAN network, is allowed by the HBFW to communicate to other LAN resources as well as any whitelisted sites outside the LAN on the Internet. Hoy, [0062]*).

As per **claim 3**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the Internet-based cloud service comprises one or more of an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS) (*through Comodo's proprietary Directory Services Platform, Comodo, page 17*).

As per **claim 4**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the processor is configured to select the proxy server from a plurality of proxy servers, the plurality of proxy servers comprising one or more of an Internet-based proxy server or a local network-based proxy server (*A proxy/web-content filter 4 is connected with and cooperates with the firewall hardware 3 to control the type of data permitted to pass from the Internet 5 into the local system 1, filtering e.g., pornographic material or data not intended for the system 1, and*

also blocks communications from users on the LAN trying to reach disallowed sites, e.g., requests to access www.onlinecasino.com. Hoy, [0038]).

As per **claim 5**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the processor is configured to determine whether to send web traffic to a local network-based proxy server or an Internet-based proxy server based on a location of the host computer system (*Proxy content filter 4 may optionally be used to screen undesirable or inappropriate incoming or outgoing data, Hoy, [0073]).*

As per **claim 6**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the processor is configured to determine whether to send web traffic to a local network-based proxy server or an Internet-based proxy server based on an identity of a network to which the host computer system is connected (*Proxy content filter 4 may optionally be used to screen undesirable or inappropriate incoming or outgoing data, Hoy, [0073]).*

As per **claim 7**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the processor is configured to determine whether to send web traffic to a local network-based proxy server or an Internet-based proxy server based on an identity of the at least one application running in the isolated computing environment (*The virtual guest system 13 shows no software installed except for a browser and possibly some related supportive software, such as Adobe or Windows Media Player that cooperate with the browser when certain types of files are accessed on the Internet, and potentially an email program such as Microsoft Outlook for certain configurations. Hoy, [0048]).*

As per **claim 8**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the internal isolation firewall is configured to segregate the first memory space from the second memory space and is configured to enforce policies for communication between the first

Art Unit: 2492

memory space and the second memory space using the internal isolation firewall (*The guest computer and the host computer communicate with each other by a limited permissible internal host-based firewall in the host system that is provided by the hypervisor or some other local program. Communications across this internal firewall between the guest system and the host system are limited to cut and paste of displayed documents or files, commands to print documents, and file transfer requested manually by the host, Hoy, [0030]*).

As per **claim 9**, Hoy in view of Comodo teaches the host computer system of claim 8, wherein the internal isolation firewall is further configured to generate a message to prompt a user of the host computer system, the message indicating whether to allow communication between the first memory space and the second memory space (*i.e., directed intentionally by the human user of the given system. Hoy, [0030]*).

Claims 10, 11 and 14-20 have limitations similar to those treated in the above rejection, and are met by the references as discussed above, and are rejected for the same reasons of obviousness as used above. In regards to **claim 10**, “a server” is taught by Hoy (*A host computer supports a virtual guest system running thereon. ABSTRACT*), and by Comodo (*The Virtual Desktop creates a folder Shared Space in the location "C:\Documents and Settings\All Users\ApplicationData\Shared Space". The 'Shared Space' folder can be shared by your host operating system and the Virtual Desktop. Page 223*).

As per **claim 12**, Hoy in view of Comodo teaches the cloud computing system of claim 11, wherein the proxy comprises is a first proxy, and the server is configured to determine whether to send traffic to the first proxy or a second proxy, (*Proxy and Host Settings - Allows you to select the host from which updates are downloaded. By default, CIS will directly download updates from Comodo servers. However, advanced users and network admins may*

Art Unit: 2492

wish to first download updates to a proxy/staging server and have individual CIS installations collect the updates from there. The 'Proxy and Host Settings' interface allows you to point CIS at this proxy/staging server. Comodo, page 259).

Hoy in view of Comodo are analogous art to the claimed invention, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious to a person of ordinary skill in the art before the effective filing date of the claimed invention to modify Hoy in view of Comodo. This helps conserve overall bandwidth consumption and accelerates the update process when large number of endpoints are involved (Comodo, page 259).

As per **claim 13**, Hoy in view of Comodo teaches the cloud computing system of claim 12, wherein the server is configured to determine whether to send traffic to the first proxy or the second proxy based on user-provided credentials (*Select the 'Use Proxy' check-box. • Enter the host name and port numbers. If the proxy server requires access credentials, select the 'Use Authentication' check-box and enter the login / password accordingly. • You can add multiple servers from which updates are available. To do this, click the handle at the bottom center of the 'Servers' panel, click the 'Add' button then enter the host name in the 'Edit Property' dialog. Comodo, page 260).*

Hoy in view of Comodo are analogous art to the claimed invention, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious to a person of ordinary skill in the art before the effective filing date of the claimed invention to modify Hoy in view of Comodo. This helps conserve overall bandwidth consumption and accelerates the update process when large number of endpoints are involved (Comodo, page 259).

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or

Art Unit: 2492

improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP §§ 706.02(l)(1) - 706.02(l)(3) for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely

Art Unit: 2492

online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-l.jsp.

Claims 1-17, 19 and 20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 10554475, and over claims 1-20 of U.S. Patent No. 10558798. Although the claims at issue are not identical, they are not patentably distinct from each other because all elements of claims 1-17, 19 and 20 of the instant application correspond to elements of claims 1-20 of the cited patents. The above claims of the present application would have been obvious over claims of the U.S. Patent No. 10554475, and over claims of U.S. Patent No. 10558798 because each element of the claims of the present application is anticipated by the claims of the U.S. Patent No. 10554475, and the claims of U.S. Patent No. 10558798 and as such are unpatentable for obviousness-type double patenting (*In re Goodman* (CAFC) 29 USPQ2D 2010 (12/3/1993)).

Claims 1-17, 19 and 20 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claims of copending Applications No. 16/059381, 16/109275, 16/141,535, 16/138,696, 16/144,609, 16/144,761, 16/146,149, 16/142,810, 16/146,490, 16/163,796, 16/163,884, and 16/164,342. Although the claims at issue are not identical, they are not patentably distinct from each other because each element of the claims of the present application is anticipated by the claims of cited applications and as such are unpatentable for obviousness-type double patenting (*In re Goodman* (CAFC) 29 USPQ2D 2010 (12/3/1993)).

This is a provisional nonstatutory double patenting rejection because the patentably indistinct claims have not in fact been patented.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OLEG KORSACK whose telephone number is (571)270-1938. The examiner can normally be reached on 5:00 AM- 4:00 PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, SALEH NAJJAR can be reached on (571) 272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/OLEG KORSAK/
Primary Examiner, Art Unit 2492

<i>Notice of References Cited</i>	Application/Control No. 16/141,378		Applicant(s)/Patent Under Reexamination Coleman et al.	
	Examiner OLEG KORSAK		Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
	A					
	B					
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Comodo (Comodo Internet Security Software Version 7.0 User Guide Version 7.0.111114, 579 pages, 2014) (Year: 2014)
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes 	Application/Control No. 16/141,378	Applicant(s)/Patent Under Reexamination Coleman et al.
	Examiner OLEG KORSAK	Art Unit 2492

CPC - Searched*		
Symbol	Date	Examiner
H04L63/0209 G06F9/45558 G06F21/53 H04L63/0236 H04L63/0281 H04L63/029 H04L63/145 H04L63/20 H04L67/10	05/19/2020	OK
H04L63/0209 G06F9/45558 G06F21/53 H04L63/0236 H04L63/0281 H04L63/029 H04L63/145 H04L63/20 H04L67/10	09/07/2020	OK

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
H04L63/0209 G06F9/45558 G06F21/53 H04L63/0236 H04L63/0281 H04L63/029 H04L63/145 H04L63/20 H04L67/10	05/19/2020	OK
EAST search limited by keywords	05/19/2020	OK
GOOGLE NPL search	05/20/2020	OK
H04L63/0209 G06F9/45558 G06F21/53 H04L63/0236 H04L63/0281 H04L63/029 H04L63/145 H04L63/20 H04L67/10	09/07/2020	OK
Updated EAST search limited by keywords	09/07/2020	OK
GOOGLE NPL search	09/07/2020	OK

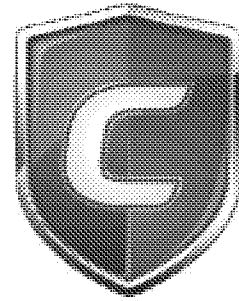
/OLEG KORSAK/ Primary Examiner, Art Unit 2492	
--	--

<i>Search Notes</i> 	Application/Control No. 16/141,378	Applicant(s)/Patent Under Reexamination Coleman et al.
	Examiner OLEG KORSAK	Art Unit 2492

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/OLEG KORSAK/ Primary Examiner, Art Unit 2492	
--	--

COMODO
Creating Trust Online®



Comodo Internet Security

Software Version 7.0

User Guide
Guide Version 7.0.111114

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

Table of Contents

1. Introduction to Comodo Internet Security	6
1.1. Special Features	10
1.2. System Requirements	14
1.3. Installation	14
1.3.1. CIS Premium - Installation	14
1.3.2. CIS Pro - Installation and Activation	31
1.3.3. CIS Complete - Installation and Activation	45
1.3.4. Activating CIS Pro/Complete Services after Installation	60
1.3.4.1. Activating Your License	60
1.3.4.2. Activating Your Guarantee Coverage	67
1.3.4.3. Renewal of Your License	70
1.4. Starting Comodo Internet Security	71
1.5. The Main Interface	73
1.5.1. The Home Screen	75
1.5.2. The Tasks Interface	85
1.5.3. The Widget	86
1.5.4. The System Tray Icon	87
1.6. Understanding Security Alerts	89
2. General Tasks - Introduction	108
2.1. Scan and Clean Your Computer	108
2.1.1. Run a Quick Scan	110
2.1.2. Run a Full Computer Scan	114
2.1.3. Run a Rating Scan	119
2.1.4. Run a Custom Scan	124
2.1.4.1. Scan a Folder	124
2.1.4.2. Scan a File	128
2.1.4.3. Create, Schedule and Run a Custom Scan	131
2.2. Instantly Scan Files and Folders	139
2.3. Processing Infected Files	144
2.4. Manage Virus Database and Program Updates	149
2.5. Manage Quarantined Items	152
2.6. View CIS Logs	156
2.6.1. Antivirus Logs	158
2.6.1.1. Filtering Antivirus Logs	159
2.6.2. Firewall Logs	163
2.6.2.1. Filtering Firewall Logs	165
2.6.3. Defense+ Logs	171
2.6.3.1. Filtering Defense+ Logs	172
2.6.4. 'Website Filtering' Logs	176
2.6.4.1. Filtering 'Website Filtering' Logs	177
2.6.5. 'Alerts' Logs	180
2.6.5.1. Filtering 'Alerts Displayed' Logs	181
2.6.6. Tasks	187
2.6.6.1. Filtering 'Tasks Launched' Logs	187

2.6.7.Configuration Changes.....	191
2.6.7.1.Filtering 'Configuration Changes' Logs.....	193
2.7.Get Live Support.....	197
2.8.View Active Internet Connections.....	197
2.9.View Active Process List.....	201
3.Firewall Tasks - Introduction.....	204
3.1.Allow or Block Internet Access to Applications Selectively	205
3.2.Stealth your Computer Ports	206
3.3.Manage Network Connections.....	208
3.4.Stop all Network Activities.....	209
3.5.Advanced Firewall Settings.....	209
4.Sandbox Tasks - Introduction	211
4.1.The Virtual Desktop.....	212
4.1.1.Starting the Virtual Desktop.....	213
4.1.2.The Main Interface.....	215
4.1.3.Running Browsers inside the Virtual Desktop.....	220
4.1.4.Opening Files and Running Applications inside the Virtual Desktop.....	221
4.1.5.Configuring the Virtual Desktop.....	222
4.1.6.Closing the Virtual Desktop.....	223
4.2.Run an Application in the Sandbox	224
4.3.Reset the Sandbox.....	228
5.Advanced Tasks - Introduction	230
5.1.Create a Rescue Disk	231
5.1.1.Downloading and Burning Comodo Rescue Disk.....	233
5.2.Remove Deeply Hidden Malware	237
5.3.Submit Files.....	240
5.4.Identify and Kill Unsafe Running Processes.....	242
5.5.Manage CIS Tasks.....	245
6.Advanced Settings.....	249
6.1.General Settings.....	251
6.1.1.Customize User Interface.....	251
6.1.2.Configure Program and Virus Database Updates.....	256
6.1.3.Log Settings.....	259
6.1.4.Manage CIS Configurations.....	261
6.1.4.1.Comodo Preset Configurations.....	261
6.1.4.2.Importing/Exporting and Managing Personal Configurations.....	262
6.2.Security Settings.....	270
6.2.1.Antivirus Settings.....	271
6.2.1.1.Real-time Scanner Settings.....	271
6.2.1.2.Scan Profiles.....	274
6.2.1.3.Exclusions.....	283
6.2.2.Defense+ Settings.....	300
6.2.2.1.HIPS Behavior Settings.....	301
6.2.2.2.Active HIPS Rules.....	307
6.2.2.3.HIPS Rule Sets.....	315
6.2.2.4.Protected Objects.....	318

6.2.2.4.1.Protected Files.....	319
6.2.2.4.2.Blocked Files.....	327
6.2.2.4.3.Protected Registry Keys.....	329
6.2.2.4.4.Protected COM Interfaces.....	335
6.2.2.4.5.Protected Data Folders.....	340
6.2.2.5.Behavior Blocker.....	343
6.2.2.5.1.The Sandbox - An Overview.....	349
6.2.2.5.2.Unknown File: The Auto-Sandboxing and Scanning Processes.....	350
6.2.2.6.Configure the Sandbox.....	352
6.2.3.Firewall Settings.....	363
6.2.3.1.Firewall Behavior Settings.....	364
6.2.3.2.Application Rules.....	369
6.2.3.3.Global Rules.....	383
6.2.3.4.Firewall Rule Sets.....	385
6.2.3.5.Network Zones.....	388
6.2.3.5.1.Network Zones.....	389
6.2.3.5.2.Blocked Zones.....	394
6.2.3.6.Port Sets.....	398
6.2.3.7.Website Filtering.....	402
6.2.3.7.1.Creating and Modifying Website Filtering Rules.....	403
6.2.3.7.2.Defining or Modifying Website Categories.....	413
6.2.4.Manage File Rating.....	420
6.2.4.1.File Rating Settings.....	421
6.2.4.2.Trusted Files.....	422
6.2.4.3.Unrecognized Files.....	424
6.2.4.4.Submitted Files.....	429
6.2.4.5.Trusted Vendors List.....	431
7.Comodo GeekBuddy.....	436
7.1.Overview of Services.....	437
7.2.Activation of Service.....	437
7.3.Launching the Client and Using the Service.....	441
7.4.Accepting Remote Desktop Requests.....	444
7.5.Chat History.....	446
7.6.Using Issue Tracker.....	448
7.7.Uninstalling Comodo GeekBuddy.....	452
8.TrustConnect Overview.....	453
9.Comodo Dragon.....	457
9.1.Introduction to PrivDog.....	459
9.1.1.Using PrivDog.....	459
9.1.2.PrivDog Settings Configuration.....	460
9.1.3.Threats.....	461
9.1.4.Exceptions.....	462
9.1.5.Preferences.....	463
10.Comodo BackUp.....	463
Appendix 1 - CIS How to... Tutorials.....	466
Enable / Disable AV, Firewall and Auto-Sandbox Easily.....	467

Set up the Firewall For Maximum Security and Usability.....	468
Block Internet Access while Allowing Local Area Network (LAN) Access	477
Block/allow Websites Selectively to Users of Your Computer.....	483
Set up the HIPS for Maximum Security and Usability.....	492
Set up the Behavior Blocker for Maximum Security and Usability.....	495
Password Protect Your CIS Settings	497
Reset Forgotten Password (Advanced).....	499
Run an Instant Antivirus Scan on Selected Items.....	502
Create an Antivirus Scanning Schedule.....	507
Run Untrusted Programs in the Sandbox.....	513
Run Browsers Inside Sandbox.....	516
Run Untrusted Programs Inside Virtual Desktop	517
Run Browsers Inside the Virtual Desktop.....	519
Restore Incorrectly Quarantined Item(s).....	521
Submit Quarantined Items to Comodo for Analysis.....	523
Enable File Sharing Applications like BitTorrent and Emule.....	526
Block any Downloads of a Specific File Type.....	532
Disable Behavior Blocker and Auto-Sandboxing on a Per-application Basis	535
Switch Between Complete CIS Suite and Individual Components (just AV or FW).....	537
Switch Off Automatic Antivirus and Software Updates.....	541
Suppress CIS Alerts Temporarily while Playing Games.....	545
Renew or Upgrade your License.....	546
How to use CIS Protocol Handlers	548
Appendix 2 - Comodo Secure DNS Service.....	551
Router - Manually Enabling or Disabling Comodo Secure DNS Service.....	551
Windows XP - Manually Enabling or Disabling Comodo Secure DNS Service.....	553
Windows 7 / Vista - Manually Enabling or Disabling Comodo Secure DNS Service.....	557
Appendix 3 - Glossary Of Terms.....	563
Appendix 4 - CIS Versions.....	576
About Comodo.....	577

1. Introduction to Comodo Internet Security

Overview

Comodo Internet Security offers 360° protection against internal and external threats by combining a powerful antivirus, an enterprise class packet filtering firewall and an advanced host intrusion prevention system called Defense+.

When used individually, each of the Antivirus, Firewall and Defense+ components delivers superior protection against their specific threat challenge. When used together as a full suite they provide a complete 'prevention, detection and cure' security system for your computer.



CIS is available in Premium (free), Pro and Complete editions. While the core CIS software is identical for all three versions, the Pro and Complete packages each offer a range of additional services. The software is designed to be secure 'out of the box' - so even the most inexperienced users need not have to deal with complex configuration issues after installation.

Comodo Internet Security - Key Features:

- **Antivirus** - Proactive antivirus engine that automatically detects and eliminates viruses, worms and other malware. Apart from the powerful on-demand, on-access and scheduled scan capabilities, CIS users can now simply drag-and-drop items onto the home screen to run an instant virus scan.
- **Firewall** - Highly configurable packet filtering firewall that constantly defends your system from inbound and outbound Internet attacks.
- **Defense+** - A collection of prevention based security technologies designed to preserve the integrity, security and privacy of your operating system and user data.
 - **Behavior Blocker** - Authenticates every executable and process running on your computer and prevents them from taking actions that could harm your computer. Unrecognized processes and applications will be

auto-sandboxed and run under a set of restrictions so they cannot harm your computer. This gives untrusted (but harmless) applications the freedom to operate whilst untrusted (and potentially malicious) applications are prevented from damaging your PC or data.

- **Host Intrusion Protection (HIPS)** - A rules-based intrusion prevention system that monitors the activities of all applications and processes on your computer. HIPS blocks the activities of malicious programs by halting any action that could cause damage to your operating system, system-memory, registry keys or personal data.
- **Viruscope** - Monitors the activities of processes running on your computer and alerts you if they take actions that could potentially threaten your privacy and/or security. Using a system of behavior 'recognizers', Viruscope not only detects unauthorized actions but also allows you to completely undo them. Apart from representing another hi-tech layer of protection against malware, this also provides you with the granular power to reverse unwanted actions taken by legitimate software without blocking the software entirely.
- **Virtual Desktop** - The Virtual Desktop is a sandboxed operating environment inside of which you can run programs and browse the Internet without fear that those activities will damage your real computer. Featuring a virtual keyboard to thwart key-loggers, home users will find the virtual desktop is ideally suited to sensitive tasks like online banking. Advanced users will appreciate the ability to run beta-software in an environment that will not upset the stability or file structure of their production systems
- **Website Filtering** - Protects you from phishing sites while surfing the 'net and allows you to create rules to prevent specific users from accessing certain websites. CIS ships with several preset lists of malicious websites which form an effective website screening and protection feature for all Internet users. Furthermore, you can easily add or import your own lists of banned URLs and can set up custom access rules for each user on your computer.
- **Rescue Disk** - Built-in wizard that allows you to burn a boot-disk which will run antivirus scans in a pre-Windows / pre-boot environment.
- **Additional Utilities** - The advanced tasks section contains links that allow you to install other, free, Comodo security products - including Comodo Cleaning Essentials and KillSwitch.
- **Comodo Dragon** - Fast and versatile Internet Browser based on Chromium, infused with Comodo's unparalleled level of Security.
- **GeekBuddy** - 24x7 online support service in which Comodo technicians are ready to deal with any computer issues you may have over an instant messenger style interface.
- **Secure Wireless Internet Connectivity (Complete version only)** - TrustConnect makes surfing the web safe from any public Wi-Fi location
- **Comodo Guarantee (Pro and Complete versions only)** - If your computer becomes damaged as a result of malware and Comodo support services cannot return it to a working condition then we'll pay the costs of getting it repaired. Please see the **End User License Agreement** for full details.
- **Online BackUp (Complete version only)** - Back-up your important data to Comodo's highly secure servers. Data is encrypted and can be accessed only by the user from any Internet connected computer in the world (50GB storage space).

Guide Structure

This introduction is intended to provide an overview of the basics of Comodo Internet Security and should be of interest to all users.

- Introduction
 - Special Features
 - System Requirements
 - Installation
 - CIS Premium - Installation
 - CIS Pro - Installation and Activation
 - CIS Complete - Installation and Activation
 - Activating CIS Pro/Complete Services after Installation
- Starting Comodo Internet Security
- The Main Interface
- Understanding Security Alerts

The remaining sections of the guide cover every aspect of the configuration of Comodo Internet Security.

- General Tasks - Introduction
 - Scan and Clean your Computer
 - Run a Quick Scan
 - Run a Full Computer Scan
 - Run a Rating Scan
 - Run a Custom Scan
 - Instantly Scan Files and Folders
 - Processing Infected Files
 - Manage Virus Database and Program Updates
 - Manage Quarantined Items
 - View CIS Logs
 - Manage CIS Tasks
 - View Active Internet Connections
- Firewall Tasks - Introduction
 - Allow or Block Internet Access to applications Selectively
 - Stealth your Computer Ports
 - Manage Network Connections
 - Stop all Network Activities
 - Advanced Firewall Settings
- Sandbox Tasks - An Introduction
 - The Virtual Desktop
 - Starting the Virtual Desktop
 - The Main Interface
 - Running Browsers inside the Virtual Desktop
 - Opening Files and Running Applications inside Virtual Desktop
 - Configuring the Virtual Desktop
 - Closing the Virtual Desktop
 - Run an Application in the Sandbox
 - Reset the Sandbox
- Advanced Tasks - An Introduction
 - Create a Rescue Disk
 - Downloading and Burning Comodo Rescue Disk
 - Remove Deeply Hidden Malware
 - Submit Files
 - Identify and Kill Unsafe Running Processes
- Advanced Settings
 - General Settings
 - Customize User Interface
 - Configure Program and Virus Database Updates
 - Log Settings
 - Manage CIS Configurations
 - Security Settings
 - Antivirus Settings
 - Real-time Scanner Settings
 - Scan Profiles

- Exclusions
- Defense+ Settings
 - HIPS Behavior Settings
 - Active HIPS Rules
 - HIPS Rule Sets
 - Protected Objects
 - Behavior Blocker
 - The Sandbox - An Overview
 - Unknown Files: The Sand-boxing and Scanning Processes
 - Configure the Sandbox
- Firewall Settings
 - Firewall Behavior Settings
 - Application Rules
 - Global Rules
 - Firewall Rule Sets
 - Network Zones
 - Port Sets
 - Website Filtering
- Manage File Rating
 - File Rating Settings
 - Trusted Files
 - Unrecognized Files
 - Submitted Files
 - Trusted Vendors List

The final sections contain configuration and technical help for GeekBuddy and TrustConnect.

- Comodo GeekBuddy
 - Overview of Services
 - Activation of Service
 - Launching the Client and Using the Service
 - Accepting Remote Desktop Requests
 - Chat History
 - Using Issue Tracker
 - Uninstalling Comodo GeekBuddy
- TrustConnect Overview
- Comodo Dragon
 - Introduction to PrivDog
- Comodo Backup
- Appendix 1 - CIS How to... Tutorials
 - Enable / Disable AV, Firewall and Auto-Sandbox Easily
 - Set up the Firewall For Maximum Security and Usability
 - Block Internet Access while Allowing Local Area Network (LAN) Access
 - Block/allow Websites Selectively to Users of Your Computer
 - Set up the HIPS for Maximum Security and Usability
 - Set up the Behavior Blocker for Maximum Security and Usability
 - Password Protect Your CIS Settings

- Reset Forgotten Password (Advanced)
- Run an Instant Antivirus Scan on Selected Items
- Create an Antivirus Scanning Schedule
- Run Untrusted Programs in the Sandbox
- Run Browsers inside Sandbox
- Run Untrusted Programs inside Virtual Desktop
- Run Browsers inside the Virtual Desktop
- Restore Incorrectly Quarantined Item(s)
- Submit Quarantined Items to Comodo for Analysis
- Enable File Sharing Applications like BitTorrent and Emule
- Block any Downloads of a Specific File Type
- Disable Behavior Blocker and Auto-Sandboxing on a per-application basis
- Switch Between Complete CIS Suite and Individual Components (just AV or FW)
- Switch Off Automatic Antivirus and Software Updates
- Suppress CIS Alerts Temporarily while Playing Games
- Renew or upgrade your License
- How To Use CIS Protocol Handlers
- Appendix 2 - Comodo Secure DNS Service
- Appendix 3 - Glossary of Terms
- Appendix 4 - CIS Versions

1.1. Special Features

Behavior Blocker

- Authenticates the integrity of every program before allowing it to load into your computer's memory
- Performs Cloud Based Behavior Analysis for immediate identification of Malware
- Alerts you every time an unknown or untrusted applications attempts to run or install
- Blocks Viruses, Trojans and Spy-ware before they can ever get onto your system
- Prevents unauthorized modification of critical operating system files and registry entries
- Detects suspicious actions taken by processes all allows you to undo them
- Includes auto-sandbox feature to completely isolate untrusted files from the rest of your computer

Host Intrusion Prevention System

- Virtually Bulletproof protection against root-kits, inter-process memory injections, key-loggers and more;
- Monitors the activities of all applications and processes on your computer and allows executables and processes to run if they comply with the prevailing security rules
- Blocks the activities of malicious programs by halting any action that could cause damage to your operating system, system-memory, registry keys or personal data.
- Enables advanced users to enhance their security measures by quickly creating custom policies and rulesets using the powerful rules interface.

Virtual Desktop

An innovative sandboxed environment to run programs and browse the Internet isolated from your real computer. Applications

and browsers running inside the virtual desktop leave no cookies or history behind on your real system, making it an extremely secure environment for Internet banking and online shopping.

- Prevents malicious websites from installing viruses malware, rootkits and spyware onto your computer and provides protection against hacking
- Features a virtual keyboard that allows you to securely enter user-names, credit card numbers and passwords without fear of key-logging software recording your physical keystrokes
- Enables advanced users to run beta-software in an environment that will not upset the stability or file structure of their production systems

Advanced Network Firewall Engine

The Firewall component of Comodo Internet Security offers the highest levels of perimeter security against inbound and outbound threats - meaning you get the strongest possible protection against hackers, malware and identity thieves. Now we've improved it again by adding new features like,

- Stealth Mode to make your PC completely invisible to opportunistic port scans;
- Wizard based auto-detection of trusted zones;
- Predefined Firewall policies allow you to quickly implement security rules;
- Diagnostics to analyze your system for potential conflicts with the firewall and much more;
- Website Filtering enables you to set up user based access restriction to specific websites.

Comprehensive Antivirus Protection

- Detects and eliminates viruses from desktops, laptops and network workstations;
- Performs Cloud based Antivirus Scanning;
- Employs heuristic techniques to identify previously unknown viruses and Trojans;
- Scans even Windows Registry and System Files for possible spyware infection and cleans them;
- Constantly protects with real-time, On-Access scanning;
- Comodo AV shows the percentage of the completed scanning;
- Rootkit scanner detects and identifies hidden malicious files and registry keys stored by rootkits;
- Highly configurable On-Demand scanner allows you to run instant checks on any file, folder or drive;
- Comodo AV realtime scanning performance in Stateful mode;
- Seamless integration into the Windows operating system allows scanning specific objects 'on the fly';
- Daily, automatic updates of virus definitions;
- Isolates suspicious files in quarantine preventing further infection;
- Built in scheduler allows you to run scans at a time that suits you;
- Simple to use - install it and forget it - Comodo AV protects you in the background.

Intuitive Graphical User Interface

- Advanced and Compact View summary screens gives an at-a-glance snapshot of your security settings;
- Easy and quick navigation between each module of the firewall, Antivirus and Defense+;
- Simple point and click configuration - no steep learning curves;
- New completely redesigned security rules interface - you can quickly set granular access rights and privileges on a global or per application. The firewall also contains preset policies and wizards that help simplify the rule setting process.

Comodo GeekBuddy (Pro, Complete versions only)

CIS Pro and Complete customers receive Comodo GeekBuddy - Live expert remote support for virtually all personal computer issues. Pro and Complete users benefit from the convenience of having a computer security expert on tap 24/7 to help them fix problems right in front of their eyes.

The services include:

- Virus & Malware Removal
- Internet and Online Identity Security

- Printer or Email Account Setup
- Software Activation
- General PC Troubleshooting
- Computer Power Setting Optimization
- Comodo Software Installation and Set up
- Comodo Account Questions.

Please visit <http://www.geekbuddy.com/> for full product details.

Note: To use the GeekBuddy service on a continuous basis, you have to purchase the product at <http://www.geekbuddy.com/>, register and activate your account.

Comodo TrustConnect

Included with a Complete subscription, Comodo TrustConnect is a fast, secure internet proxy service that makes surfing the web safe.

- At Coffee shops, Hotels and Airports;
- At any other public Wi-Fi location;
- At your home location;
- For Enterprises with remote workers and road-warriors that need secure access to internal networks.

Comodo Backup

CIS Complete customers receive Comodo Backup - powerful and easy to use desktop application that helps home and business users protect their valuable data against damage or loss.

- Quickly create backups of your priceless data to a wide range of storage media
- 50 GB of highly secure online storage space that allows you to access your files from anywhere
- Step-by-step wizards allow you to create your first backup within minutes
- Flexible storage options allow you to specify full, incremental or differential backups.
- Granular scheduling options to take automatic backups at a time that suits you.
- Quick recovery of files with a few clicks of the mouse.
- Powerful encryption options to protect your files so that it cannot be accessed by anyone but you.

Comodo Dragon

Fast and versatile Internet Browser based on Chromium, infused with Comodo's unparalleled level of Security.

- Improved Privacy over Chromium
- Easy SSL Certificate Identification
- Fast Website Access
- Greater Stability and Less Memory Bloat
- Incognito Mode Stops Cookies, Improves Privacy
- Very easy to switch from your Browser to the Dragon

Comodo Internet Security - Extended Features

Highly Configurable Security Rules Interface

Comodo Internet Security offers more control over security settings than ever before. Users can quickly set granular internet access rights and privileges on a global or per application basis using the flexible and easy to understand GUI. This version also sees the introduction of preset security policies which allow you to deploy a sophisticated hierarchy of firewall rules with a couple of mouse clicks.

Application Behavior Analysis

Comodo Internet Security features an advanced protocol driver level protection - essential for the defense of your PC against Trojans that run their own protocol drivers.

Cloud Based Behavior Analysis

Comodo Internet Security features cloud based analysis of unrecognized files, in which any file that is not recognized and not in Comodo's white-list will be sent to Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer in around 15 minutes.

Viruscope

The innovative Viruscope feature monitors the activities of all processes running on your system and generates alerts if any suspicious activities are identified. Apart from forming yet another layer of malware detection and prevention, the sub-system represents a valuable addition to the core process-monitoring functionality of the Behavior Blocker by introducing the ability to reverse potentially undesirable actions of software without necessarily blocking the software entirely. This feature can provide you with more granular control over otherwise legitimate software which requires certain actions to be implemented in order to run correctly.

Website Filtering

Comodo Internet Security enables you to configure rules to allow or block access to specific websites. Rules can be created for particular users of your computer, which makes this feature very useful for both home and work environments. For example, parents can block juvenile users from visiting inappropriate websites while companies can prevent employees from visiting social networking sites during working hours.

Event logging

Comodo Internet Security features a vastly improved log management module - allowing users to export records of Antivirus, Firewall and Defense+ activities according to several user-defined filters. Beginners and advanced users alike are greatly benefited from this essential troubleshooting feature.

Memory Firewall Integration

Comodo Internet Security now includes the buffer-overflow protection original featured in Comodo Memory Firewall. This provides protection against drive-by-downloads, data theft, computer crashes and system damage.

'Training Mode' and 'Clean PC' Mode

These modes enable the firewall and host intrusion prevention systems to automatically create 'allow' rules for new components of applications you have decided to trust, so you won't receive pointless alerts for those programs you trust. The firewall learns how they work and only warn you when it detects truly suspicious behavior.

Application Recognition Database (Extensive and proprietary application safe list)

The Firewall includes an extensive white-list of safe executables called the 'Comodo Safe-List Database'. This database checks the integrity of every executable and the Firewall alerts you of potentially damaging applications before they are installed. This level of protection is new because traditionally firewalls only detect harmful applications from a blacklist of known malware - often-missing new forms of malware as might be launched in day zero attacks.

The Firewall is continually updated and currently over 1,000,000 applications are in Comodo Safe list, representing virtually one of the largest safe lists within the security industry.

Self Protection against Critical Process Termination

Viruses and Trojans often try to disable your computer's security applications so that they can operate without detection. CIS protects its own registry entries, system files and processes so malware can never shut it down or sabotage the installation.

Sandboxing as a security feature

Comodo Internet Security's new 'Virtual Desktop' is an isolated operating environment for unknown and untrusted applications. Because they are virtualized, applications running in the sandbox cannot make permanent changes to other processes, programs or data on your 'real' system. Comodo have also integrated auto-sandboxing directly into the security architecture of CIS to complement and strengthen the Firewall, Defense+ and Antivirus modules.

Submit Suspicious Files to Comodo

Are you the first victim of a brand new type of spyware? Users can help combat zero-hour threats by using the built in submit feature to send files to Comodo for analysis. Comodo then analyzes the files for any potential threats and update our database

for all users.

Enhanced Browser Privacy

PrivDog, a new browser extension that can be installed with CIS, improves your online privacy by detecting and blocking any 3rd party trackers or ad networks that are monitoring your activity while on a website. Supported browsers include Comodo Dragon, Comodo Ice Dragon, Google Chrome and Mozilla Firefox.

1.2. System Requirements

To ensure optimal performance of Comodo Internet Security, please ensure that your PC complies with the minimum system requirements as stated below:

Windows 8 (Both 32-bit and 64-bit versions)	• 384 MB available RAM
Windows 7 (Both 32-bit and 64-bit versions)	• 210 MB hard disk space for both 32-bit and 64-bit versions
Windows Vista (Both 32-bit and 64-bit versions)	• Internet Explorer Version 5.1 or above
Windows XP (Both 32-bit and 64-bit versions)	• 256 MB available RAM
	• 210 MB hard disk space for both 32-bit and 64-bit versions
	• Internet Explorer Version 5.1 or above

1.3. Installation

Before you install Comodo Internet Security, read the installation instructions carefully and also review the system requirements. Additional services and features such as activation of your GeekBuddy account and/or Comodo Guarantee are carried out after the base installation has been completed.

Please note - the CIS software itself is identical for all customers regardless of the package type. All versions (including free) include all security features, technologies and updates. The difference between the package types lies in the availability of additional services such as GeekBuddy, TrustConnect, Online Storage and the Comodo Guarantee. Activation of additional services is carried out after the base installation has been completed.

Note - Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on your computer. More specifically, remove any other products of the same *type* as those Comodo products you plan to install. For example, if you plan to install only the firewall then you do not need to remove 3rd party antivirus solutions and vice-versa. If you are installing full CIS (both FW and AV) then you need to remove both types of product if they are present on your system. Failure to remove products of the same type could cause conflicts that mean CIS will not function correctly. Users should consult their vendor's documentation for precise uninstallation guidelines, however the following rough steps will help most Windows users:

- Click the Start button to open the Windows Start menu
- Select Control Panel > Programs and Features (Win 8, Win 7, Vista); Control Panel > Add or Remove Programs (XP)
- Select your current antivirus or firewall program(s) from the list
- Click Remove/Uninstall button
- Repeat process until all required programs have been removed

Click the links below for detailed explanations:

- [CIS Premium - Installation](#)
- [CIS Pro - Installation](#)
- [CIS Complete - Installation](#)

1.3.1. CIS Premium - Installation

Note - Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on

your computer. Click [here](#) to read the full note.

In order to install Comodo Internet Security - Premium, you need to download the setup file from <http://www.comodo.com/home/download/download.php?prod=cis>.

- Choose whether you want the 32 or 64 bit version of CIS then click 'download'
- If you are unsure which version you need, select the 32/64-bit Windows Installer. This executable contains BOTH 32 and 64 bit installers. The setup routine will automatically detect which version of Windows you have and install the appropriate version. Please note, the Universal Windows Installer is a much larger download than the individual 32 or 64 bit setup files.



After downloading the required Comodo Internet Security setup file to your local hard drive, double click on it to start the installation wizard.

Step 1 - Choosing the Interface Language

The installation wizard starts automatically and the 'Select the language' dialog is displayed. Comodo Internet Security is available in several languages.



- Select the language in which you want Comodo Internet Security to be installed from the drop-down menu and click 'OK'.

Step 2 - Installation Configuration

The installation configuration screen will be displayed.



- If you click 'Customize Installation' then you can choose advanced options. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

Receive Comodo News and Notifications

Comodo Internet Security Premium is activated free of cost for lifetime usage. If you wish to sign up for news about Comodo products then enter your email address in the space provided. This is optional.

Cloud Based Behavior Analysis

Any file that is identified as unrecognized is sent to the Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled. Read the privacy policy by clicking the 'Privacy Policy' link.

Send Program Usage Data

Comodo collects the usage details from millions of CIS users to analyze their usage patterns for the continual enhancement of the product. Your CIS installation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. Comodo recommends users leave this setting enabled. You can change this setting from **Advanced Settings > General Settings > Log Settings** interface, at anytime after installation.

- Please review and/or modify the settings in the dialog.
- Click the 'Next' button.

In the next screen, you can choose to configure your DNS Settings and Browser Home page.



DNS Settings

Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Comodo's worldwide network of redundant DNS servers provide fast and secure Internet browsing experience without any hardware or software installation.

In addition, Comodo's Secure DNS ensures safety against attacks in the form of malware, spyware, phishing etc., by blocking access to malware-hosting sites, by any program running in your system.

In this step of installation of Comodo Internet Security, the DNS settings of your computer can be changed automatically to direct to our DNS servers. You can disable the service at anytime and revert to your previous settings.

For more details on Comodo Secure DNS Service and to know how to enable or disable the service, refer to [Appendix 2 Comodo Secure DNS Service](#).

To enable Comodo Secure DNS, select 'I want to enable added security while in the internet by change my DNS Servers to COMODO SecureDNS Servers'. Click the 'What is this' link to know more about Comodo Secure DNS servers.

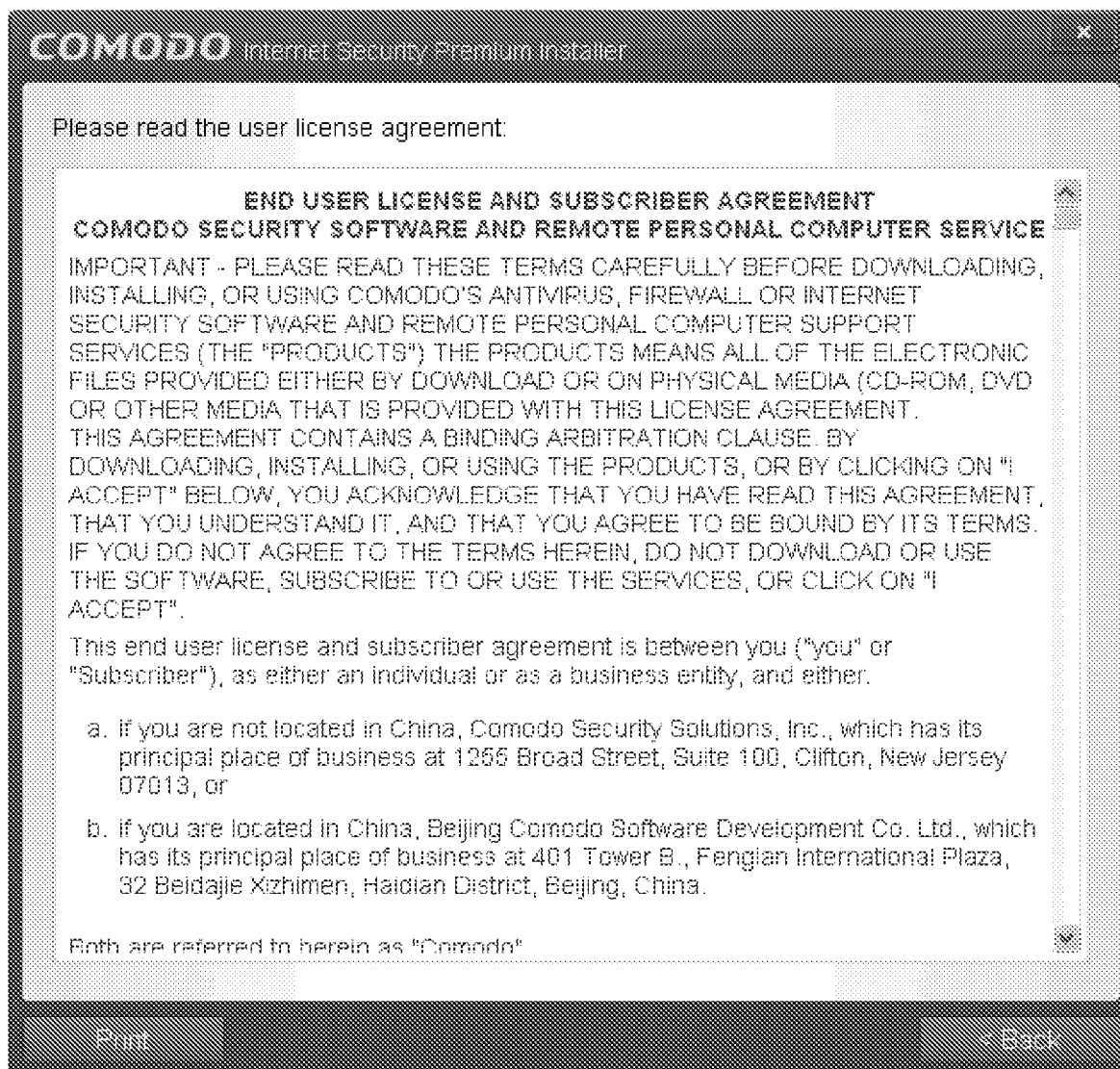
Browser Homepage

Your default home page and search engine will be set to Yahoo!

- Please review and/or modify the settings in the dialog.

End User License Agreements

- Read the complete User License Agreements by clicking the 'License Agreement' links of Comodo Internet Security and PrivDog respectively before proceeding with the installation. To read the PrivDog privacy policy link, click the Privacy Policy link next to it.



After reading the agreements, click the 'Back' button to return to the installation configuration screen.

Once back at the main installer screen, if you wish to configure advanced options, click 'Customize Installation'.

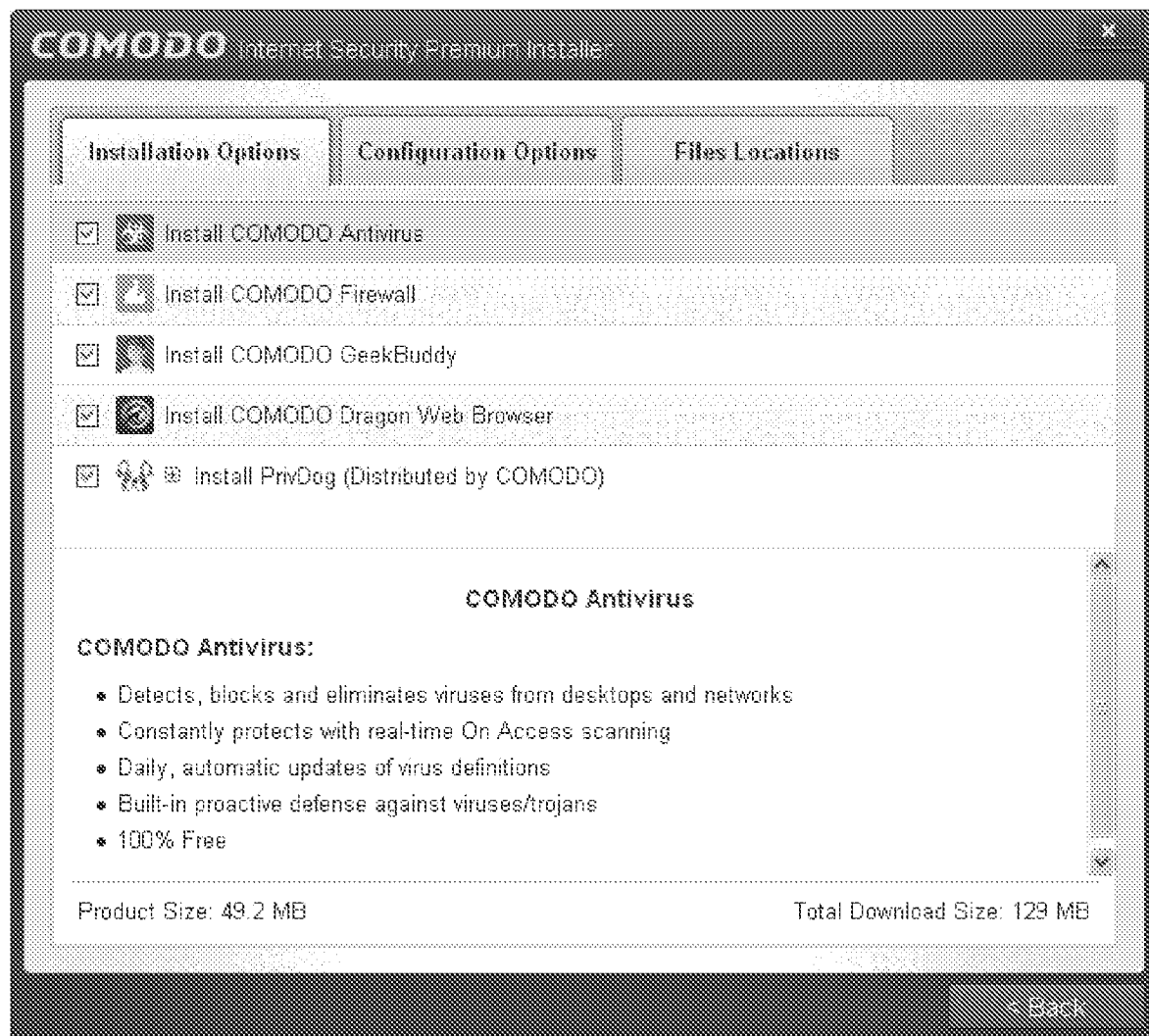
Otherwise, click 'Agree and Install' to begin installation.

Customizing Installation

Clicking the 'Customize Installation' link opens an advanced options interface that enables you to choose which elements you would like to install, configure security popup alerts and choose the installation path. In order to obtain maximum protection, Comodo recommends that you uninstall any third party personal Firewall and Antivirus in your system and select all the components to get the full benefit of the product.

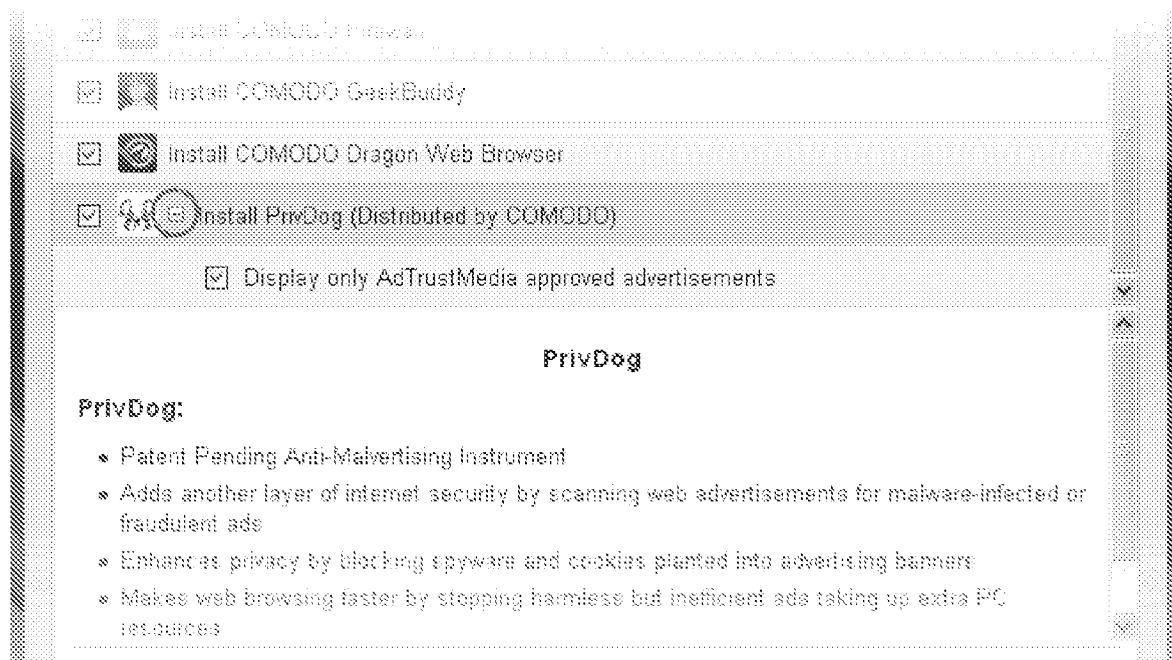
Select Components to Install (Click to go back to Step 2)

Click the 'Installation Options' tab to select the components to be installed.



- **Install COMODO Firewall** - Selecting this option installs Comodo Firewall and Defense+ components. Deselect this option, if you already have third party Firewall protection activated in your computer system. Comodo Firewall installation is mandatory to qualify for the virus free guarantee.
- **Install COMODO Antivirus** - Selecting this option installs Comodo Antivirus and Defense+ components. Deselect this option, if you already have a third party virus protection activated in your computer system. Comodo Antivirus installation is mandatory to qualify for the virus free guarantee.
- **Install COMODO GeekBuddy** - Selecting this option installs GeekBuddy, a 24 x 7 remote support service in which Comodo experts can help you solve any computer related problems you may encounter. Refer to the section Comodo GeekBuddy for more details.
- **Install COMODO Dragon Web Browser** - Selecting this option installs Comodo Dragon, a fast and versatile Internet browser based on Chromium technology and infused with Comodo's unparalleled level of security. Refer to the section Comodo Dragon for more details.
- **Install PrivDog** - PrivDog is a browser extension that improves the transparency, privacy and speed of your online experience by automatically detecting and blocking processes that are attempting to track your online activity. Whenever you visit a website, PrivDog will display the number of privacy threats it has blocked in the top-right corner of your browser. Clicking the PrivDog icon will reveal a more detailed breakdown of the types of threats it has stopped, which can include advertising networks, 3rd party trackers, cookies, widgets and other data collection processes. The extension can also block all current banner ads in a webpage and replace them with safe and trusted ads. If you elect to install PrivDog, the extension will be automatically installed in any supported browsers detected on your system (Comodo Dragon, Comodo IceDragon, Google Chrome and Mozilla Firefox). You can remove the extension at any time from within the browser itself. Refer to the section Introduction to PrivDog for more details.

- Select the checkbox 'Install PrivDog' if you want to install PrivDog.



- Click the '+' button beside 'Install PrivDog' and select the 'Display only AdTrustMedia approved advertisements' checkbox. If you choose to view only ads from AdTrustMedia in your browser.

Configuration Options

- Click the 'Configuration Options' tab to configure pop-up alert options.



- **Do Not show alerts that request security decisions as much as possible** - When this option is selected, CIS is configured to automatically deal with most issues in a secure manner without raising a popup alert - thus minimizing user intervention. Most users should leave this option at the default state of enabled. Advanced users wishing to gain greater insight into CIS actions and/or to have more control over security decisions may wish to disable this option.

Choosing Installation Location

Click the 'Files Locations' tab to choose the installation path.



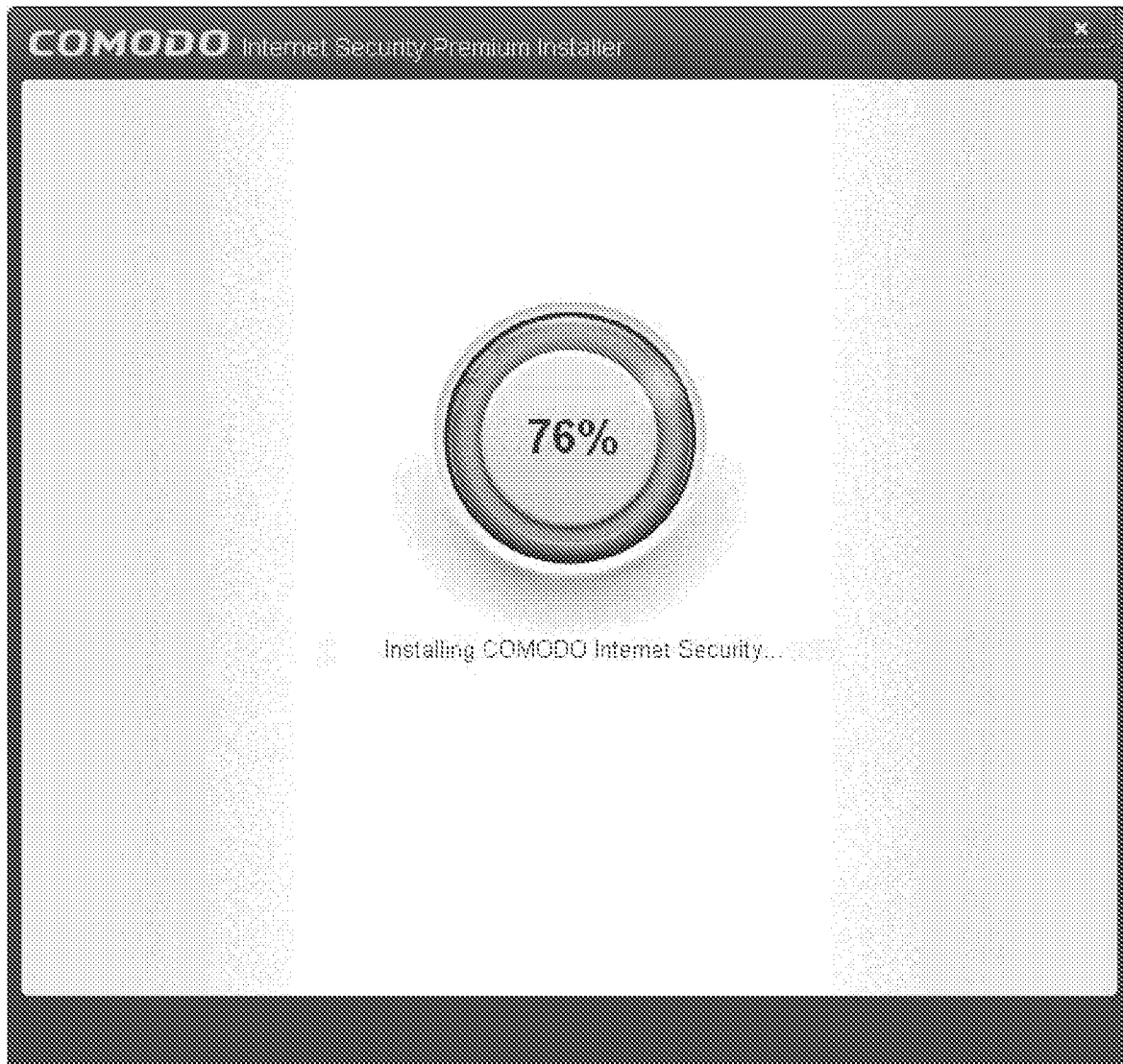
This screen allows you to select the folder in your hard drive for installing Comodo Internet Security. The default path is C:\Program Files\COMODO\COMODO Internet Security. If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

After customizing your installation, click the 'Back' button to return to the installation configuration screen.

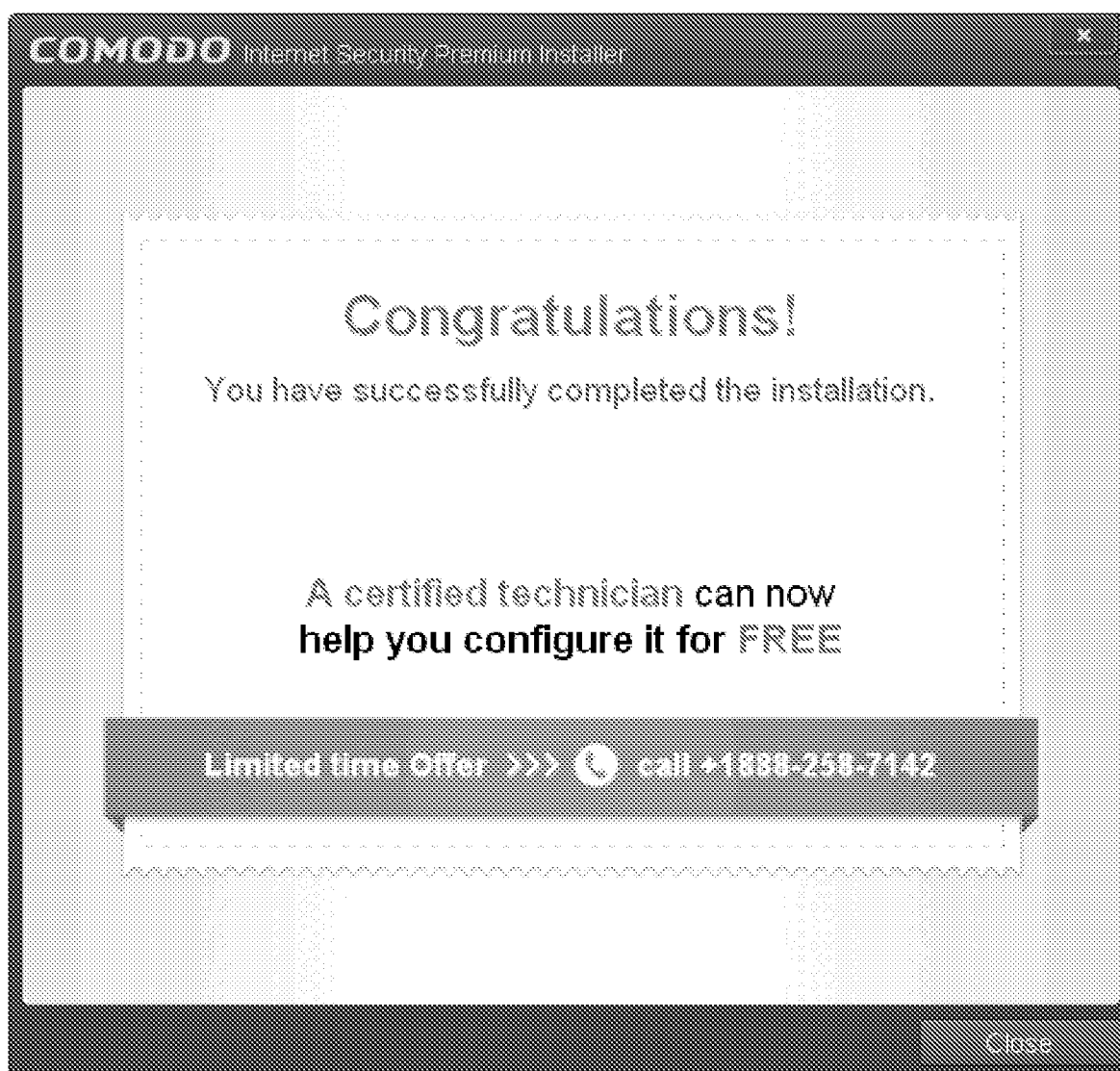
- Once you are satisfied with your settings, click 'Agree and Install' to begin installation (Click to go back to Step 2).

Step 3 - Installation Progress

The installation progress will be displayed...



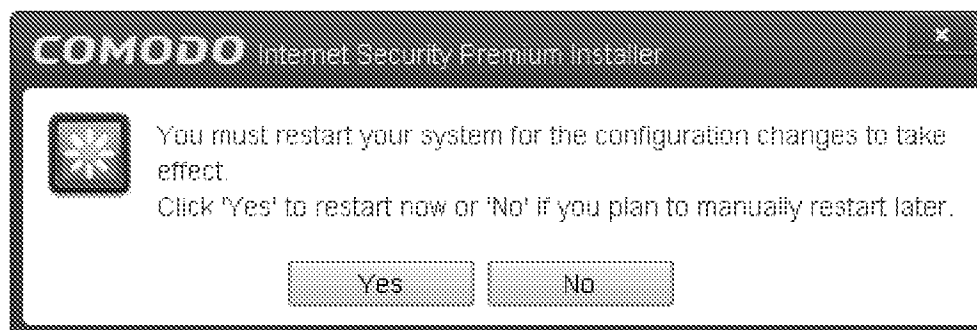
...and on completion, the successfully completed dialog will be displayed.



- Click the 'Close' button.

Step 4 - Restarting Your System

In order for the installation to take effect, your computer needs to be restarted.



Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

Note: The installation will take effect only on the next restart of the computer.

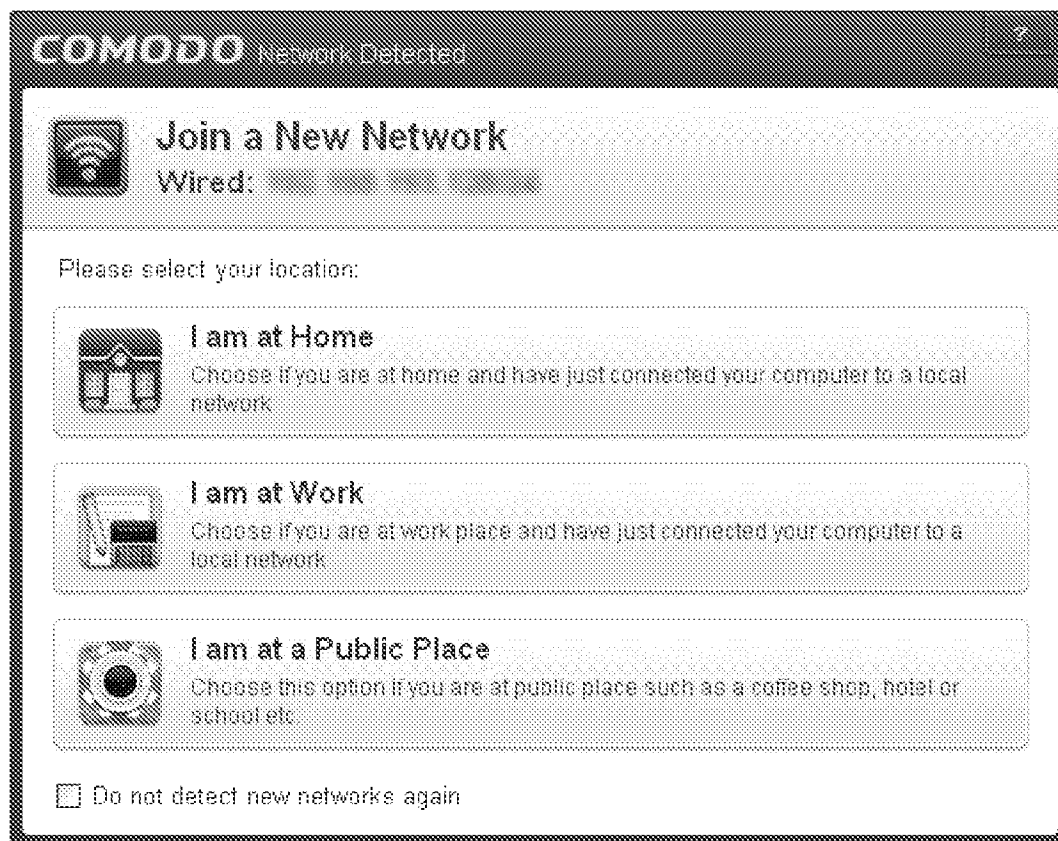
Step 5 - After Restarting Your System

After restarting, a 'thankyou' screen will appear. This contains a summary of the components you chose to install as well as some friendly advice.



This screen will appear every time you start your system. If you do not want the screen to be displayed on every start up, select the check box 'Do not show this window again' before closing the window.

If your computer is connected to a home or work network, then you are prompted to configure it at the 'Network Detected!' dialog. At the top of the dialog, the connectivity mode will be displayed, whether wired or wireless.



- Select your location from the three options above
- Select 'Do not automatically detect new networks' if you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in 'Network Zones' and through the 'Stealth Ports Wizard')

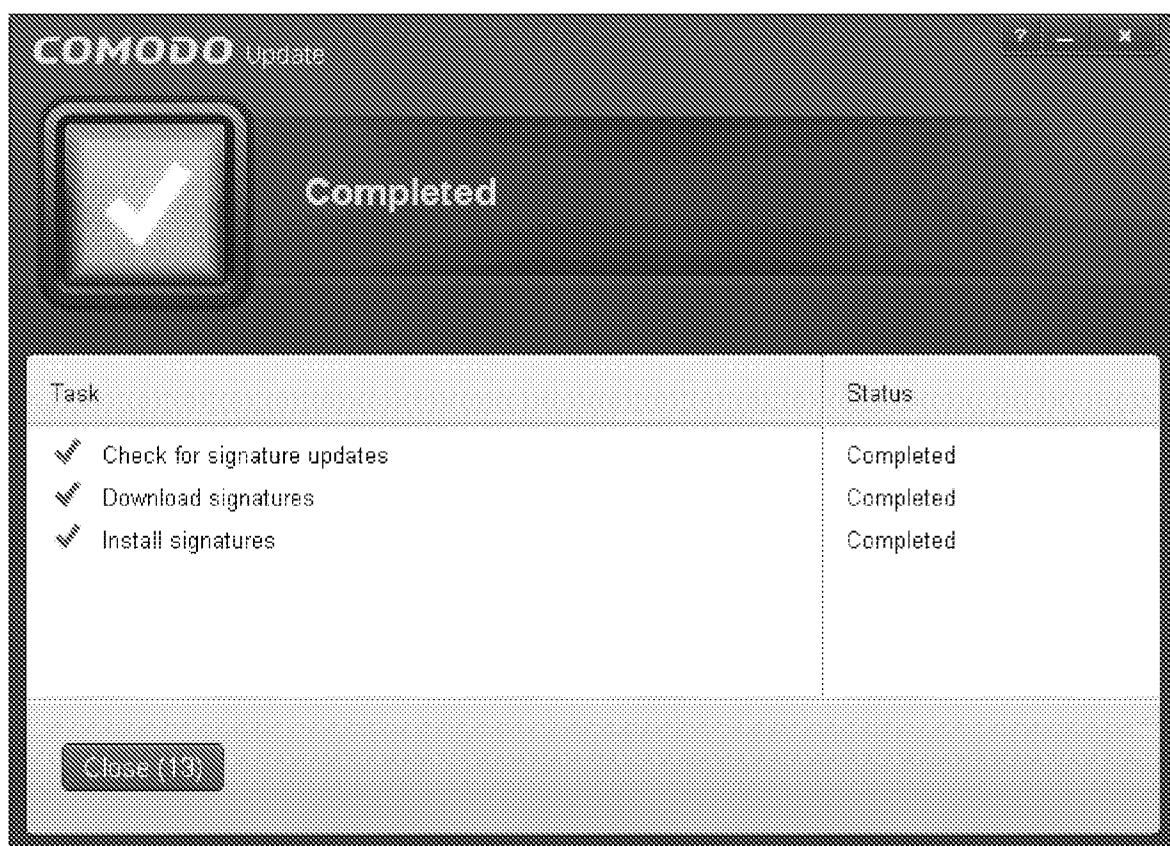
The CIS interface will open.



The virus database will be updated automatically for the first time after installation.



The screen will display details such as download speed, how much has been downloaded and the progress of the process. You can also send this task to the background by pressing the 'Send to Background' button and retrieve it in the 'Task Manager' interface. Refer to the section 'Manage CIS Tasks' for more details. When the virus database has been downloaded, the 'Completed' dialog will be displayed.

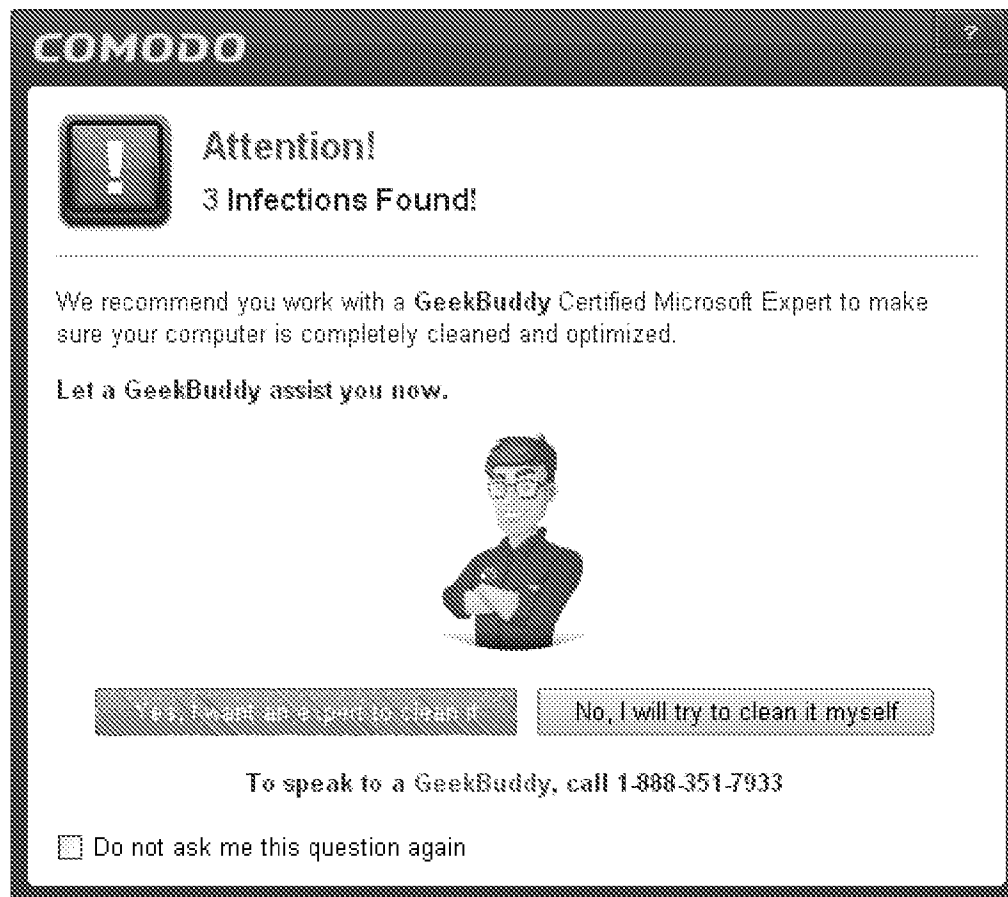


CIS will commence a Quick Scan of system memory, autorun entries, hidden services, boot sectors and other critical areas automatically after the virus database has been updated.



If you do not want the scan to continue at this time, click the 'Stop' button.

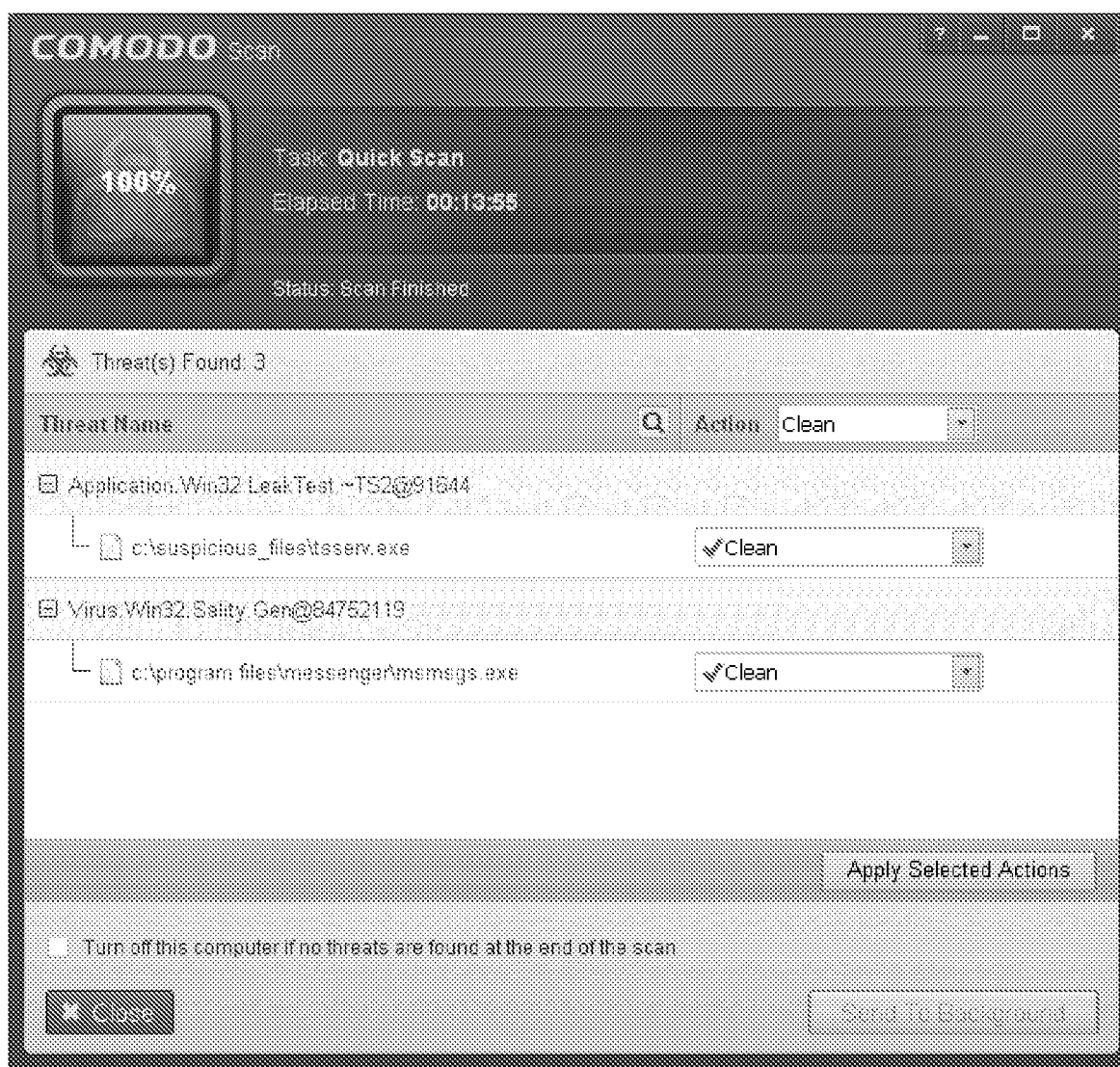
After the scanning is complete, and any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the GeekBuddy chat session will start and a skilled technician will offer to clean your system.

For more details on GeekBuddy, refer to the section [Comodo GeekBuddy](#).

- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed. The results will contain a list of files identified with threats or infections (Viruses, Rootkits, Malware and so on) and provide you the options for cleaning. An example results screen is shown below:



If any threats are detected, they will be displayed and you can choose to take appropriate action from any of the drop-down fields in the screen and click 'Apply Selected Actions' button. Refer to the section 'Processing Infected Files' for more details.

1.3.2. CIS Pro - Installation and Activation

Note - Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on your computer. [Click here to read the full note.](#)

Comodo Internet Security Pro can be downloaded from <http://www.comodo.com/home/download/download.php?prod=cis-pro> after signing up for subscription and includes, Comodo Dragon, GeekBuddy and the Comodo Guarantee.

- Choose whether you want the 32 or 64 bit version of CIS then click 'download'
- If you are unsure which version you need, select the 32/64-bit Windows Installer. This executable contains BOTH 32 and 64 bit installers. The setup routine will automatically detect which version of Windows you have and install the appropriate version. Please note, the Universal Windows Installer is a much larger download than the individual 32 or 64 bit setup files.

After downloading the required Comodo Internet Security setup file to your local hard drive, double click on the setup file to start the installation wizard.

Step 1 - Choosing the Interface Language

The installation wizard starts automatically and the 'Select the language' dialog is displayed. Comodo Internet Security is available in several languages.



- Select the language in which you want Comodo Internet Security to be installed from the drop-down menu and click 'OK'.

Step 2 - Installation Configuration

The installation configuration screen will be displayed.



- If you click 'Customize Installation' then you can choose advanced options. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

Receive Comodo News and Notifications

If you wish to sign up for news about Comodo products then enter your email address in the space provided. This is optional.

Cloud Based Behavior Analysis

Any file that is identified as unrecognized is sent to the Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled. Read the privacy policy by clicking the 'Privacy Policy' link.

Send Program Usage Data

Comodo collects the usage details from millions of CIS users to analyze their usage patterns for the continual enhancement of the product. Your CIS installation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. Comodo recommends users leave this setting enabled. You can change this setting from **Advanced Settings > General Settings > Log Settings** interface, at anytime after installation.

- Please review and/or modify the settings in the dialog.
- Click the 'Next' button.

In the next screen, you can choose to configure your DNS Settings and Browser Home page.



- If you click 'Customize Installation' then you can choose advanced options. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

DNS Settings

Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Comodo's worldwide network of redundant DNS servers provide fast and secure Internet browsing experience without any hardware or software installation.

In addition, Comodo's Secure DNS ensures safety against attacks in the form of malware, spyware, phishing etc., by blocking access to malware-hosting sites, by any program running in your system.

In this step of installation of Comodo Internet Security, the DNS settings of your computer can be changed automatically to direct to our DNS servers. You can disable the service at anytime and revert to your previous settings.

For more details on Comodo Secure DNS Service and to know how to enable or disable the service, refer to Appendix 2 Comodo Secure DNS Service.

To enable Comodo Secure DNS, select 'Change my DNS Servers to COMODO SecureDNS Servers. Click the 'What is this' link to know more about Comodo Secure DNS servers.

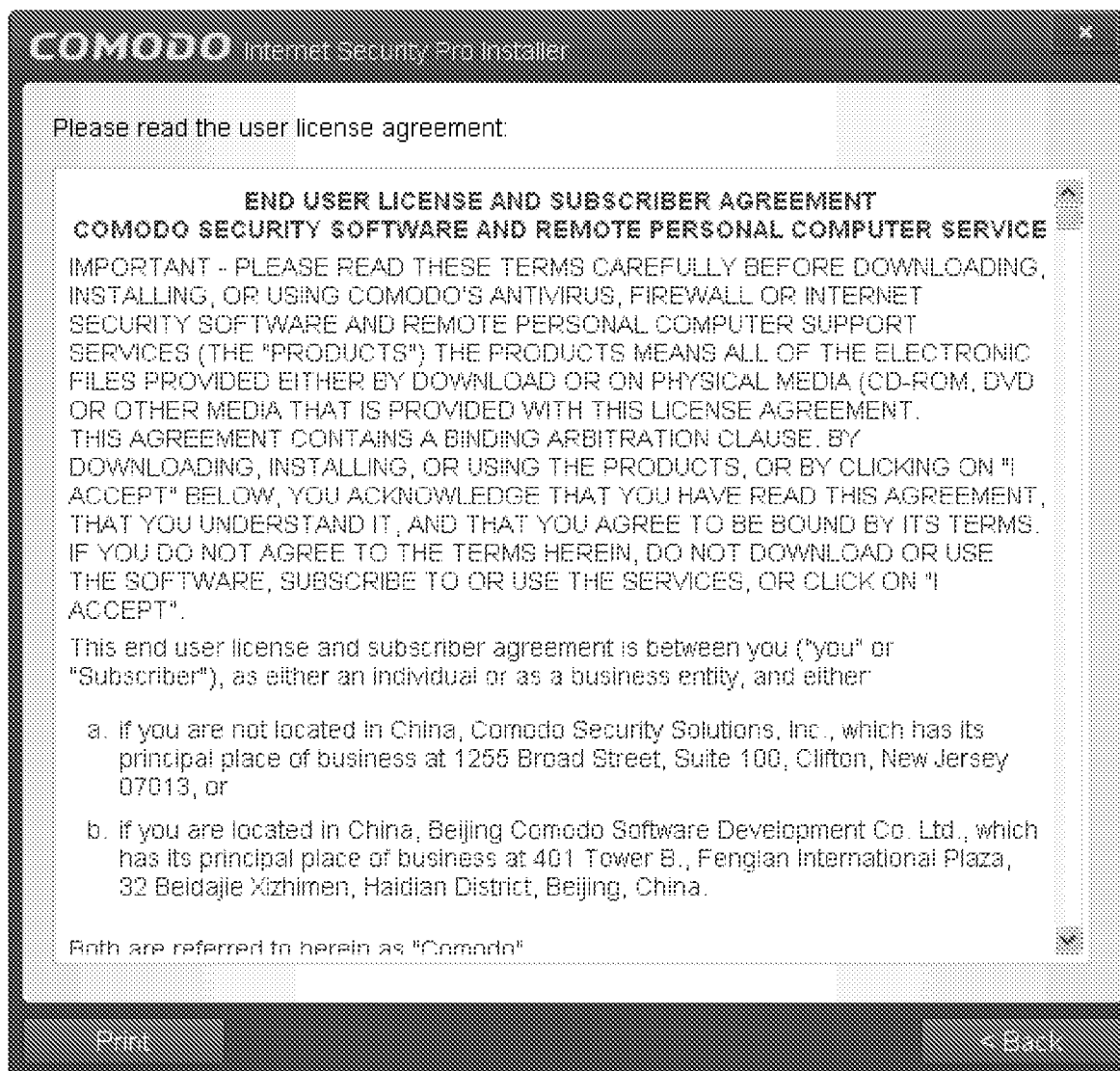
Browser Homepage

Your default browser home page and the search engine will be set as Yahoo!

- Please review and/or modify the settings in the dialog.

End User License Agreement

Read the complete User License Agreements by clicking the 'License Agreement' links of Comodo Internet Security and PrivDog respectively before proceeding with the installation. To read the PrivDog privacy policy link, click the Privacy Policy link next to it.



After reading the agreement, click the 'Back' button to return to the installation configuration screen.

Once back at the main installer screen, if you wish to configure advanced options, click 'Customize Installer'. Otherwise, click 'Agree and Install' to begin installation.

Customizing Installation

Clicking the 'Customize Installer' link opens an advanced options interface that enables you to choose which elements you would like to install, configure security popup alerts and choose the installation path. In order to obtain maximum protection, Comodo recommends that you uninstall any third party personal Firewall and Antivirus in your system and select all the

components to get the maximum benefit from Comodo Internet Security Pro 2013.

Select the Components to Install (Click to go back to Step 2)

- Click the 'Installation Options' tab to select the components to be installed.



- Install COMODO Internet Security Pro** - Selecting this option installs Comodo Antivirus, Comodo Firewall, Defense+ components and PrivDog. Installing CIS Pro is mandatory to qualify for the virus free guarantee.
- Install COMODO GeekBuddy** - Selecting this option installs GeekBuddy, a 24 x 7 remote support service in which Comodo experts can help you solve any computer related problems you may encounter. Refer to the section Comodo GeekBuddy for more details.
- Install COMODO Dragon Web Browser** - Selecting this option installs Comodo Dragon, a fast and versatile Internet browser based on Chromium technology and infused with Comodo's unparalleled level of security. Refer to the section Comodo Dragon for more details.

Configuration Options

- Click the 'Configuration Options' tab to configure pop-up alert options.



- **Do Not show alerts that request security decisions as much as possible** - When this option is selected, CIS is configured to automatically deal with most issues in a secure manner without raising a popup alert - thus minimizing user intervention. Most users should leave this option at the default state of enabled. Advanced users wishing to gain greater insight into CIS actions and/or to have more control over security decisions may wish to disable this option.

Choose the Installation Location

- Click the 'Files Locations' tab to choose the installation path.



This screen allows you to select the folder in your hard drive for installing Comodo Internet Security. The default path is C:\Program Files\COMODO\COMODO Internet Security. If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

After customizing your installation, click the 'Back' button to return to the installation configuration screen.

Click the 'Agree and Install' button to proceed with the installation.

Step 3 - Installation Progress (Click to go back to Step 2)

The installation progress will be displayed...



...and on completion, the restart dialog will be displayed.

Step 4 - Restarting Your System

In order for the installation to take effect, your computer needs to be restarted.



Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

Note: The installation will take effect only on the next restart of the computer.

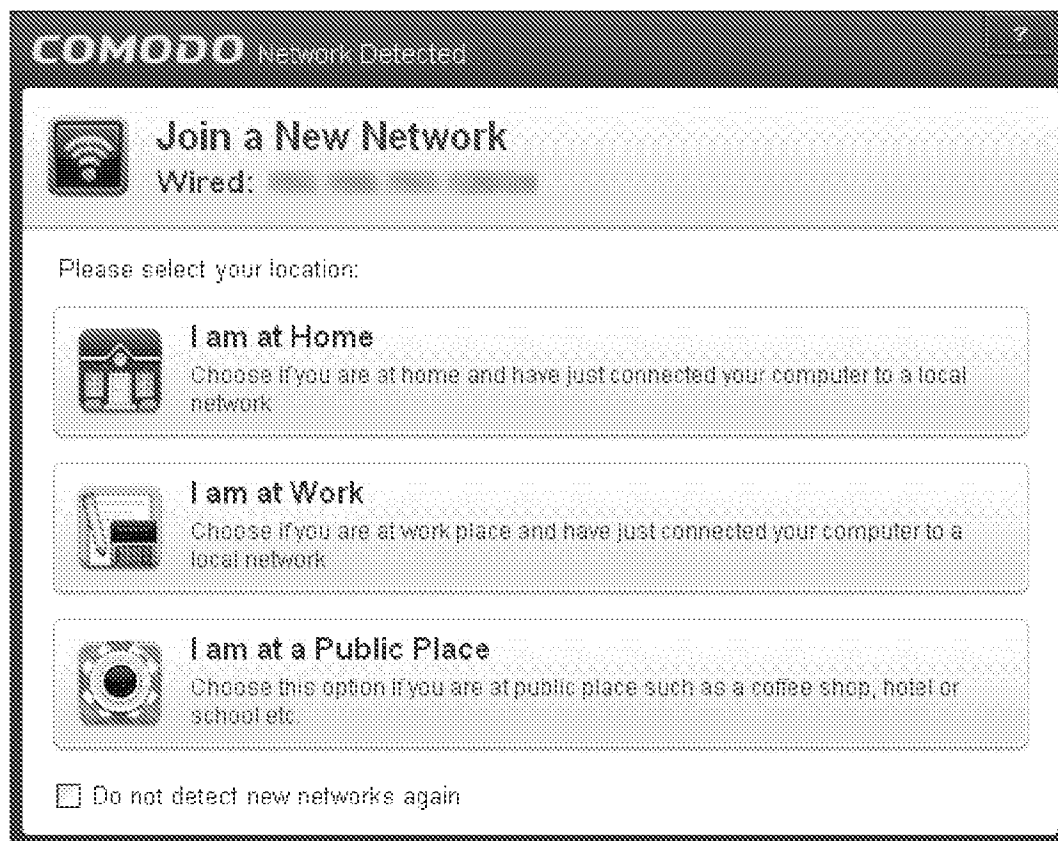
Step 5 - After Restarting Your System

After restarting, a 'thankyou' screen will appear. This contains a summary of the components you chose to install as well as some friendly advice. You can also purchase license key from this screen if you have not done so already.



This screen will appear every time you start your system. If you do not want the screen to be displayed on every start up, select the check box 'Do not show this window again' before closing the window.

If your computer is connected to a home or work network, then you are prompted to configure it at the 'New Network Detected!' dialog. At the top of the dialog, the connectivity mode will be displayed, whether wired or wireless.



- Select your location from the three options above
- Select 'Do not automatically detect new networks' if you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in 'Network Zones' and through the 'Stealth Ports Wizard')

The main interface will be displayed:



CIS will start its first virus database update at the background. You can view the progress by bringing the update task to foreground from the Task Manager interface. Refer to the section 'Manage CIS Tasks' for more details.



The screen will display details such as download speed, how much has been downloaded and the progress of the process. You can also send this task to the background by pressing the 'Send to Background' button and retrieve it in the 'Task Manager' interface. Refer to the section 'Manage CIS Tasks' for more details.

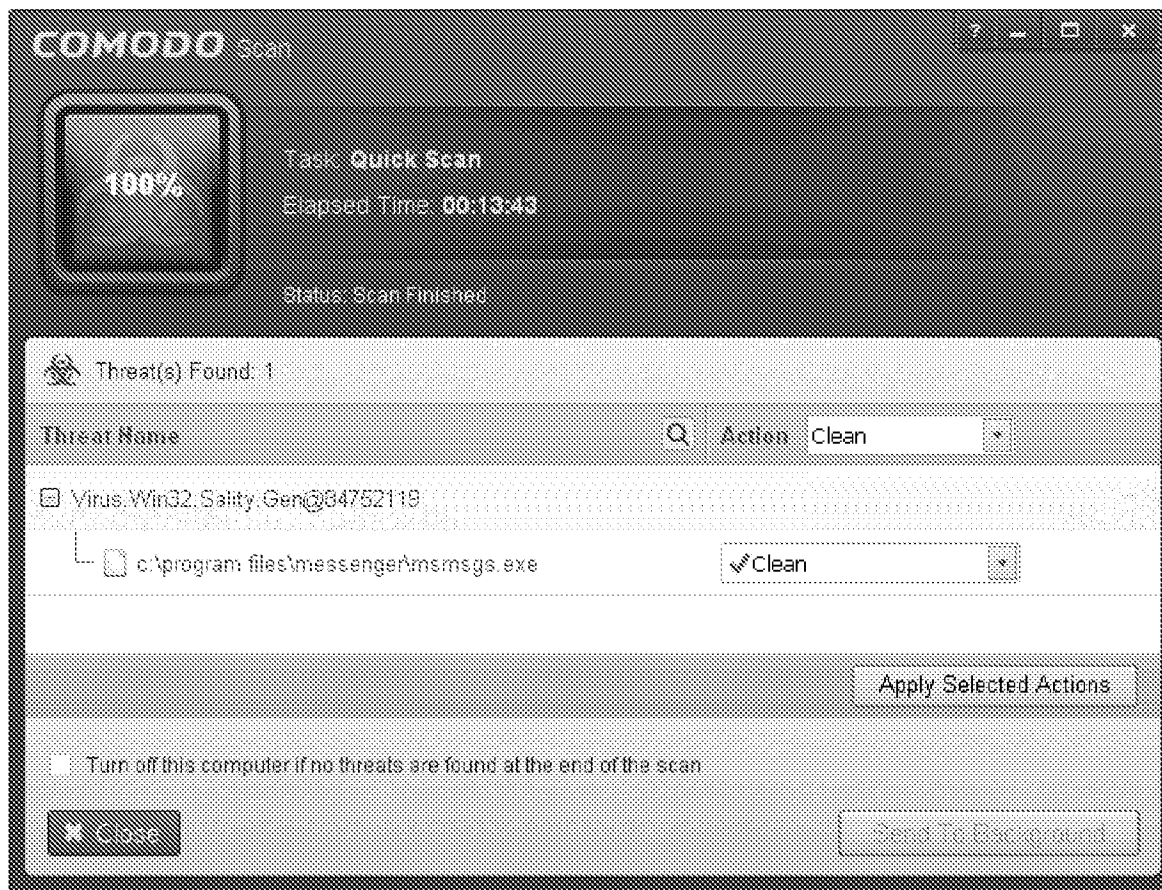


CIS will commence a Quick Scan of system memory, autorun entries, hidden services, boot sectors and other critical areas automatically after the virus database has been updated.



- If you do not want the scan to continue at this time, click the 'Stop' button.

After the scanning is complete, the results screen will be displayed.



If any threats are detected, they will be displayed and you can choose to take appropriate action from any of the drop-down fields in the screen and click 'Apply Selected Actions' button. Refer to the section 'Processing Infected Files' for more details.

Important Note: After successful installation, you need to activate the license for using the product. In order to get your guarantee coverage, you need to activate the license first.

- For full explanation on activation of license after installation of the product, refer to [Activating Your License](#).
- For full explanation on activation of your guarantee, refer to [Activating Your Guarantee Coverage](#).

1.3.3. CIS Complete - Installation and Activation

Note - Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on your computer. [Click here to read the full note.](#)

Comodo Internet Security Complete can be downloaded from www.comodo.com/home/internet-security/internet-security-complete.php after signing up for subscription and includes Comodo Dragon, GeekBuddy, Comodo Backup, TrustConnect and the Comodo Guarantee.

- Choose whether you want the 32 or 64 bit version of CIS then click 'download'
- If you are unsure which version you need, select the 32/64-bit Windows Installer. This executable contains BOTH 32 and 64 bit installers. The setup routine will automatically detect which version of Windows you have and install the appropriate version. Please note, the Universal Windows Installer is a much larger download than the individual 32 or

64 bit setup files.

After downloading the required Comodo Internet Security setup file to your local hard drive, double click on the setup file to start the installation wizard.

Step 1 - Choosing the interface Language

The language selection dialog will be displayed.



Comodo Internet Security is available in several languages.

- Select the language in which you wish the wizard should continue and Comodo Internet Security Complete is to be installed, from the drop-down menu and click 'OK'.

Step 2 - Installation Configuration

The installation configuration screen will be displayed.



- If you click 'Customize Installation' then you can choose advanced options. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

Receive Comodo News and Notifications

If you wish to sign up for news about Comodo products then enter your email address in the space provided. This is optional.

Cloud Based Behavior Analysis

Any file that is identified as unrecognized is sent to the Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled. Read the privacy policy by clicking the 'Privacy Policy' link.

Send Program Usage Data

Comodo collects the usage details from millions of CIS users to analyze their usage patterns for the continual enhancement of the product. Your CIS installation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. Comodo recommends users leave this setting enabled. You can change this setting from Advanced Settings > General Settings > Log Settings interface, at anytime after installation.

- Please review and/or modify the settings in the dialog.

- Click the 'Next' button.

In the next screen, you can choose to configure your DNS Settings and Browser Home page.



- If you click 'Customize Installation' then you can choose advanced options. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

DNS Settings

Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Comodo's worldwide network of redundant DNS servers provide fast and secure Internet browsing experience without any hardware or software installation.

In addition, Comodo's Secure DNS ensures safety against attacks in the form of malware, spyware, phishing etc., by blocking access to malware-hosting sites, by any program running in your system.

For more details on Comodo Secure DNS Service and to know how to enable or disable the service, refer to Appendix 2 Comodo Secure DNS Service.

In this step of installation of CIS Complete, the DNS settings of your computer can be changed automatically to direct to our DNS servers. You can disable the service at anytime and revert to your previous settings.

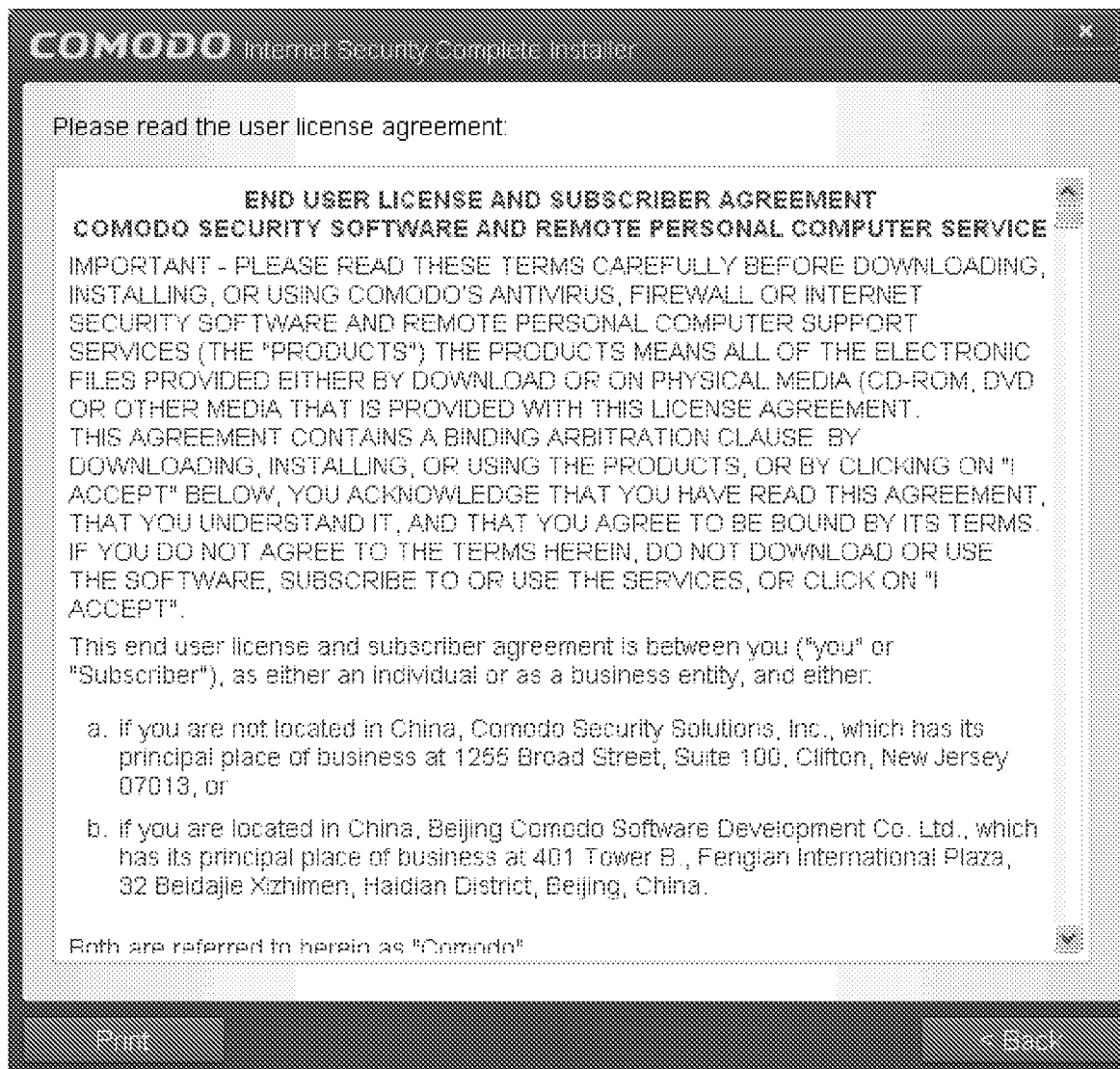
To enable Comodo Secure DNS, select 'Change my DNS Servers to COMODO SecureDNS Servers. Click the 'What is this' link to know more about Comodo Secure DNS servers.

Browser Homepage

Your default browser home page and the search engine will be set as Yahoo!

End User License Agreements

Read the complete User License Agreements by clicking the 'License Agreement' links of Comodo Internet Security and PrivDog respectively before proceeding with the installation. To read the PrivDog privacy policy link, click the Privacy Policy link next to it.



After reading the agreement, click the 'Back' button to return to the installation configuration screen.

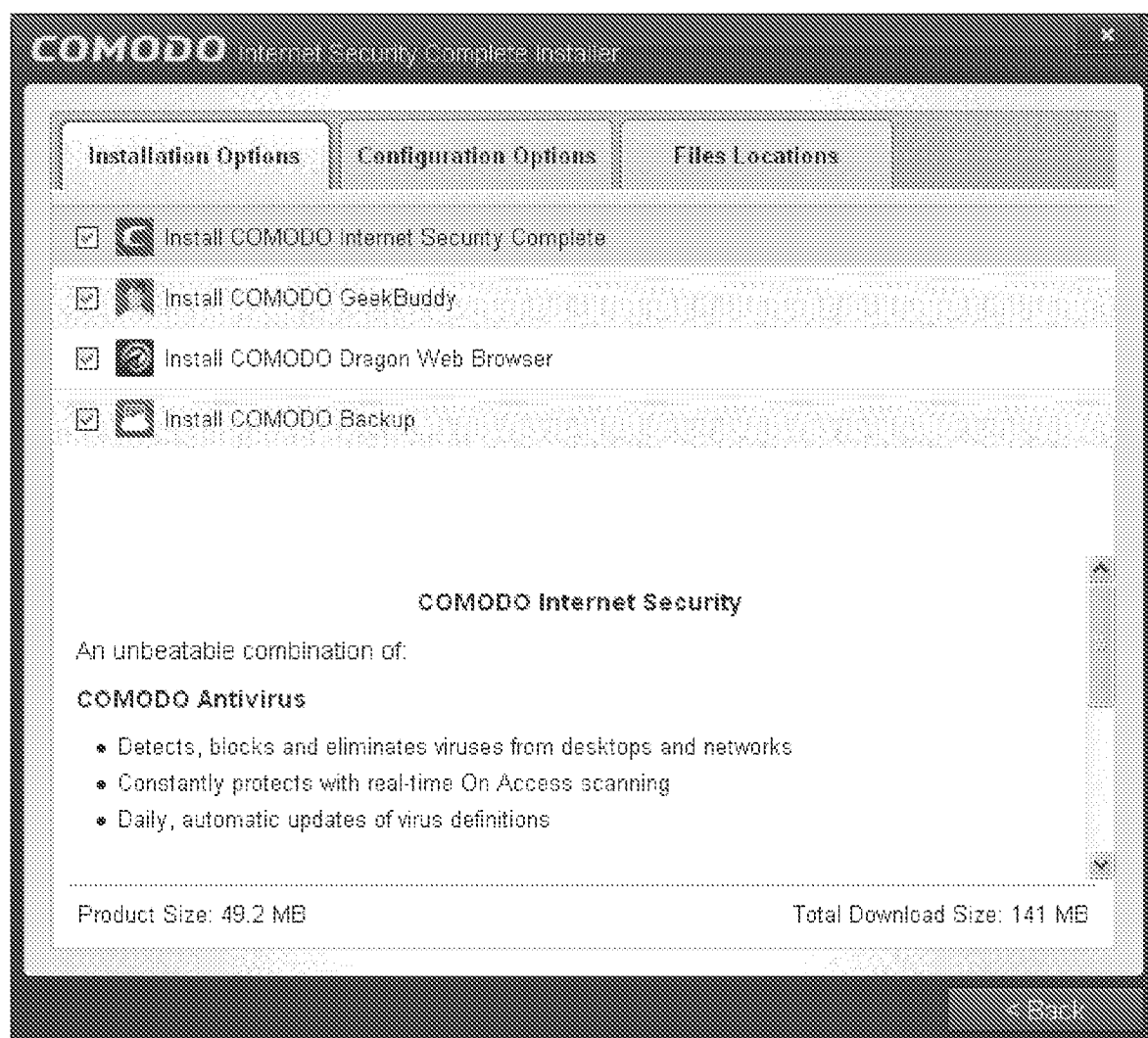
Once back at the main installer screen, if you wish to configure advanced options, click 'Customize Installation'. Otherwise, click 'Agree and Install' to begin installation.

Customizing Installation

Click the 'Customize Installation' link to select the components to be installed, enable security popup alerts to be minimized and choose installation path.

Selecting Components to Install (Click to go back to Step 2)

- Click the 'Installation Options' tab to select the components to be installed.



- **Install COMODO Internet Security Complete** - Selecting this option installs Comodo Antivirus, Comodo Firewall, Defense+ components and Comodo PrivDog. Installing CIS Complete is mandatory to qualify for the virus free guarantee.
- **Install COMODO GeekBuddy** - Selecting this option installs GeekBuddy, a 24 x 7 remote support service in which Comodo experts can help you solve any computer related problems you may encounter. Refer to the section Comodo GeekBuddy for more details.
- **Install COMODO Dragon Web Browser** - Selecting this option installs Comodo Dragon, a fast and versatile Internet browser based on Chromium technology and infused with Comodo's unparalleled level of security. Refer to the section Comodo Dragon for more details.
- **Install COMODO Backup** - Selecting this option installs Comodo Backup, a powerful and easy-to-use desktop application that helps home and business users protect their valuable data against damage or loss. Refer to the section Comodo Backup for more details.

Configuration Options

- Click the 'Configuration Options' tab to configure pop-up alert options.



- **Do Not show alerts that request security decisions as much as possible** - When this option is selected, CIS is configured to automatically deal with most issues in a secure manner without raising a popup alert - thus minimizing user intervention. Most users should leave this option at the default state of enabled. Advanced users wishing to gain greater insight into CIS actions and/or to have more control over security decisions may wish to disable this option.

Choosing Installation Location

- Click the 'Files Locations' tab to choose the installation path.



This interface allows you to set the installation folder for Comodo Internet Security. The default path is C:\Program Files\COMODO\COMODO Internet Security. If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

After customizing your installation, click the 'Back' button to return to the installation configuration screen.

- Click the 'Agree and Install' button to proceed with the installation.

Step 3 - Installation progress (Click to go back to Step 2)

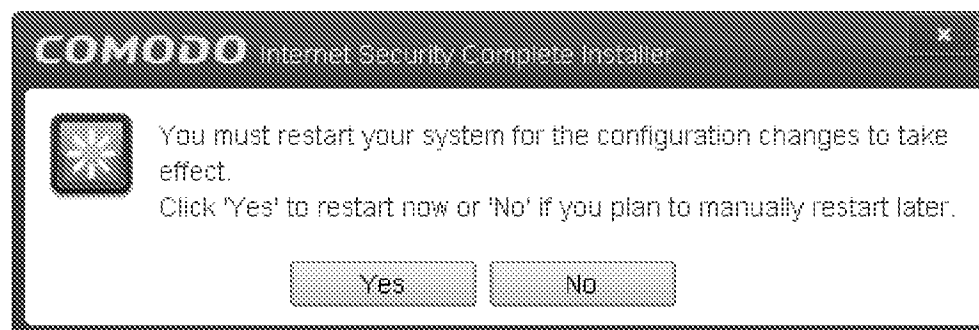
The installation progress will be displayed...



...and on completion, the restart dialog will be displayed.

Step 4 - Restarting Your System

In order for the installation to take effect, your computer needs to be restarted.



Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

Note: The installation will take effect only on the next restart of the computer.

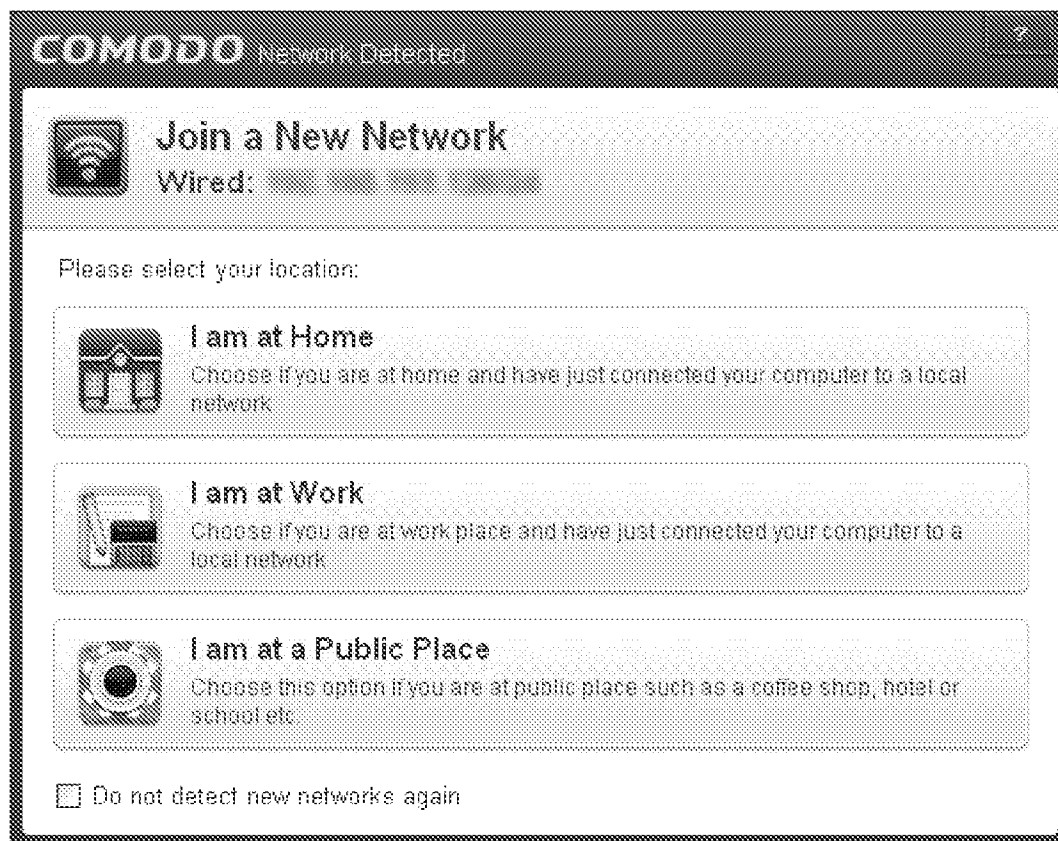
Step 5 - After Restarting Your System

After restarting, a 'Start Up' screen will appear. This contains a summary of the components you chose to install as well as some friendly advice. You can also purchase license key from this screen if you have not done so already.



This screen will appear every time you start your system. If you do not want the screen to be displayed on every start up, select the check box 'Do not show this window again' before closing the window.

If your computer is connected to a home or work network, then you are prompted to configure it at the 'New Network Detected!' dialog. At the top of the dialog, the connectivity mode will be displayed, whether wired or wireless.



- Select your location from the three options
- Select 'Do not automatically detect new networks' if you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in 'Network Zones' and through the 'Stealth Ports Wizard').

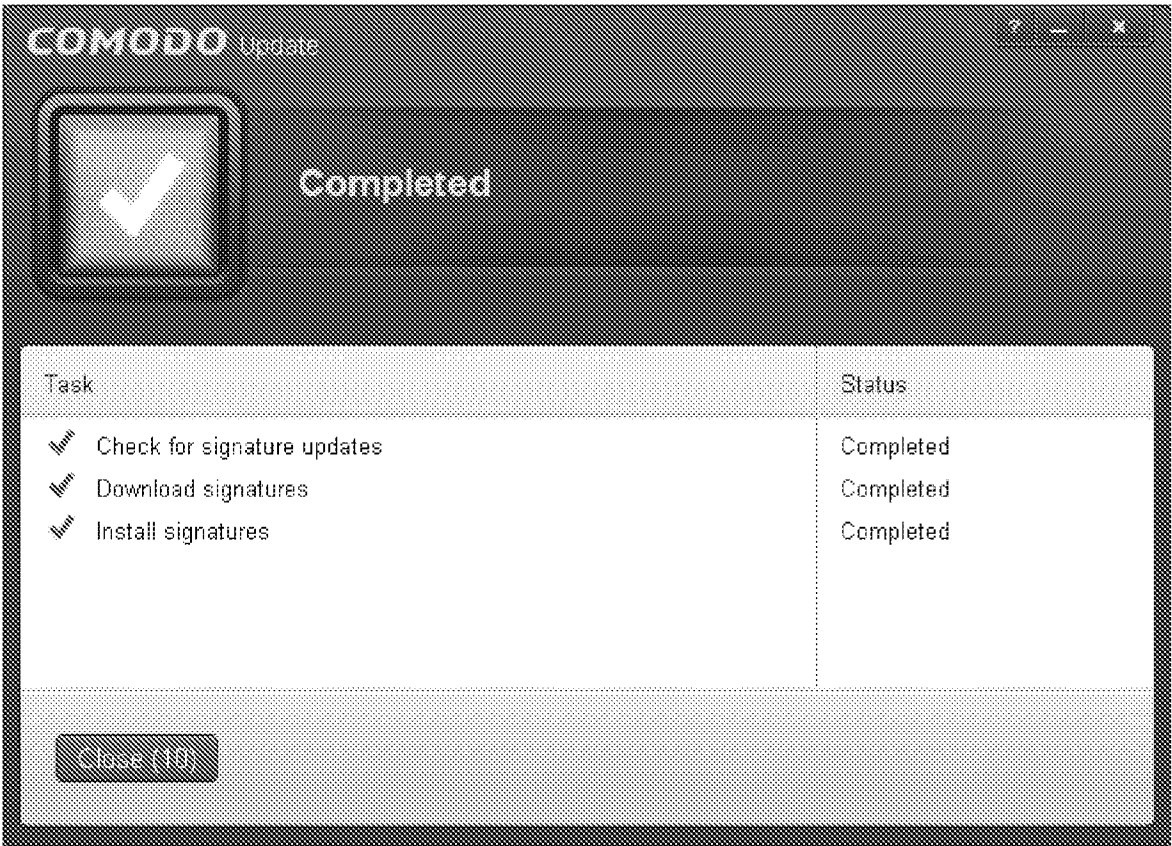
The main interface will be displayed:



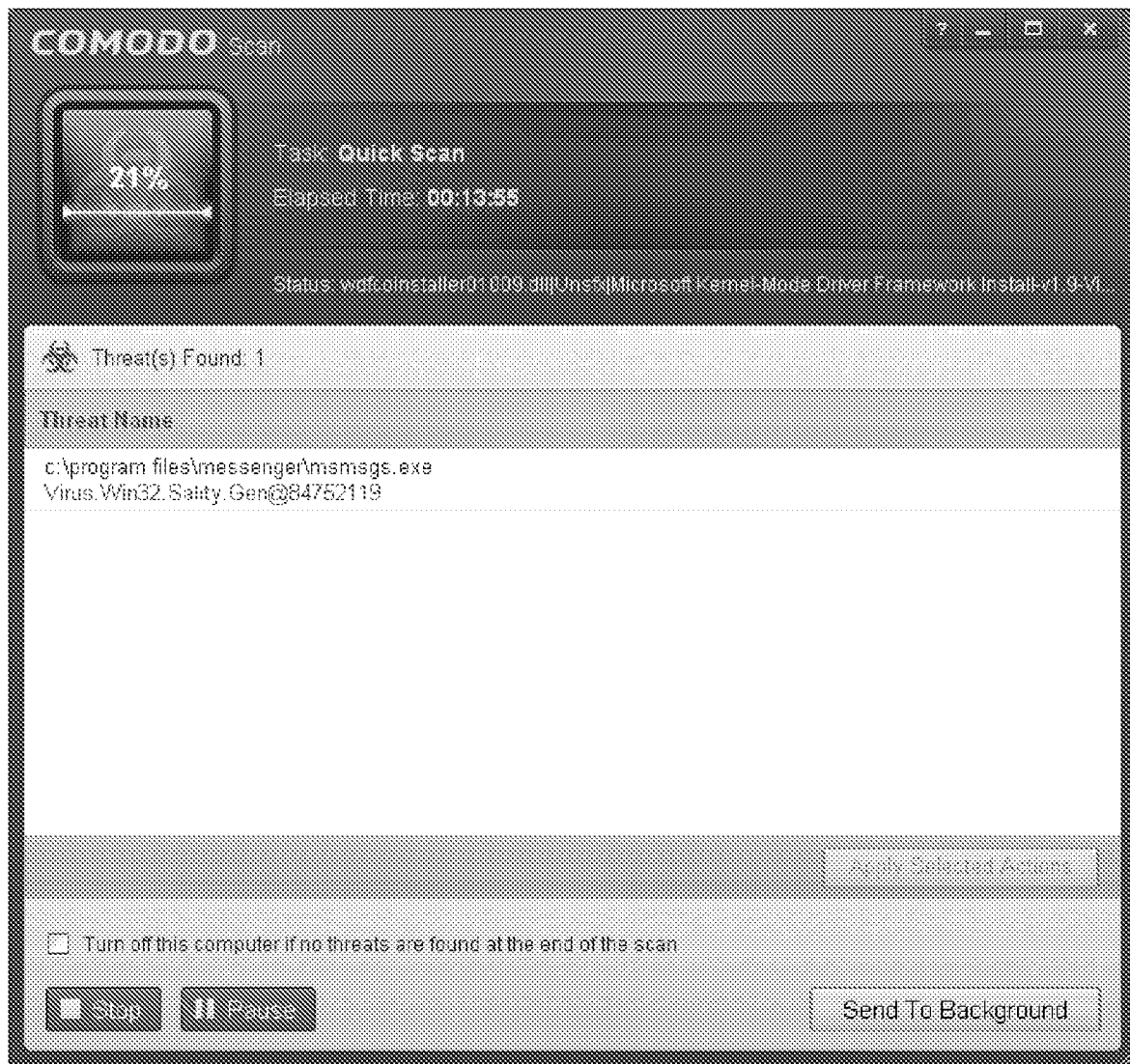
CIS will start its first virus database update at the background. You can view the progress by bringing the update task to foreground from the Task Manager interface. Refer to the section 'Manage CIS Tasks' for more details.



The screen will display details such as download speed, how much has been downloaded and the progress of the process. You can also send this task to the background by pressing the 'Send to Background' button and retrieve it in the 'Task Manager' interface. Refer to the section 'Manage CIS Tasks' for more details.

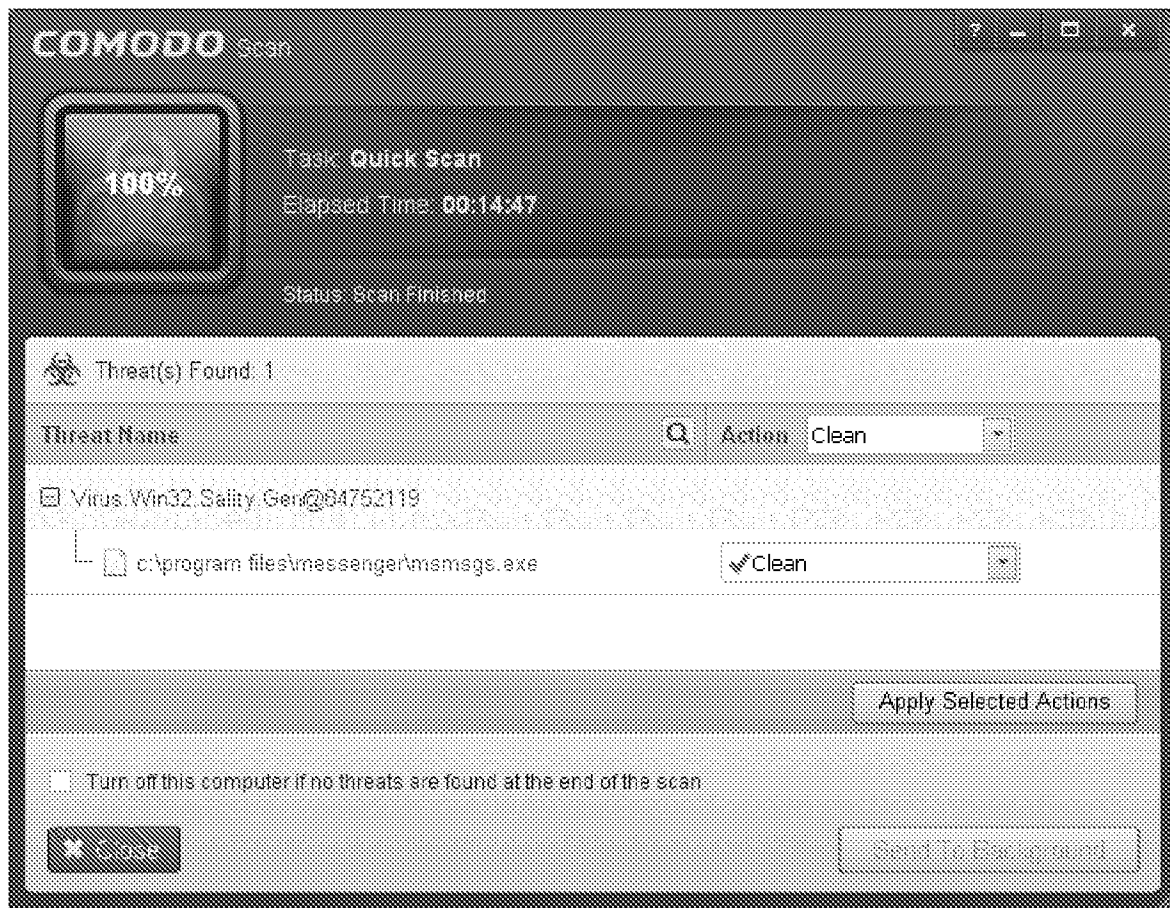


CIS will commence a Quick Scan of system memory, autorun entries, hidden services, boot sectors and other critical areas automatically after the virus database has been updated.



- If you do not want the scan to continue at this time, click the 'Stop' button.

After the scanning is complete, the results screen will be displayed.



If any threats are detected, they will be displayed and you can choose to take appropriate action from any of the drop-down fields in the screen and click 'Apply Selected Actions' button. Refer to the section 'Processing Infected Files' for more details.

Important Note: After successful installation, you need to activate the license for using the product. In order to get your guarantee coverage and TrustConnect service enabled, you need to activate the license first.

- For full explanation on activation of license after installation of the product, refer to [Activating Your License](#).
- For full explanation on activation of your guarantee, refer to [Activating Your Guarantee Coverage](#).

1.3.4. Activating CIS Pro/Complete Services after Installation

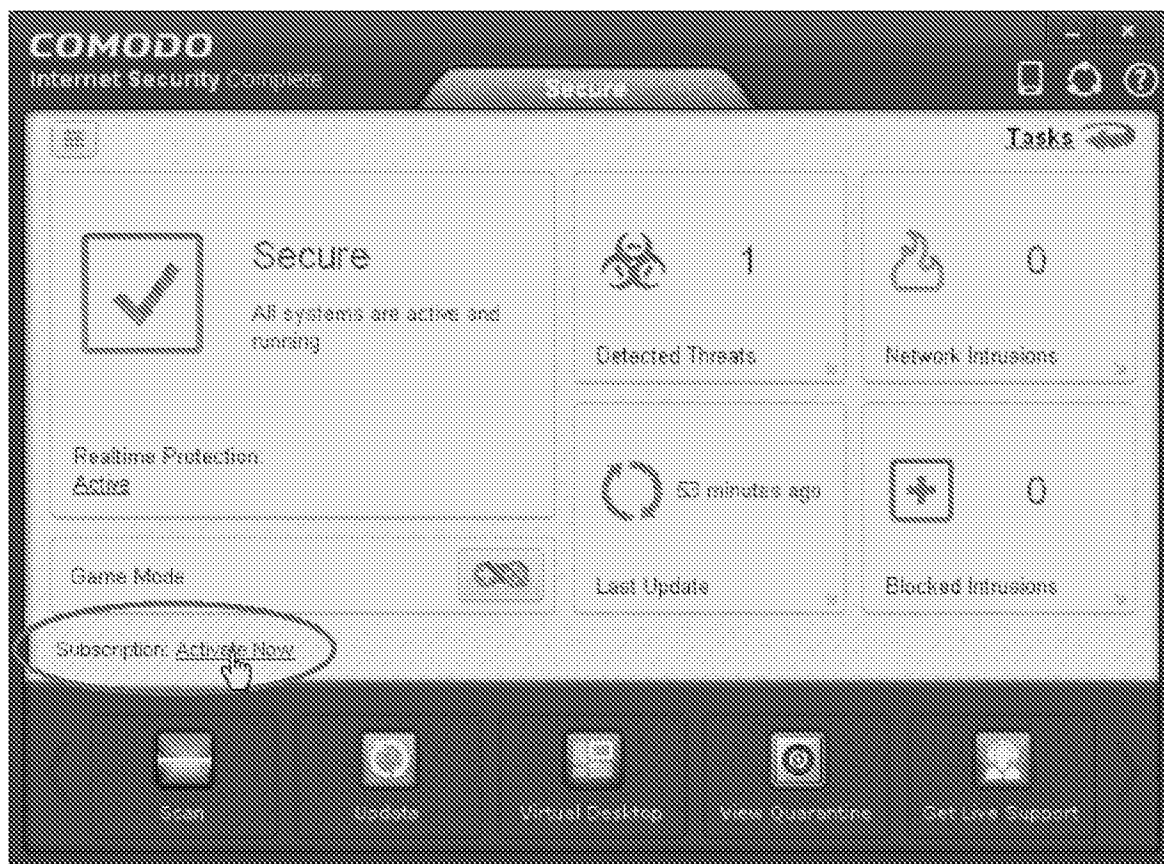
CIS Pro and CIS Complete should be activated after installation for continued use of the product. You will get alerts to activate the license if it has not been done so.

- [Activating Your License](#);
- [Activating Your Guarantee Coverage](#);
- [Renewal of Your License](#).

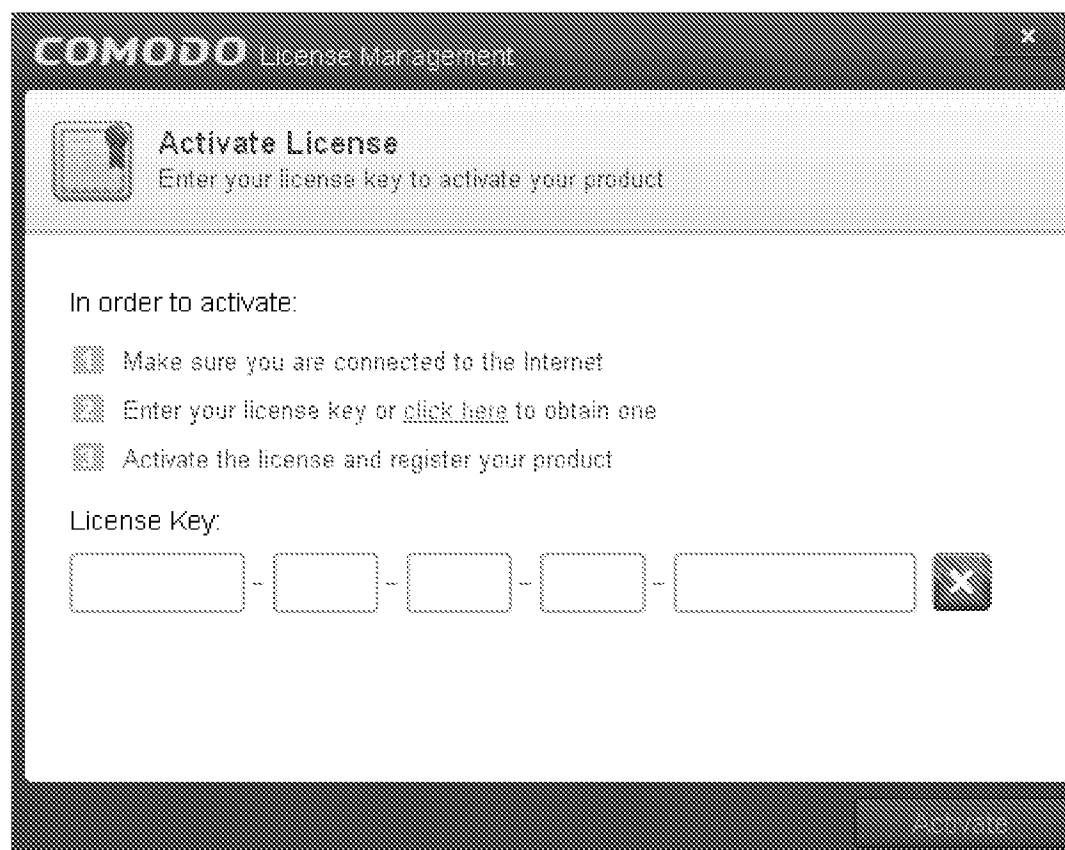
1.3.4.1. Activating Your License

- Start the Comodo Internet Security application as explained in the section [Starting Comodo Internet Security](#).

Step 1: To activate your License, click 'Activate Now' beside 'Subscription' in the home screen.

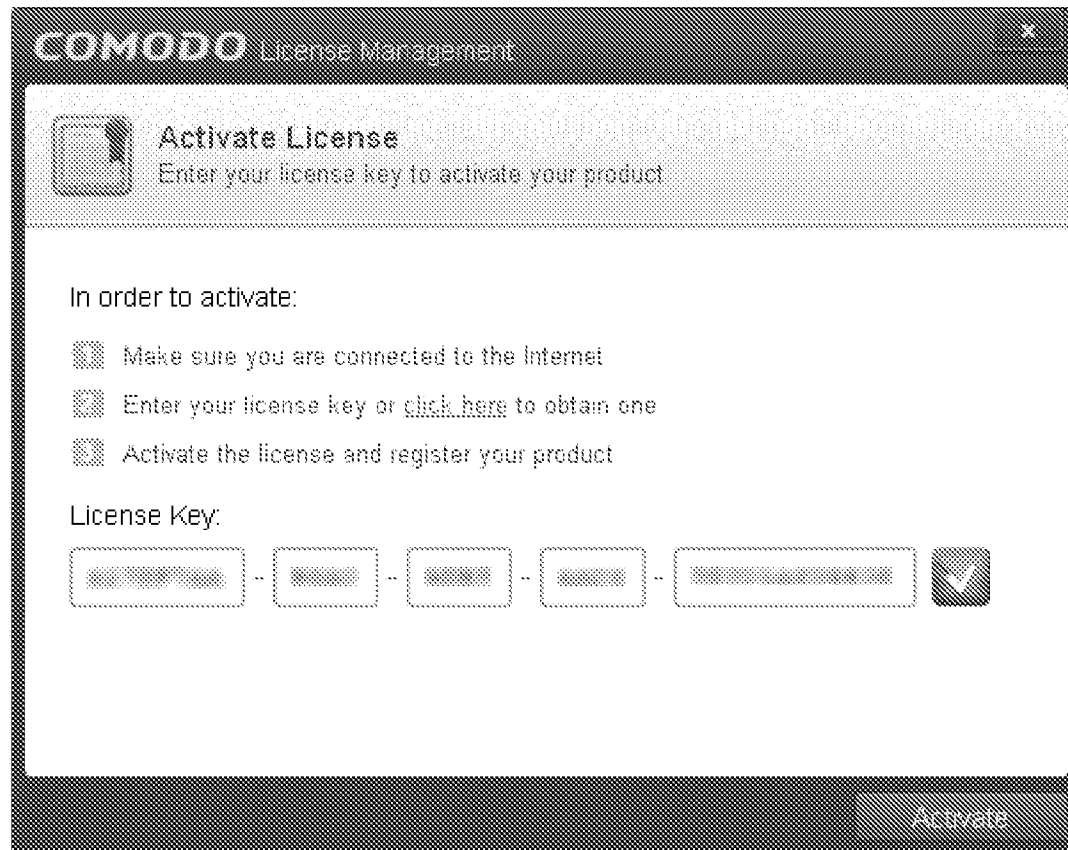


The License Activation Wizard will start.



- You should have received your License key through email if you have purchased CIS Pro. For CIS Complete, the license key is available on the DVD itself or printed on an insert included in the box packaging. Enter the license key and click 'Activate'.

Tip: If you haven't subscribed for Comodo Internet Security - Pro or Complete so far, click the 'click here' link. You will be taken to the Comodo website enabling you to purchase the license.



- The wizard starts validating your key.



If you have not registered as an user in Comodo Accounts Manager (CAM), the following screen will be displayed.

COMODO License Management

Register Product
Enter user details to register your product

* First Name * Last Name

* Email Address

Country

City State

Address

Choose a username and password and create a COMODO account. You can use your account to manage your licenses through <https://accounts.comodo.com>

* Username * Password

* Mandatory Field

Register

- Fill up the registration form with the login details and password for your Comodo Accounts Manager (CAM) account.

COMODO License Management

Register Product
Enter user details to register your product

* First Name * Last Name

* Email Address

Country

City State

Address

Choose a username and password and create a COMODO account. You can use your account to manage your licenses through <https://accounts.comodo.com>

* Username * Password

* Mandatory Field

Register

Field	Description
Name	Enter your first name
Last Name	Enter your last name
Email	Enter your email address
Address	Enter your address
City	Enter your city name
Country	Select your country from the drop-down box
State	Select your state from the drop-down box
Address	Enter your full address
Create a new COMODO Account	
<ul style="list-style-type: none"> Enter your username and password to create a new Comodo account with Comodo Accounts Manager (CAM) 	

- Click 'Register'

On successful validation, your subscription will be activated and a confirmation screen will be displayed.



- Click 'Continue' to exit the wizard.

For CIS Pro users - Your CIS Pro product will be activated.

For CIS Complete users - Your CIS Complete product will be activated along with Comodo Backup and TrustConnect

- Accessing Comodo Backup online storage space - Use the login credentials provided during the CIS Complete registration step.
- Using the TrustConnect service - The TrustConnect service will be automatically enabled after successful activation of the license. Please refer to the section TrustConnect Overview for more details on how to use the service.

Tip: You can also enter your activation key by clicking the link 'Enter a license key' in the About dialog, accessible by clicking Help icon > About from the title bar.

The main interface will display the number of days left for the license before it should be renewed.



1.3.4.2. Activating Your Guarantee Coverage

The Comodo Guarantee is available to customers of CIS Pro and CIS Complete versions. Before enabling guarantee coverage, customers should first have activated their licence. Full details on activating the license can be found in [Activating Your License](#) section.

- Please note that if you wish to use and activate the Comodo guarantee then you must have installed Comodo Internet Security (both Antivirus and Firewall components) and Comodo GeekBuddy. You must also have run and passed a Comodo Antivirus scan using the latest signature database. Please see the End User License Agreement (EULA) for full details.

Limits: The guarantee is limited to the lesser of:

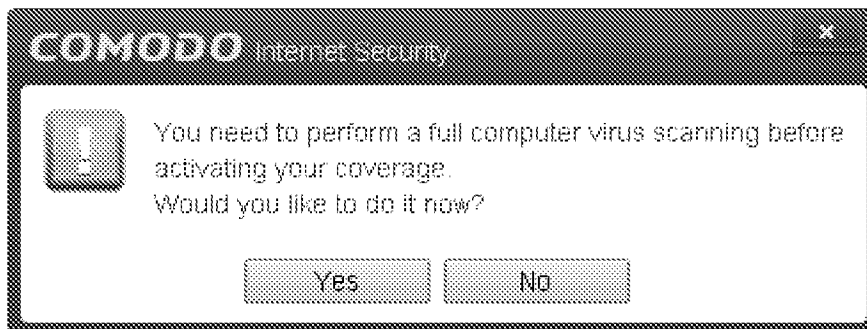
- The actual cost of the computer;
- An aggregate total of \$500 for all claims paid under a single license key, and
- The actual cost of a Comodo specified and authorized third party provider to repair the computer to an operating condition ('Guarantee Limit').
- The guarantee is limited to repairing the computer over the Internet to an operational state and excludes all claims for lost or expected profits, lost or corrupted data, lost or deleted work, or lost or damaged personal files. Comodo does not guarantee against the loss of any file or information. The guarantee is void if you breached this agreement, failed to follow the procedures described in this Section 3 of the EULA or failed to pay any fees applicable to your use of the Software.
- Full Terms and Conditions on the Comodo Guarantee Coverage can be read in Section 3 of CIS EULA (Step 2 of the Installation process for CIS Pro and Step 1 for CIS Complete).

more details on running an Antivirus Scan [Click here](#).

Step 1: To activate your guarantee coverage, click 'Not Activated' beside 'Warranty' in the home screen.



A full system scan to remove all known viruses is a mandatory requirement if your computer is to be eligible for guarantee coverage. If this step has already been performed (and your system is clean), then the process moves to step 2.



Click 'Yes' to run a full computer scan. Refer to the section [Run a Full Computer Scan](#) for more details on scanning your full computer and cleaning the infected files. All the infections and threats identified during the scan should be cleaned for your computer to be qualify for the warranty.

Step 2: The next stage is to run the Guarantee Activation Wizard again.

- Click 'Not Activated' beside 'Warranty:' again. The Guarantee Activation Wizard will start and on completion the 'successfully activated' screen will be displayed.



- Click 'Continue' to complete the activation wizard

Successfully activating your Guarantee will change the information displayed beside 'Warranty:' in the Home screen.

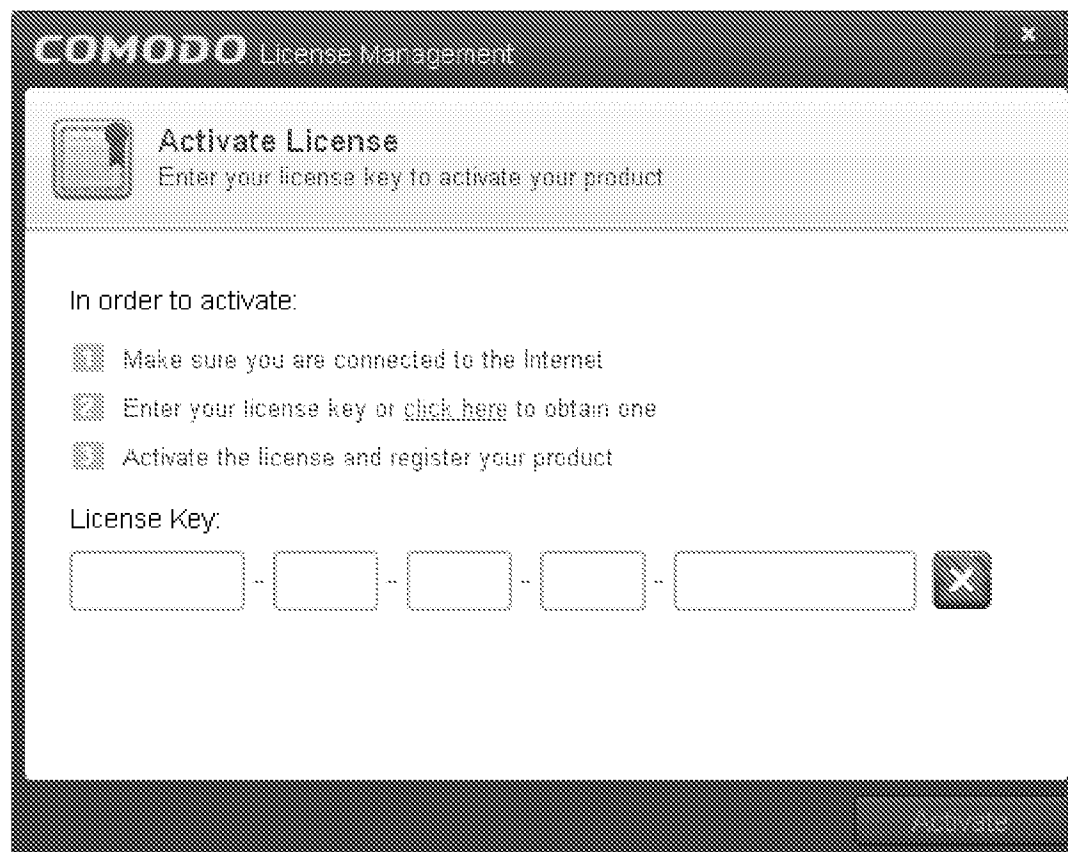


1.3.4.3. Renewal of Your License

In order to enjoy continuous services from Comodo after the license period of your CIS Pro/Complete has expired, you need to renew your License.

To renew or upgrade your license, click the 'Activate Now' link beside 'Subscription' on the CIS home screen (alternatively, click 'No. of days left').

The Product Activation Wizard will start.



- Click the '[click here](https://secure.comodo.com/home/purchase.php?aff=Comodo&rs=7&pid=9&cid=RkJEMUZENjMzQUM4RDIDNOE4MzBDQjc1NDIENUizRkY&lid=8)' link. You will be taken to <https://secure.comodo.com/home/purchase.php?aff=Comodo&rs=7&pid=9&cid=RkJEMUZENjMzQUM4RDIDNOE4MzBDQjc1NDIENUizRkY&lid=8>.
- Select your CIS Package.
- Select 'returning user' in the 'Sign-up Information' area, enter your login and password and complete the payment procedures.
- The License key will be sent to you by email. Activate your License using the new key to enjoy the continued services.

1.4. Starting Comodo Internet Security

After installation, Comodo Internet Security automatically starts whenever you start Windows and the CIS Widget will be displayed. In order to configure and view settings within Comodo Internet Security, you need to access the main interface.

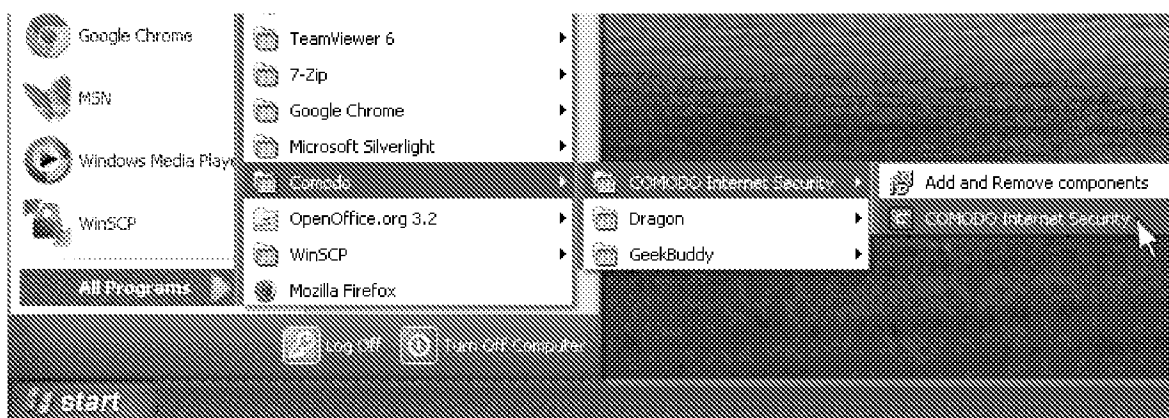
There are 4 different ways to access the main interface of Comodo Internet Security:

- Windows Start Menu
- Windows Desktop
- Widget
- System Tray Icon

Start Menu

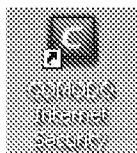
You can access Comodo Internet Security via the Windows Start Menu.

- Click **Start** and select **All Programs > Comodo > COMODO Internet Security > COMODO Internet Security**.



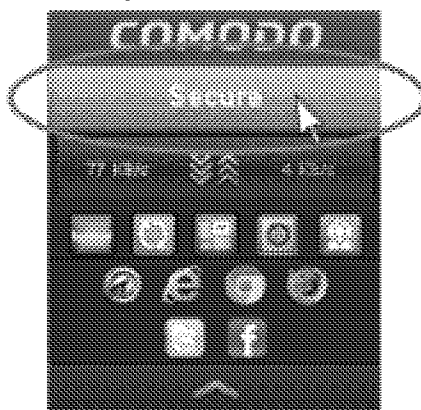
Windows Desktop

- Just double click the shield icon in the desktop to start Comodo Internet Security.



Widget

- Just click the information bar in the widget to start CIS.



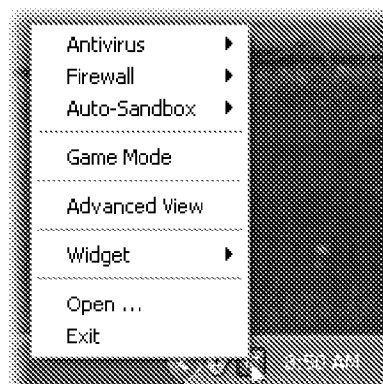
You can also view other details in the widget such as inbound and outbound traffic, number of tasks running, shortcuts to common CIS tasks and browsers and links to social media sites Twitter and Facebook. Refer to the section 'The Widget' for more details.

CIS Tray Icon

- Just double click the shield icon to start the main interface.



By right-clicking on the tray icon, you can access short cuts to selected settings such as enabling or disabling Antivirus real-time scan, Firewall, Behavior Blocker, Widget, Game Mode option and switch the CIS to Advanced or Compact View.



Game Mode - Switches CIS to Game Mode to enable you to play your games without any interruptions from various alerts in your computer. The operations that can interfere with users' gaming experience are either suppressed or postponed.

In game mode:

- Defense+/Firewall alerts are suppressed as if they are in training mode;
- AV database updates and scheduled scans are postponed until the gaming is over;
- Automatic isolation of unknown applications and real-time virus detection are still functional.

Deactivate Game Mode to resume alerts and scheduled scans.

Widget - Click [here](#) for more details on CIS Widget.

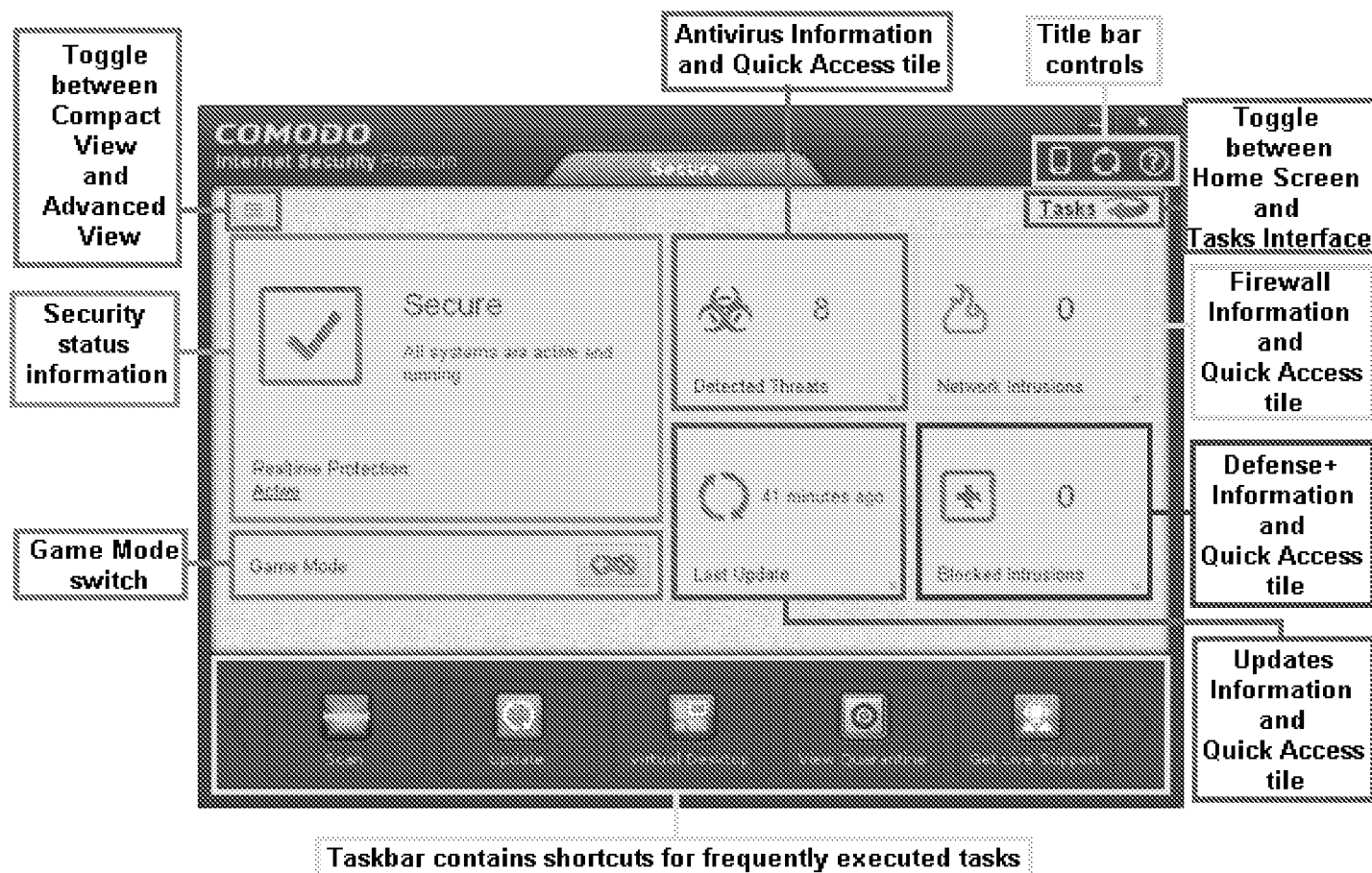
Refer to the section "The System Tray Icon" for more details.

1.5. The Main Interface

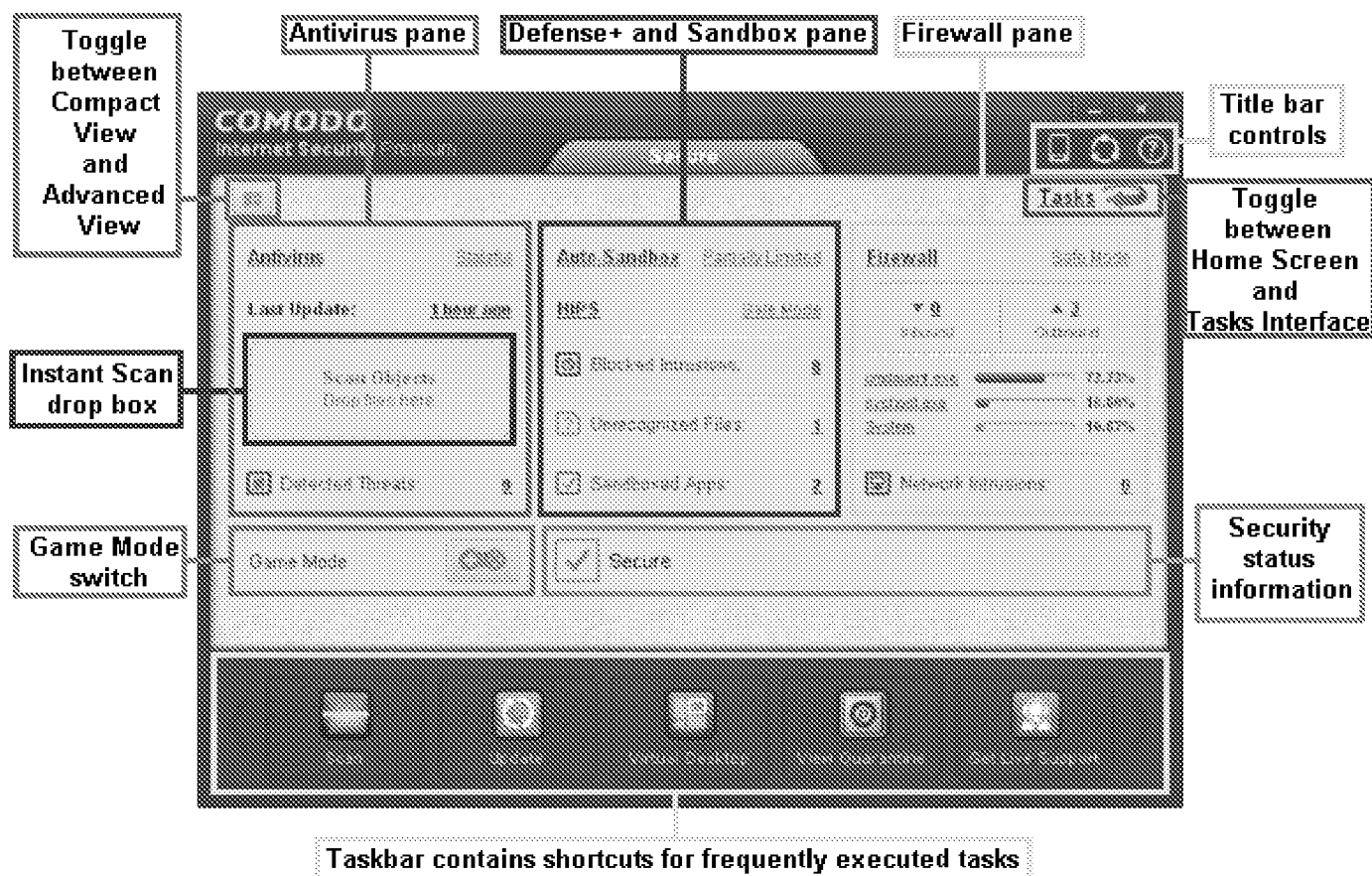
The CIS interface is designed to be as clean and informative as possible while letting you carry out any task you want with the minimum of fuss. Each tile on the home screen contains important security and update information and allows you to quickly delve further into areas of interest.

- Click the curved arrow at the upper right to switch between the home screen and the tasks interface.
- Instantly run a virus scan on a file or folder by dragging it into the scan box.
- Switch on 'Game Mode' to make sure nothing interrupts you while you play a full screen game.
- Change the entire look and feel of the home screen from Advanced Settings.
- The Task Bar at the bottom of the home screen allows one-click access to important features such as the antivirus scanner, the Virtual Desktop, the update checker and the CIS Task Manager.
- Flip between 'Compact View' and 'Advanced View' by using the toggle button at the upper left  or from the system tray icon

Compact View



Advanced View



The advanced view shows antivirus, firewall and sandbox activity in greater detail. This includes the number of detected threats, last virus database update time, number of inbound and outbound connections and more.

This view also allows you to quickly change security settings for each component.

Click the following links for more information:

- [The Home Screen](#)
- [The Tasks Interface](#)
- [The Widget](#)
- [The System Tray Icon](#)

1.5.1. The Home Screen

You can switch the display between the 'Home' screen and the 'Tasks' interface by clicking the green arrow at the upper right of the interface: 

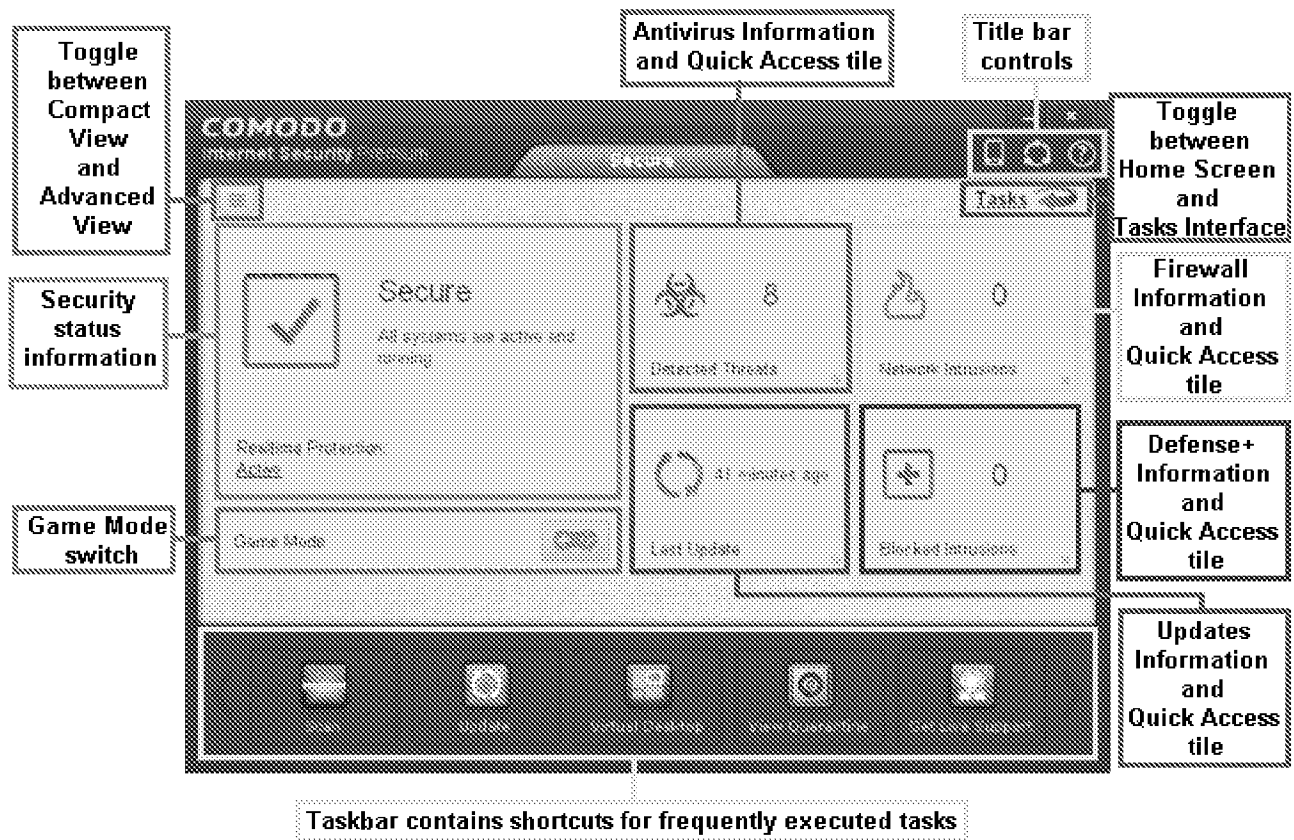
The home screen itself is available in two formats, 'Compact' view and 'Advanced' view. Use the button at the top-left to switch between them.  

The following areas are common to both compact and advanced views:

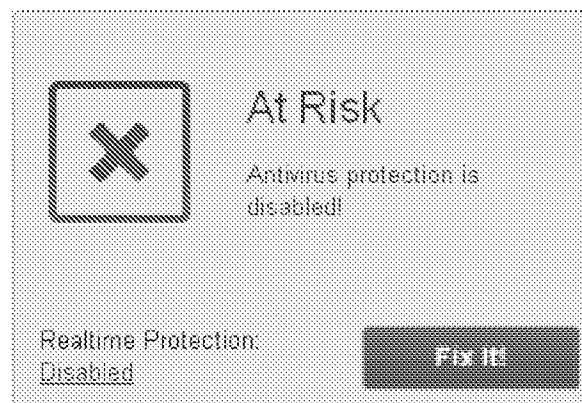
- Adding tasks to the Task Bar
- Title bar controls
- Game mode

Compact View

Compact View presents a simple, easy to understand interface that allows users to quickly launch key tasks and gain an immediate overview of the security of their computer. The large 'security information' tile on the left provides at-a-glance information on overall system security and allows you to run an appropriate CIS task if threats are found. The four tiles on the right provide information from specific CIS security components and act as shortcuts to run an instant antivirus scan, run an update, view network traffic and to configure sandbox/host intrusion settings.



The security information tile on the left will inform you if any component is disabled or any if other problems are found:



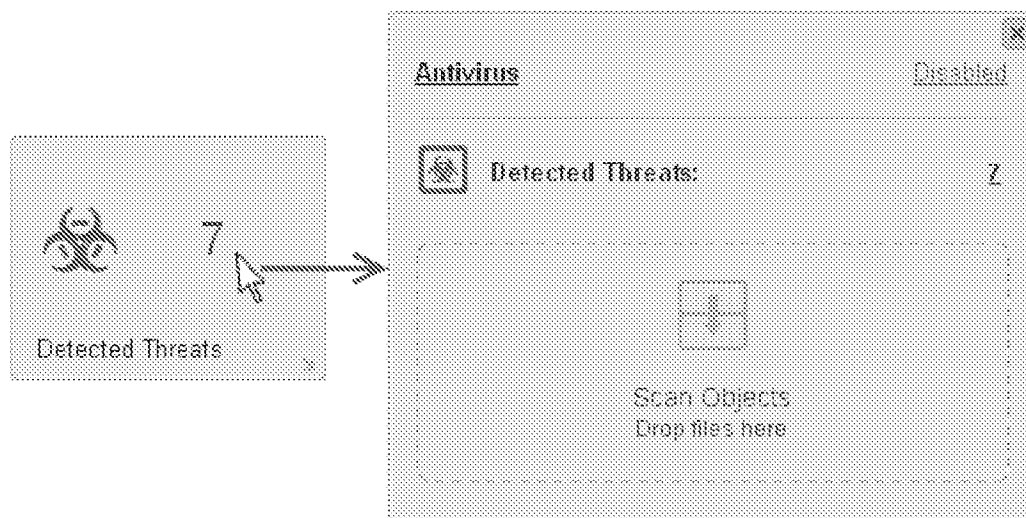
You can easily rectify the issue by clicking the 'Fix It!' button. CIS will automatically take necessary actions to resolve the problem.

From the Compact View of the home screen you can:

- Instantly scan objects
- Enable or disable security components

Instantly scan objects

Click the 'Antivirus' tile in the middle of the (compact) home screen to open the drag-and-drop scanner:

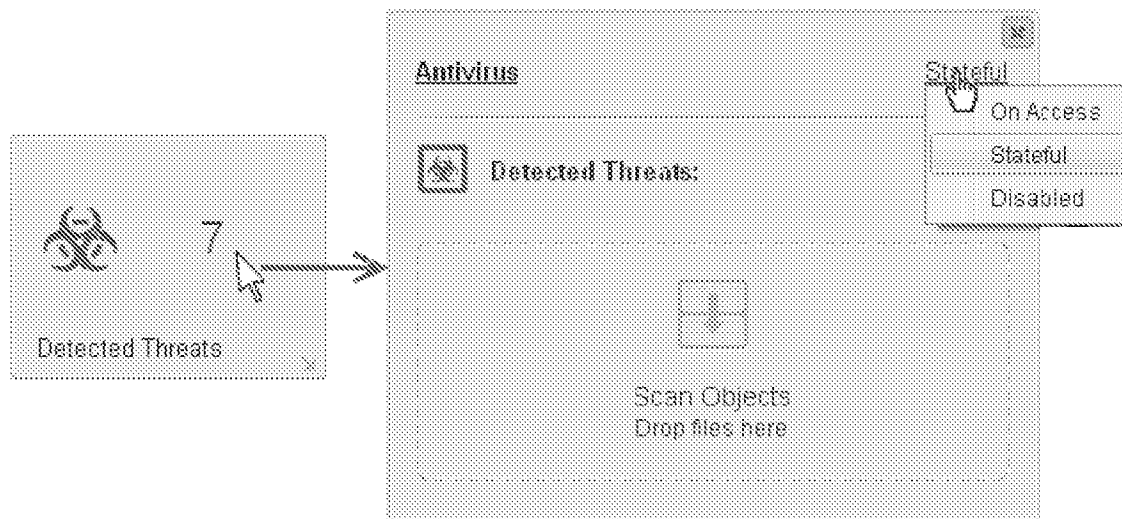


To run an instant scan, navigate to the file/folder that you want to scan and just drag-and-drop the file into the 'Scan Objects' box. The virus scan will commence immediately. Refer to 'Instantly Scan Individual Files and Folders' for more details.

Enable or disable security components

The four tiles on the right can each be flipped to display more detailed information and options

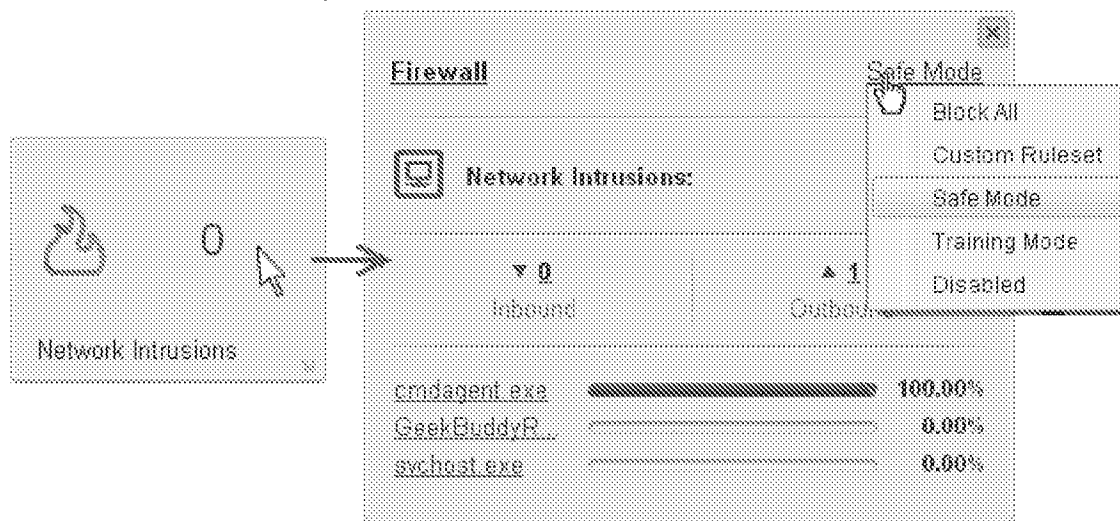
- **Antivirus** - Click the Antivirus tile to flip open a more detailed tile which displays current antivirus settings, the number of detected threats and the drag-and-drop scanner.
 - Click the link at the top-right to quickly switch AV modes between 'On Access', 'Stateful' and 'Disabled'. Refer to the section 'Real-time Scanner Settings' for more details.



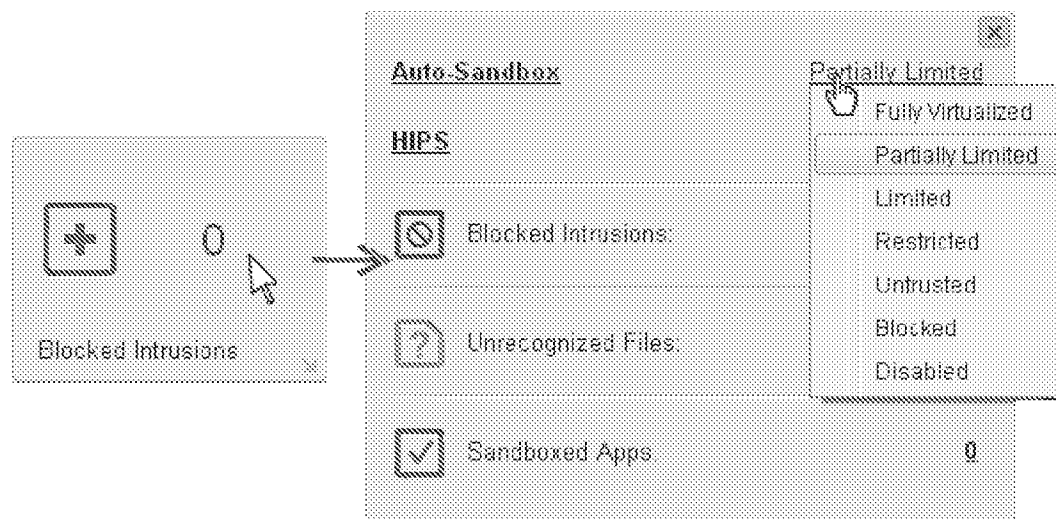
- Click 'Antivirus' at upper-left to open the 'Realtime Scanner Settings' interface. Refer to the section 'Real-

time Scanner Settings' for more details.

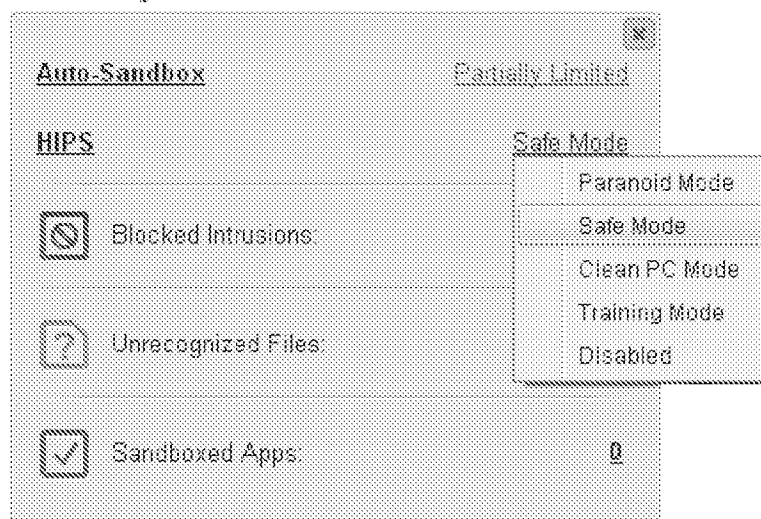
- Click the number of threats detected to open the Antivirus Log Viewer Module.
- Click the 'X' in the top right corner to return to the 4-tile view.
- **Firewall** - Click the Firewall tile to flip open a more detailed pane which displays the current firewall mode, the number of detected network intrusions, the number of current inbound and outbound connections and the share of network bandwidth used by internet-connected applications.
 - Click the link at the top-right to view or modify the current firewall mode. Refer to the section 'Firewall Behavior Settings' for more details.



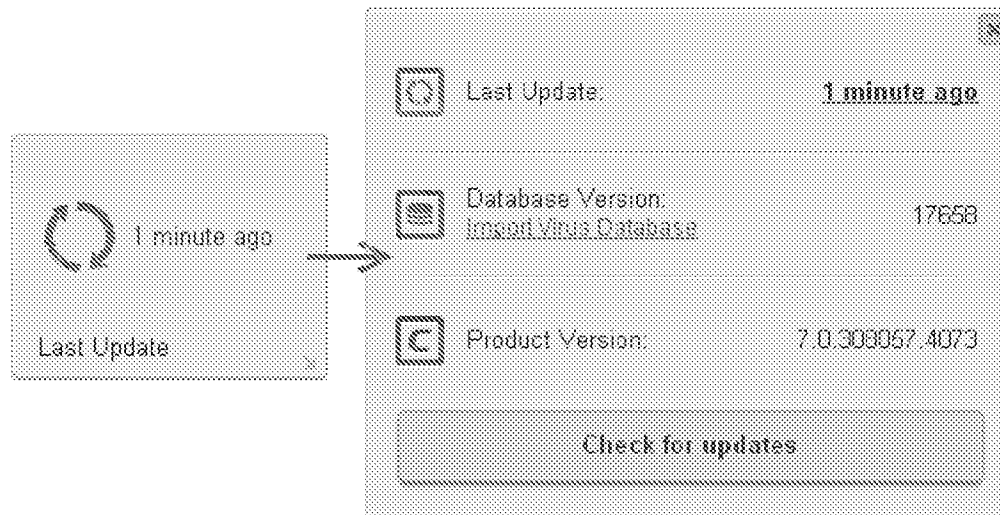
- Click 'Firewall' to open the detailed 'Firewall Settings' interface. Refer to the section 'Firewall Behavior Settings' for more details.
- Click the number of detected network intrusions to open the Firewall Log Viewer Module.
- Click the numbers over 'inbound' and 'outbound' to open the View Connections dialog. You can also do this by clicking the application names at the bottom of the pane.
- Click the 'X' in the top right corner to return to the 4-tile view.
- **Defense+** - Click the Defense+ tile to flip open a more detailed pane which displays the current Auto-Sandbox and HIPS modes and a statistical summary of events handled by the Behavior Blocker component.
 - Click **Auto-Sandbox** to open the Behavior Blocker Settings interface. Refer to the section 'Behavior Blocker' for more details.
 - Click the link to the right of this to view and modify auto-sandbox security levels. Refer to the section 'Behavior Blocker' for more details.



- Click **HIPS** to open the 'HIPS Settings' interface. Refer to the section 'HIPS Behavior Settings' for more details.
- Click the link to the right of this to view and modify HIPS security modes. Refer to the section 'HIPS Behavior Settings' for more details.



- Click the number of Blocked Intrusions to open the Defense+ Log Viewer module.
- Click the number of Unrecognized Files to open the Unrecognized Files interface.
- Click the number of Sandboxed Apps to open the Active Process List dialog.
- **Updates** - Click the 'Updates' tile to open a more detailed pane which displays when the virus database was last updated, the database version number and the software version number.

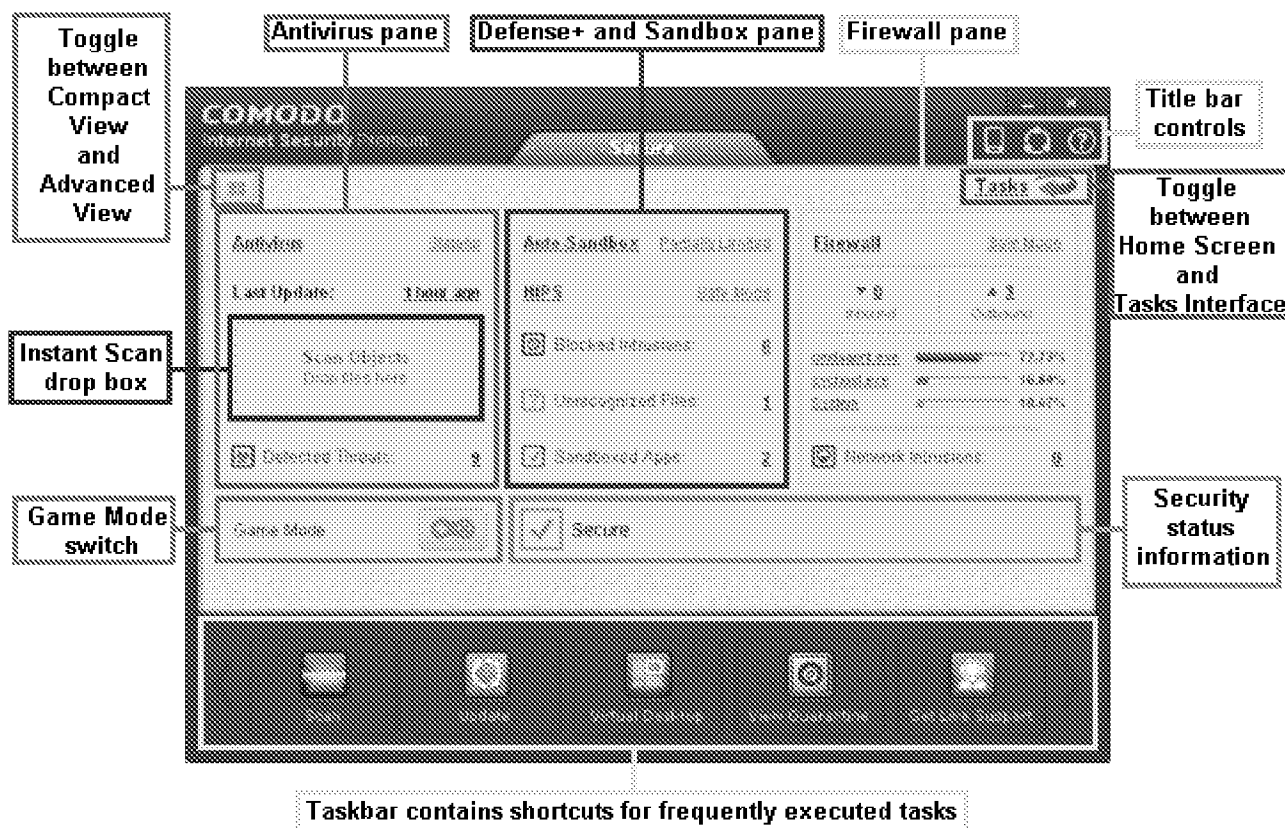


- Click on either the time of the last update or the 'Check for Updates' button to manually check for available updates. Refer to the section Manage Virus Database and Product Updates section for more details.
- Click the 'X' in the top right corner to return to the 4-tile view.

Advanced View

The 'Advanced View' provides a more finely-detailed view of the security status of each of the Antivirus, Defense+ and Firewall components.

Switch to advanced view by clicking the toggle button at the top-left of the home screen:

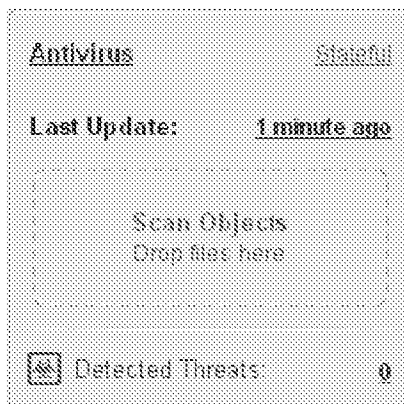


Click the following links to find out more:

- [Antivirus Pane](#)
- [Defense+ and Sandbox Pane](#)
- [Firewall Pane](#)

Antivirus Pane

The Antivirus pane allows you to configure antivirus mode, see when the virus database was last updated, view antivirus logs and instantly scan files and folders.

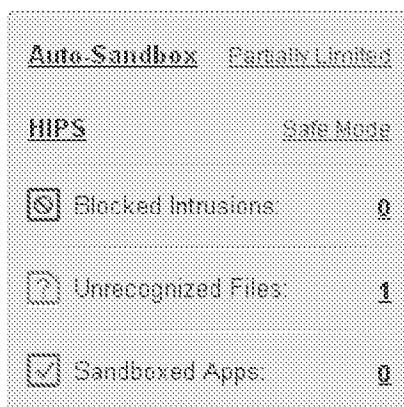


- **Antivirus** - Displays the current security level of the real-time antivirus scanner. Click on the security mode text to quickly switch between modes. Click 'Antivirus' to open the Realtime Scanner Settings interface. Refer to the section 'Real-time Scanner Settings' for more details.
- **Last Update** - Displays when the virus database was updated. Click the text link to start the updates again.

- **Detected Threats** - Displays the number of malware threats discovered so far from the start of current session as a link. Clicking this number will open the Antivirus Logs panel.
- **Scan Objects** - Drag-and-drop files, folders or even entire drives into this box to instantly scan them. Refer to the section *Instantly Scan Files and Folders* for more details.

Defense+ and Sandbox Pane

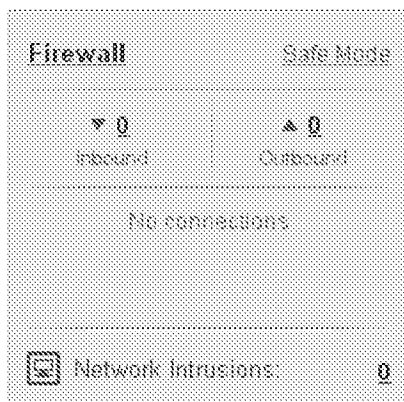
The Defense+ and Sandbox Pane allows you to quickly configure Auto-Sandbox and HIPS settings, view Defense+ logs and easily view the number of blocked intrusions, unrecognized files and sandboxed applications.



- **Auto-Sandbox** - Displays the current security level of the Behavior Blocker. Click on the security level itself to view or change it. Click **Auto-Sandbox** to open the 'Behavior Blocker Settings interface.' Refer to the section 'Behavior Blocker' for more details.
- **HIPS** - Click the text of the current HIPS mode to view or modify the mode. Click the word HIPS to open the 'HIPS Settings' interface. Refer to the section 'HIPS Behavior Settings' for more details.
- **Blocked Intrusions** - Displays the number of intrusions blocked by HIPS. Clicking on the numbered link will open the Defense+ logs. Refer to the section *Defense+ Logs* for more details.
- **Unrecognized Files** - Displays the number of files that are not recognized by CIS. These files may be considered as awaiting categorization. Clicking on the numbered link will open the Unrecognized Files screen which will allow you to run a file-lookup and to submit unknown files to Comodo for analysis. Refer to the section *Unrecognized Files* for more details.
- **Sandboxed Apps** - Displays the number of applications that are currently running inside the sandbox. Clicking the numbered link beside it will open the 'Active Processes List (Sandboxed Only)', which provides details of currently sandboxed applications. Refer to the section *View Active Process List* for more details.

Firewall Pane

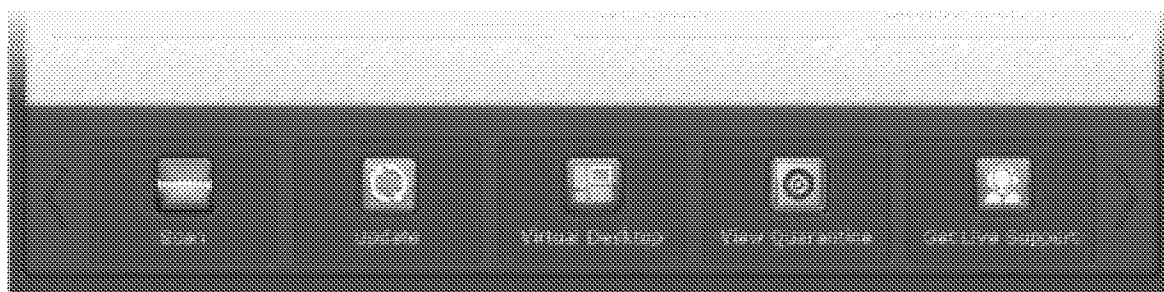
The Firewall Pane allows you to configure Firewall settings, view the number of inbound and outbound connections and the number of network intrusion attempts blocked by Firewall since the start of current session of CIS.



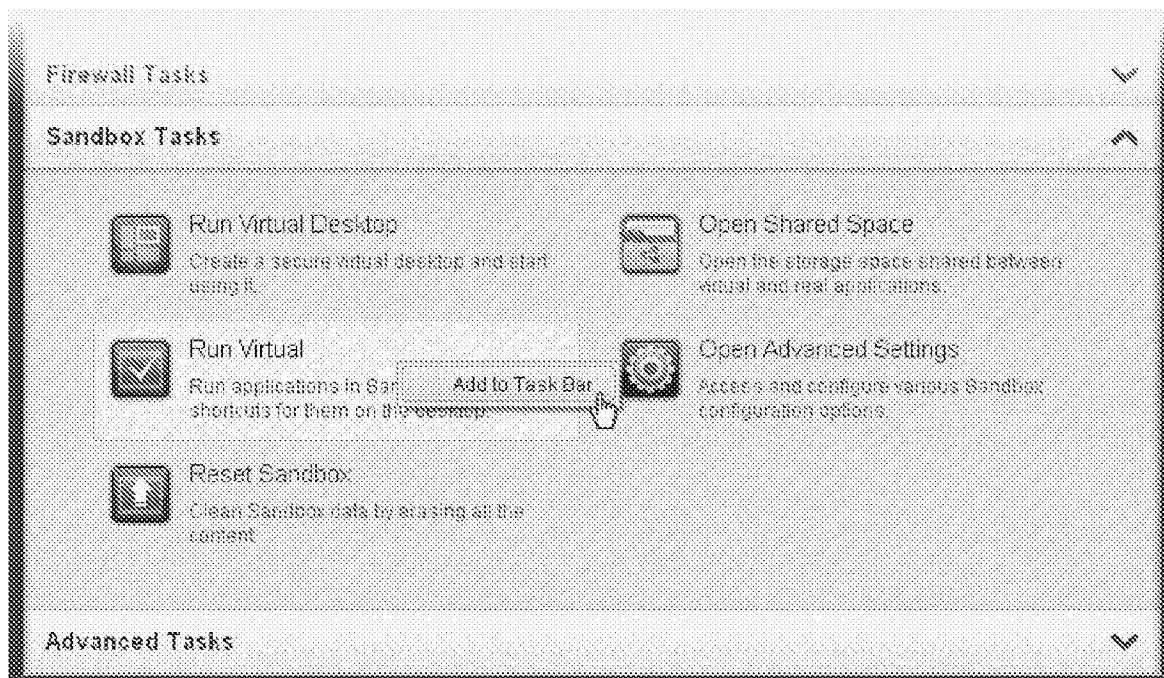
- **Firewall** - Displays the firewall's current security mode. Click on the level itself to quickly view and modify it. Click on **'Firewall'** to open the Firewall Settings interface. Refer to the section 'Firewall Behavior Settings' for more details.
- **Inbound / Outbound Connections** - A numerical summary of currently active inbound and outbound connections to and from the system. Clicking on the numbered link will open the View Connections screen. Refer to the section 'View Active Internet Connections' for more details.
- **Traffic** - The Traffic area of the pane displays a bar graph showing applications that are currently connected to the internet and are sending or receiving data. The summary also displays the % of total traffic each application is responsible for and the filename of the executable. Clicking on any application name will open the View Connections screen.
- **Network Intrusions** - Displays the total number of intrusion attempts blocked by firewall since the start of the current session. Clicking on the numbered link will open the Firewall Logs screen. Refer to the section 'Firewall Logs' for more details.

Adding tasks to the Task Bar

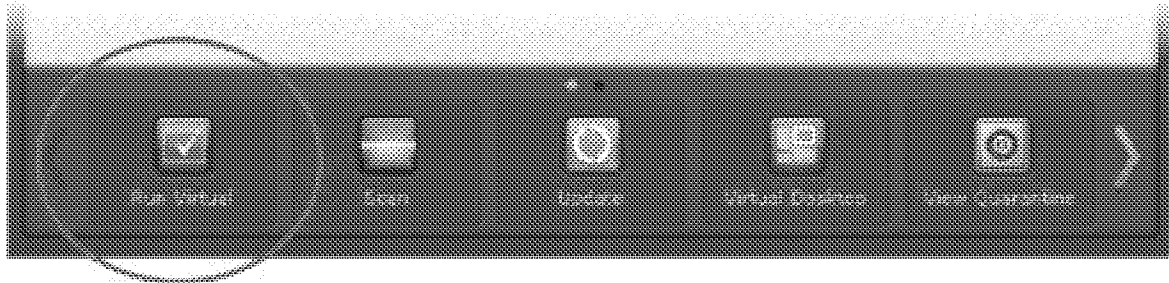
The task bar contains a set of shortcuts which will launch common tasks with a single click. You can add any task you wish to this toolbar. Click the handles < > on the left and right sides of the task bar to scroll through all tasks.



- To add a task to the Task Bar, first open the tasks interface by clicking the curved arrow at the top right: 
- Expand any one of the 'General', 'Firewall', 'Sandbox' or 'Advanced Tasks' menus.
- Right-click on the task you wish to add then click the message 'Add to Task Bar'.

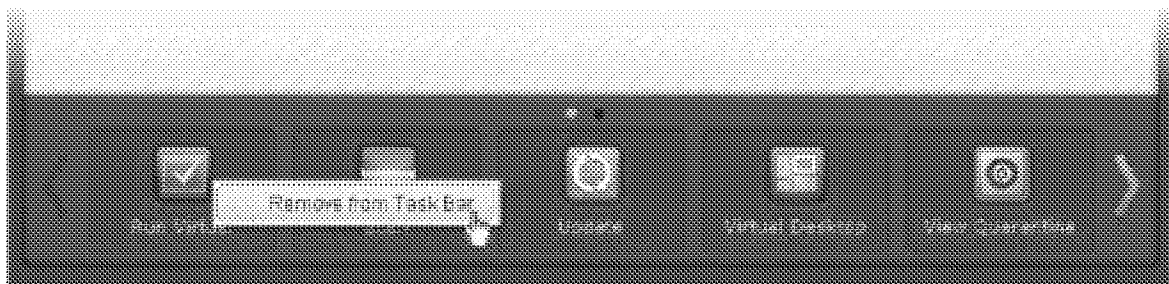


- The selected task will be added to the Task Bar.



Tip - Many will find it useful to add 'Open Advanced Settings' to the task-bar as it contains several areas important to the configuration of CIS. To do this, from the 'Home' screen, click the 'Tasks' arrow at upper-right, click 'Advanced Tasks' then right-click on 'Open Advanced Settings' and select 'Add to Task Bar'.

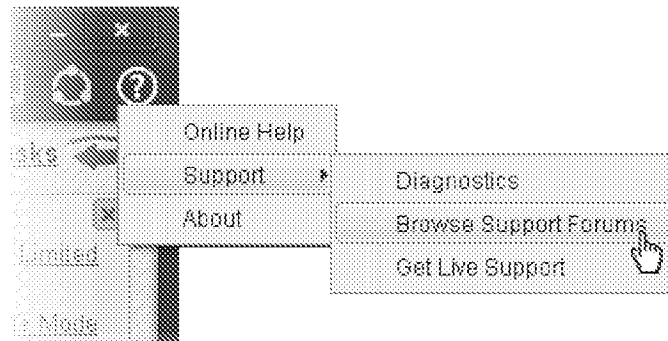
- To remove a task shortcut from the Task Bar, right click on it and choose 'Remove from task bar'.



Title bar controls

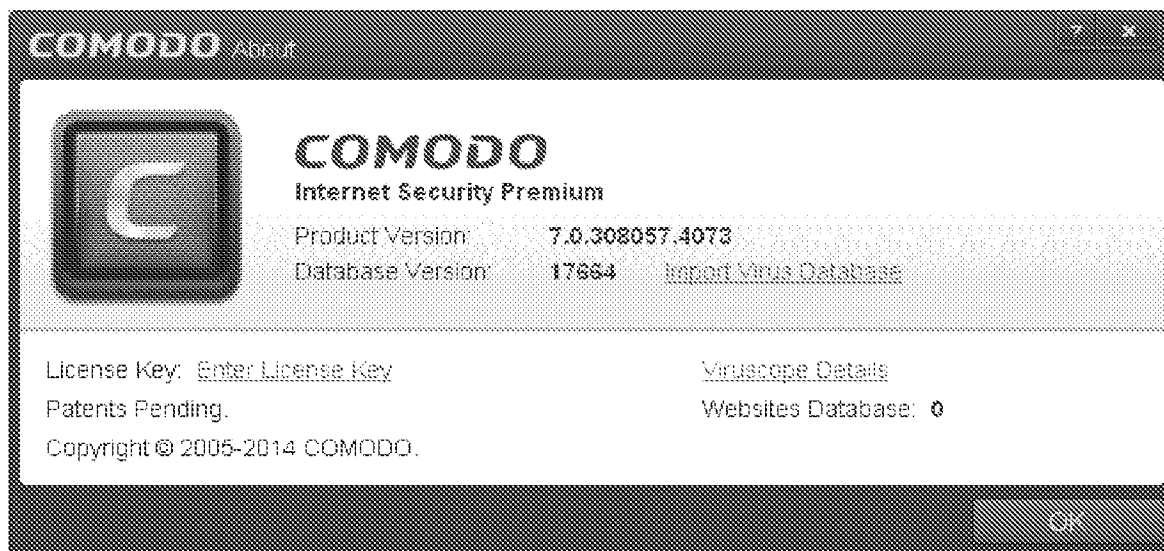
The title bar (top right) contains shortcuts for:

- Comodo Mobile Security app for Android phones and tablets. - Click the mobile icon  and scan the QR code with your device to download the latest version of the app. You can also get the app from our website, <https://im.comodo.com/> or from the Google Play app store at <https://play.google.com/store/apps/details?id=com.comodo.pimsecure>
- Refer your Friends - Click the  icon to open the 'Comodo Friends' website. Register an account for free, recommend CIS to your friends and get attractive rewards. Visit <http://friends.comodo.com/> for more details.
- Get Help - Click the help icon  for the following options:



- Online Help - Opens Comodo Internet Security's online help guide at <http://help.comodo.com/topic-72-1-522-6207-Introduction-to-Comodo-Internet-Security.html>.
- Support - Click this link for the following options:
- Diagnostics - Helps to identify any problems with your installation.

- Browse Support Forum - Links to Comodo User Forums.
- Get Live Support - Launches the GeekSuddy support client.
- **About** - Displays the product version, virus signature database version, website database version (website filtering URLs), details of active Viruscope Recognizers and copyright information. The 'About' dialog also allows you to import a locally stored virus database and to enter a license key for CIS Pro.



- Click [Import Virus Database](#) to import a locally stored virus signature database into CIS.
- Click [Enter License Key](#) to upgrade to CIS Pro. Refer to the section 'Activating CIS Pro/Complete Services after Installation' for more details.
- Click [Viruscope Details](#) to open a dialog which shows the Viruscope Recognizers that are active on your system. Refer to the Behavior Blocker section for more details.

Game mode

Game Mode enables you to play your games without interruptions or alerts. Operations that can interfere with a user's gaming experience are either suppressed or postponed.

In game mode:

- Defense+/Firewall alerts are suppressed.
- AV database updates and scheduled scans are postponed until the gaming is over;
- Automatic isolation of unknown applications and real-time virus detection are still functional.

To switch to Game mode

- Click the Game Mode switch at the bottom left of the Home Screen



- Deactivate Game Mode to resume alerts and scheduled scans.

1.5.2. The Tasks Interface

The items in the 'Tasks' area allow you to configure every aspect of Comodo Internet security.



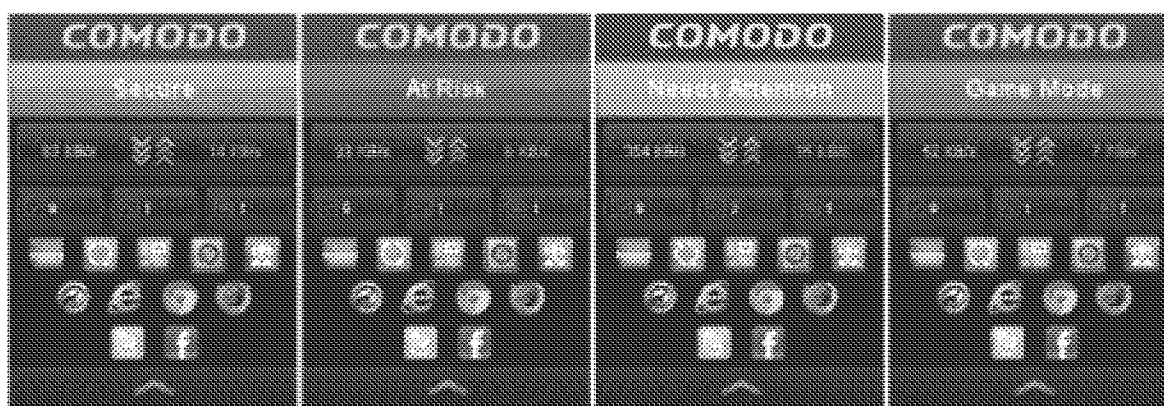
Tasks are broken down into four main sections. Click the following links for more details on each:

- **General Tasks** - Run antivirus scans, update virus database, view and manage quarantined threats, view logs of security events, activity and alerts and get live support. Refer to the section **General Tasks** for more details.
- **Firewall Tasks** - Allow or block applications, manage ports, manage networks and configure advanced firewall settings. Refer to the section **Firewall Tasks** for more details.
- **Sandbox Tasks** - Run applications in a virtual environment and configure sandbox settings. Refer to the section **'Sandbox Tasks'** for more details.
- **Advanced Tasks** - Create a boot disk to clean up highly infected systems; install other Comodo software like KillSwitch and Clearing Essentials; submit files to Comodo for analysis and gain access to the **'Advanced Settings'** interface. Refer to the section **'Advanced Tasks'** for more details.

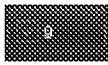
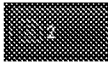
1.5.3. The Widget

The CIS Widget is a handy control that lives on your desktop and provides at-a-glance information about overall security status, inbound and outbound traffic, sandboxed applications, unrecognized files and more. The Widget starts automatically with CIS unless it is disabled from the System Tray icon or in the **'User Interface'** of **General Settings**.

Right clicking on the Widget opens a context sensitive menu similar to the one displayed when you right click on the CIS system tray icon. The context sensitive menu allows you to enable or disable CIS components and configure various settings. Refer to section **The System Tray Icon** for more details.



- The color coded row at the top of the widget displays your current security status. Double-clicking on 'At Risk' or 'Needs Attention' opens the appropriate interface for you to take action immediately.
- The second row displays information about incoming and outgoing network traffic. The network traffic row is displayed only if 'Show Traffic pane' under 'Widget options' of CIS tray icon or Widget right click menu is enabled. Refer to The System Tray Icon for more details. **(Default = Enabled)**
- The third row tells you current status of the CIS application:

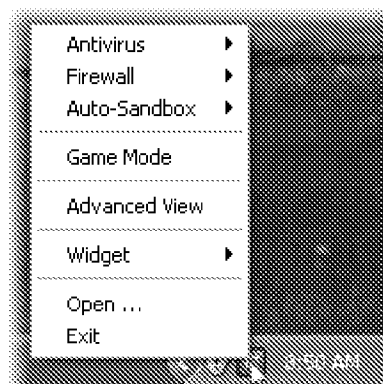
- The first button  displays the number of programs/processes that are currently running in the sandbox. Clicking the button opens the Active Process List interface, which allows you to identify and terminate unnecessary processes. Clicking the 'More' button in this interface will open the KillSwitch application. If KillSwitch is not yet installed, clicking this button will prompt you to download the application. Refer to the sections View Active Process List and Identify and Kill Unsafe Processes for more details.
- The second button  tells you how many CIS tasks are currently running. Clicking this button opens the Windows Task Manager interface.
- The third button  displays how many files have been added to the 'Unrecognized Files' list and are pending submission to Comodo for analysis. Clicking this button opens the Unrecognized Files interface.

The status row is displayed only if 'Show Status Pane' is enabled. Check this by right clicking the tray icon or the widget itself and look under 'Widget' options. Refer to The System Tray Icon for more details. **(Default = Disabled)**

- The forth row contains shortcuts for the five common tasks you have in the task bar at the bottom of the home screen. Clicking the shortcut on the widget will run the task. The 'Common Tasks' row is displayed only if 'Show Common Tasks Pane' is enabled under 'Widget' options of the CIS tray icon or the widget right-click menu. Refer to The System Tray Icon for more details. **(Default = Enabled)**
- The fifth row displays the browsers installed on your computer. Clicking on a browser icon will open the browser inside the sandbox for a secure browsing session. You can tell the browser is running in the sandbox because it will have a green border around it. Refer to Running an application inside the sandbox for more details. The 'Browsers' row is displayed only if 'Show Browsers Pane' is enabled under the 'Widget' section of the CIS tray right-click menu. This can also be viewed by right-clicking the widget itself. Refer to The System Tray Icon for more details. **(Default = Enabled)**
- The last row on the widget provides links to social networking sites. This row is displayed only if 'Show Connect Pane' is enabled. To check this setting, right-click on the CIS tray icon and look at the 'Widget' section. Alternatively, right-click the widget itself. Refer to The System Tray Icon for more details. **(Default = Enabled)**
- You can expand or collapse the Widget by clicking the arrow at the bottom.

1.5.4. The System Tray Icon

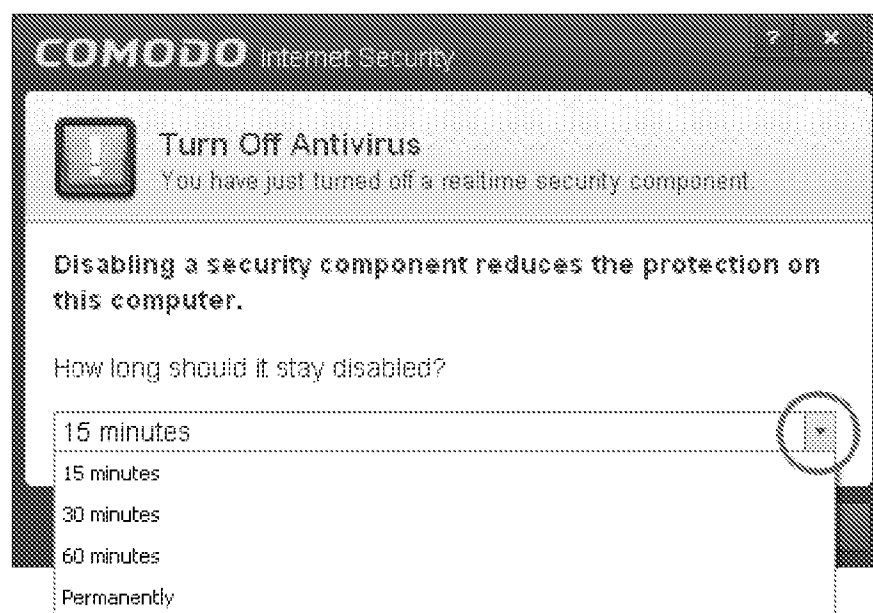
Double-clicking the system tray icon  will quickly open the CIS interface. Right-clicking the icon opens a context sensitive menu that allows you to configure various application settings:



The options available for the Antivirus, Firewall and Auto-sandbox menu-items depend on whether you are using Compact View or Advanced View.

Compact View	Advanced View
<p>Antivirus - You can enable or disable Real-time antivirus scan.</p> <p>Firewall - You can enable or disable Firewall.</p> <p>Auto-Sandbox - You can enable or disable Auto-Sandbox. Refer to the section 'Behavior Blocker' for more details.</p>	<p>Antivirus - Options available are On Access, Stateful and Disabled. Refer to Antivirus Pane for more details.</p> <p>Firewall - Options available are Block All, Custom Ruleset, Safe Mode, Training Mode and Disabled. Refer to the section 'Firewall Behavior Settings' for more details.</p> <p>Auto-Sandbox - Options available are Fully Virtualized, Partially Limited, Limited, Restricted, Untrusted, Blocked and Disabled. Refer to the section 'Behavior Blocker' for more details.</p> <p>HIPS - Options available are Paranoid Mode, Safe Mode, Clean PC Mode, Training Mode and Disabled. Refer to the section HIPS Behavior Settings for more details.</p>

If you disable either the antivirus, the firewall or the auto-sandbox from the right-click menu, then the security info bars on the main interface and the widget will turn red. You will also see a pop-up warning which allows you to specify how long the feature should remain disabled:



Select the period and click 'OK'. Unless you have selected 'Permanently', the security component will be automatically re-enabled after the stated time period has elapsed. You can, of course, manually re-enable at any time by right-clicking the tray icon and selecting 'Enable' for the component in question.

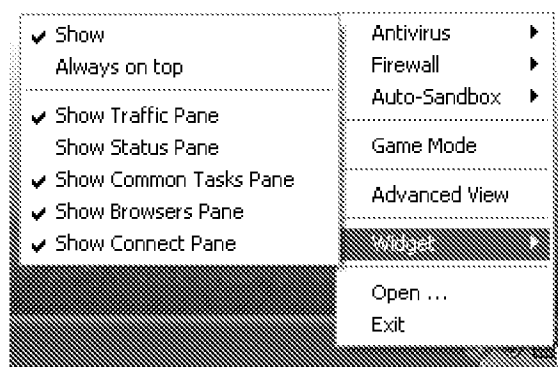
- **Game Mode** - Switches CIS into Game Mode so you can play your games without any interruptions from various alerts in your computer. Operations that can interfere with the gaming experience are either suppressed or postponed.

In game mode:

- Defense+/Firewall alerts are suppressed.
- AV database updates and scheduled scans are postponed until the gaming is over;
- Automatic isolation of unknown applications and real-time virus detection are still functional.

Deactivate Game Mode to resume alerts and scheduled scans.

- **Advanced View** - Switches the Home Screen between Compact View and Advanced View
- **Widget** - Select whether the Widget is shown and which widget components are included:



- **Show:** Toggles the widget on or off (*Default = Enabled*)
- **Always on top:** Displays the widget on top of all windows currently running on your computer. (*Default = Disabled*)
- **Show Traffic Pane:** Displays the network traffic row on the widget. (*Default = Enabled*)
- **Show Status Pane:** Displays the security status tab at the top of the widget. (*Default = Disabled*)
- **Show Common Tasks Pane:** Displays the row containing shortcuts to common CIS tasks. (*Default = Disabled*)
- **Show Browsers Pane:** Displays the row containing shortcuts to your installed browsers. (*Default = Enabled*)
- **Show Connect Pane:** Displays the row containing the shortcuts to social networking sites. (*Default = Enabled*)
- **Open** - Opens the CIS interface.
- **Exit** - Closes the CIS application.

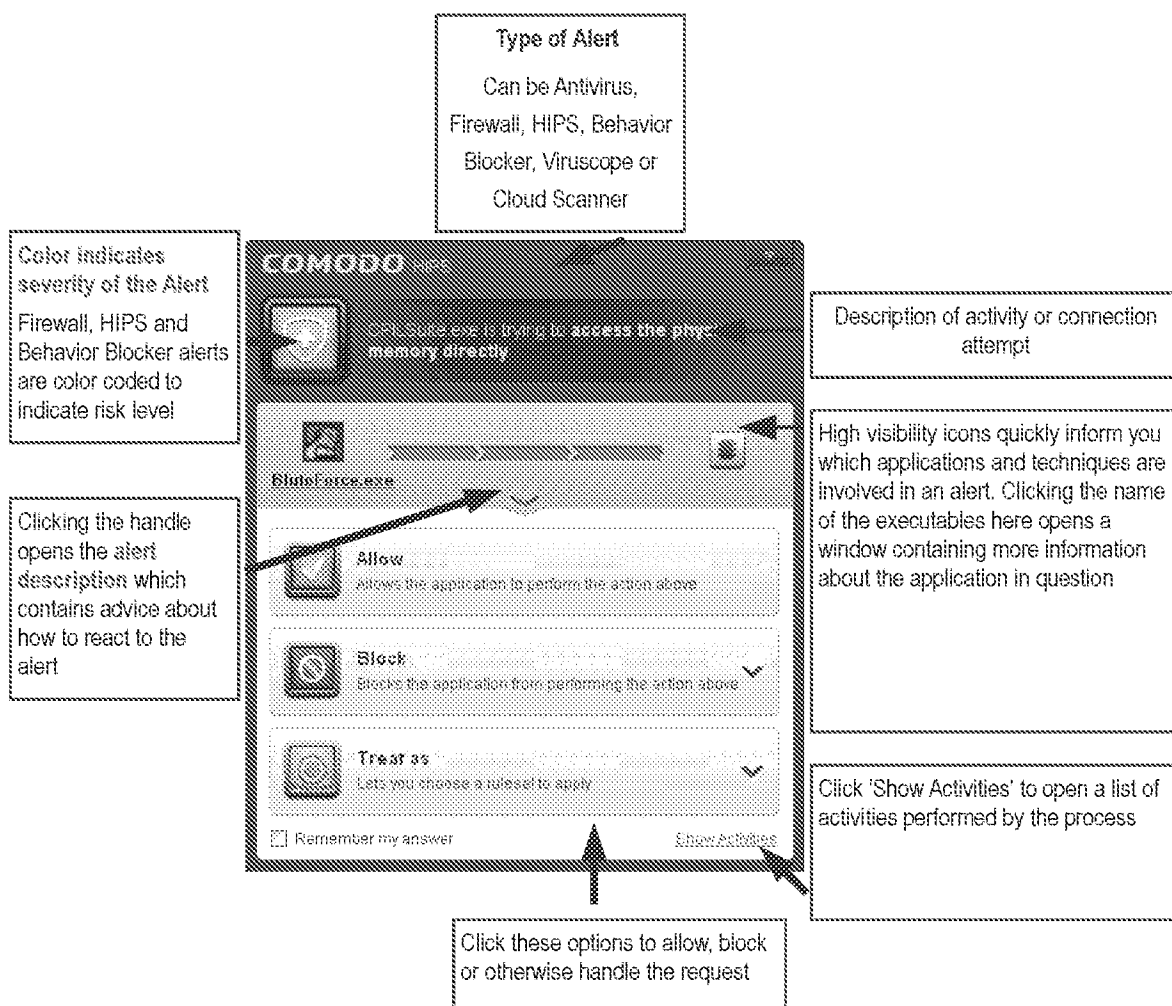
1.6. Understanding Security Alerts

- Alerts Overview
 - Alert Types
 - Severity Levels
 - Descriptions
- Antivirus Alerts
- Firewall Alerts
- HIPS Alerts

- Behavior Blocker Alerts
- Elevated Privilege Alerts
- Auto-Sandbox Alerts
- Viruscope Alerts

Alerts Overview

CIS alerts warn you about security related activities at the moment they occur. Each alert contains information about a particular issue so you can make an informed decision about whether to allow or block it. Alerts also let you specify how CIS should behave in future when it encounters activities of the same type. The alerts also enable you to reverse the changes made to your computer by the applications that raised the security related event.



Alert Types

Comodo Internet Security alerts come in five main varieties. Click the name of the alert (at the start of the following bullets) if you want more help with a particular alert type.

- **Antivirus Alerts** - Shown whenever virus or virus-like activity is detected. AV alerts will be displayed only when Antivirus is enabled and the option 'Do not show antivirus alerts' is disabled in Real-time Scanner Settings.
- **Firewall Alerts** - Shown whenever a process attempts unauthorized network activity. Firewall alerts will be displayed only when the Firewall is enabled and the option 'Do not show popup alerts' is disabled in Firewall Settings.
- **HIPS Alerts** - Shown whenever an application attempts an unauthorized action or tries to access protected

areas. HIPS alerts will only be generated if HIPS is enabled and Do NOT show popup alerts is disabled.

- **Behavior Blocker Alerts (including Elevated Privilege Alerts)** - Shown whenever an application tries to modify operating system or related files and when the Behavior Blocker automatically sandboxes an unrecognizable file. Behavior Blocker / Auto-Sandbox Alerts will be displayed only when auto-sandboxing is enabled under Behavior Blocker settings. Privilege Alerts will only be shown if enabled.
- **Viruscope Alerts** - Shown whenever a currently running process attempts to take suspicious actions. Viruscope alerts allow you to quarantine the process & reverse its changes or to let the process go ahead. Be especially wary if a Viruscope alert pops up 'out-of-the-blue' when you have not made any recent changes to your computer. Viruscope Alerts will be displayed only when Viruscope is enabled under Behavior Blocker settings.

In each case, the alert may contain very important security warnings or may simply occur because you are running a certain application for the first time. Your reaction should depend on the information that is presented at the alert.

Note: This section is concerned only with the security alerts generated by the Antivirus, Firewall, HIPS and Behavior Blocker components of CIS. For other types of alert, see Comodo Message Center notifications, Notification Messages and Information Messages.

Severity Level

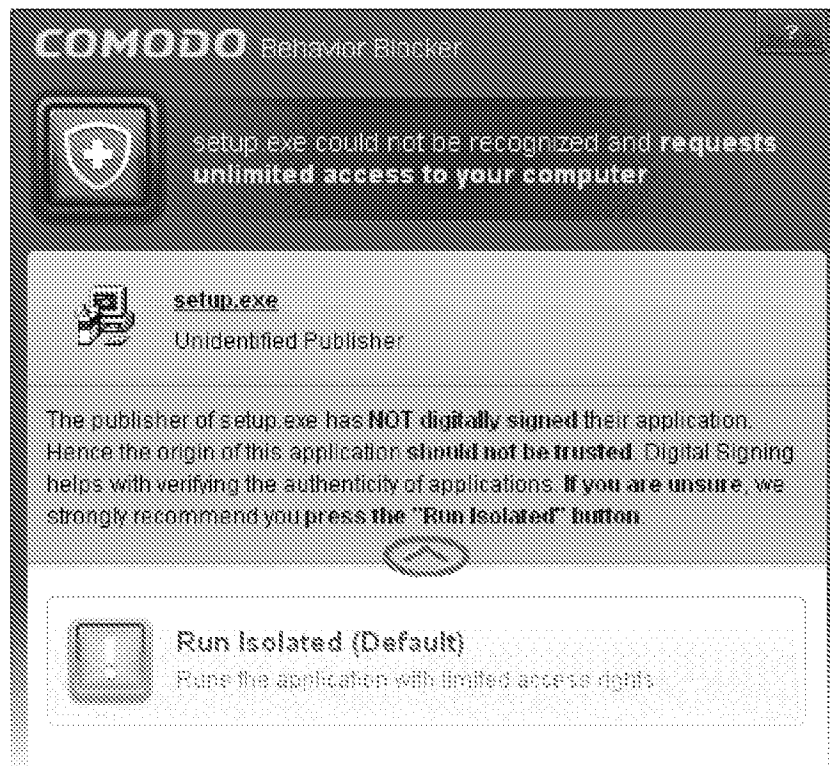
The shield icons at the upper left of each alert are color coded according to the risk level presented by the activity or request. However, it cannot be stressed enough that you should read the entire alert before reaching a decision on whether to allow or block the alert.

- **Yellow icons** - Low Severity - In most cases, you can safely approve these requests. The 'Remember my answer' option is automatically pre-selected for safe requests
- **Orange icons** - Medium Severity - Carefully read the information in the alert description area before making a decision. These alerts could be the result of a harmless process by a trusted program or indicative of a malware attack. If you know the application to be safe, then it is usually okay to allow the request. If you do not recognize the application performing the activity or connection request then you should block it.
- **Red icons** - High Severity - These alerts indicate highly suspicious behavior that is consistent with the activity of a Trojan horse, virus or other malware program. Carefully read the information provided when deciding whether to allow it to proceed.

Note: Antivirus alerts are not ranked in this way. They always appear with a red icon.

Alert Description

The description is a summary of the nature of the alert and can be revealed by clicking the handle as shown:



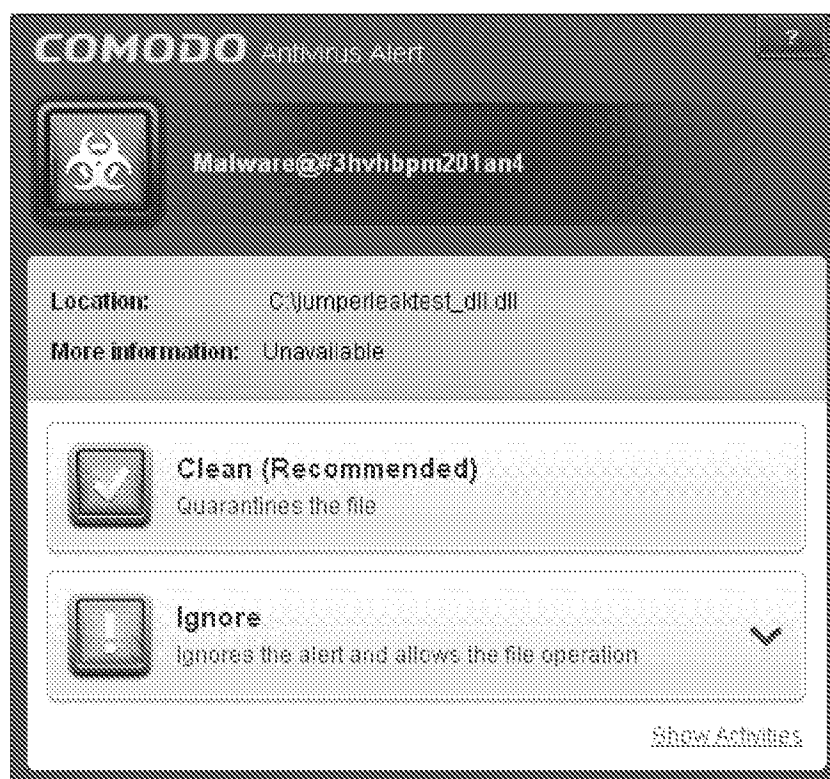
The description tells you the name of the software/executable that caused the alert; the action that it is attempting to perform and how that action could potentially affect your system. You can also find helpful advice about how you should respond.

Now that we've outlined the basic construction of an alert, let's look at how you should react to them.

Answering an Antivirus Alert

Comodo Internet Security generates an Antivirus alert whenever a virus or virus-like activity is detected on your computer. The alert contains the name of the virus detected and the location of the file or application infected by it. Within the alert, you are also presented with response-options such as 'Clean' or 'Ignore'.

Note: Antivirus alerts will be displayed only if the option 'Do not show antivirus alerts' is disabled. If this setting is enabled, antivirus notifications will be displayed. This option is found under 'Security Settings > Antivirus > Realtime Scan'. Refer to Real-time Scanner Settings for more details.



Tip: Clicking the [Show Activities](#) link at the bottom right will open the **Process Activities List** dialog. The Process Activities dialog will display the list activities of the processes run by the application.

The [Show Activities](#) link is available only if Viruscope is enabled under **Advanced Settings > Defense+ > Behavior Blocker Settings**. If none of the processes associated with the infected application has started before the alert is generated, the [Show Activities](#) link is disabled and will not open the Process Activities List dialog.

The following response-options are available:

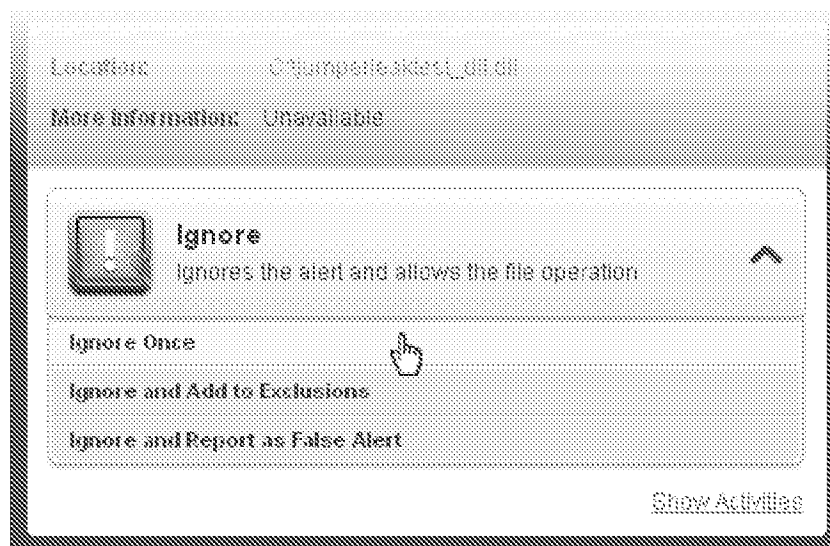
- **Clean** - Disinfects the file if a disinfection routine exists. If no routine exists for the file then it will be moved to Quarantine. If desired, you can submit the file/application to Comodo for analysis from the Quarantine interface. Refer to [Manage Quarantined Items](#) for more details on quarantined files.

The Viruscope subsystem integrated with the Antivirus, also monitors the changes made to your computer by the virus or virus-like activities automatically reverts them, if you choose to clean the infected file or application, when Viruscope is enabled under Behavior Blocker settings.

Note: Though Viruscope has power to reverse majority of types of changes effected by the process(es) evoked by blocked applications, it has some limitations. Very few of the file activities that make permanent changes could be reverted. Examples include:

- Deletion of a file
- Moving a file to a different folder/location
- Loading a file image into a process, i.e. DLL file loading

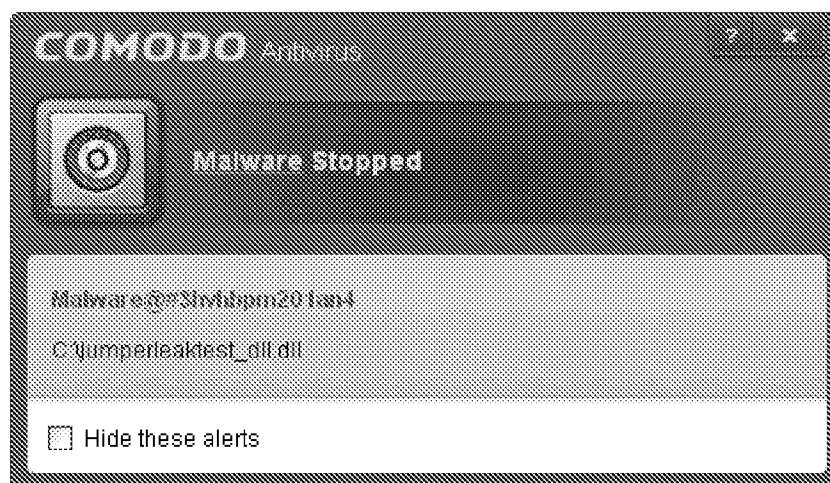
- **Ignore** - Allows the process to run and does not attempt to clean the file or move it to quarantine. Only click 'Ignore' if you are absolutely sure the file is safe. Clicking 'Ignore' will open three further options:



- **Ignore Once** - The file is allowed to run this time only. If the file attempts to execute on future occasions, another antivirus alert is displayed.
- **Ignore and Add to Exclusions** - The file is allowed to run and is moved to the Exclusions list - effectively making this the 'Ignore Permanently' choice. No alert is generated if the same application runs again.
- **Ignore and Report as a False Alert** - If you are sure that the file is safe, select 'ignore and Report as a False Alert'. CIS will then submit this file to Comodo for analysis. If the false-positive is verified (and the file is trustworthy), it will be added to the Comodo safe list.

Antivirus Notification

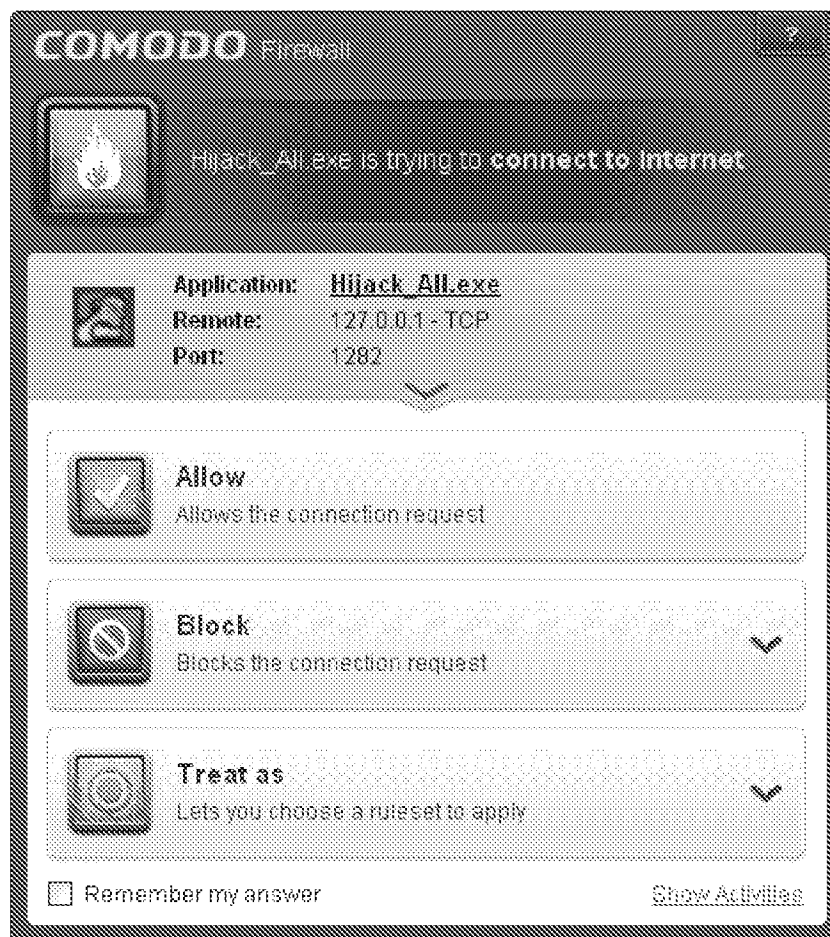
If you have chosen to not to show Antivirus Alerts through **Advanced Settings > Security Settings > Antivirus Settings > Realtime Scanner Settings** by leaving the option 'Do not show antivirus alerts' enabled (**default-enabled**) and if CIS identifies a virus or other malware in real time, it will immediately block malware and provide you with instant on-screen notification:



Please note that these antivirus notifications will be displayed only when 'Do not show antivirus alerts' check box in **Antivirus > Real-time Scan settings** screen is selected and 'Show notification messages' check box is enabled in **Advanced Settings > User interface** screen.

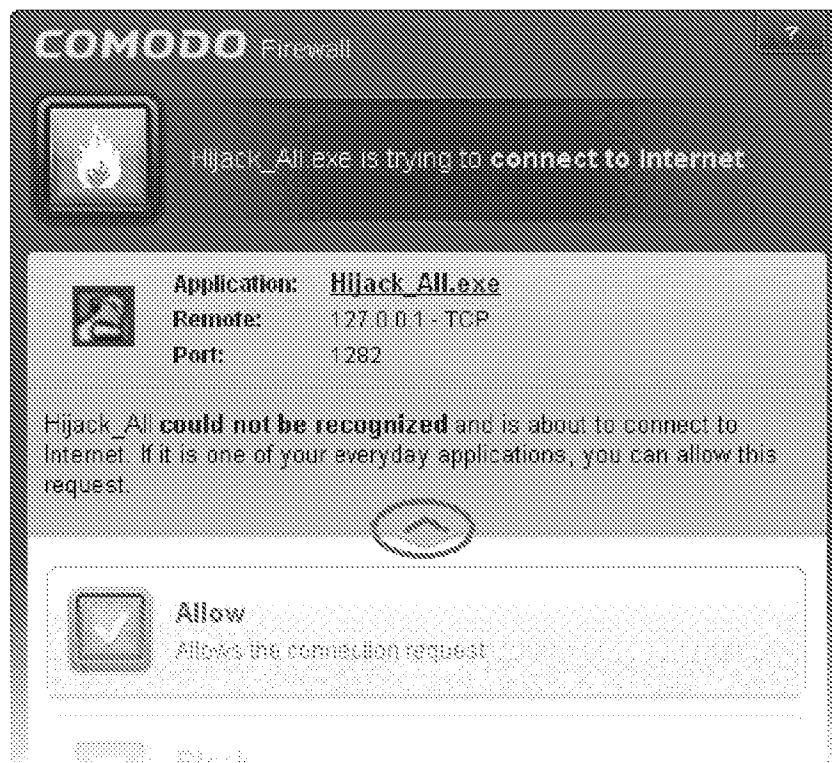
Answering Firewall Alerts

CIS generates a firewall alert when it detects unauthorized network connection attempts or when traffic runs contrary to one of your application or global rules. Each firewall alert allows you to set a default response that CIS should automatically implement if the same activity is detected in future. The followings steps will help you answer a Firewall alert:



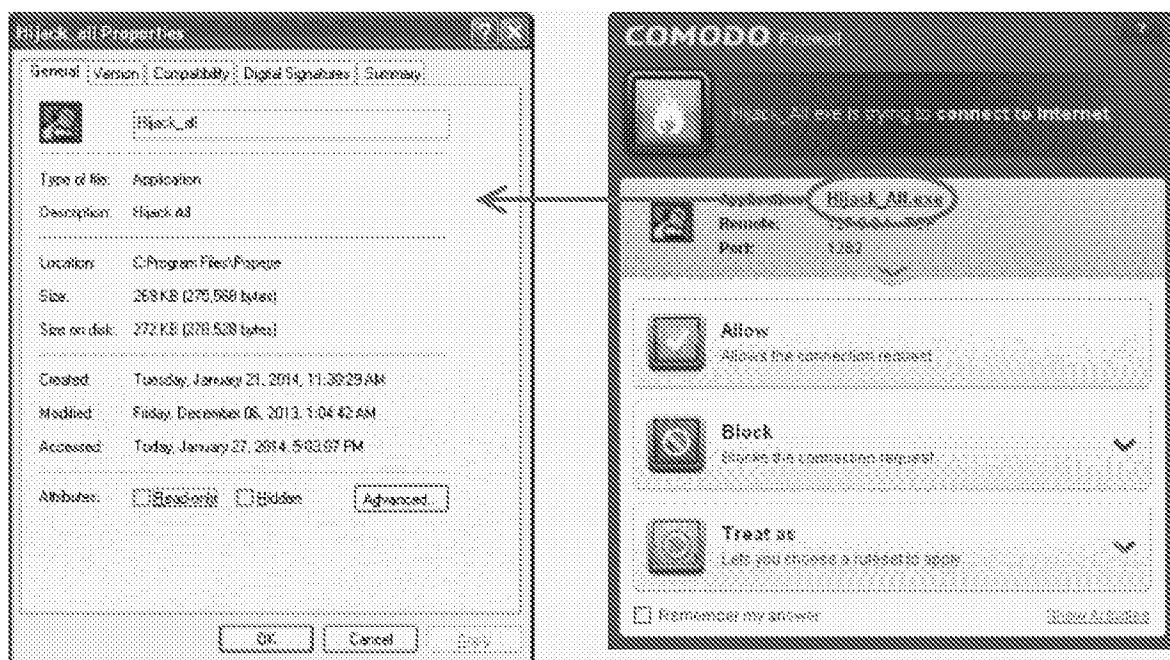
Tip: Clicking the [Show Activities](#) link at the bottom right will open the Process Activities List dialog. The Process Activities dialog will display the list activities of the processes run by the application.

The [Show Activities](#) link is available only if Viruscope is enabled under **Advanced Settings > Defense+ > Behavior Blocker Settings**. If none of the processes associated with the application that makes the connection attempt has started before the alert is generated, the [Show Activities](#) link is disabled and will not open the Process Activities List dialog.



1. Carefully read the information displayed in clicking the down arrow in the alert description area. The Firewall can recognize thousands of safe applications. (For example, Internet Explorer and Outlook are safe applications). If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe to proceed. Similarly, if the application is unknown and cannot be recognized you are informed of this.

If it is one of your everyday applications and you want to allow it Internet access to then you should select **Allow**.



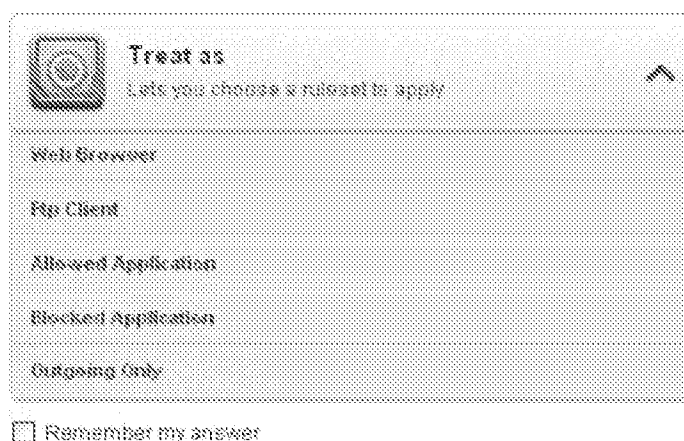
In all cases, clicking on the name of the application opens a properties window that can help you determine whether or not to proceed:

If you don't recognize the application then we recommend you **Block** the application. By clicking the handle to expand

the alert, you can choose to block the connection (connection is not allowed to proceed) or block & terminate (connection is not allowed to proceed and the process/application that made the request is shut down).



2. If you are sure that it is one of your everyday application, try to use the **'Treat As'** option as much as possible. This allows you to deploy a predefined firewall ruleset on the target application. For example, you may choose to apply the policy **Web Browser** to the known and trusted applications 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application.



Remember to check the box **Remember My Answer** for the ruleset to be applied in future.

3. If the Firewall alert reports a behavior, consistent with that of a malware in the security considerations section, then you should block the request AND select **Remember My Answer** to make the setting permanent.

Answering NIPS Alerts

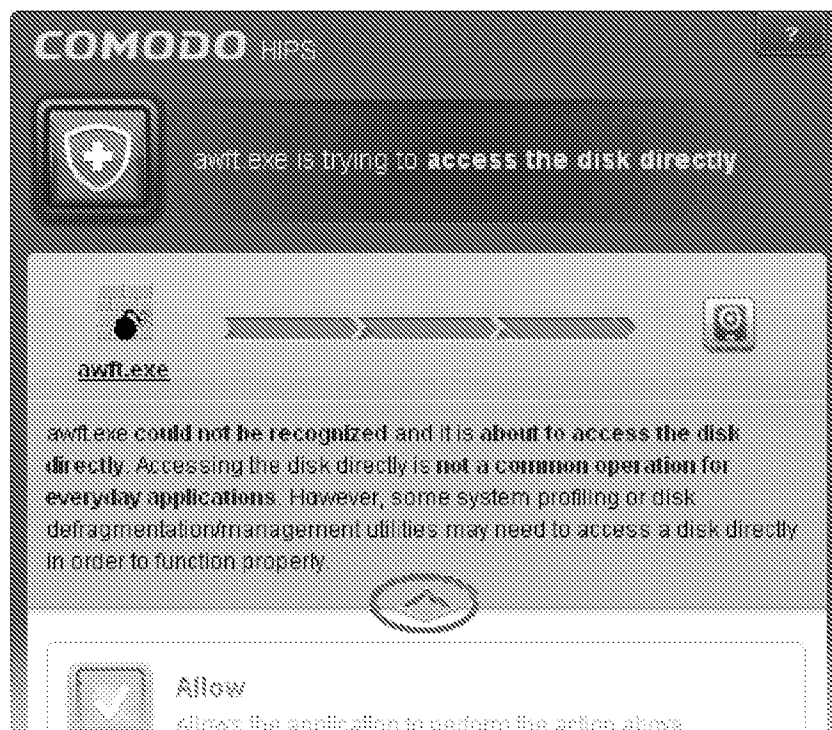
Comodo Internet Security generates a HIPS alert based on the behavior of applications and processes running on your system. Please read the following advice before answering a HIPS alert:



Tip: Clicking the [Show Activities](#) link at the bottom right will open the Process Activities List dialog. The Process Activities dialog will display the list activities of the processes run by the application.

The [Show Activities](#) link is available only if VirusScope is enabled under **Advanced Settings > Defense+ > Behavior Blocker Settings**. If none of the processes associated with the application has started before the alert is generated, the [Show Activities](#) link is disabled and will not open the Process Activities List dialog.

1. Carefully read the information displayed after clicking the handle under the alert description. Comodo Internet Security can recognize thousands of safe applications. If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe to proceed. Similarly, if the application is unknown and cannot be recognized, you are informed of this.



If it is one of your everyday applications and you simply want it to be allowed to continue then you should select **Allow**.

If you don't recognize the application then we recommend you select **Block** the application. You can choose to just block the connection or to block & terminate.



2. If you are sure that it is one of your everyday applications and want to enforce a security policy (ruleset) to it, please use the 'Treat As' option. This applies a predefined HIPS ruleset to the target application.

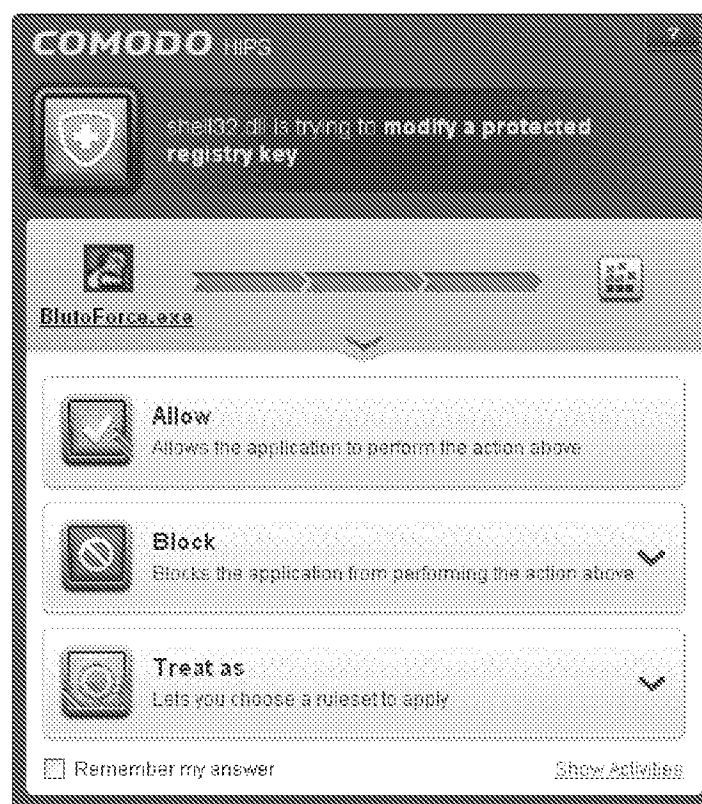


Avoid using the **Installer or Updater** ruleset if you are not installing an application. This is because treating an application as an 'Installer or Updater' grants maximum possible privileges onto to an application - something that is not required by most 'already installed' applications. If you select 'Installer or Updater', you may consider using it temporarily with **Remember My Answer** left unchecked.

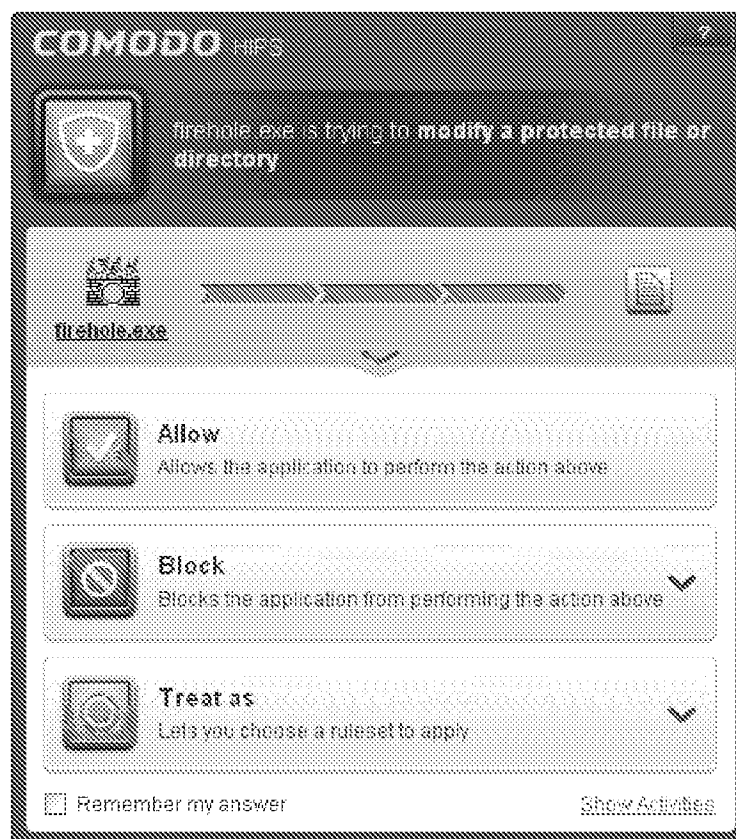
3. Pay special attention to **Device Driver Installation** and **Physical Memory Access** alerts. Again, not many legitimate applications would cause such an alert and this is usually a good indicator of malware / rootkit like behavior. Unless you know for a fact that the application performing the activity is legitimate, then Comodo recommends blocking these requests.



4. **Protected Registry Key Alerts** usually occur when you install a new application. If you haven't been installing a new program and do not recognize the application requesting the access, then a 'Protected Registry Key Alert' should be a cause for concern.



5. **Protected File Alerts** usually occur when you try to download or copy files or when you update an already installed application.



Were you installing new software or trying to download an application from the Internet? If you are downloading a file

from the 'net, select **Allow**, without selecting **Remember my answer** option to cut down on the creation of unnecessary rules within the firewall.

If an application is trying to create an executable file in the Windows directory (or any of its subdirectories) then pay special attention. The Windows directory is a favorite target of malware applications. If you are not installing any new applications or updating Windows then make sure you recognize the application in question. If you don't, then click **Block** and choose **Block Only** from the options, without selecting **Remember My answer** option.

If an application is trying to create a new file with a random file name e.g. "hughbasd.dll" then it is probably a virus and you should block it permanently by clicking **Treat As** and choosing **'Isolated Application'** from the options.

6. If a HIPS alert reports a malware behavior in the security considerations area then you should **Block the request** permanently by selecting **Remember My Answer** option. As this is probably a virus, you should also submit the application in question, to Comodo for analysis.
7. Unrecognized applications are not always bad. Your best loved applications may very well be safe but not yet included in the Comodo certified application database. If the security considerations section says "If xxx is one of your everyday applications, you can allow this request", you may allow the request permanently if you are sure it is not a virus. You may report it to Comodo for further analysis and inclusion in the certified application database.
8. If HIPS is in Clean PC Mode, you probably are seeing the alerts for any new applications introduced to the system - but not for the ones you have already installed. You may review the **'Unrecognized Files'** section for your newly installed applications and remove them from the list for them to be considered as clean.
9. Avoid using Trusted Application or Windows System Application policies for you email clients, web browsers, IM or P2P applications. These applications do not need such powerful access rights.

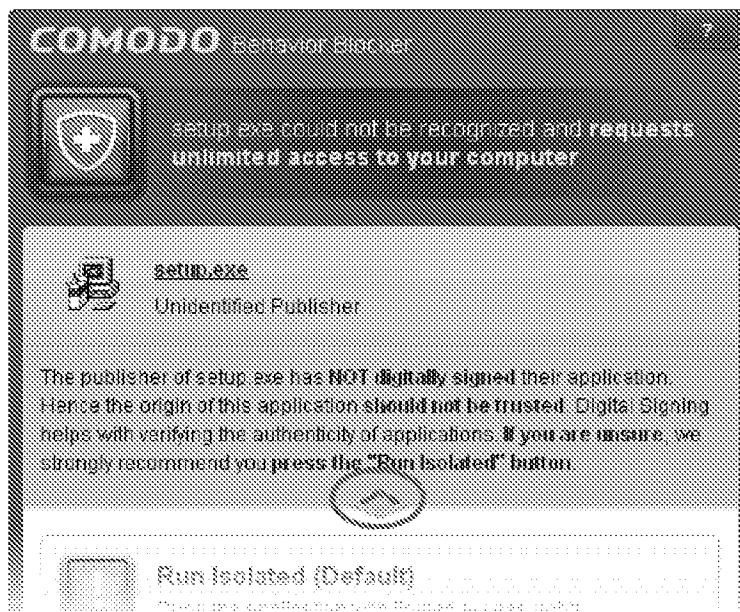
Answering a Behavior Blocker Alert

Comodo Internet Security generates a Behavior Blocker alert if an application or a process tries to perform certain modifications to the operating system, its related files or critical areas like Windows Registry and when it automatically sandboxes an unknown application.

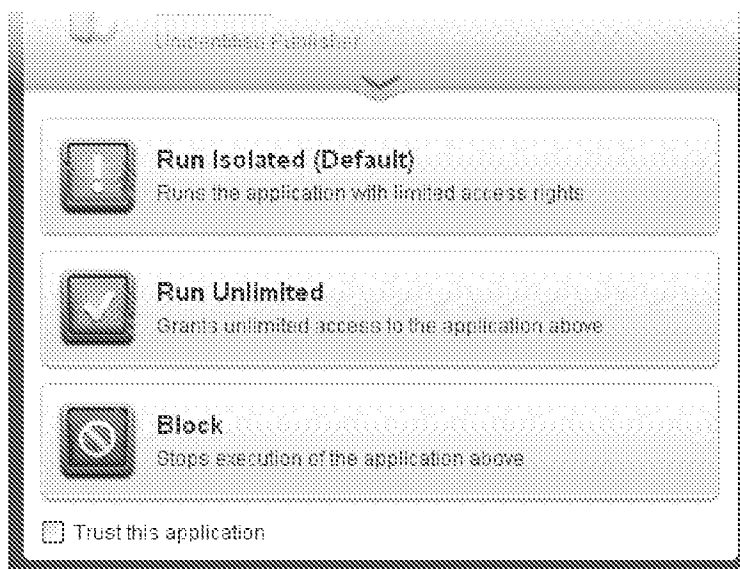
Please read the following advice before answering a Behavior Blocker alert:



1. Carefully read the information displayed after clicking the handle under the alert description. Comodo Internet Security can recognize thousands of safe applications. If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe to proceed. Similarly, if the application is unknown and cannot be recognized, you are informed of this.



- If you are sure that the application is authentic and safe and you simply want it to be allowed to continue then you should select **Run Unlimited**. If you want the application not to be monitored in future, select 'Trust this application' checkbox. The application will be added to Trusted Files list.



- If you are unsure of the safety of the software, then Comodo recommends that you run it with limited privileges and access to your system resources by clicking the 'Run Isolated' button. Refer to the section Unknown Files: The Auto-Sandboxing and Scanning process for more explanations on applications run with limited privileges.
- If you don't recognize the application then we recommend you select Block the application.

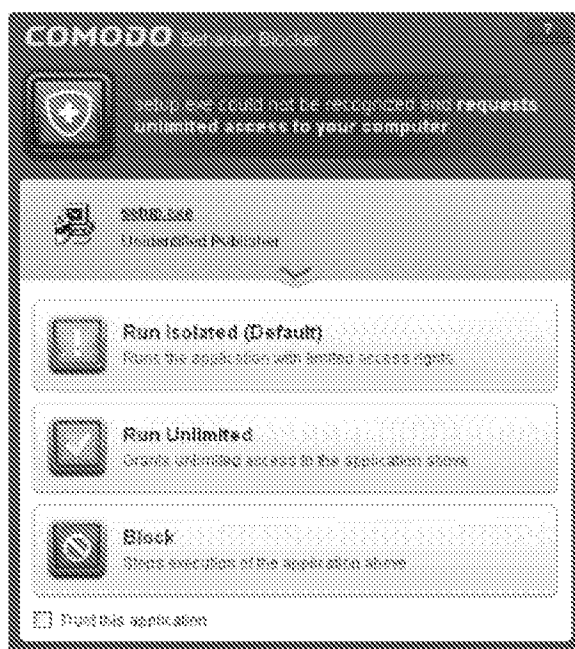
Run with Elevated Privileges Alert

The Behavior Blocker will display this kind of alert when the installer of an unknown application requires administrator, or elevated, privileges to run. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of your computer such as the registry.

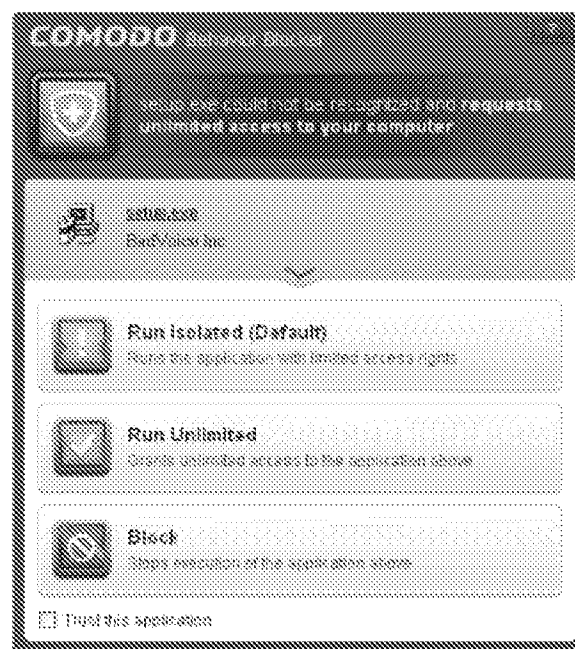
- If you have good reason to trust the publisher of the software then you can click the **'Run Unlimited'** button. This will grant the elevated privilege request and allow the installer to run.
- If you are unsure of the safety of the software, then Comodo recommends that you run it with restricted access to your system resources by clicking the **'Run Isolated'** button.
- If this alert is unexpected then you should abort the installation by clicking the **'Block'** button (for example, you have not proactively started to install an application and the executable does not belong to an updater program that you recognize)
- If you select **'Trust this application'** then CIS will include this to Trusted Files list and no future alerts will be generated when you run the same application.

Note: You will see this type of alert only if 'Detect installers and show privilege elevation alerts' is enabled. This can be found in 'Advanced Settings > Security Settings > Defense+ > Behavior Blocker'

There are two versions of this alert - one for unknown installers that are not digitally signed and the second for unknown installers that are digitally signed but the publisher of the software has *not yet* been white-listed (they are not yet a 'Trusted Software Vendor').



Unknown and not Digitally Signed



**Unknown and Digitally Signed but not yet whitelisted
(Not yet a 'Trusted Vendor')**

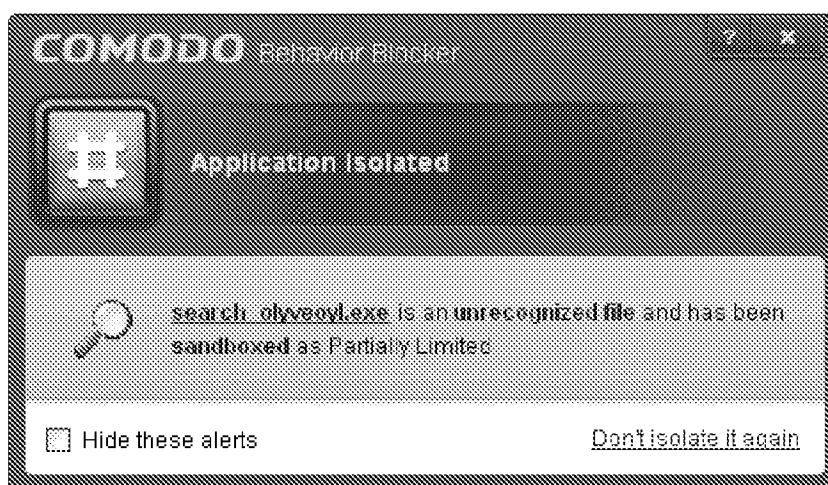
- Unknown and unsigned installers should be either isolated or blocked.
- Unknown but signed installers can be allowed to run if you trust the publisher, or may be isolated if you would like to evaluate the behavior of the application.

Also see:

- 'Unknown Files: The Auto-Sandboxing and Scanning Processes' - to understand the decision making process behind why CIS chooses to sandbox certain applications.
- 'Trusted Software Vendors' - for an explanation of digitally signed files and 'Trusted Software Vendors'.

Auto-Sandbox Alerts

The Behavior Blocker will display an alert whenever it auto-sandboxes an unknown application:



The alert will show the name of the executable that has been auto-sandboxed. The application will be automatically added to Unrecognized Files list.

- Clicking the name of the application will open the Unrecognized Files interface, that displays a list of the unrecognized files including the currently auto-sandboxed application.
- Clicking [Don't isolate it again](#) removes the application from the Unrecognized Files list and adds it to the Trusted Files list, so that the application will not be auto-sandboxed in future. Choose this option if you are absolutely sure that the executable is safe.

Users are also reminded that they should submit such unknown applications to Comodo via the 'Unrecognized Files' interface. This will allow Comodo to analyze the executable and, if it is found to be safe, to add it to the global safe list. This will ensure that unknown but ultimately safe applications are quickly white-listed for all users.

Also see:

- 'Unknown Files: The Auto-Sandboxing and Scanning Processes' - to understand the decision making process behind why CIS chooses to auto-sandbox certain applications.

Answering a Viruscope Alert

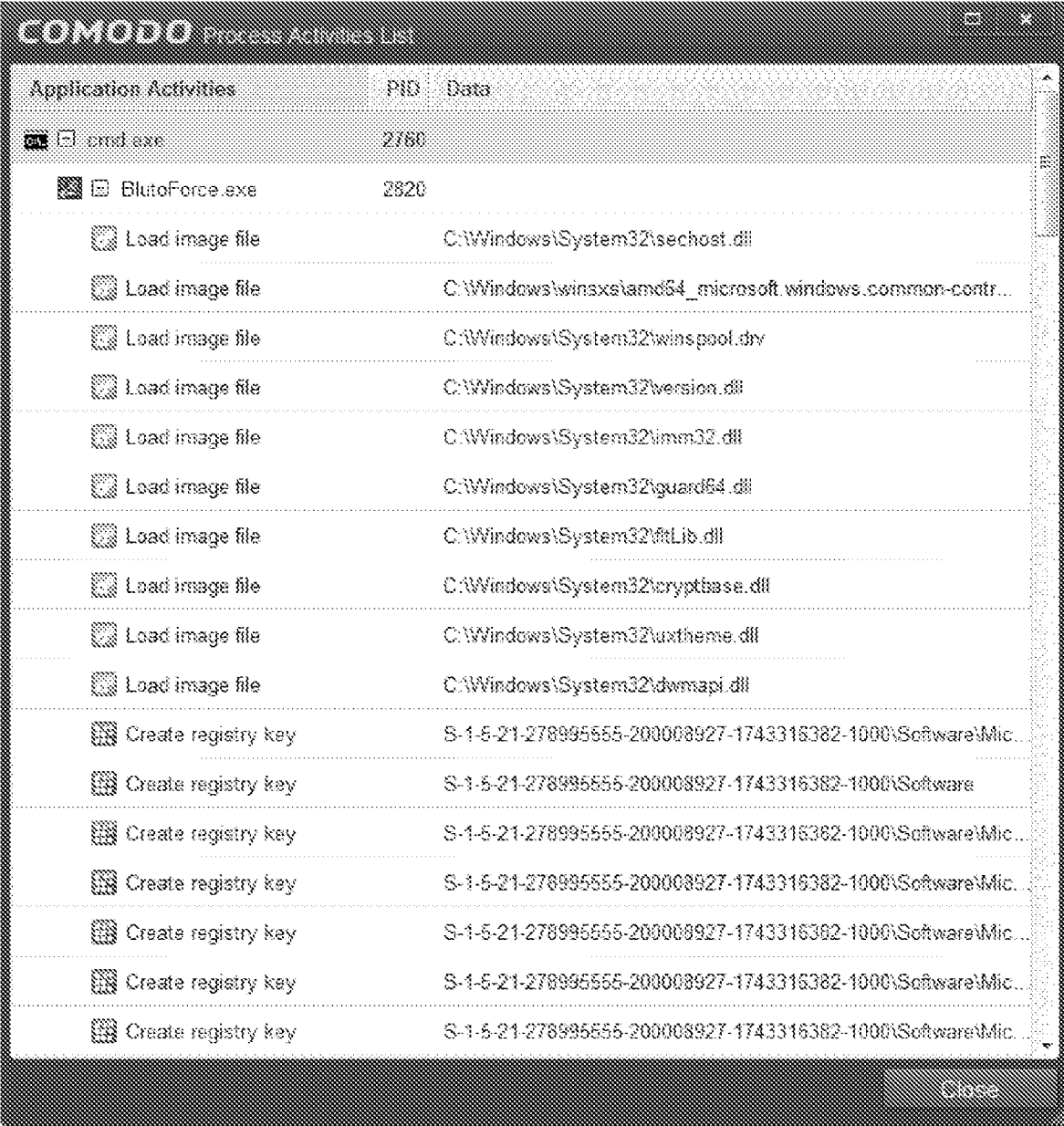
Comodo Internet Security generates a Viruscope alert if a running process performs an action that might represent a threat to your privacy and/or security. Please note that Viruscope alerts are not always definitive proof that malicious activity has taken place. Rather, they are an indication that a process has taken actions that you ought to review and confirm because they have the potential to be malicious. You can review all actions taken by clicking the '[Show Activities](#)' link.

Please read the following advice before answering a Viruscope alert:

1. Carefully read the information displayed in the alert. The 'More Information' section provides you the nature of the suspicious action.



- If you are not sure on the authenticity of the parent application indicated in the 'Application' field, you can safely reverse the changes effected by the process and move the parent application to quarantine by clicking 'Clean'.
- If it is a trusted application, you can allow the process to run, by clicking Ignore and selecting the option from the drop-down.
 - Ignore Once - The process is allowed to run this time only. If the process attempts to execute on future occasions, another Viruscope alert is displayed.
 - Ignore and Add to Trusted Files - The process is allowed to run and the parent application is moved to the Trusted Files list - effectively making this the 'Ignore Permanently' choice. No alert is generated if the same application runs again.
- To view the activities of the processes, click the [Show Activities](#) link at the bottom right. The Process Activities List dialog will open with a list of activities exhibited by the process.



Application Activities	PID	Data
cmd.exe	2760	
BlutoForce.exe	2820	
Load image file		C:\Windows\System32\sechost.dll
Load image file		C:\Windows\winsxs\xamd64_microsoft.windows.common-contr...
Load image file		C:\Windows\System32\winspool.drv
Load image file		C:\Windows\System32\version.dll
Load image file		C:\Windows\System32\imm32.dll
Load image file		C:\Windows\System32\guard64.dll
Load image file		C:\Windows\System32\ftLib.dll
Load image file		C:\Windows\System32\cryptbase.dll
Load image file		C:\Windows\System32\uxtheme.dll
Load image file		C:\Windows\System32\dwmapi.dll
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software\Mic...
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software\Mic...
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software\Mic...
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software\Mic...
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software\Mic...
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software\Mic...

Column Descriptions

- Application Activities - Displays the activities of each of the processes run by the parent application.
 -  - File actions: The process performed a file-system operation (create/modify/rename/delete file) which you might not be aware of.
 -  - Registry: The process performed a registry operation (created/modified a registry key) which might not be authorized.
 -  - Process: The process created a child process which you may not have authorized or have been aware of.
 -  - Network: The process attempted to establish a network connection that you may not have been aware of.
 - If the process has been terminated, the activities will be indicated with gray text and will appear in the list until you view the 'Process Activities List' interface. If you close the interface and reopen the list within five minutes, the activities will appear in the list. Else, the terminated activities will not be displayed in the list.
- PID - Process Identification Number.

- Data - Displays the file affected by the action.

2. General Tasks - Introduction

The 'General Tasks' interface allows you to quickly perform antivirus scans, update the virus database, manage quarantined files, view CIS event logs, view and manage internet connections and manage CIS running tasks.



'General Tasks' contains the following areas. Click the links to jump to the help page for that topic.

- [Scan and Clean your Computer](#)
- [Manage Virus Database and Program Updates](#)
- [Manage Quarantined Items](#)
- [View CIS Logs](#)
- [Get Live Support](#)
- [Manage CIS Tasks](#)
- [View Active Internet Connections](#)

2.1. Scan and Clean Your Computer

Comodo Antivirus leverages multiple technologies, including Real-time/On-Access Scanning and On-Demand Scanning to immediately start cleaning or quarantining suspicious files from your hard drives, shared disks, emails, downloads and system memory. The application also allows users to create custom scan profiles, time-table scheduled scans and features full event logging, quarantine and file submission facilities. When you want to run a virus scan on your system, you can launch an **On-Demand Scan** using the **Scan** option. This executes an instant virus scan on the selected item.



There are multiple types of antivirus scan that can be run from the 'Scan' interface. Click the links below to find out more on each:

- [Run a Quick Scan](#)
- [Run a Full Computer Scan](#)
- [Run a Rating Scan](#)
- [Run a Custom Scan](#)
 - [Scan a Folder](#)
 - [Scan a File](#)
 - [Create and Schedule a Custom Scan](#)

- Scan individual file/folder
- Processing Infected Files

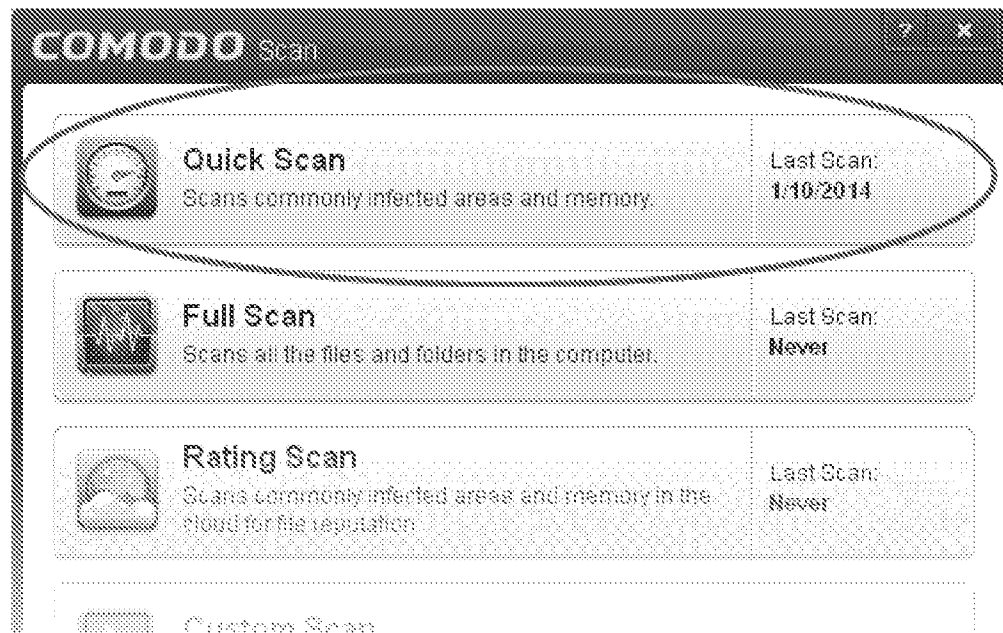
2.1.1. Run a Quick Scan

The 'Quick Scan' profile enables you to quickly scan critical areas of your computer which are highly prone to infection from viruses, rootkits and other malware. The areas scanned include system memory, auto-run entries, hidden services, boot sectors and other significant areas like important registry keys and system files. These areas are of great importance to the health of your computer so it is essential to keep them free of infection.

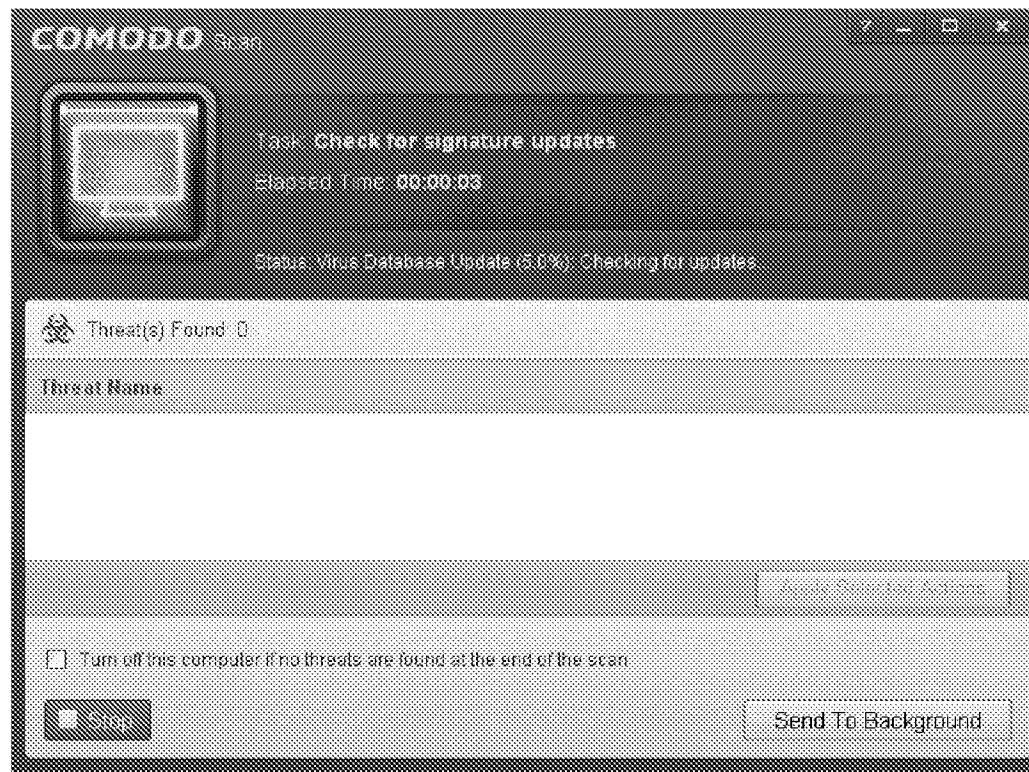
You can customize which items are scanned under a 'Quick Scan' and create a scan schedule from the 'Advanced Tasks' interface. Refer to Antivirus Settings > Scan Profiles for more details.

To run a Quick Scan

- Click 'Scan' from the General Tasks interface and click 'Quick Scan' from the 'Scan' interface.



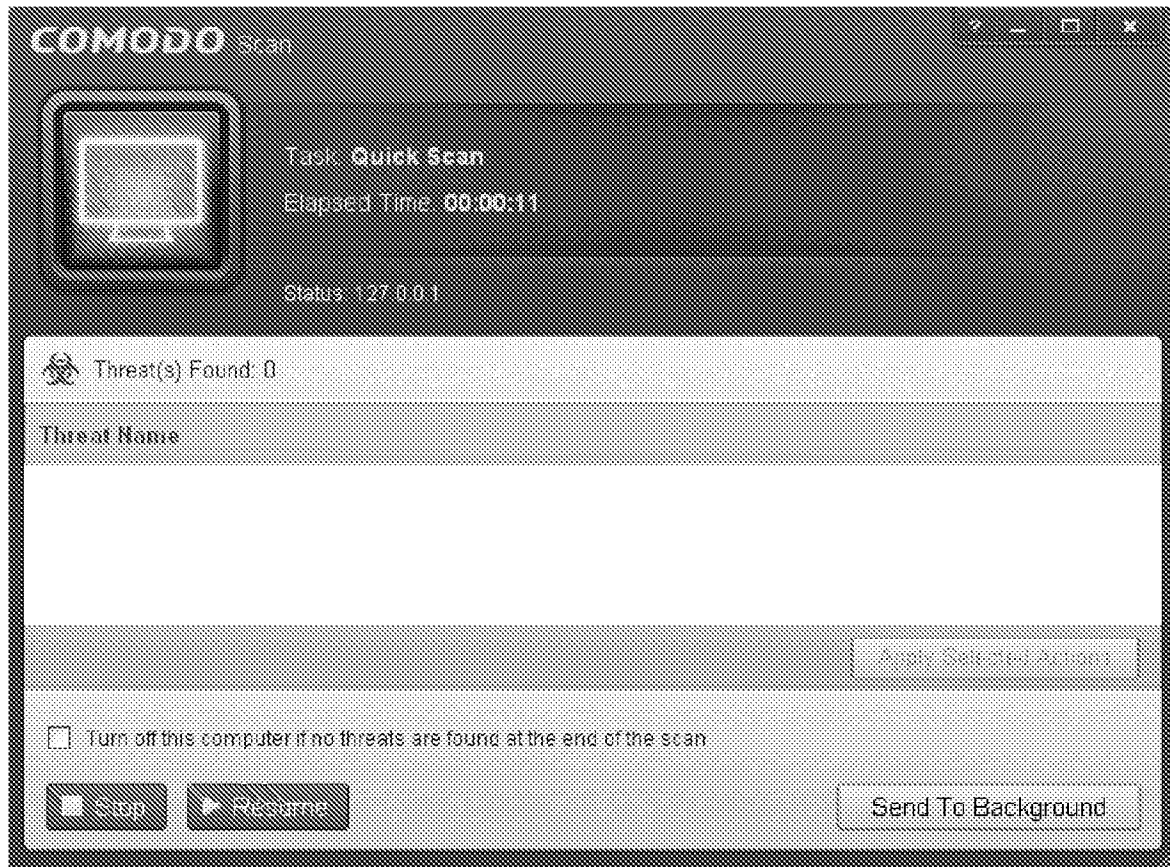
The scanner will start and first check whether your virus signature database is up-to-date:



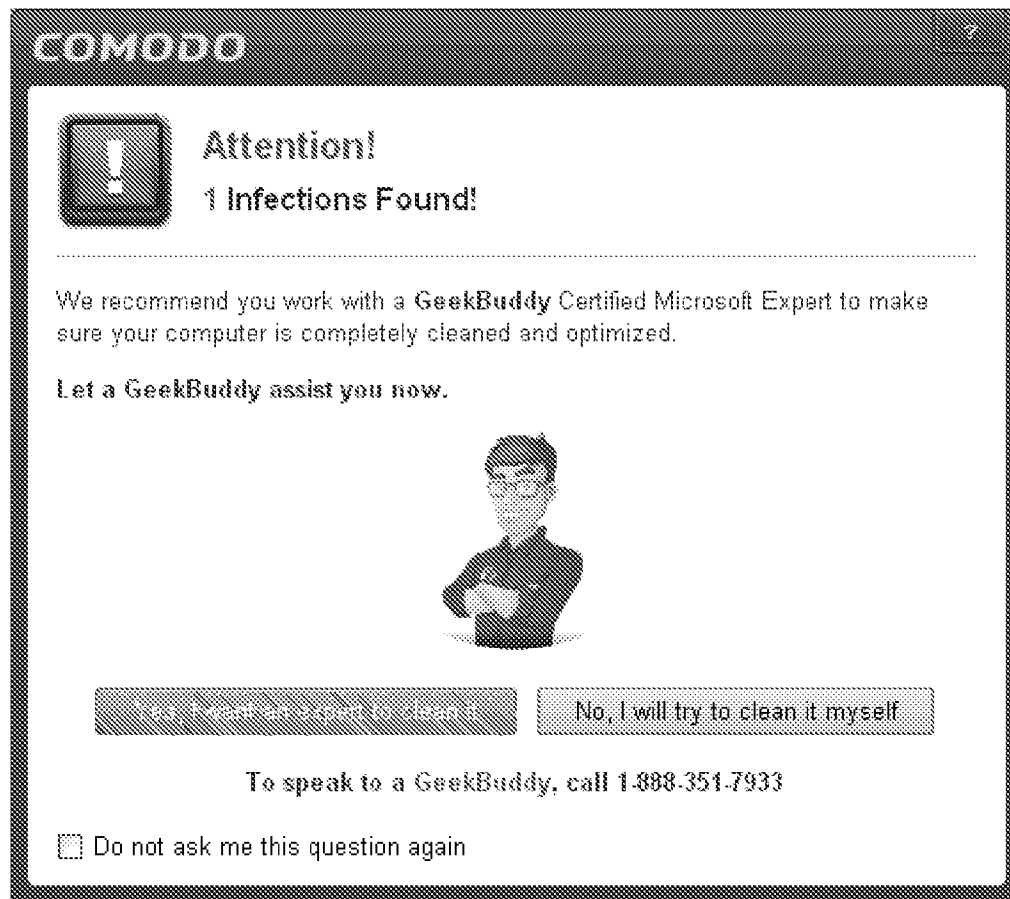
If the database is outdated, the scanner will first download and install the latest version. Once complete, the scan will begin and scan progress will be displayed:



- You can pause, resume or stop the scan by clicking the appropriate button. If you want to run the scan in the background, click 'Send to Background'. You can still keep track of the scan progress from the 'Task Manager' interface.



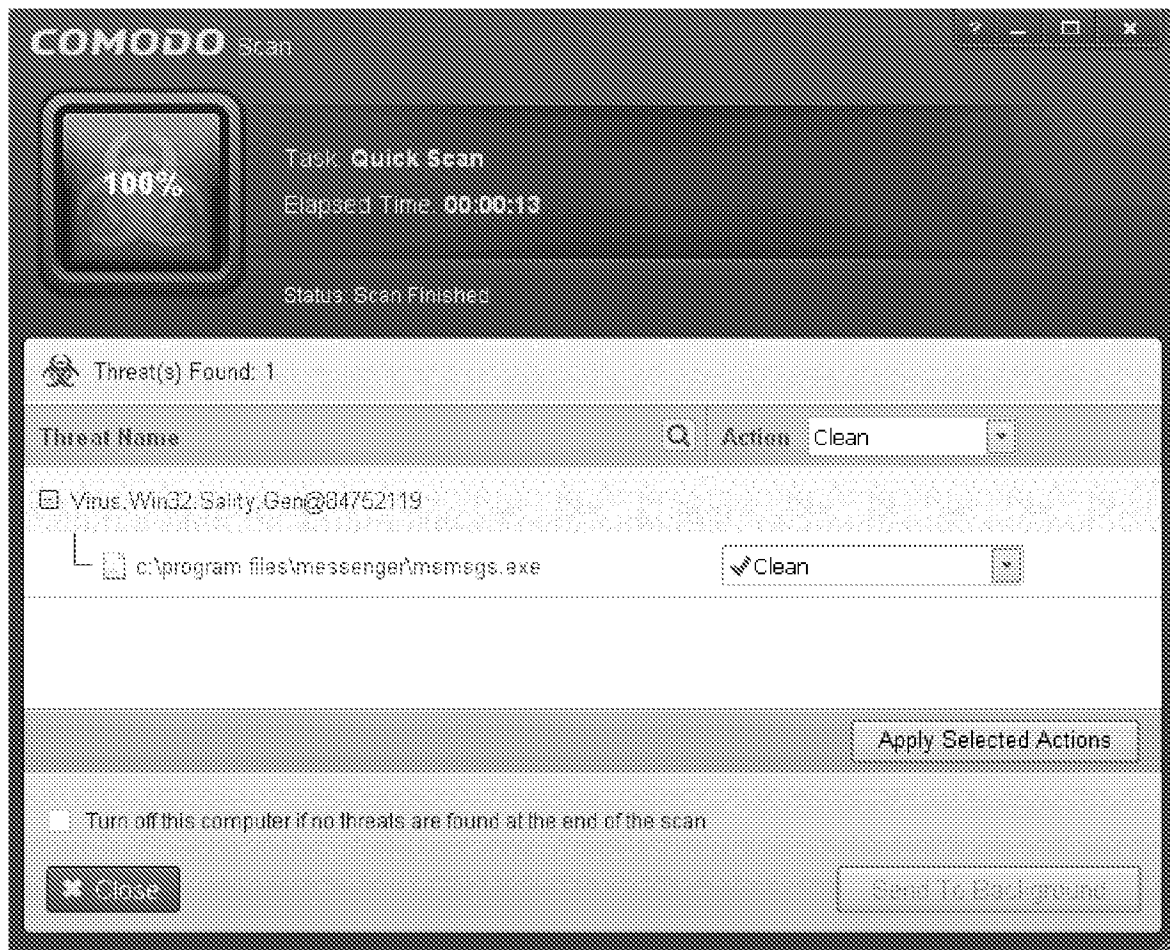
- An alert screen will be displayed at the end of the scan if issues were detected. The alert will display the number of threats/infections discovered and present you with cleaning options:



- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.

For more details on GeekBuddy Expert help, refer to the section *Comodo GeekBuddy*.

- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed.



The results window shows the number of objects scanned and the number of threats (Viruses, Rootkits, Malware). Use the drop-down menu to choose whether to clean, move to quarantine or ignore the threat. Refer to [Processing the infected files](#) for more details.

2.1.2. Run a Full Computer Scan

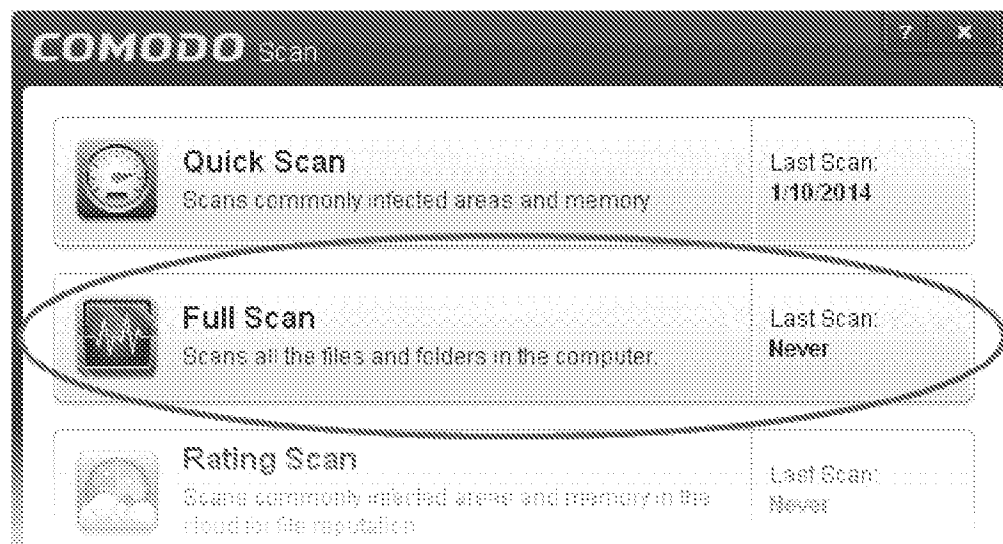
A 'Full System Scan' scans every local drive, folder and file on your system. External devices such as USB drives, storage drives and digital cameras will also be scanned.

You can customize which items are included in a full scan and set-up a scan schedule from the 'Advanced Tasks' interface.

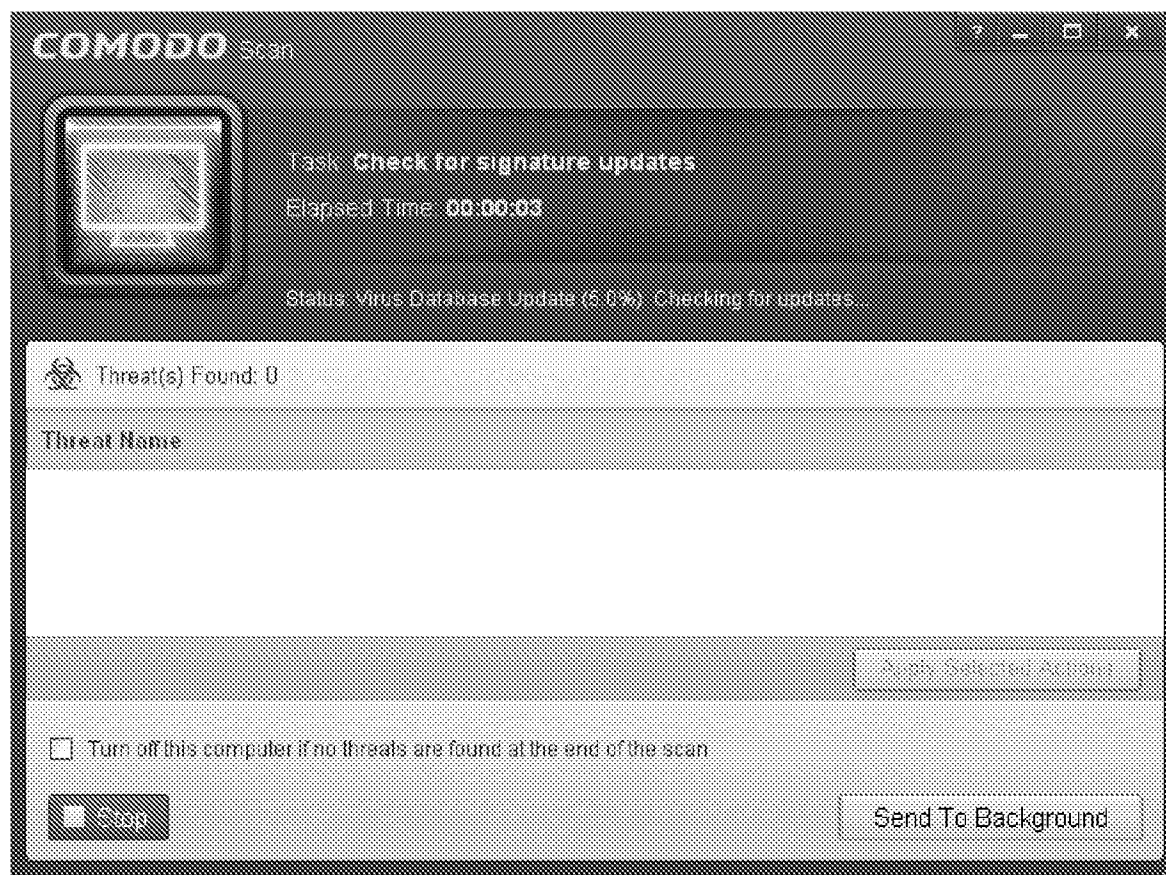
Refer to [Antivirus Settings > Scan Profiles](#) for more details.

To run a Full Computer Scan

- Click 'Scan' from the General Tasks interface then click 'Full System Scan' from the 'Scan' interface.



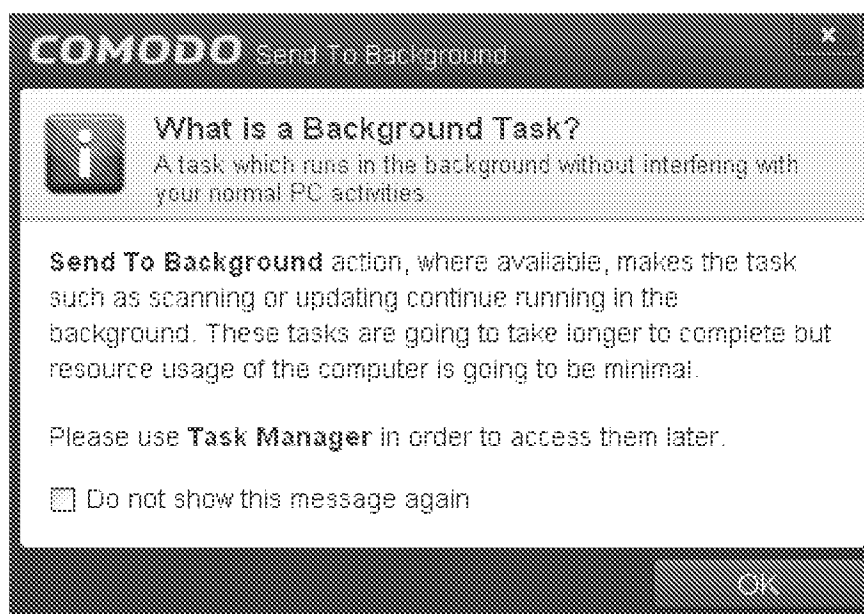
The scanner will start and first check whether your virus signature database is up-to-date.



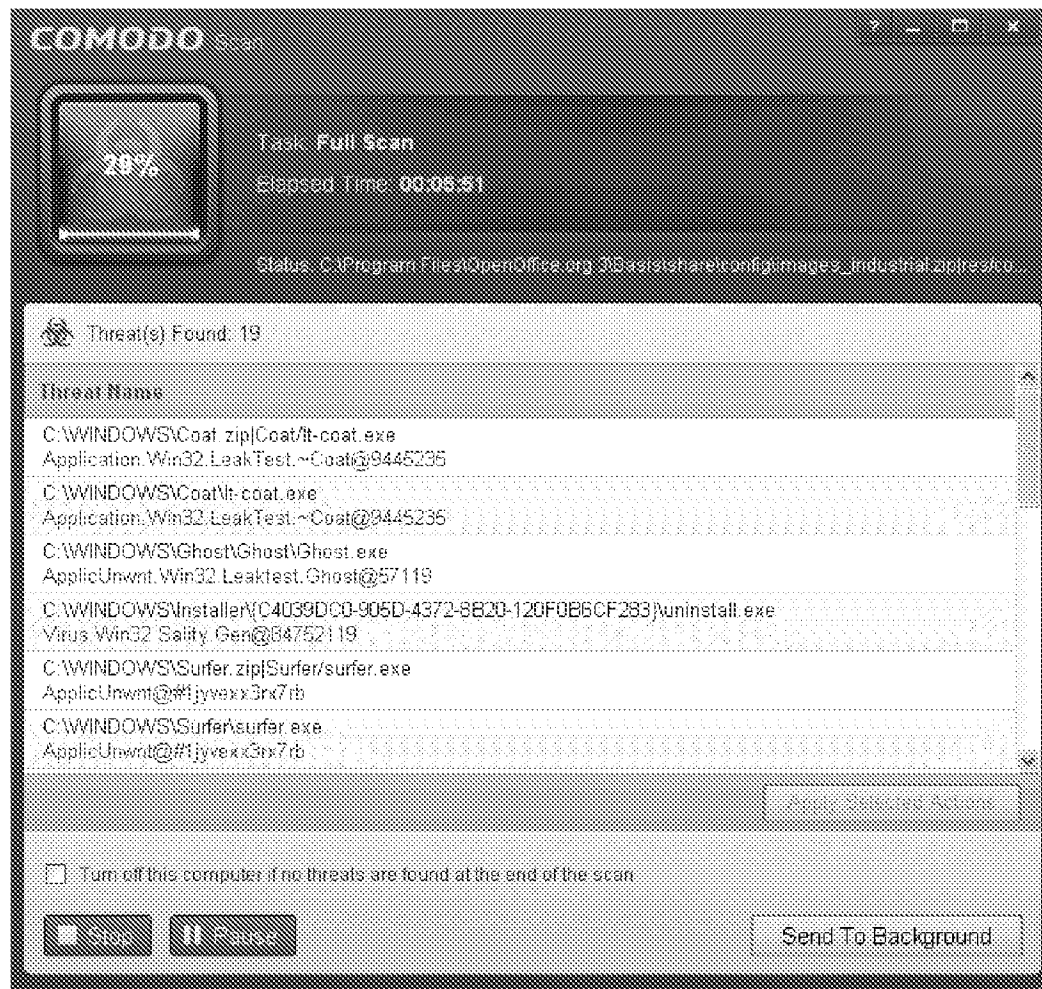
If the database is outdated, CIS will first download and install the latest database before commencing the scan.



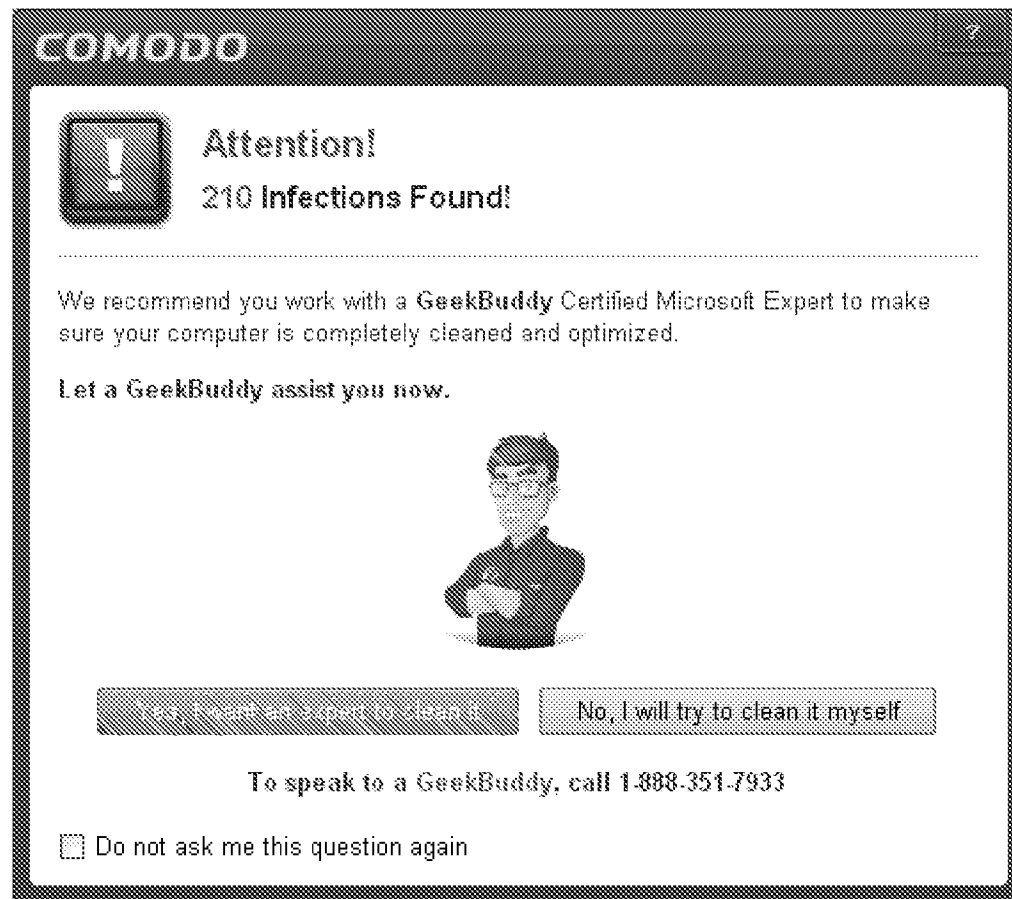
- You can pause, resume or stop the scan by clicking the appropriate button. If you want to run the scan in the background, click 'Send to Background'.



If you send to the background, you can continue to check scan progress by clicking 'Task Manager' on the home screen or by clicking 'Open Task Manager' icon from the 'Advanced Tasks' interface.



- Any detected threats will be displayed in full at the end of the scan. The alert will tell you how many threats were found; the name and location of the threats and will provide you with virus removal options:



- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
 - For more details on GeekBuddy Expert help, refer to the section Comodo GeekBuddy.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed.



The scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on). You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to [Processing the infected files](#) for more details.

2.1.3. Run a Rating Scan

The 'Rating Scan' feature runs a cloud-based assessment on files on your computer to assess how trustworthy they are.

Based on the trustworthiness, the files are rated as:

- Trusted - the file is safe
- Unknown - the trustworthiness of the file could not be assessed
- Bad - the file is unsafe and may contain malicious code. You will be presented with disinfection options for such files.

To run a Rating scan

- Click the curved 'Tasks' arrow on the home screen then click 'General Tasks' > 'Scan' > 'Rating Scan'.

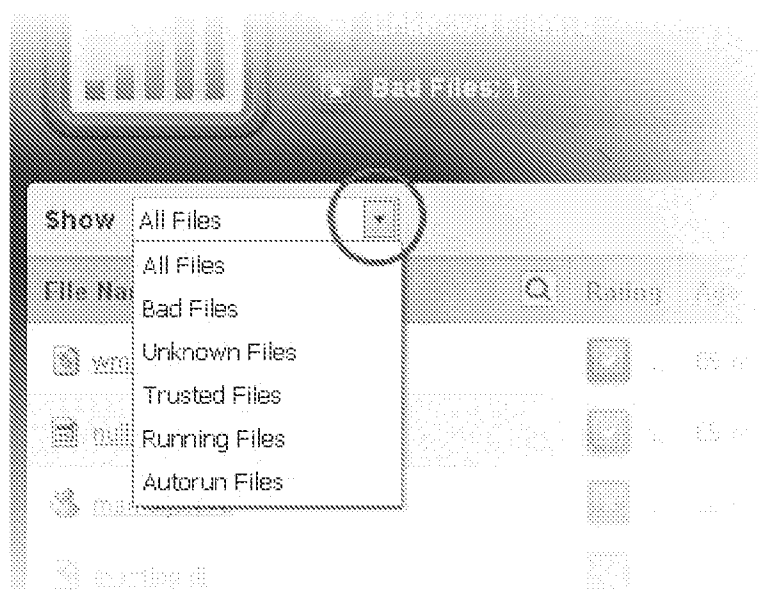


After the cloud scanners have finished their analysis, file ratings will be displayed as follows:

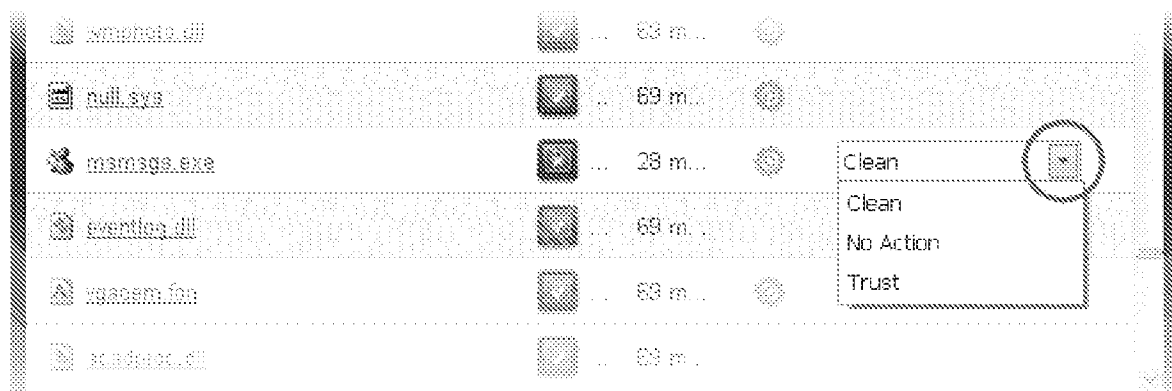


- **File Name:** The file which was scanned
- **Rating:** The rating of the file as per the cloud based analysis
- **Age:** The period of time that the file has been stored on your computer
- **Autorun:** Indicates whether the file is an auto-run file or not. Malicious auto-run files could be ruinous to your computer so we advise you clean or quarantine them immediately.

You can filter the results by rating using the 'Show' drop-down:

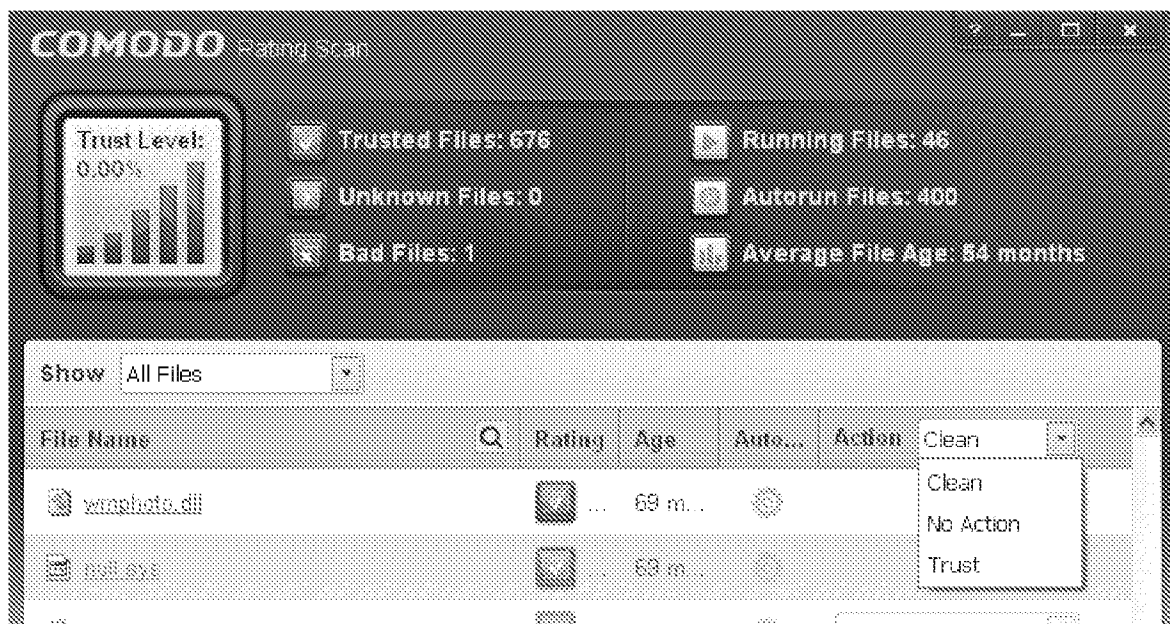


Each file identified as 'Bad' is accompanied with a drop-down box that allows you to 'Clean', 'Trust' or 'Take no action'



- **Clean** - If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application file. If a disinfection routine is not available, Comodo Antivirus will move the files to Quarantine for later analysis. See [Manage Quarantined Items](#) for more info.
- **No Action** - If you wish to ignore the file, select 'No Action'. Use this option with caution. By choosing to neither 'Clean' nor 'Trust', this file will be detected by the next ratings scan that you run.
- **Trusted** - The file will be moved to 'Trusted Files' list and will be given 'Trusted' rating from the next scan.

For the same action to be applied to all 'Bad' files, make a selection from the drop-down menu at the top of the 'Action' column.



Click 'Apply Selected Actions' to implement your choice. The selected actions will be applied and a progress bar will be displayed underneath the results:

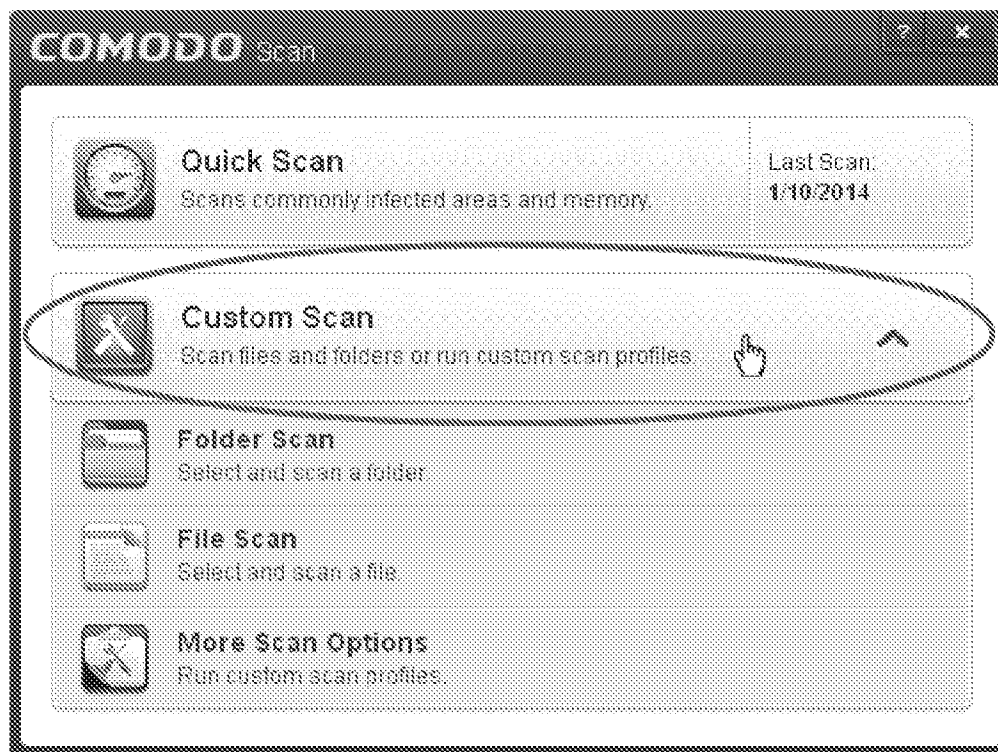


- Click 'Close' to exit.

2.1.4. Run a Custom Scan

Comodo Antivirus allows you to create custom scan profiles to scan specific areas, drives, folders or files in your computer.

To run a custom scan, click 'Scan' from the 'General Tasks' interface then click 'Custom Scan'. The Custom Scan panel will open:



The 'Custom Scan' panel contains the following scan options. Click the links to jump to the help page for that topic.

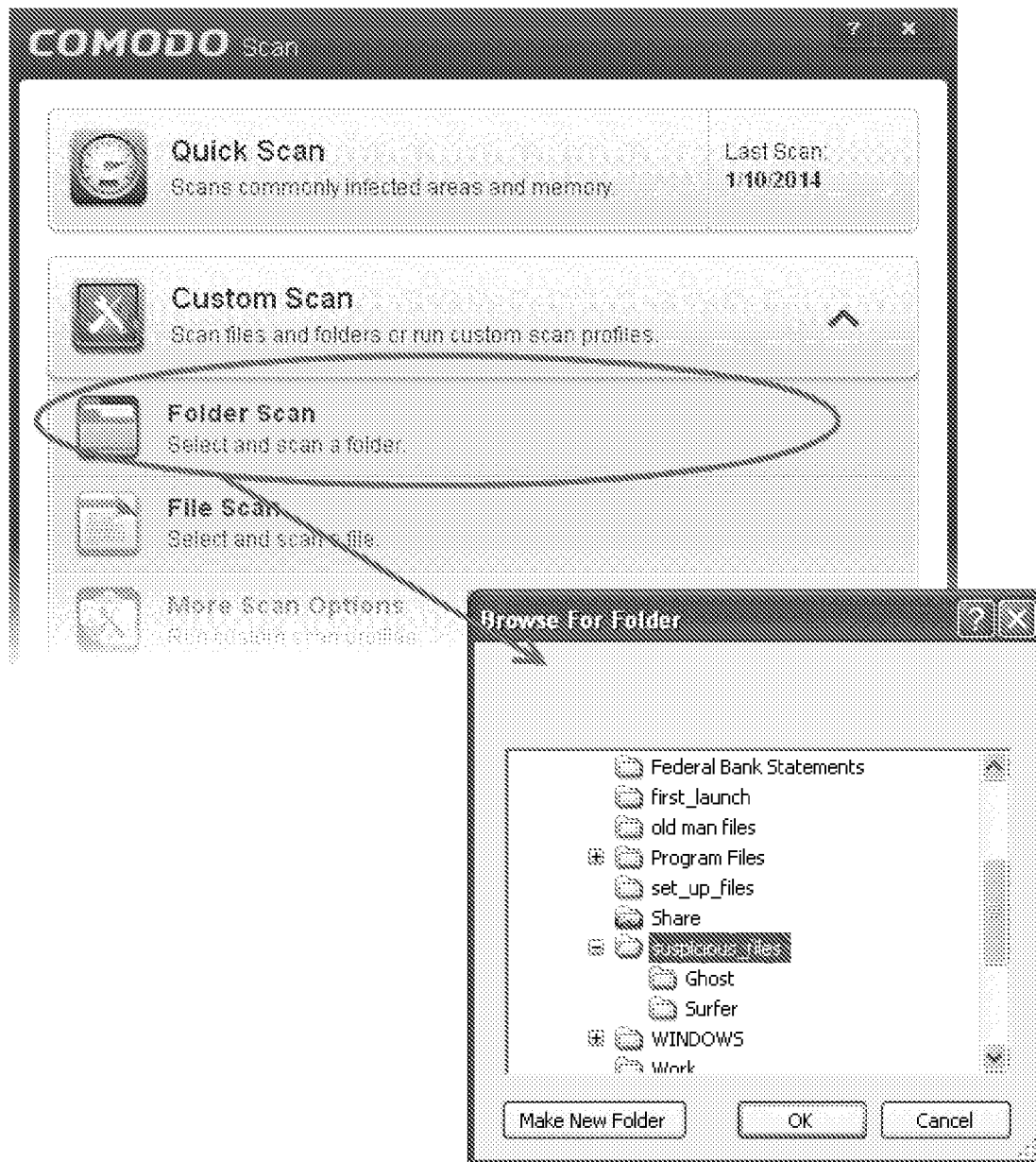
- [Folder Scan](#) - scan individual folders
- [File Scan](#) - scan an individual file
- [More Scan Options](#) - create a custom scan profile here

2.1.4.1. Scan a Folder

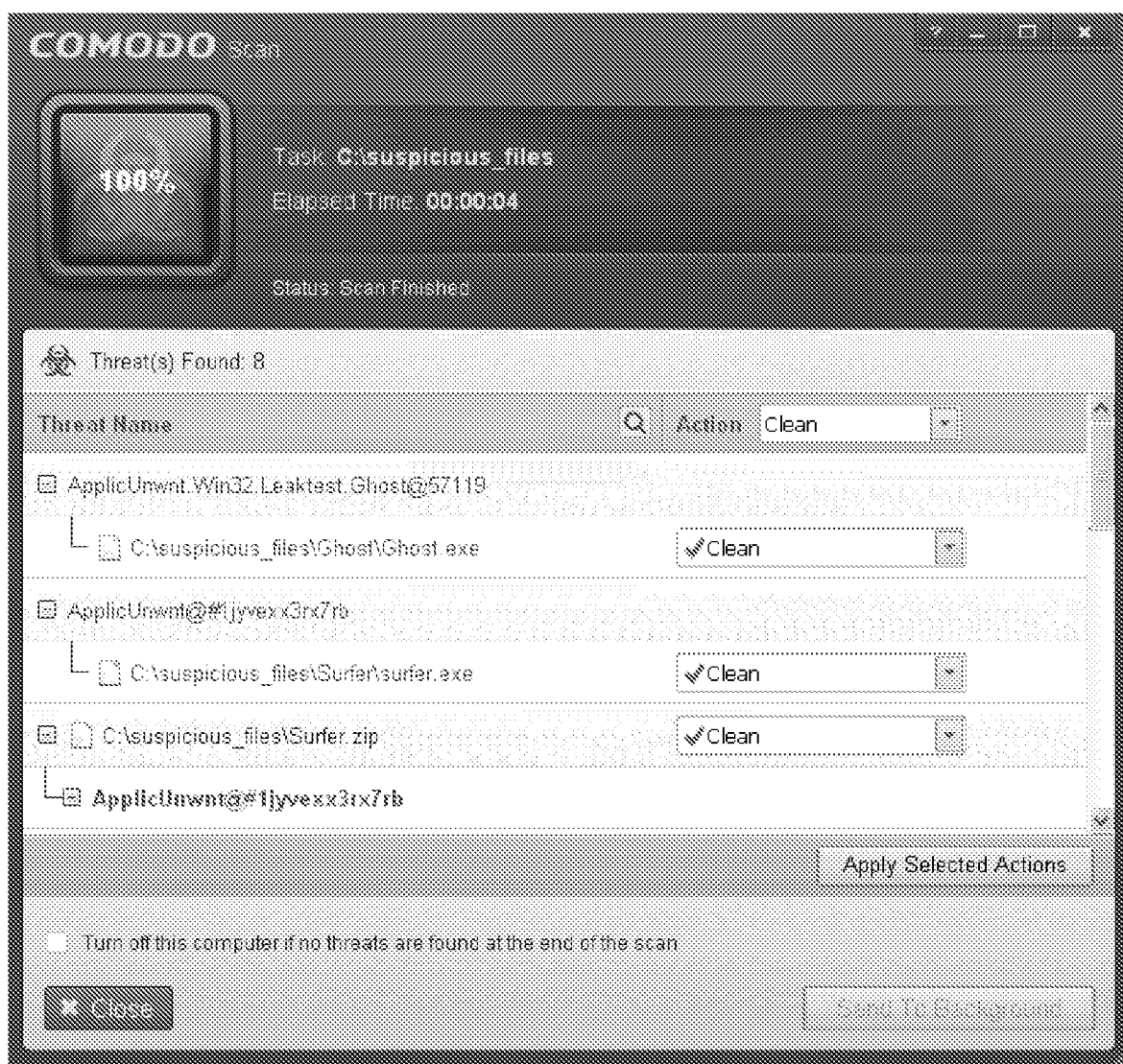
The custom scan allows you to scan a specific folder stored in your hard drive, CD/DVD or in external devices like a USB drive connected to your computer. For example you might have copied a folder from another computer in your network, an external device or downloaded from Internet and want to scan it for viruses and other threats before you open it.

To scan a specific folder

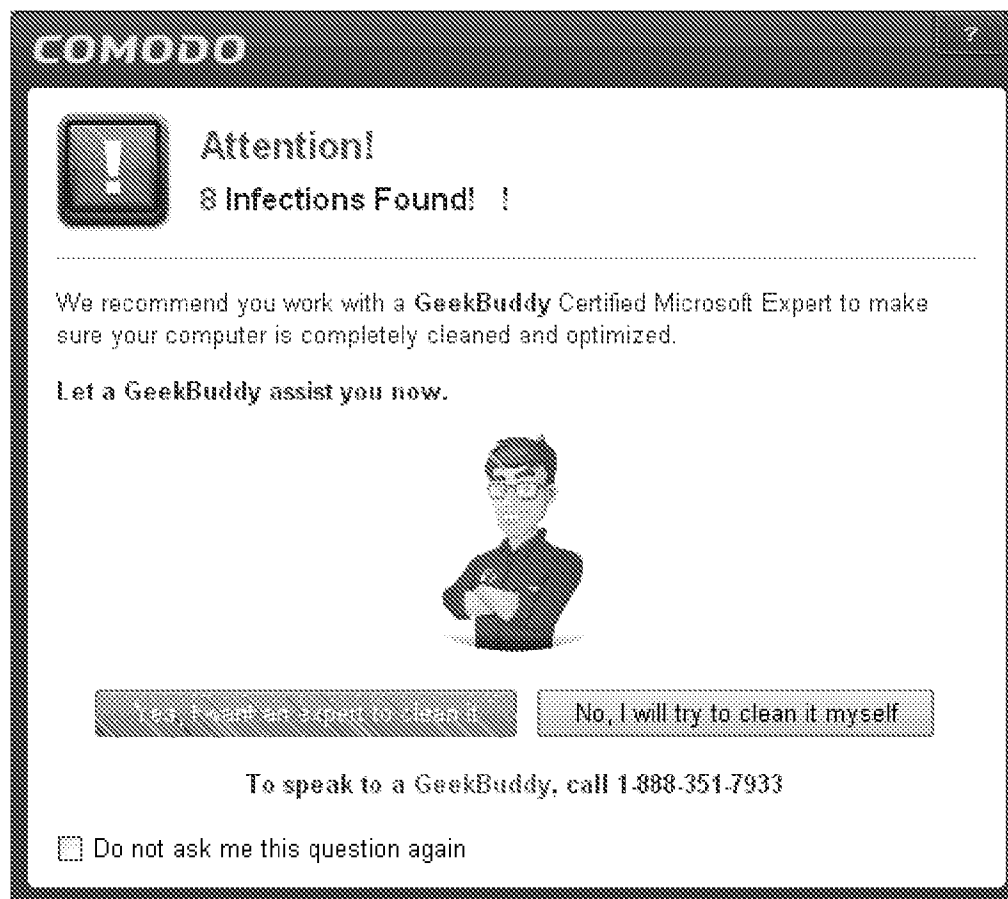
- Click Scan from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'Folder Scan' from the 'Custom Scan' pane
- Navigate to the folder to be scanned in the 'Browse for Folder' window and click OK.



The folder will be scanned instantly and the results will be displayed with a list of any identified infections



- On completion of scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
 - For more details on GeekBuddy Expert help, refer to the section *Comodo GeekBuddy*.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed.



The scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on). You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to [Processing the infected files](#) for more details.

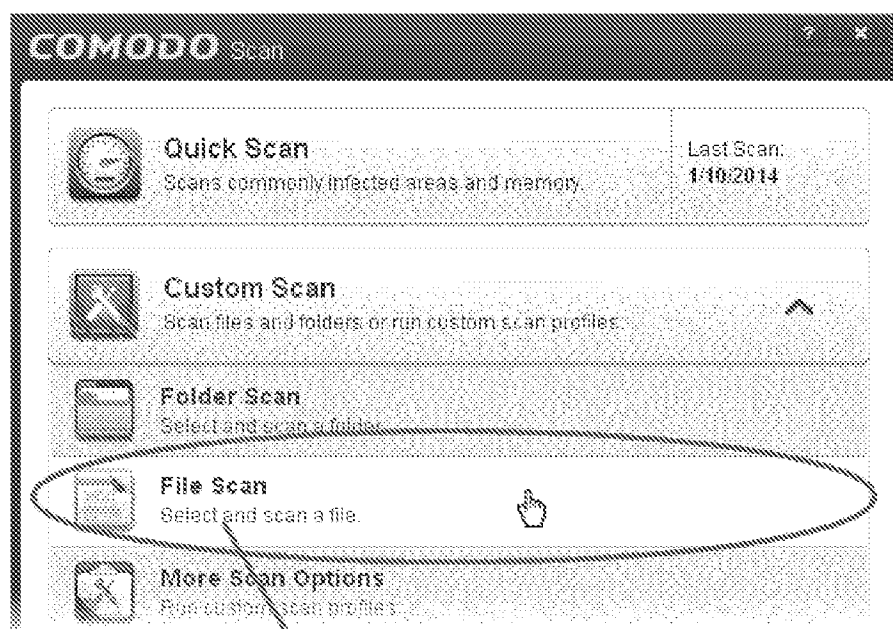
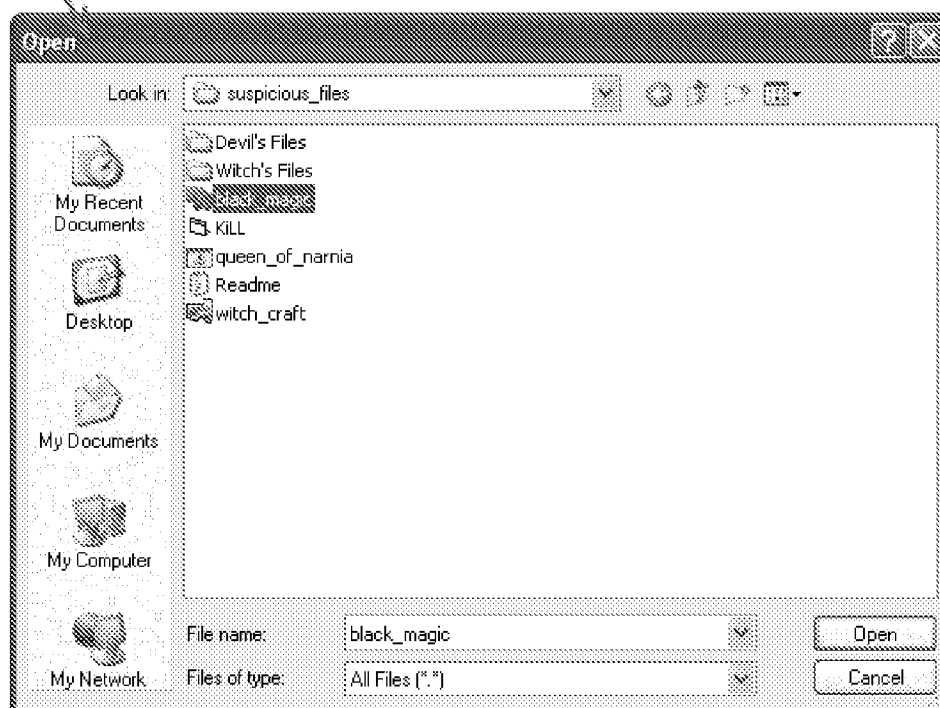
Tip: Alternatively, you can perform an express scan on a folder by dragging and dropping it onto the CIS interface or by right clicking it. Refer to [Scan Individual File/Folder](#) for more details.

2.1.4.2. Scan a File

The custom scan allows you to scan a specific file stored in your hard drive, CD/DVD or in external devices like a USB drive connected to your computer. For example you might have downloaded a file from the Internet or dragged an email attachment onto your desktop and want to scan it for viruses and other threats before you open it.

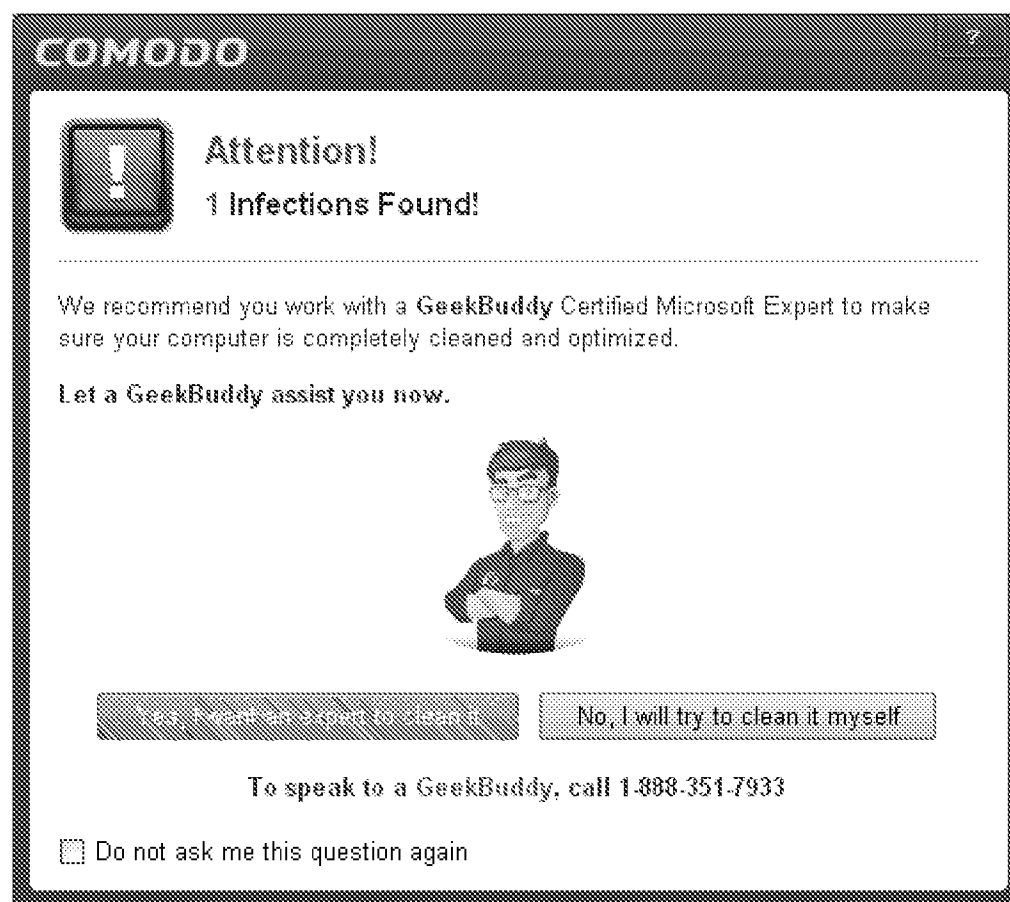
To scan a specific file

- Click Scan from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'File Scan' from the 'Custom Scan' pane
- Navigate to the file to be scanned in the 'Open' window and click 'Open'



The file will be scanned instantly.

- On completion of scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
 - For more details on GeekBuddy Expert help, refer to the section Comodo GeekBuddy.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed.



The scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on). You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to [Processing the infected files](#) for more details.

Tip: Alternatively, you can perform an express scan on a file by dragging and dropping it onto the CIS interface or by right clicking it. Refer to [Scan Individual File/Folder](#) for more details.

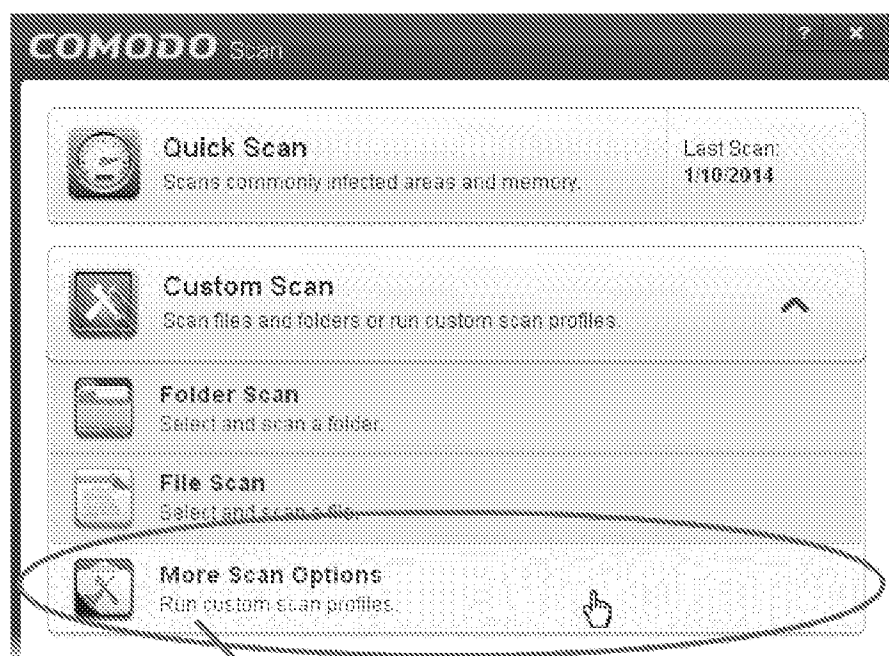
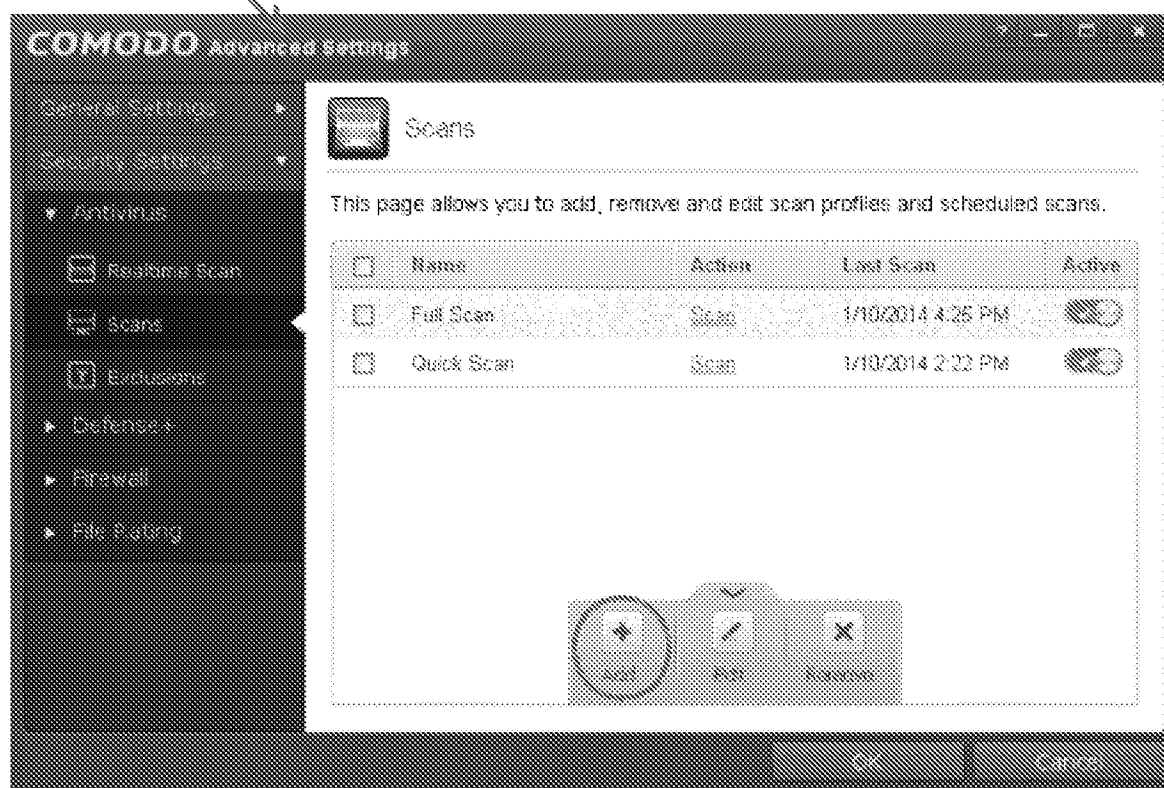
2.1.4.3. Create, Schedule and Run a Custom Scan

By creating a custom scan profile, you can choose exactly which files and folders are scanned, when they are scanned and how they are scanned. Once created and saved, your custom scan profile will appear in the scans interface and can be run, on demand, at any time.

- [Creating a Scan Profile](#)
- [Running a custom scan](#)

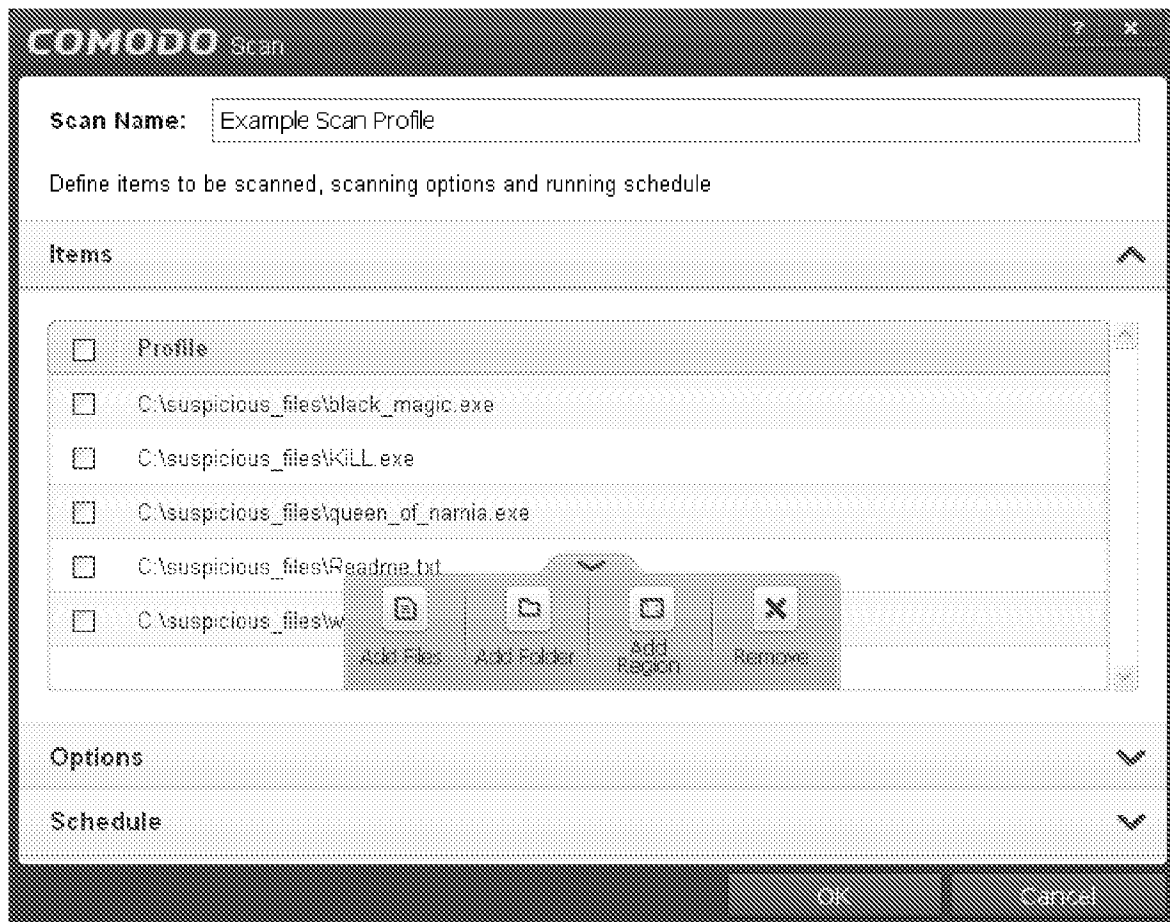
To create a custom profile

- Click the 'Tasks' arrow on the home screen to open the main Tasks menu
- In 'General Tasks', click 'Scan'
- Select 'Custom Scan' then 'More Scan Options'
- The 'Advanced Settings' interface will be displayed with 'Scans' panel opened
- Click the handle at the bottom of the interface then select 'Add':

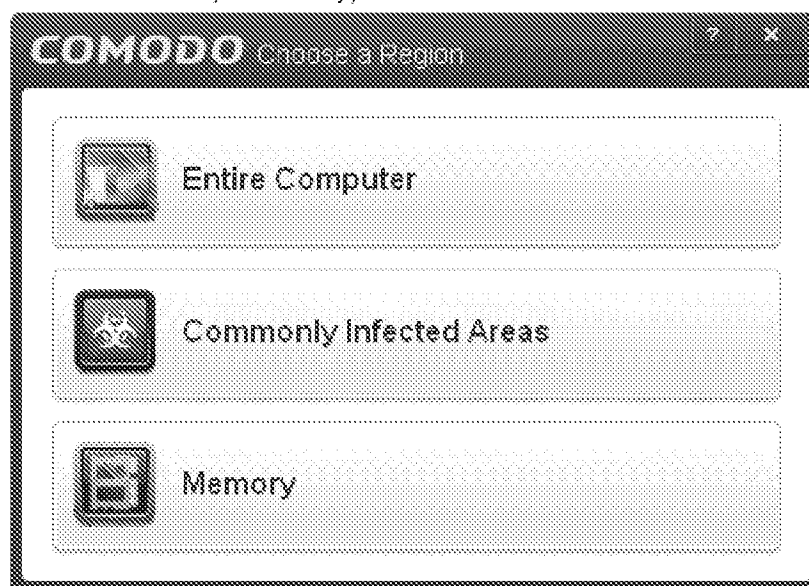


The scan profile interface will be displayed.

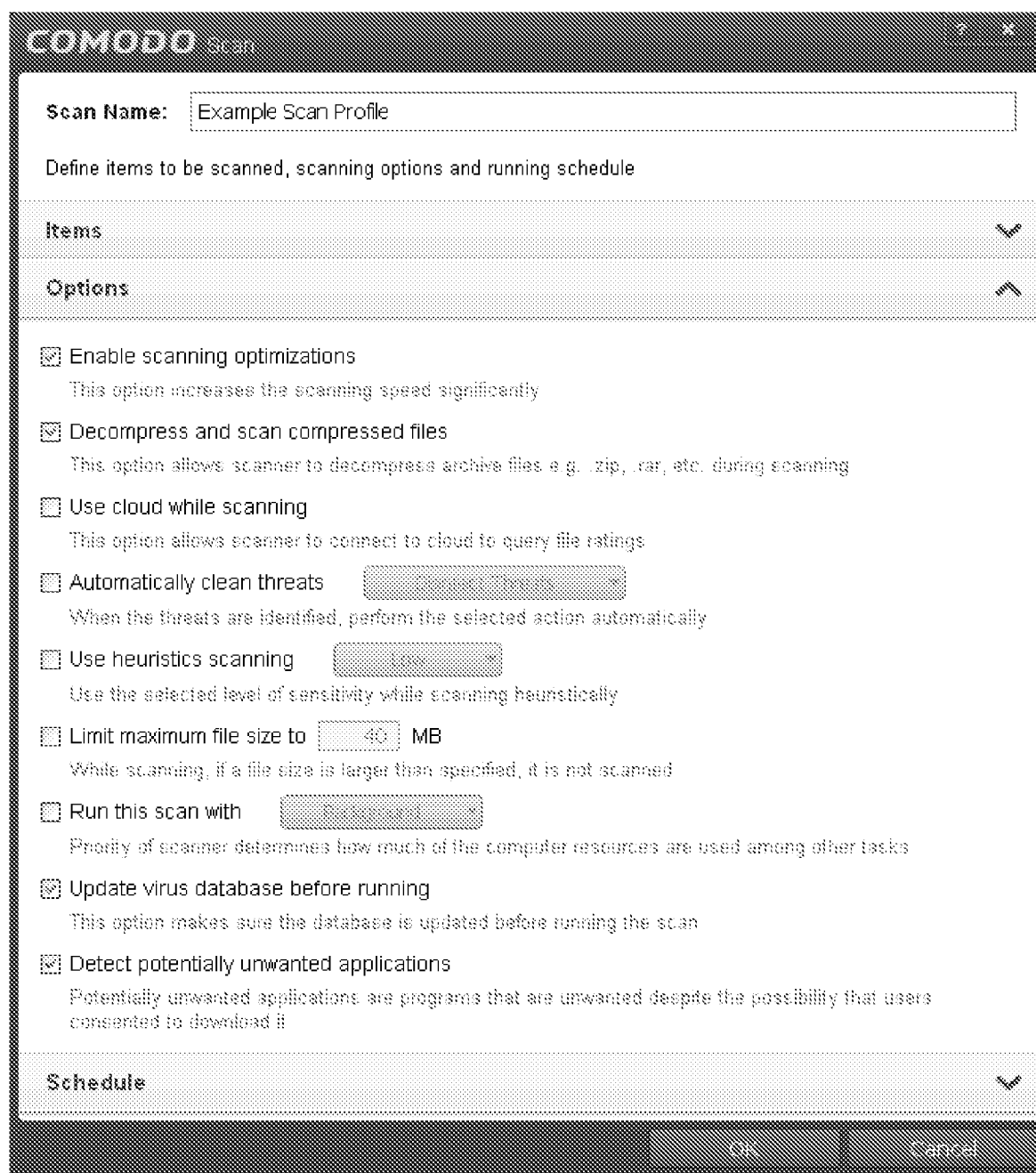
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items to be included in the profile:



- **Add File** - Allows you to add individual files to the profile.
- **Add Folder** - Allows you to select entire folders to be included in the profile
- **Add Region** - Allows you to add pre-defined regions to the profile (choice of 'Full Computer', 'Commonly Infected Areas' and 'System Memory')



- Repeat the process to add more items to the profile. Click 'OK' to confirm your choice.
- Next, click 'Options' to further customize the scan:



- Options:

- Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process (**Default = Enabled**) .
 - Decompress and scan compressed files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (**Default = Enabled**) .
 - Use cloud while scanning** - Selecting this option enables the Antivirus to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local antivirus database is out-dated. (**Default = Disabled**).
 - Automatically clean threats** - Enables you to select the action to be taken against the detected threats and infected files automatically from disinfecting Threats and moving the threats to quarantine.
 - Use heuristics scanning** - Enables you to select whether or not Heuristic techniques should be applied on

scans in this profile. You are also given the opportunity to define the heuristics scan level. (**Default = Disabled**).

Background Info: Comodo Internet Security employs various heuristic techniques to identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code patterns similar to those in known viruses. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting 'virus-like' traits or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist.

This allows CIS to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

- **Low** - Lowest sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users.
- **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
- **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.
- **Limit maximum file size to** - Select this option if you want to impose size restrictions on files being scanned. Files of size larger than that specified here, are not scanned, if this option is selected (**Default = 40 MB**).
- **Run this scan with** - Enables you to set the priority of the scan profile. You can select the priority from the drop-down. (**Default = Disabled**).
- **Update virus database before running** - Instructs Comodo Internet Security to check for latest virus signature database updates from Comodo website and download the updates automatically before starting the scanning (**Default = Enabled**).
- **Detect potentially unwanted applications** - When this check box is selected, Antivirus scans also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet (**Default = Enabled**).
- If you want the scan to run at specific times, click 'Schedule':

COMODO Scan

Scan Name:

Define items to be scanned, scanning options and running schedule

Items ⌵

Options ⌵

Schedule ⌴

Frequency:

☐ Do not schedule this task
☐ Every Day
☒ Every Week
☐ Every Month

Start Time:

Days of Week

Sun	Mon	Tue	Wed	Thu	Fri	Sat

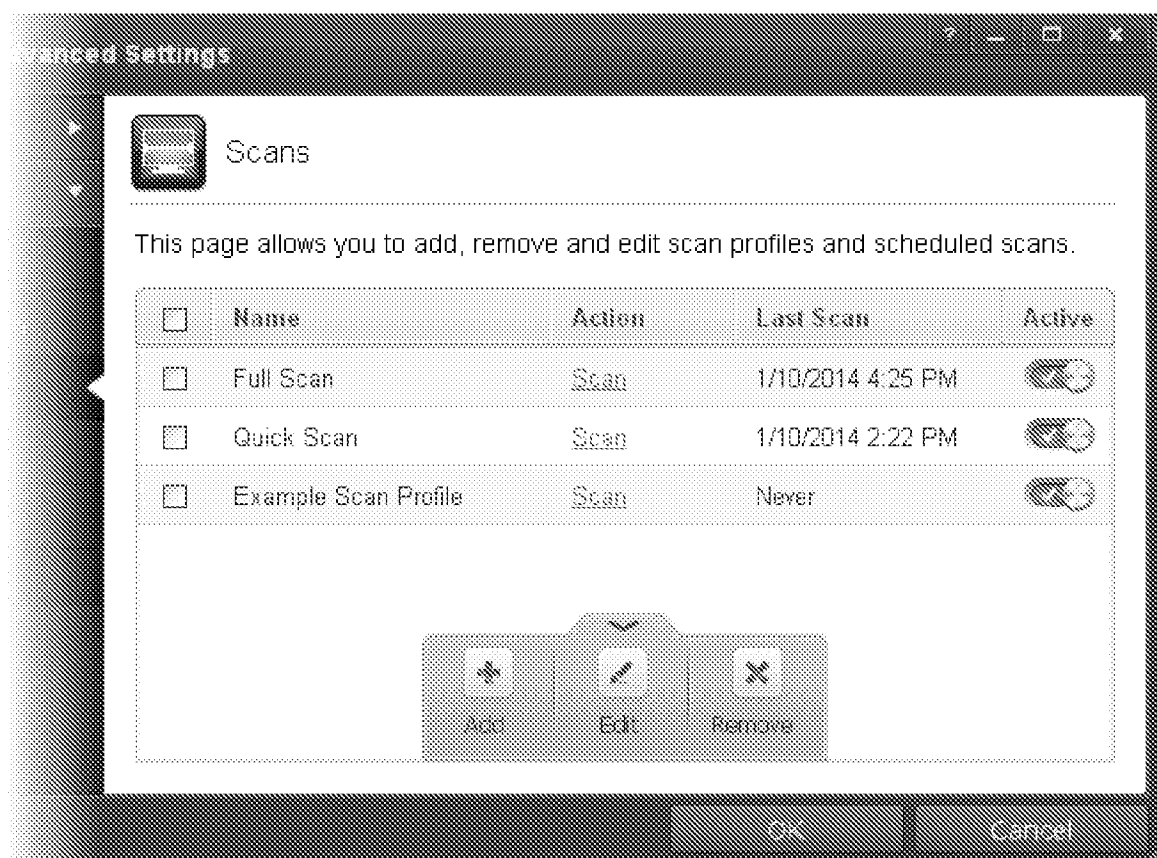
☐ Run only when computer is not running on battery
☐ Run only when computer is IDLE
☐ Turn off computer if no threats are found at the end of the scan

OK Cancel

- **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
- **Every Day** - The Antivirus starts scanning the areas defined in the scan profile every day at the time specified in the Start Time field
- **Every Week** - The Antivirus starts scans the areas defined in the scan profile on the day(s) of the week specified in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them.
- **Every Month** - The Antivirus starts scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them.
- **Run only when computer is not running on battery** - This option is useful when you are using a laptop or any other battery driven portable computer. Selecting this option runs the scan only if the computer runs with the adapter connected to mains supply and not on battery.
- **Run only when computer is IDLE** - Select this option if you do not want to be disturbed when involved in computer related activities. The scheduled scan will run only if the computer is in idle state
- **Turn off computer if no threats are found at the end of the scan** - Selecting this option turns your computer off, if no threats are found during the scan. This is useful when you are scheduling the scans to run at nights.
- Click OK to save the profile.

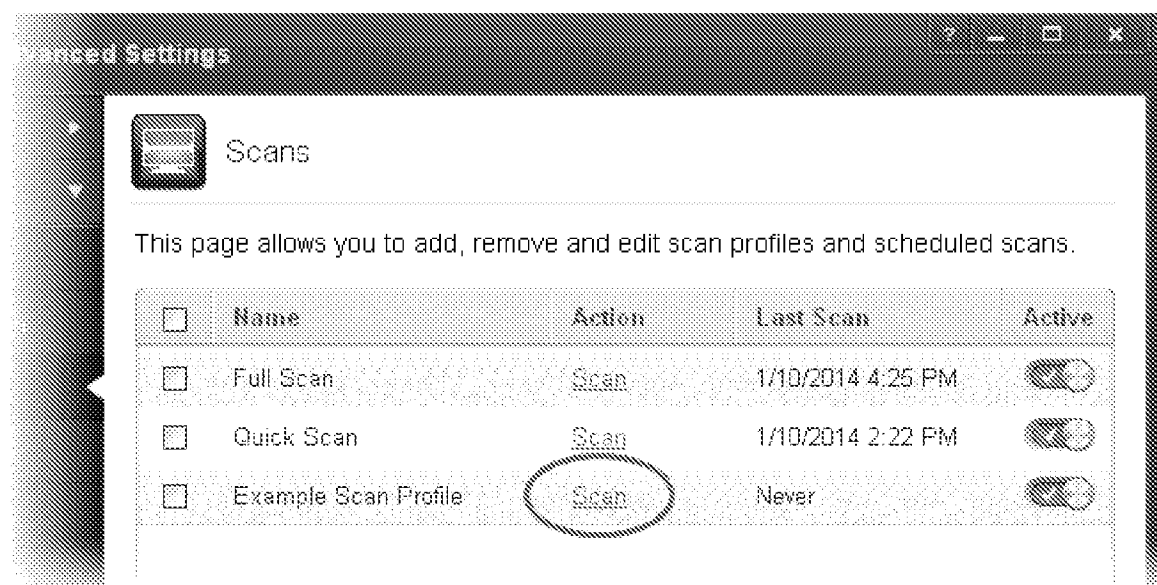
Note: The scheduled scan will run only if it is enabled. Click the button under the Active column beside the respective profile row to toggle between on and off status.

The profile will be available for deployment in future.

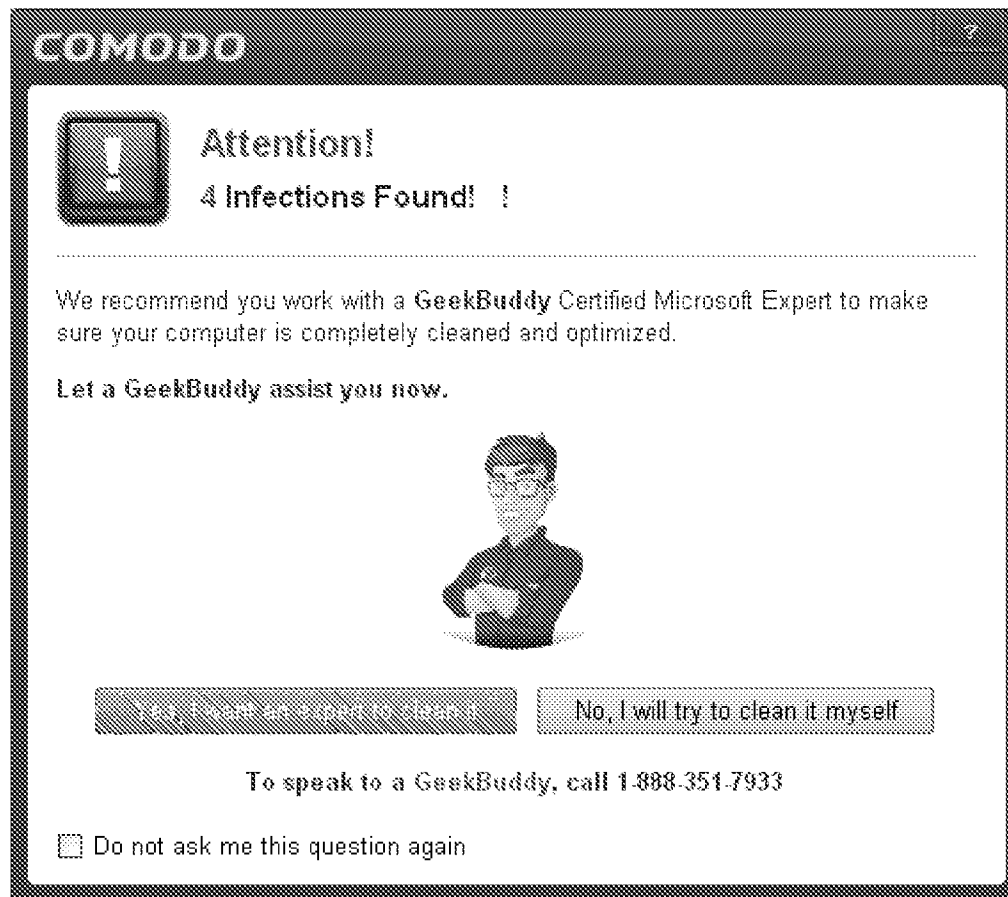


To run a custom scan

- Click 'Scan' from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'More Scan Options' from the 'Custom Scan' pane
- The 'Advanced Settings' interface will be displayed with 'Scans' panel opened.
- Click 'Scan' beside the required scan profile.



- The scan will be started.
- On completion of scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
 - For more details on GeekBuddy Expert help, refer to the section Comodo GeekBuddy.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed.



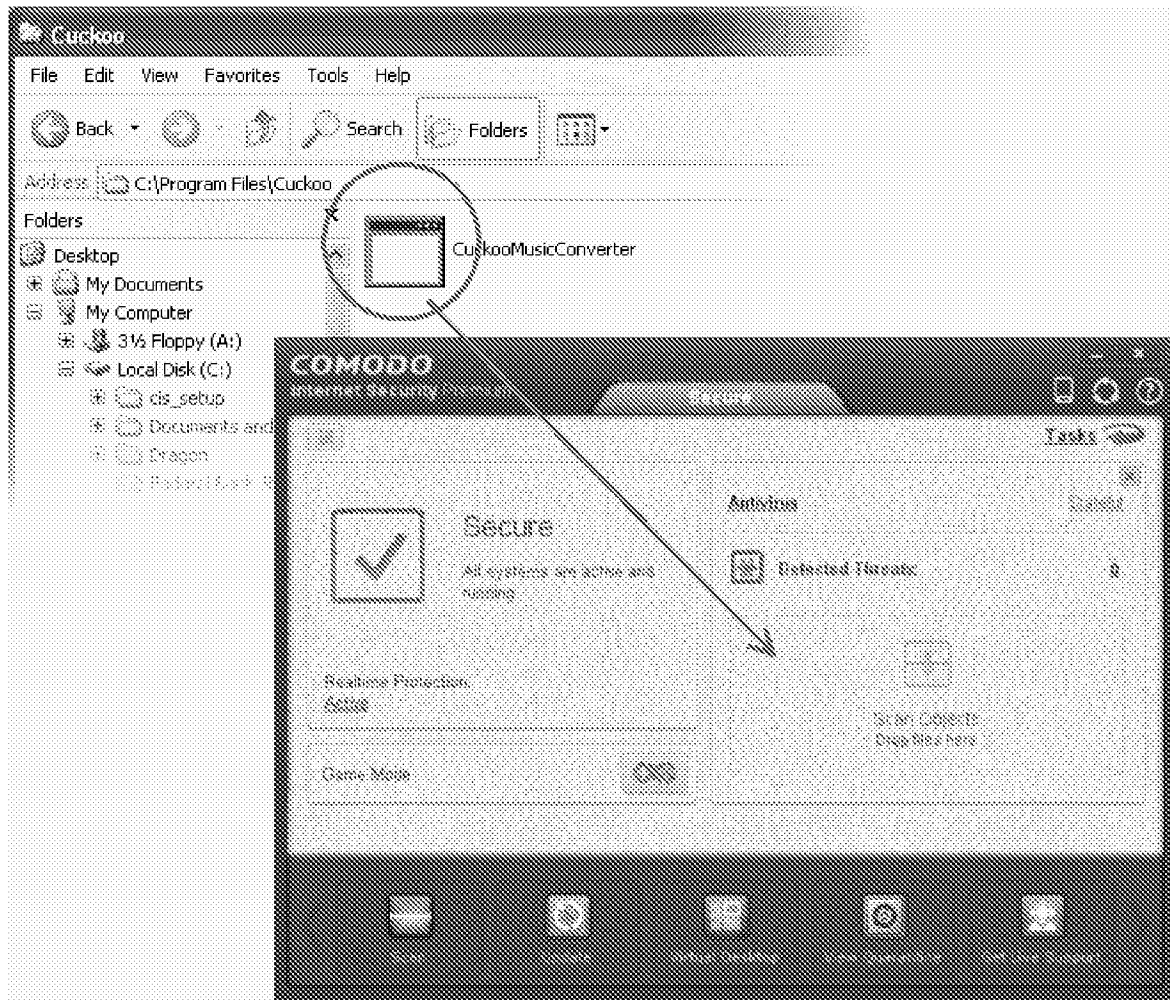
- The scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on). You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to [Processing the infected files](#) for more details.

2.2. Instantly Scan Files and Folders

You can scan individual files or folders instantly to check whether it contains any threats or infections. This is useful if you have just copied a file/folder or a program from an external device like a USB drive, another system in your network, or downloaded from Internet.

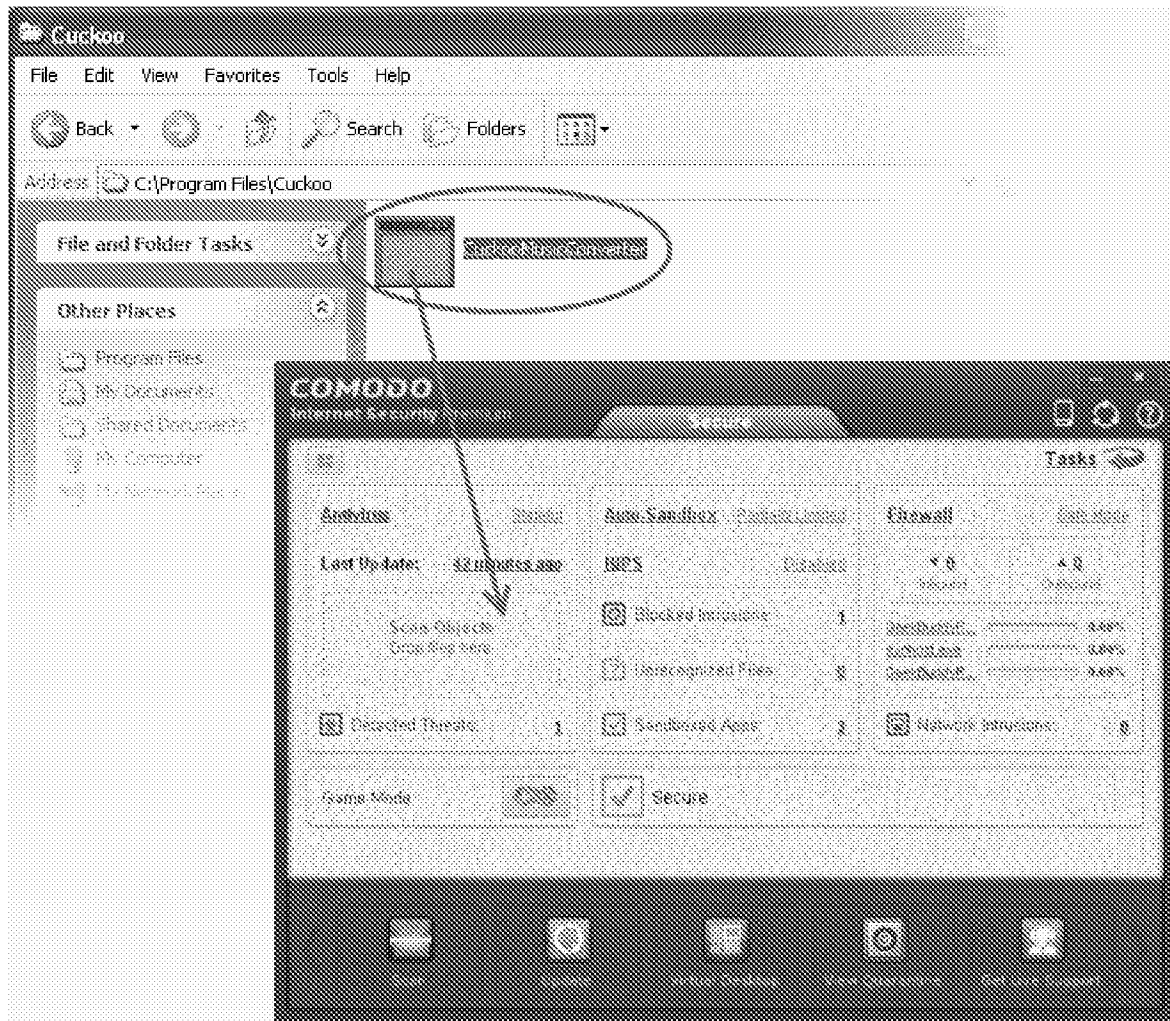
To instantly scan an item

- Click the Antivirus tile at the 'Home' screen in compact view to flip-open the Antivirus pane
- Drag and drop the item over the area marked 'Scan Objects'.



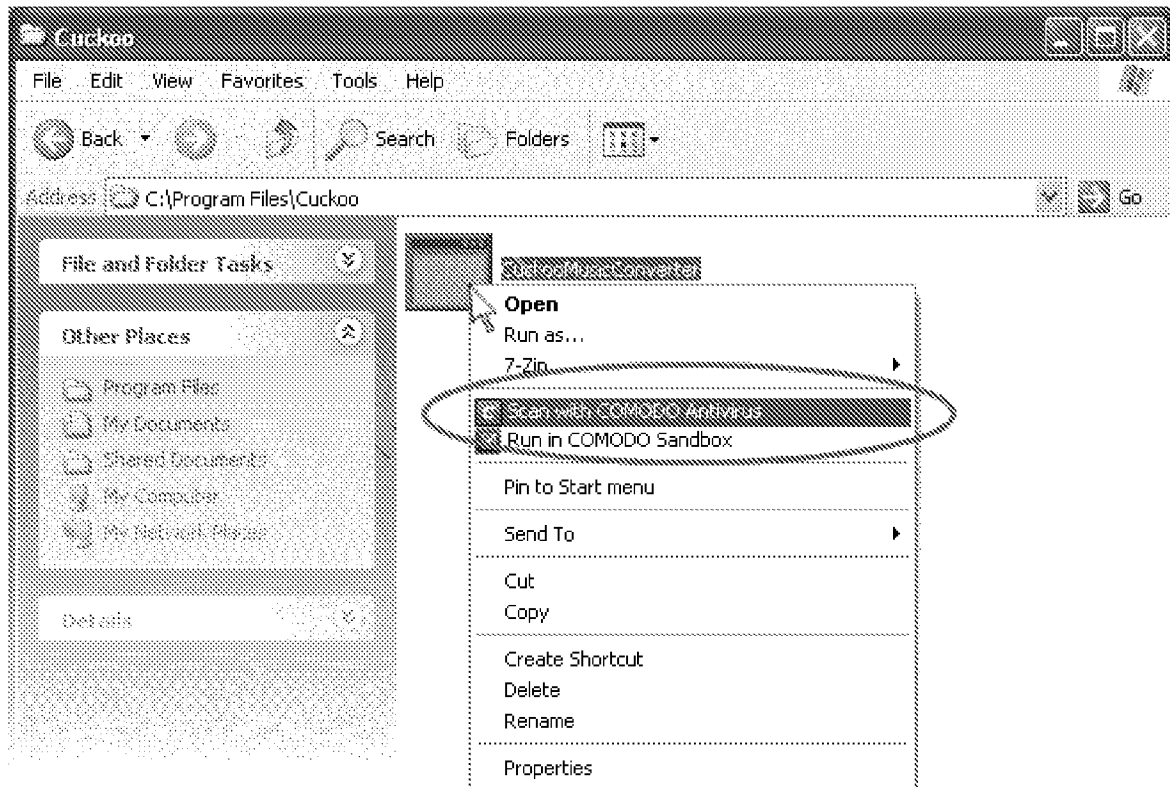
OR

- Switch to 'Advanced' View of the 'Home' screen by clicking the button at the top left of the home screen.
- Drag and drop the item over the area marked 'Scan Objects'.



OR

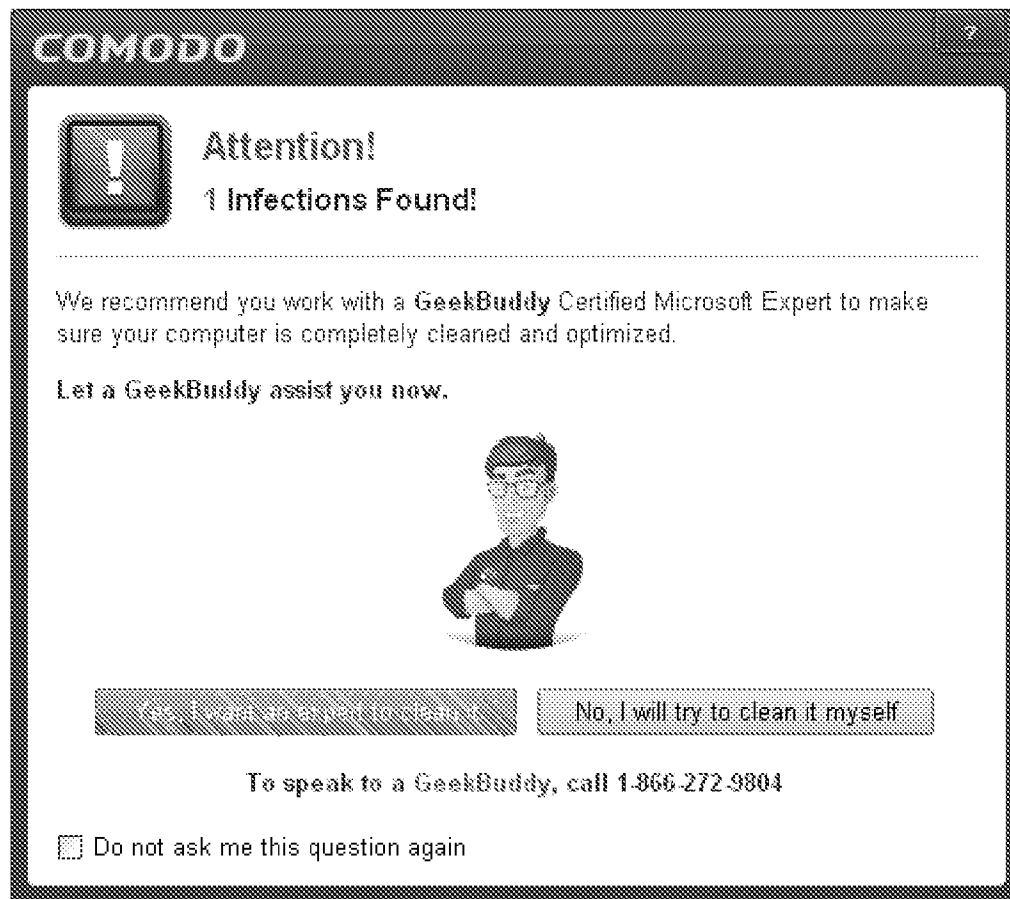
- Right click on the item and select Scan with 'Comodo Antivirus' from the context sensitive menu



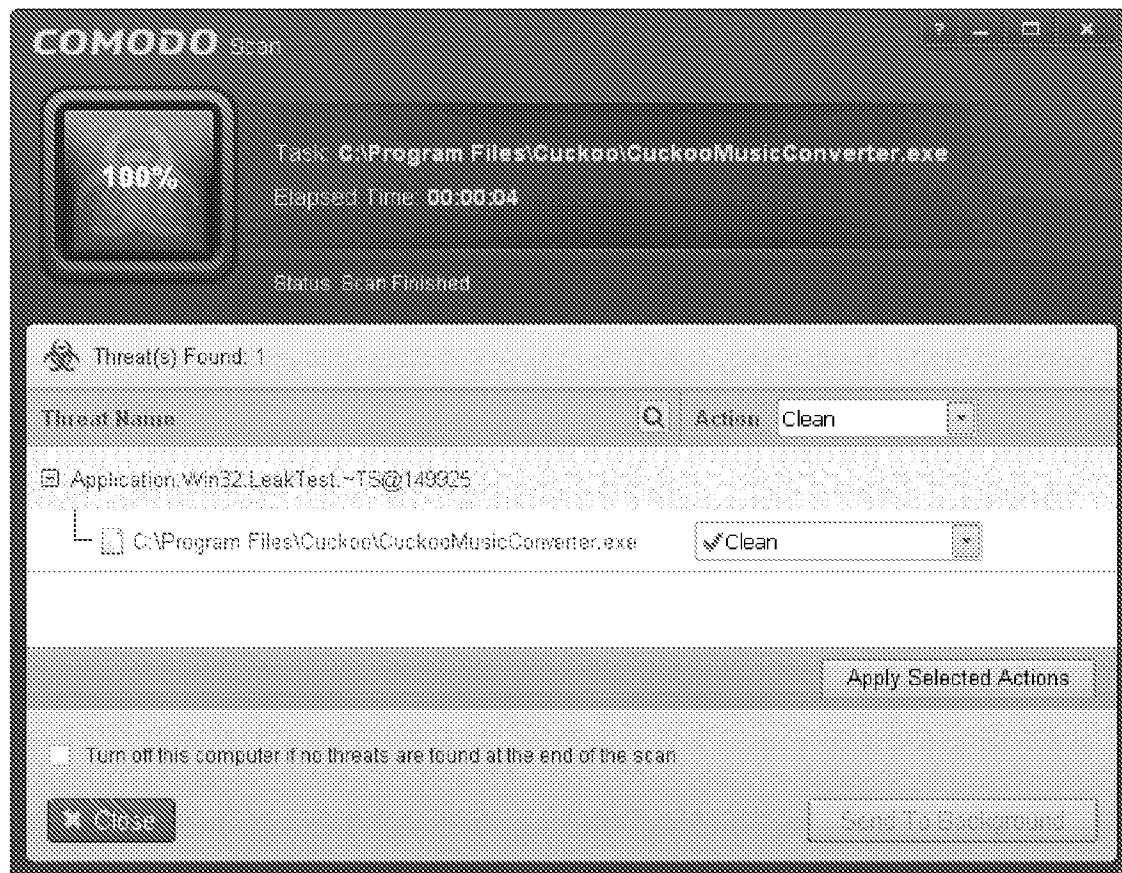
The item will be scanned immediately.



- On completion of scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



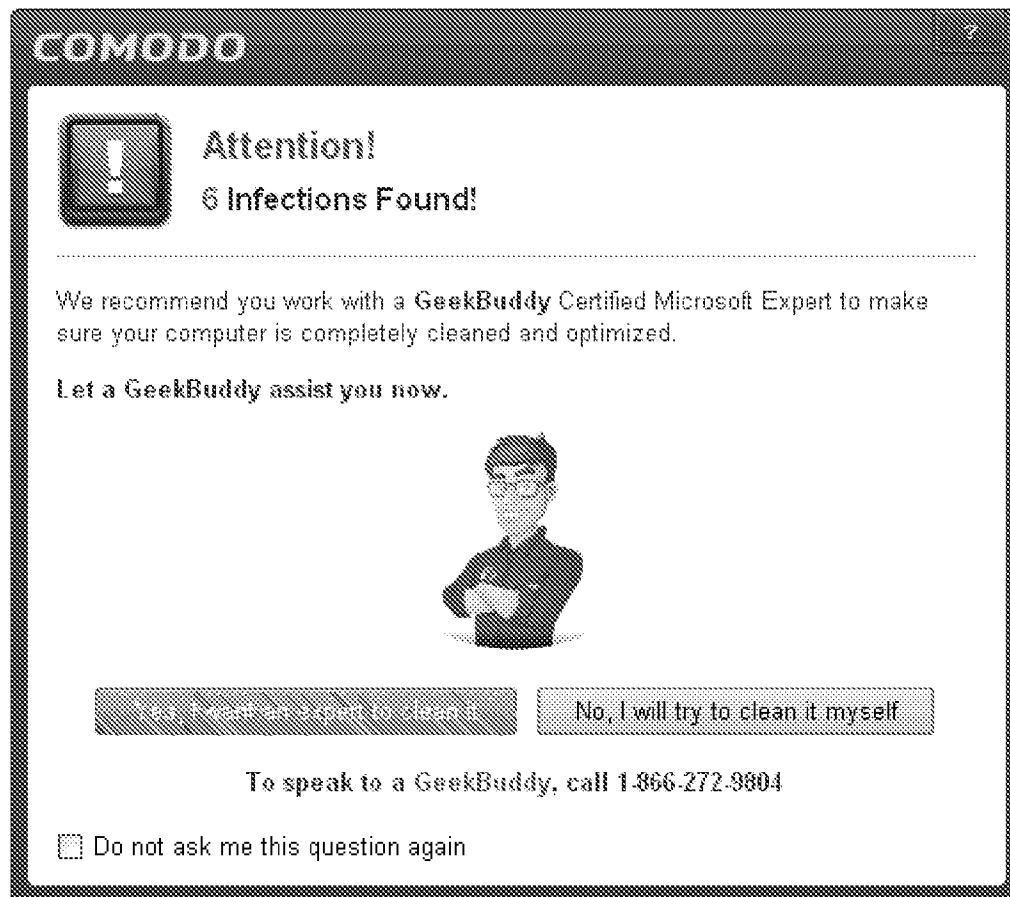
- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
 - For more details on GeekBuddy Expert help, refer to the section **Comodo GeekBuddy**.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed.



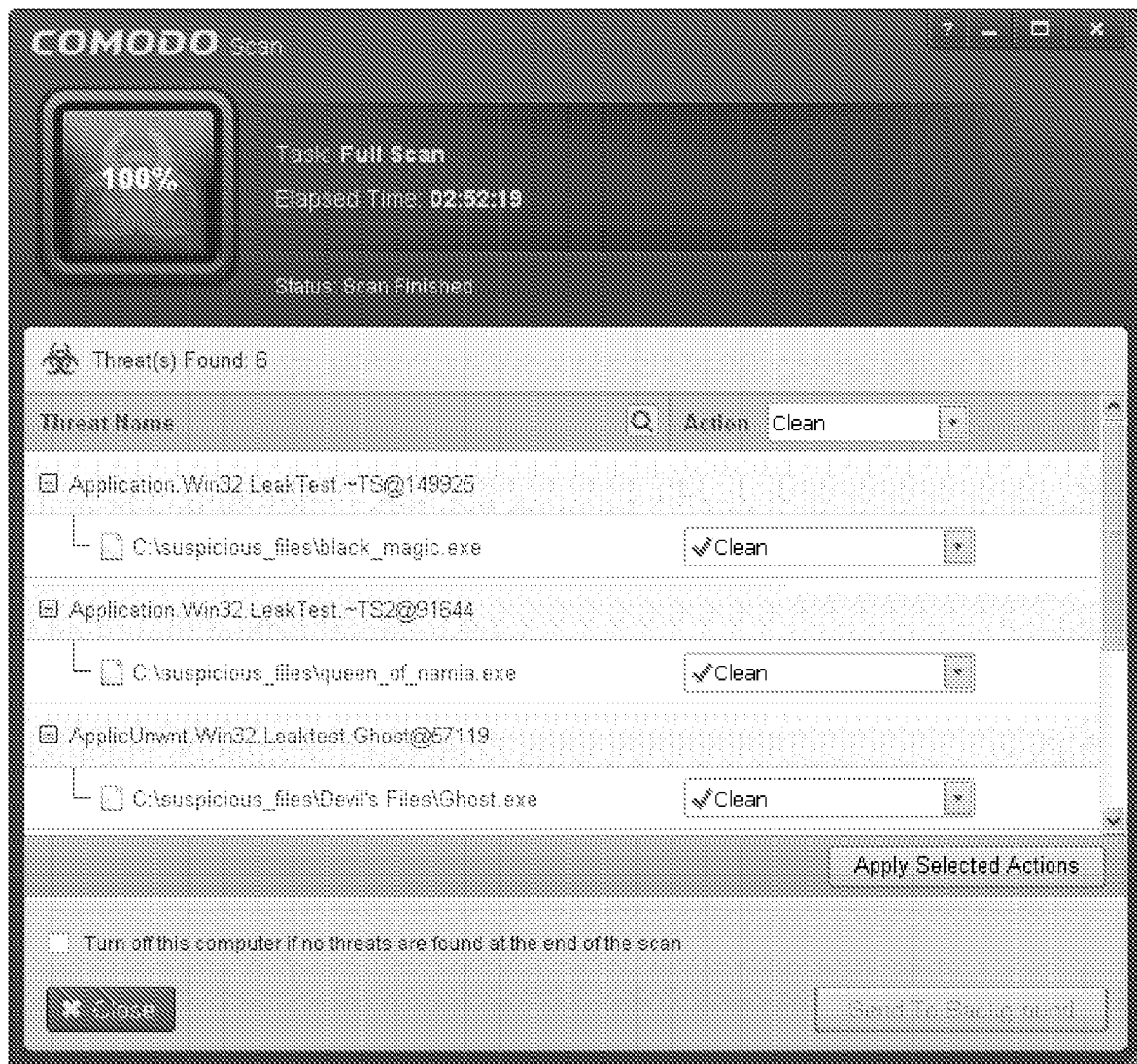
You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to [Processing the infected files](#) for more details.

2.3. Processing Infected Files

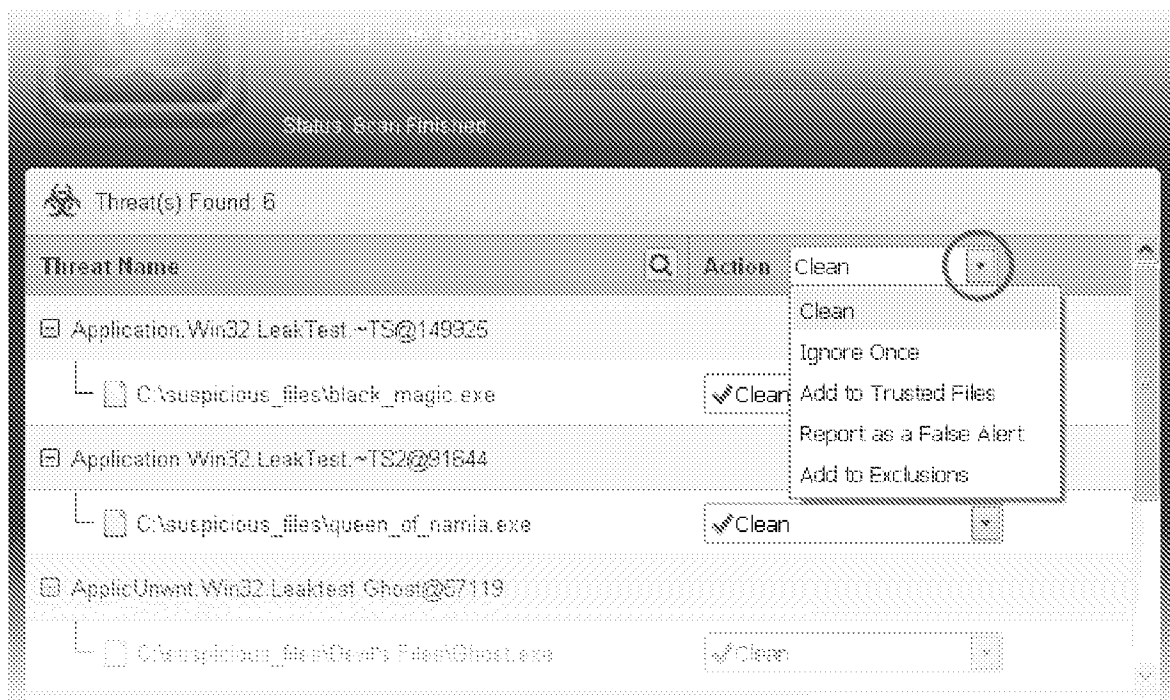
On completion of any on-demand or scheduled scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



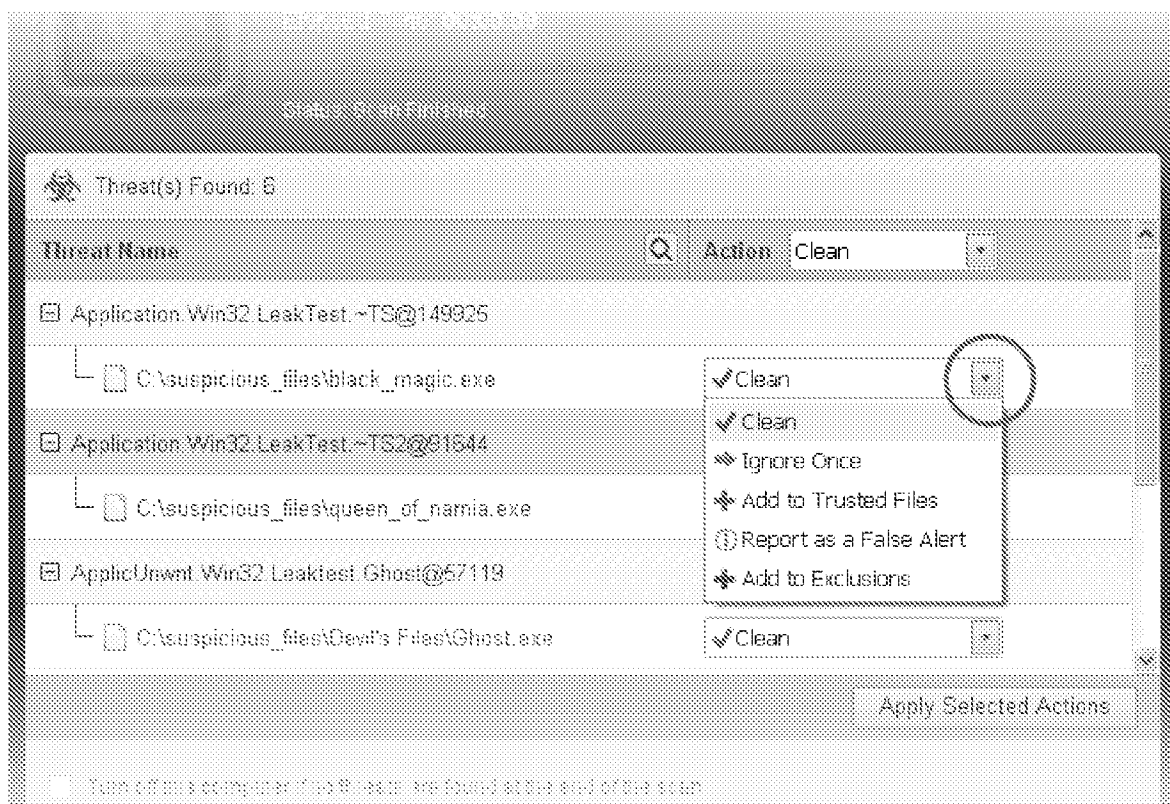
- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
 - For more details on GeekBuddy Expert help, refer to the section Comodo GeekBuddy.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed. The results will contain a list of files identified with threats or infections (Viruses, Rootkits, Malware and so on) and provide you the options for cleaning. An example results screen is shown below:



- You can select the action to be taken on all the detected threats from the 'Action' drop-down at the top right...



... or the actions to be applied to individual items from the drop-down beside each item.



The choices for the actions available are:

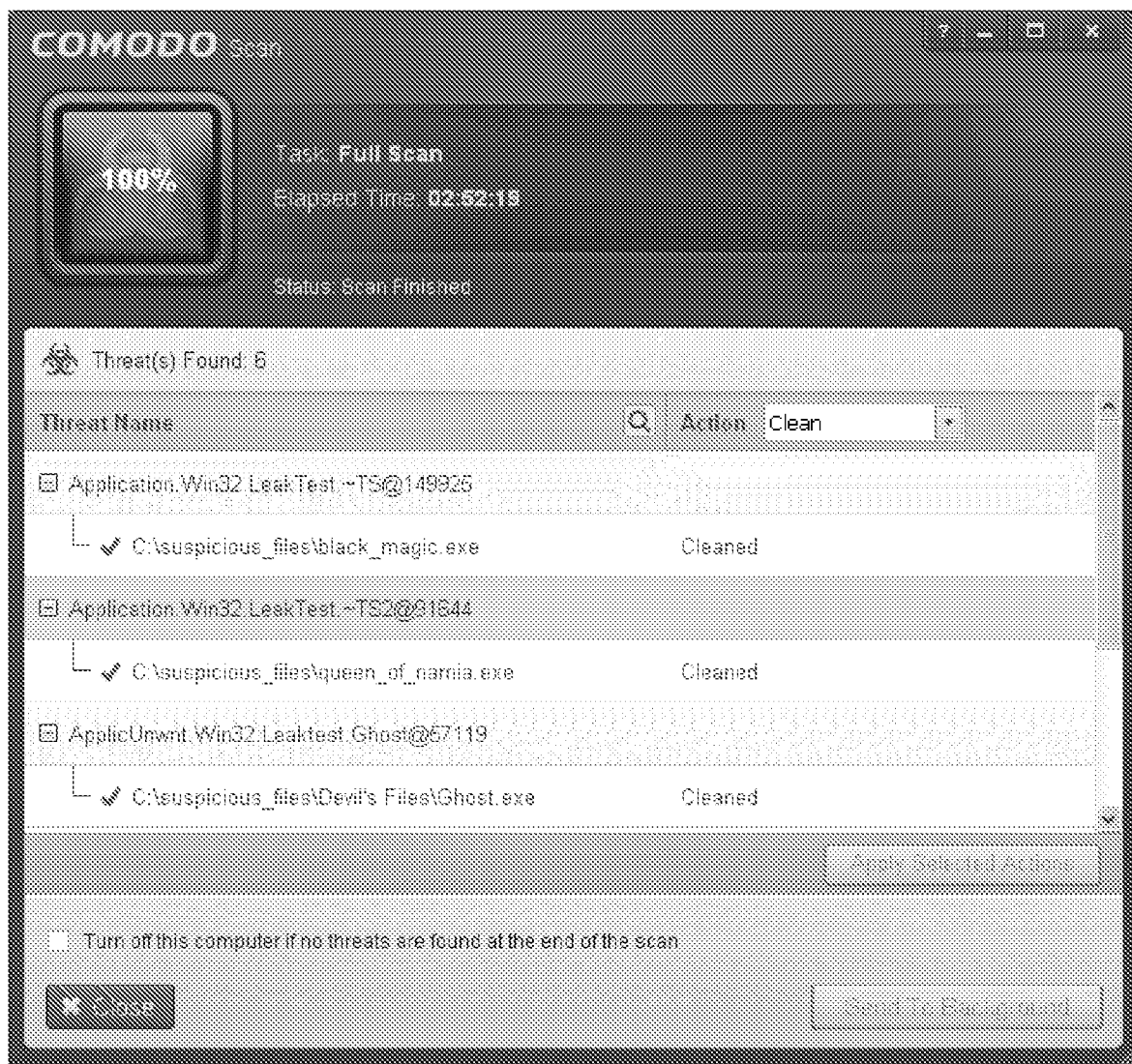
- **Clean** - If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application safe. If the disinfection routine is not available, Comodo Antivirus will

move the infections to Quarantine for later analysis and restoring/removal of the files. For more details on quarantine feature, refer to [Manage Quarantined Items](#).

- **Ignore Once** - If you want to ignore the threat this time only, select 'Ignore Once'. The file will be ignored only at that time. If the same application invokes again, the Antivirus will report it as a threat.
- **Add to Trusted Files** - If you trust the file, select 'Add to Trusted Files'. The file will be moved to Trusted Files list. The alert will not generated if the same application invokes again.
- **Report as a False Alert** - If you are sure that the file is safe, select 'Report as a False Alert'. The Antivirus will send the file to Comodo for analysis. If the file is trustworthy, it is added to the Comodo safe list.
- **Add to Exclusions** - The file will be moved to Exclusions list and will not be scanned in future. The alert will not generated if the same application invokes again.
- After selecting the action(s) to be applied, click 'Apply Selected Actions'. The files will be treated as per the action selected and the progress will be displayed.



On completion the action taken against each threat will be displayed.



- Click 'Close' to close the results window.

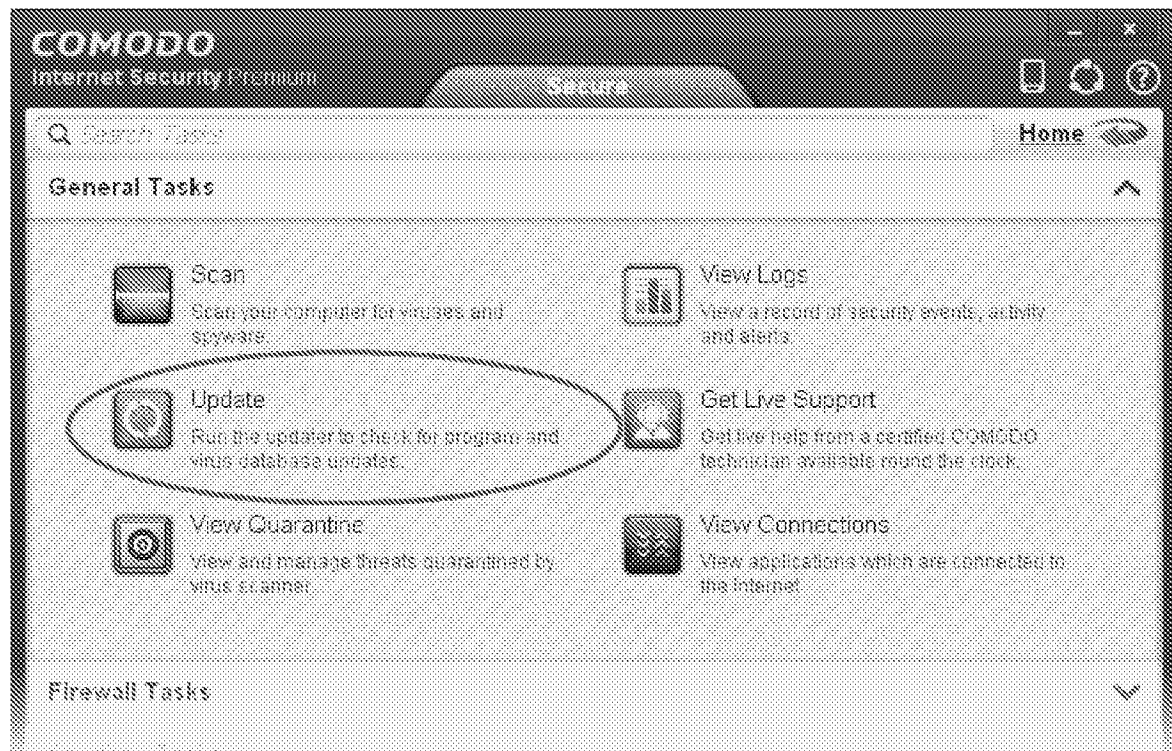
2.4. Manage Virus Database and Program Updates

In order to guarantee continued and effective antivirus protection, it is imperative that your virus databases are updated as regularly as possible. Updates can be downloaded to your system manually or automatically from Comodo's update servers.

Note: You must be connected to Internet to download updates.

To manually check for the latest virus and program updates

1. Switch to the 'Tasks' screen and click 'General Tasks' to open the 'General Tasks' interface.
2. Click 'Update'. The application will start checking for program and database updates



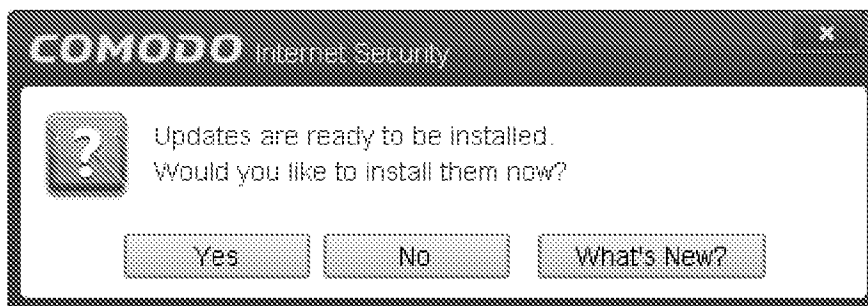
Signature updates will be downloaded and installed first if they are available:



The updater will then check for web filtering, Viruscope (recognizer) and program updates:



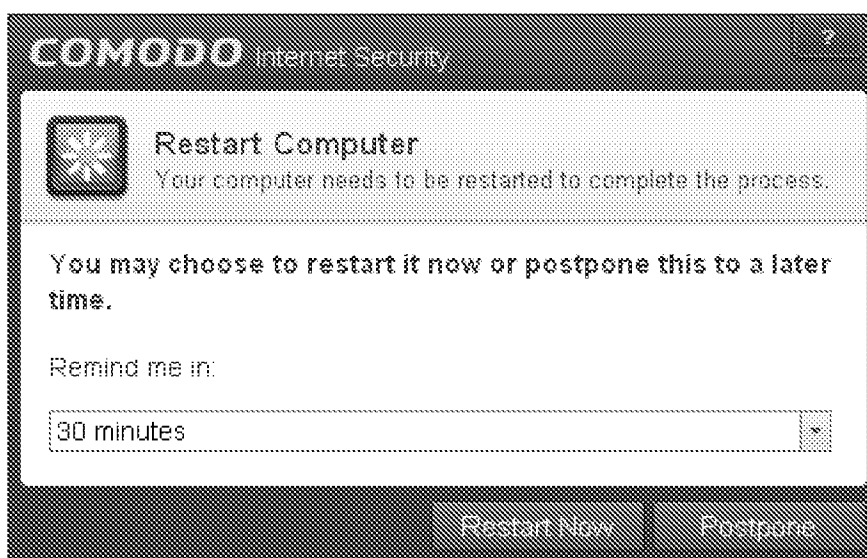
When all updates have been download you will be asked to confirm installation at the following dialog:



- Click 'Yes' to begin installation:

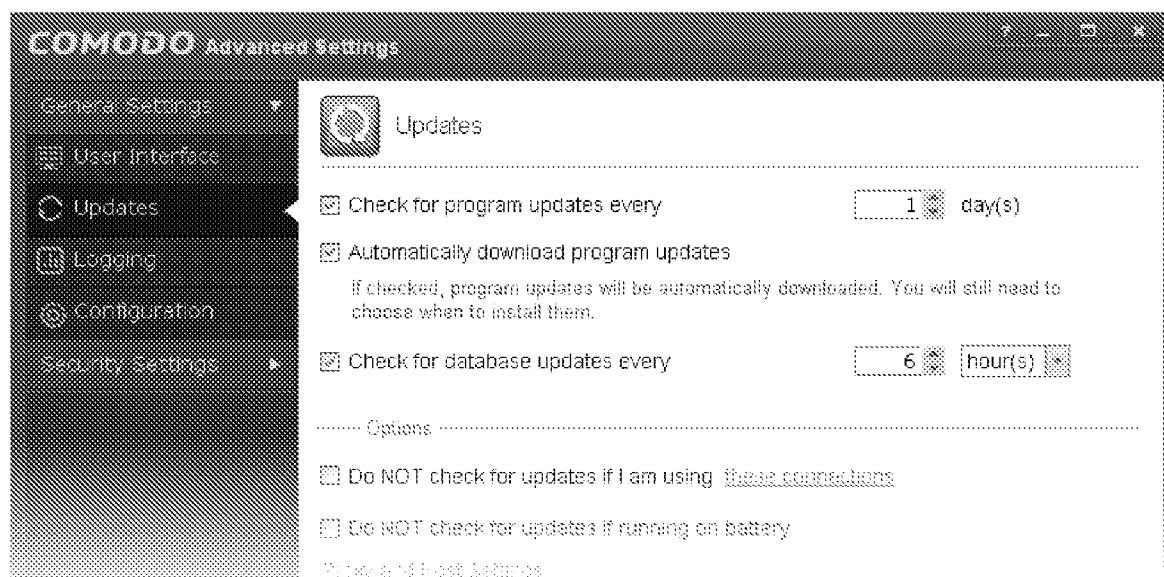
During the update process, new software components or features sometimes become available for installation. As these may alter the behavior of CIS in some manner, please carefully review these types of update before agreeing to their installation.

Your computer will need to be restarted to complete the update process. You can restart immediately or can select a period of after which you want to be reminded and click 'Postpone'.



Automatic Updates

By default, Comodo Antivirus automatically checks for and downloads database and program updates. You can modify these settings in **Advanced Tasks > Advanced Settings > Updates**.



You can also configure Comodo Antivirus to download updates automatically before any on-demand scan. Refer to **Scan Profiles** for more details.

2.5. Manage Quarantined Items

The quarantine facility removes and isolates suspicious files into a safe location before analyzing them for possible infection. Any files transferred in this fashion are encrypted- meaning they cannot be run or executed. This isolation prevents infected files from affecting the rest of your PC. If a file cannot be disinfected, then it provides a reliable safe-house until the virus database is updated- neutralizing the impact of any new virus.

The Quarantine interface can be accessed by clicking 'View Quarantine' from the 'General Tasks' interface.



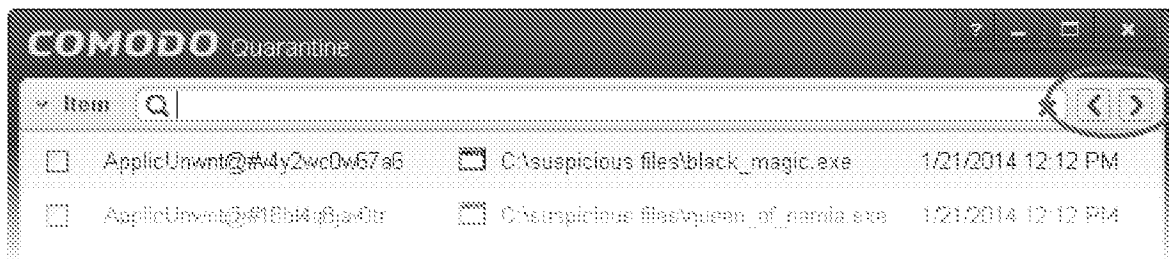
The 'Quarantine' interface displays a list of items moved to Quarantine from the results of real-time scanning, on-demand scanning and manually.

Column Descriptions

- **Item** - Indicates which application or process propagated the event;
- **Location** - Indicates the location where the application or the file is stored;
- **Date/Time** - Indicates date and time, when the item is moved to quarantine.

For details on adding executables identified as infected files during on-demand or real time scans to Quarantine, refer to **General Tasks > Scan and Clean Your Computer**.

You can use the search option to find a specific quarantined item from the list by clicking the search icon  at the far right in the column header and entering the item name in full or part. You can navigate through the successive results by clicking the left and right arrows.



The Quarantined Items interface also allows you to:

- Manually add applications, executables or other files, that you do not trust, as a Quarantined item
- Delete a selected quarantined item from the system
- Restore a quarantined item to its original location
- Delete all quarantined items
- Submit selected quarantined items to Comodo for analysis

Manually adding files as Quarantined Items

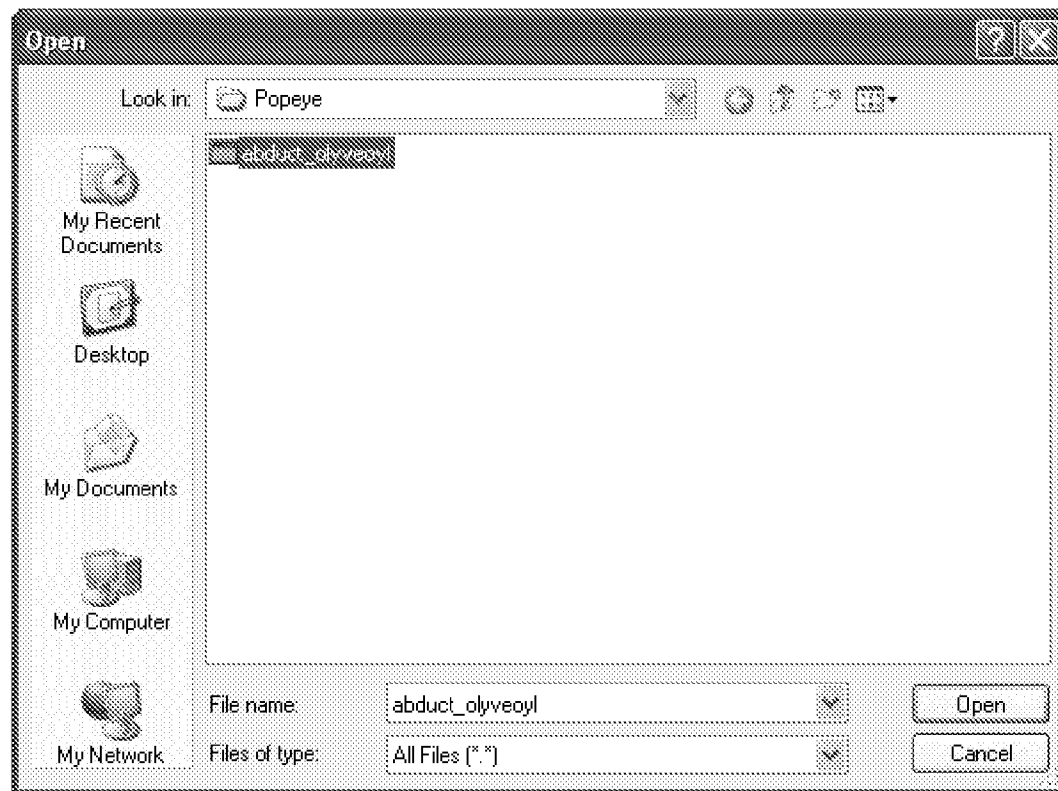
If you have a file, folder or drive that you suspect may contain a virus and not been detected by the scanner, then you have the option to isolate that item in quarantine.

To manually add a Quarantined item

1. Click the handle from the bottom of the Quarantine interface and select 'Add' from the options.



2. Navigate to the file you want to add to the quarantine and click 'Open'.



The file will be added to Quarantine. You can even send the file for analysis to Comodo, for inclusion in the white list or black list, by clicking Submit from the options.

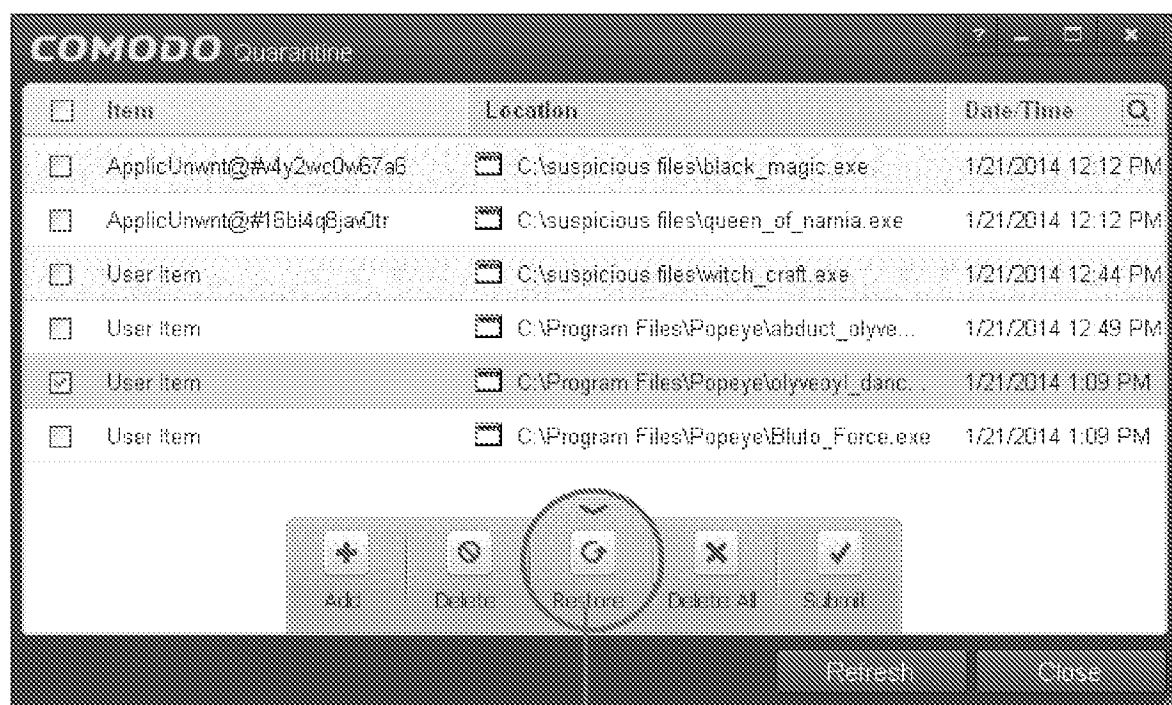
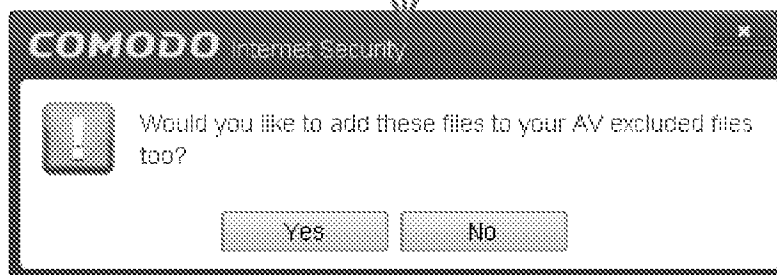
To delete a quarantined item from the system

- Select the item(s) from the 'Quarantine' interface
- Click the handle from the bottom of the interface and select 'Delete' option.

This deletes the file from the system permanently.

To restore a quarantined item to its original location

- Select the item(s) from the Quarantine interface
- Click the handle from the bottom of the interface and select 'Restore' option.



An option will be provided to add the file(s) to Exclusions list and if 'Yes' is opted, these files will not be scanned again.

The file will be restored to the original location from where it was moved to Quarantine. If the restored item does not contain a malware, it will operate as usual. But if it contains a malware, it will be detected as a threat immediately, if the Real-Time Scanning is enabled or during the next scan if it is not added to Exclusions list while restoring.

To remove all the quarantined items permanently

- Click the handle from the bottom of the interface and select 'Clear' option.

All the quarantined items will be deleted from your system permanently.

To submit selected quarantined items to Comodo for analysis

- Select the item(s) from the Quarantine interface
- Click the handle from the bottom of the interface and select 'Submit' option.

You can submit the files which you suspect to be a malware or the files which you consider as safe but identified as malware by Comodo Antivirus (False Positives). Comodo will analyze all submitted files. If they are found to be trustworthy, they will be added to the Comodo safe list (i.e. white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (i.e. black-listed).

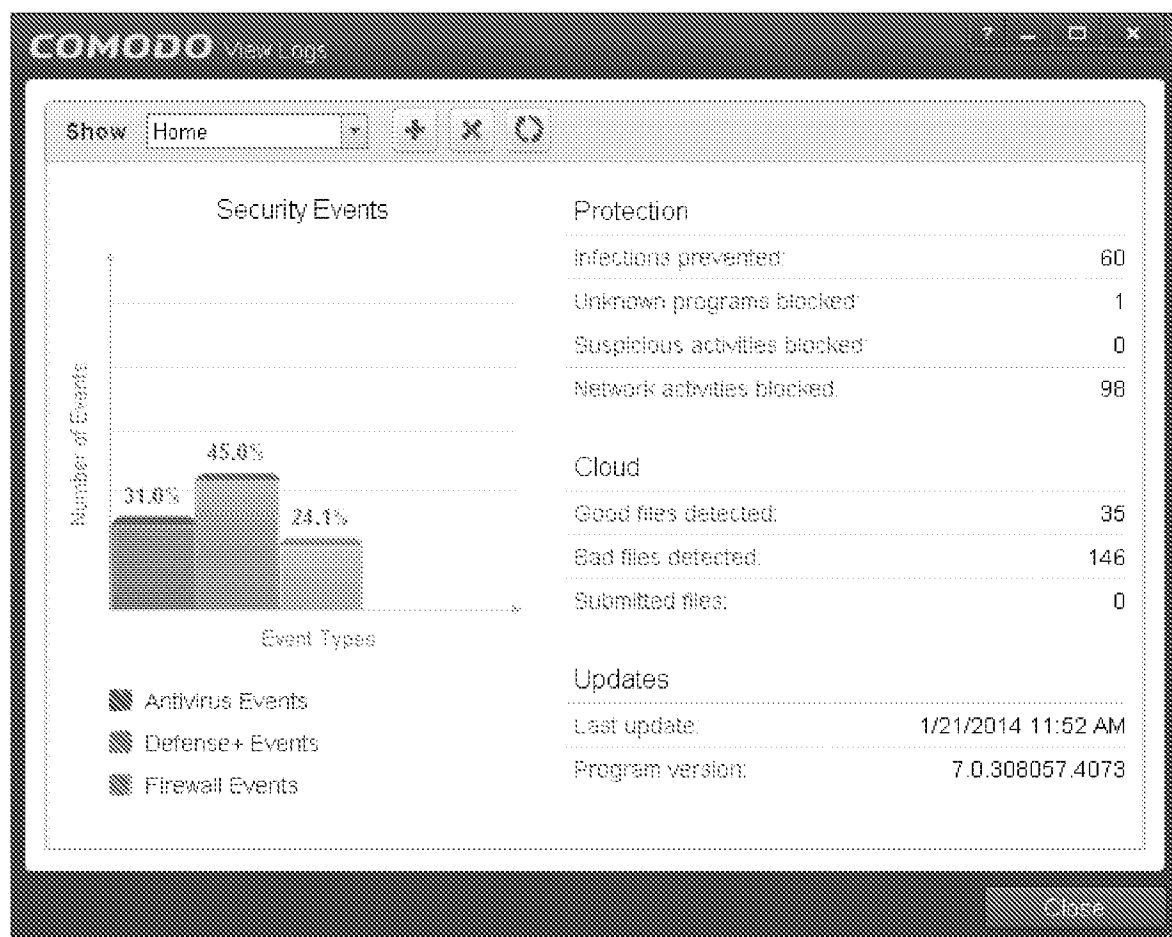
Note: Quarantined files are stored using a special format and do not constitute any danger to your computer.

2.6. View CIS Logs

CIS maintains a log of events which can be viewed at anytime by clicking 'View Logs' from the General Tasks interface.



The Log Viewer module opens with its home screen displaying a summary of CIS events:



The left hand side of the home screen displays a bar graph showing a comparison of the Antivirus events, Firewall events and Defense+ events. The right hand side displays a statistical summary of the Antivirus, Firewall and Defense+ events, the results of cloud based scanning of your system and the version and update information of the CIS installation on your system.

- The interface contains a full history of logged events of Firewall, Defense+ and Antivirus modules. Select the module from the 'Show' drop-down at the top left to display that log type in the main window.
- To open a pre-exported/stored log file, click the open button  beside the drop-down and browse to the location where the cis log file is stored
- To clear the logs, click the clear button .
- To refresh the logs, click the Refresh button .

Click the following links for more explanations of the options available for each type of filter:

'Logs per Module':

- [Antivirus](#)
- [Firewall](#)
- [Defense+](#)
- [Website Filtering](#)

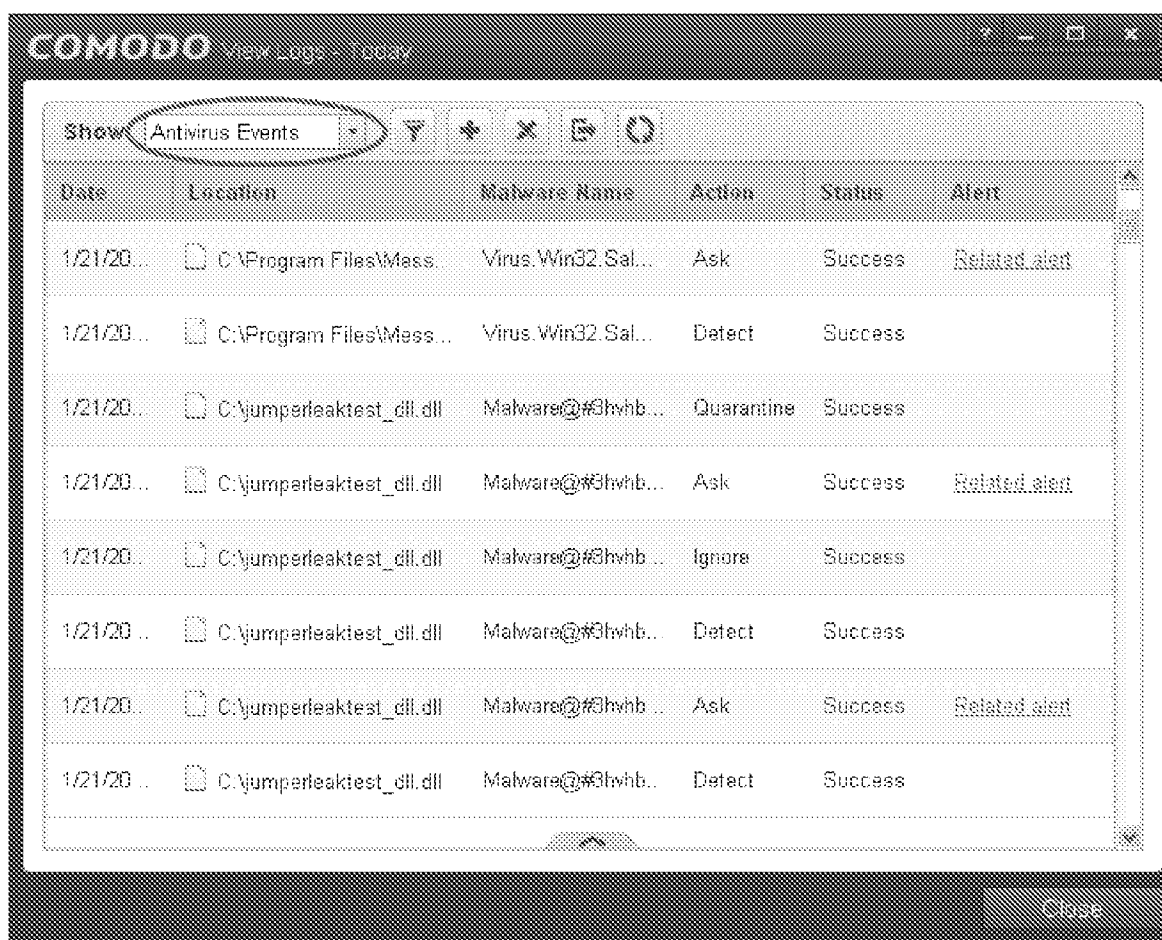
'Other Logs':

- [Alerts Displayed](#)
- [Tasks Launched](#)
- [Configuration Changes](#)

2.6.1. Antivirus Logs

Comodo Antivirus documents the results of all actions performed by it in extensive but easy to understand reports. A detailed scan report contains statistics of all scanned objects, settings used for each task and the history of actions performed on each individual file. Reports are also generated during real-time protection, and after updating the antivirus database and application modules.

The Antivirus logs can be viewed by selecting 'Antivirus Events' from the Show drop-down of the log viewer interface. Alternatively, the Antivirus log screen can be accessed by clicking the number beside 'Detected Threats' in the Advanced View of the Home screen in the Antivirus pane.



Column Descriptions

1. **Date** - Indicates the date of the event.
 2. **Location** - Indicates the location where the application detected with a threat is stored.
 3. **Malware Name** - Name of the malware event that has been detected.
 4. **Action** - Indicates action taken against the malware through Antivirus.
 5. **Status** - Gives the status of the action taken. It can be either 'Success' or 'Fail'.
 6. **Alert** - Gives the details of the alert displayed for the event
- To export the Antivirus logs as a HTML file click the 'Export' button  or right click inside the log viewer and choose 'Export' from the context sensitive menu.
 - To open a stored CIS log file, click the 'Open' button .
 - To refresh the Antivirus logs, click the 'Refresh' button  or right click inside the log viewer and choose 'Refresh' from the context sensitive menu..
 - To clear the Antivirus logs click the 'Clear' button .

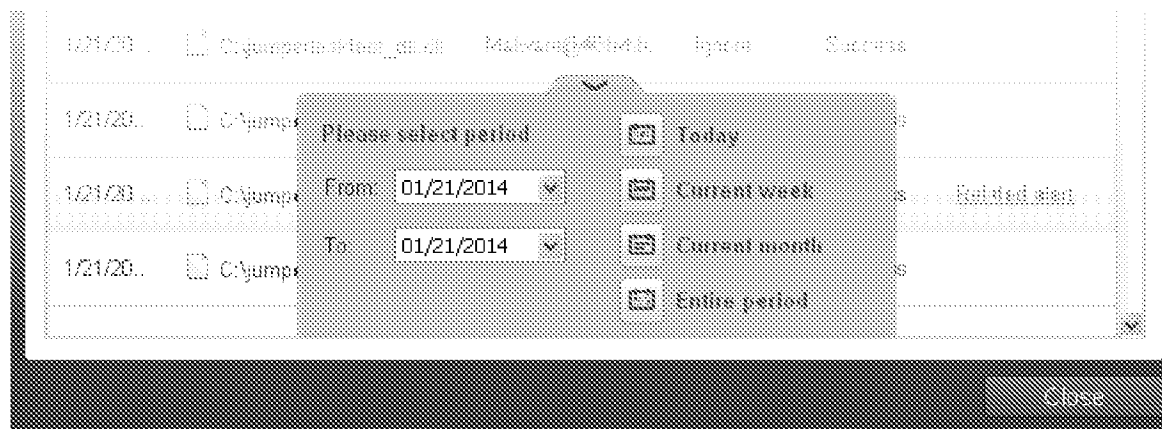
2.6.1.1. Filtering Antivirus Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- Preset Time Filters
- Advanced Filters

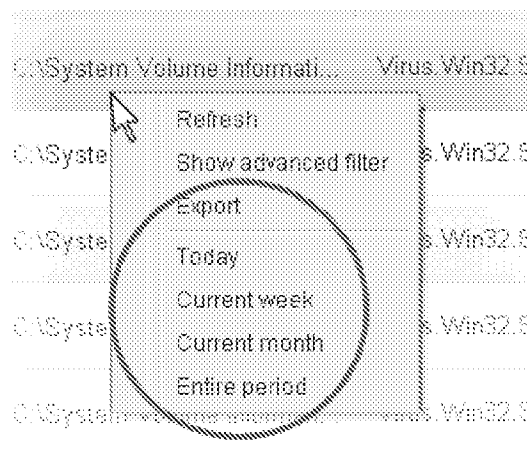
Preset Time Filters:

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Internet Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



Advanced Filters:

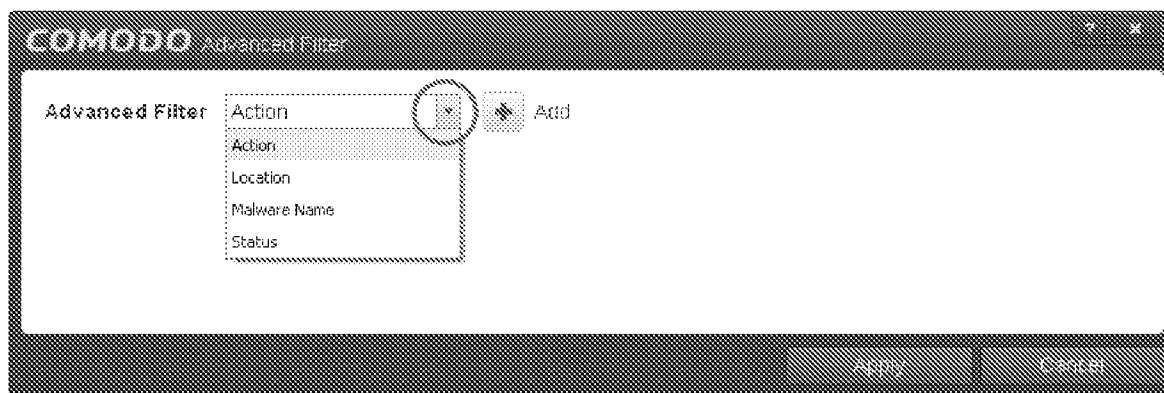
Having chosen a preset time filter, you can further refine the displayed events according to specific filters. Following are available filters for Antivirus logs and their meanings:

- **Action** - Displays events according to the response (or action taken) by the Antivirus
- **Location** - Displays only the events logged from a specific location

- **Malware Name** - Displays only the events logged corresponding to a specific malware
- **Status** - Displays the events according to the status after the action taken. It can be either 'Success' or 'Fail'

To configure Advanced Filters for Antivirus events

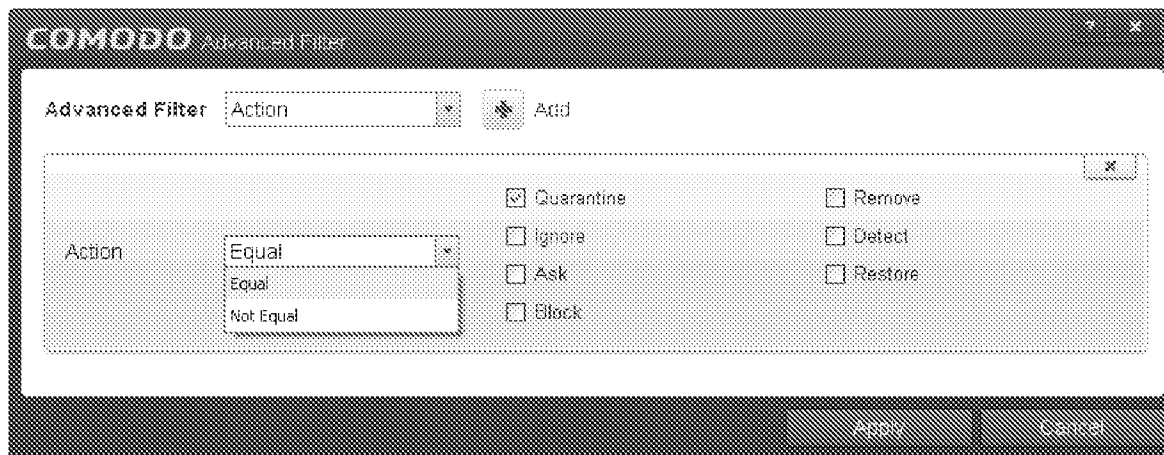
1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for AV events will open
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



You have 4 categories of filters that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are the options available in the 'Advanced Filter' drop-down:

- Action:** The 'Action' option allows you to filter the entries based on the actions taken by CIS against the detected threat. Selecting the 'Action' option displays a drop down field and a set of specific filter parameters that can be selected or deselected.

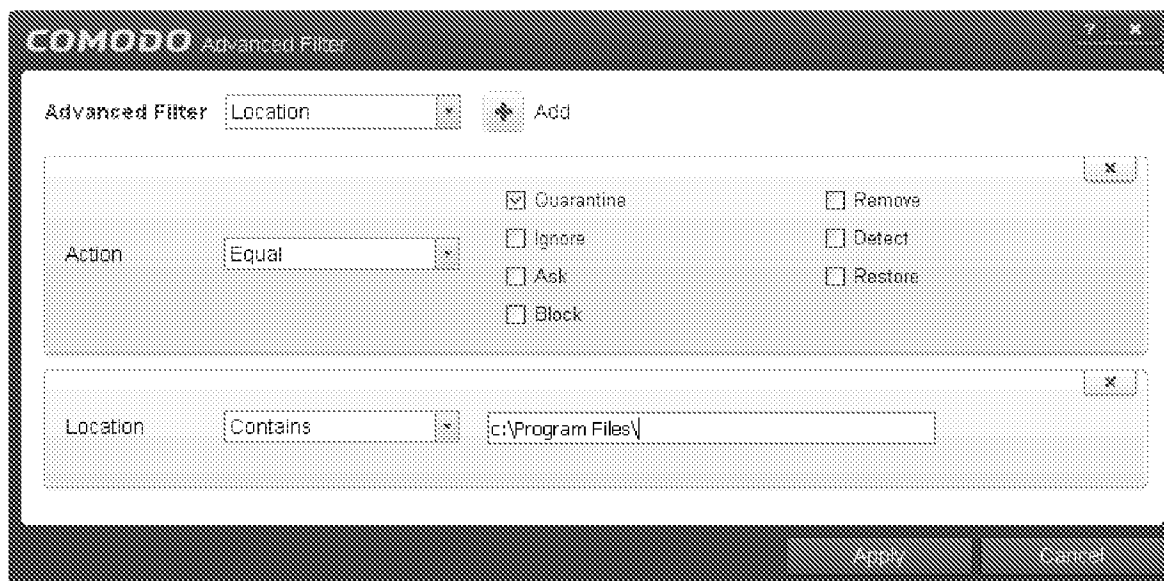


- Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.
- Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
 - Quarantine: Displays events where the user chose to quarantine a file
 - Remove: Displays events where the user chose to delete an item
 - Ignore: Displays events where the user chose to ignore an item
 - Detect: Displays events for detection of a malware

- Ask: Displays events when user was asked by alert concerning some Defense+, Firewall or Antivirus event
- Restore: Displays events of the applications that were quarantined and restored
- Block: Displays events of the applications that were blocked

For example, if you checked the 'Quarantine' box then selected 'Not Equal', you would see only those Events where the Quarantine Action was not selected at the virus notification alert.

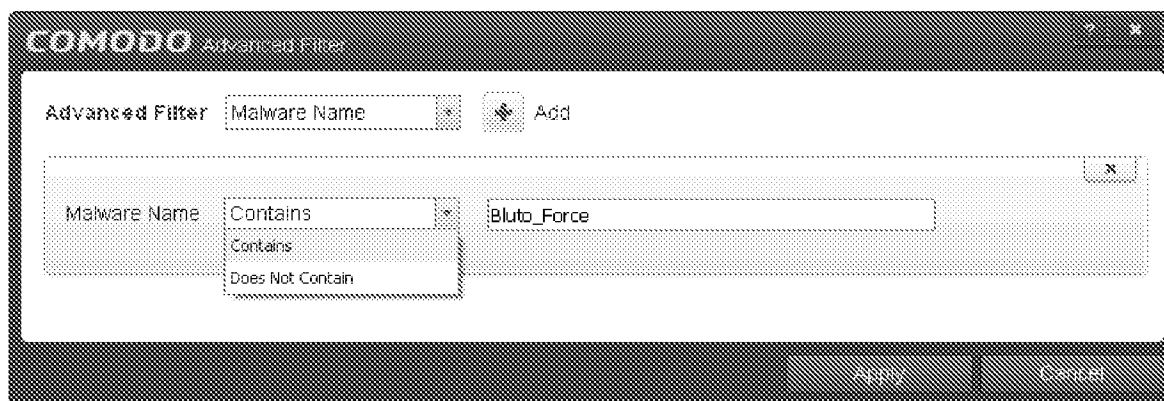
- Location:** The 'Location' option enables you to filter the log entries related to events logged from a specific location. Selecting the 'Location' option displays a drop-down field and text entry field.



- Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- Enter the text or word that needs to be filtered.

For example, if you select 'Contains' option from the drop-down and enter the phrase 'C:\Samples' in the text field, then all events containing the entry 'C:\Samples' in the Location field will be displayed. If you select 'Does Not Contain' option from the drop-down field and enter the phrase 'C:\Samples' in the text field, then all events that do not have the entry 'C:\Samples' will be displayed.

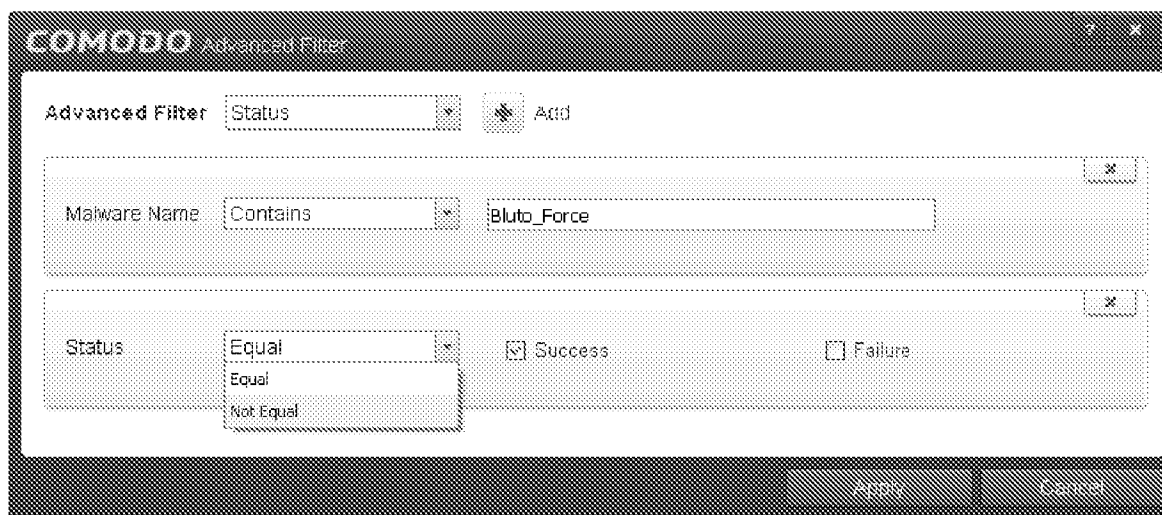
- Malware Name:** The 'Malware Name' option enables you to filter the log entries related to specific malware. Selecting the 'Malware Name' option displays a drop-down field and text entry field.



- Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- Enter the text in the name of the malware that needs to be filtered.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'Bluto-Force' in the text field, then all events containing the entry 'Bluto-Force' in the Malware Name field will be displayed. If you choose 'Does Not Contain' option from the drop-down and enter the phrase 'Bluto-Force' in the text field, then all events that do not have the entry 'Bluto-Force' in the 'Malware Name' field will be displayed.

- iv. **Status:** The 'Status' option allows you to filter the log entries based on the success or failure of the action taken against the threat by CIS. Selecting the 'Status' option displays a drop-down field and a set of specific filter parameters that can be selected or deselected.



- a) Select 'Equal' or 'Not Equal' option from the drop-down field. 'Not Equal' will invert your selected choice.
- b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
 - Success: Displays Events that successfully executed (for example, the malware was successfully quarantined)
 - Failure: Displays Events that failed to execute (for example, the database malware was not disinfected)

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

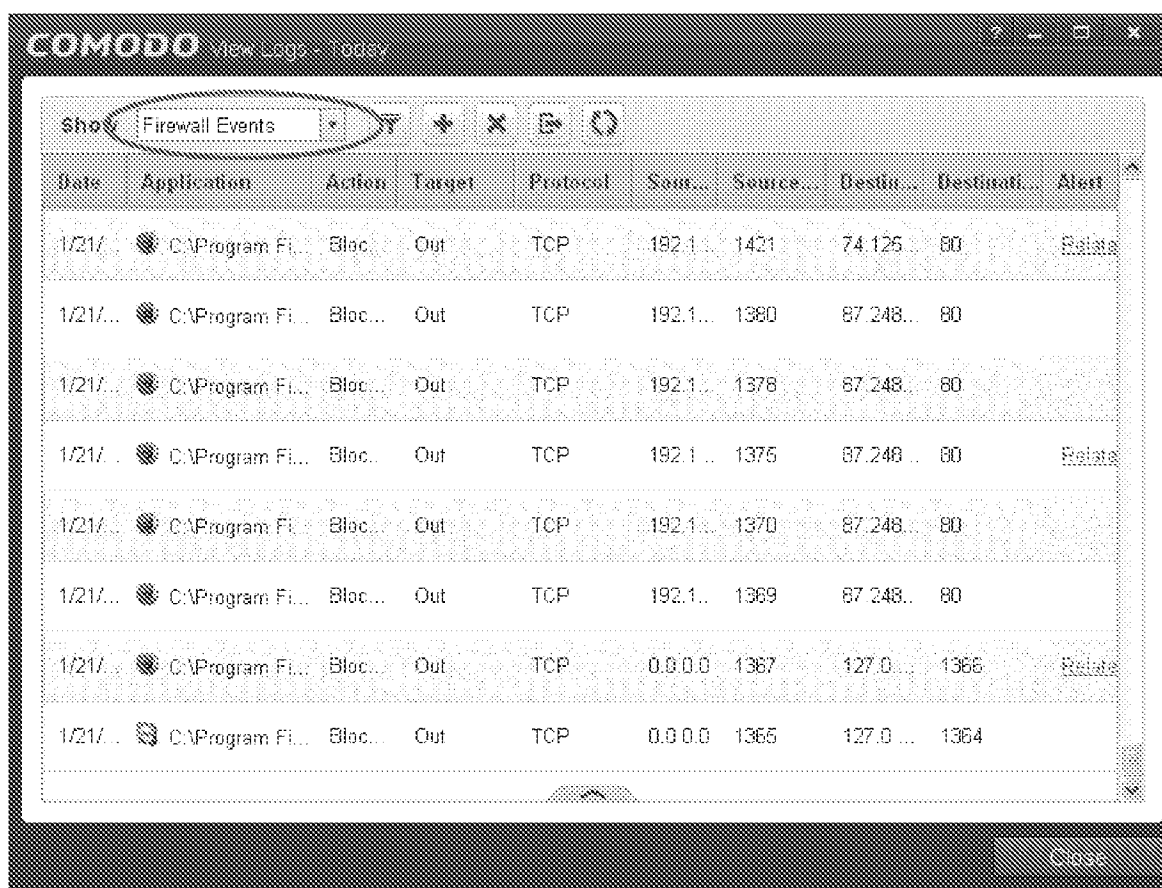
- Click 'Apply' for the filters to be applied to the Antivirus log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.6.2. Firewall Logs

Comodo Internet Security records a history of all actions taken by the firewall. Firewall 'Events' are generated and recorded for various reasons - including whenever an application or process makes a connection attempt that contravenes a rule in your Rule sets or whenever there is a change in Firewall configuration.

The Firewall logs can be viewed by selecting 'Firewall Events' from the 'Show' drop-down of the log viewer interface.

Alternatively, the Firewall log screen can be accessed by clicking the number beside 'Network Intrusions' in the Advanced View of the Home screen in the Firewall pane.



Column Descriptions

1. **Date** - Contains precise details of the date and time of the connection attempt.
2. **Application** - Indicates which application or process propagated the event. If the application has no icon, the default system icon for executable files are used
3. **Action** - Contains the flags attached to the events, indicating how the firewall has reacted to the connection attempt.
4. **Target** - Indicates whether the connection attempt is inbound or outbound.
5. **Protocol** - Represents the Protocol used by the application that attempted to create the connection. This is usually TCP/IP or UDP - which are the most heavily used networking protocols.
6. **Source IP** - States the IP address of the host that made the connection attempt. This is usually the IP address of your computer for outbound connections.
7. **Source Port** - States the port number on the host at the source IP which was used to make this connection attempt.
8. **Destination IP** - States the IP address of the host to which the connection attempt was made. This is usually the IP address of your computer for inbound connections.
9. **Destination Port** - States the port number on the host at the destination IP to which the connection attempt was made.
10. **Alert** - Gives the details of the alert displayed for the event

- To export the Firewall logs as a HTML file click the Export button  or right click inside the log viewer and choose 'Export' from the context sensitive menu.

- To open a stored CIS log file, click the Open button .

- To refresh the Firewall logs, click the Refresh button  or right click inside the log viewer and choose 'Refresh' from the context sensitive menu..
- To clear the Firewall logs click the Clear button .

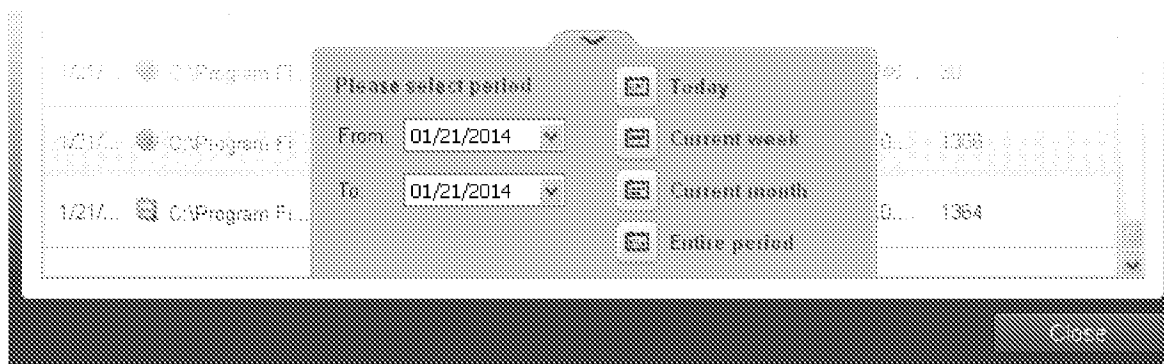
2.6.2.1. Filtering Firewall Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- Preset Time Filters
- Advanced Filters

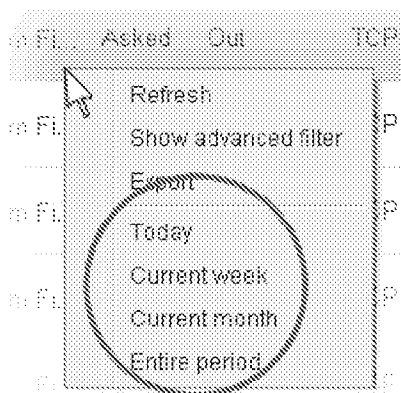
Preset Time Filters:

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Internet Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



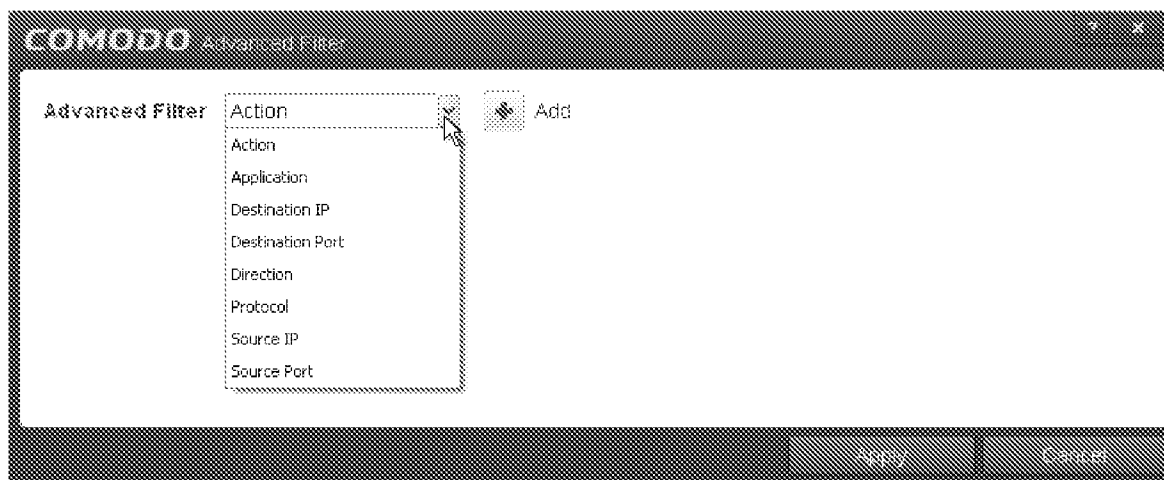
Advanced Filters

Having chosen a preset time filter, you can further refine the displayed events according to specific filters. Following are available filters for Firewall logs and their meanings:

- **Action** - Displays events according to the response (or action taken) by the firewall
- **Application** - Displays only the events propagated by a specific application
- **Destination IP** - Displays only the events with a specific target IP address
- **Destination Port** - Displays only the events with a specific target port number
- **Direction** - Displays only the events of Inbound or Outbound nature
- **Protocol** - Displays only the events that involved a specific protocol
- **Source IP address** - Displays only the events that originated from a specific IP address
- **Source Port** - Displays only the events that originated from a specific port number

To configure Advanced Filters for Firewall events

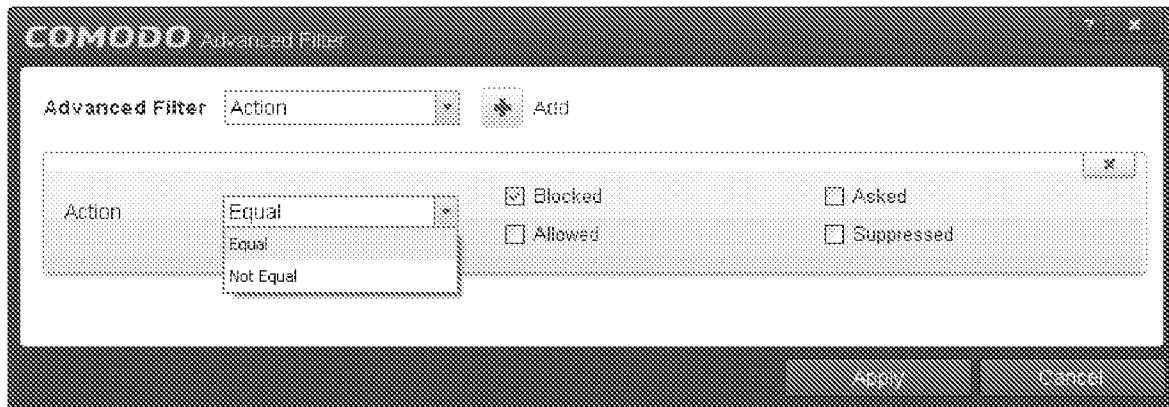
1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for Firewall events will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



You have 8 categories of filters that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are the options available in the 'Advanced Filter' drop-down:

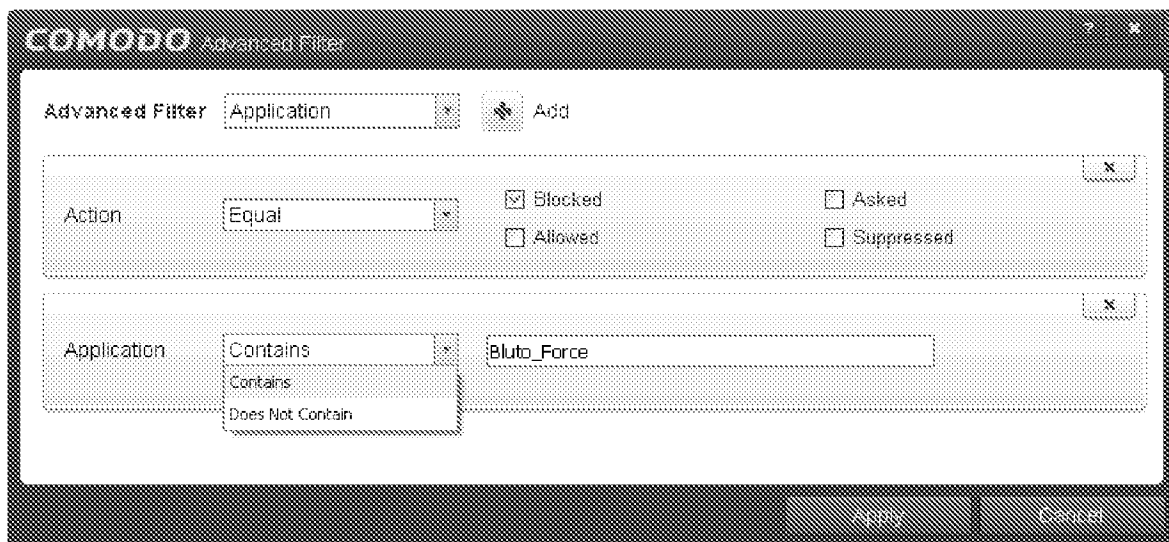
- i. **Action:** Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



- a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:

- Blocked: Displays list of events that were blocked
- Allowed: Displays list of events that were allowed
- Asked: Displays list of events that were asked to the user
- Suppressed: Displays list of events that were suppressed by the user

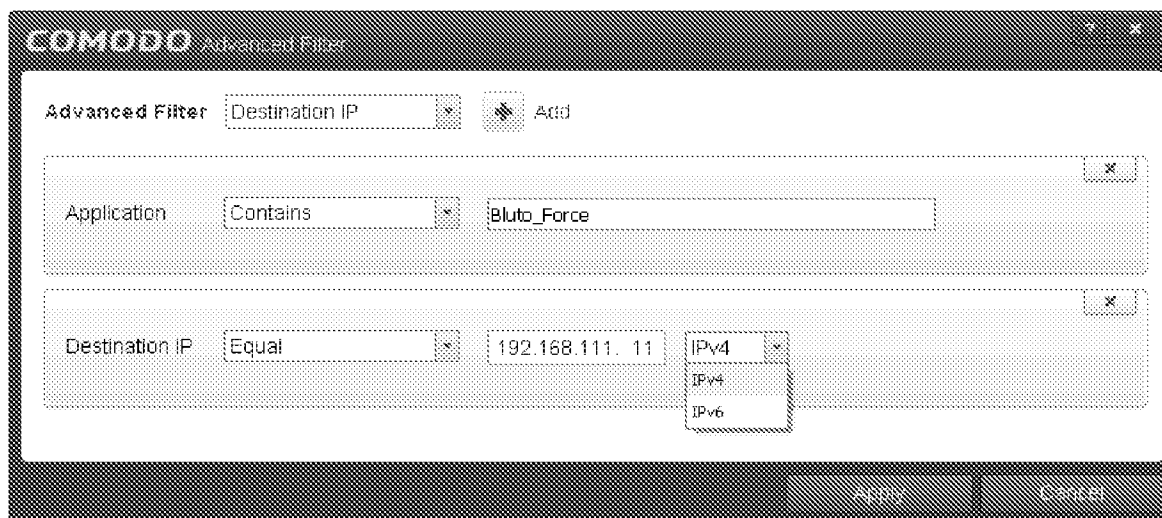
ii. **Application:** Selecting the 'Application' option displays a drop-down box and text entry field.



- a) Select 'Contains' or 'Does Not Contain' option from the drop-down box.
- b) Enter the text or word that needs to be filtered.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'Bluto-Force' in the text field, then all events containing the entry 'Bluto-Force' in the 'Application' column will be displayed. If you select 'Does Not Contain' option from the drop-down field and enter the phrase 'Bluto-Force' in the text field, then all events that do not have the entry 'Bluto-Force' in the 'Application' column will be displayed.

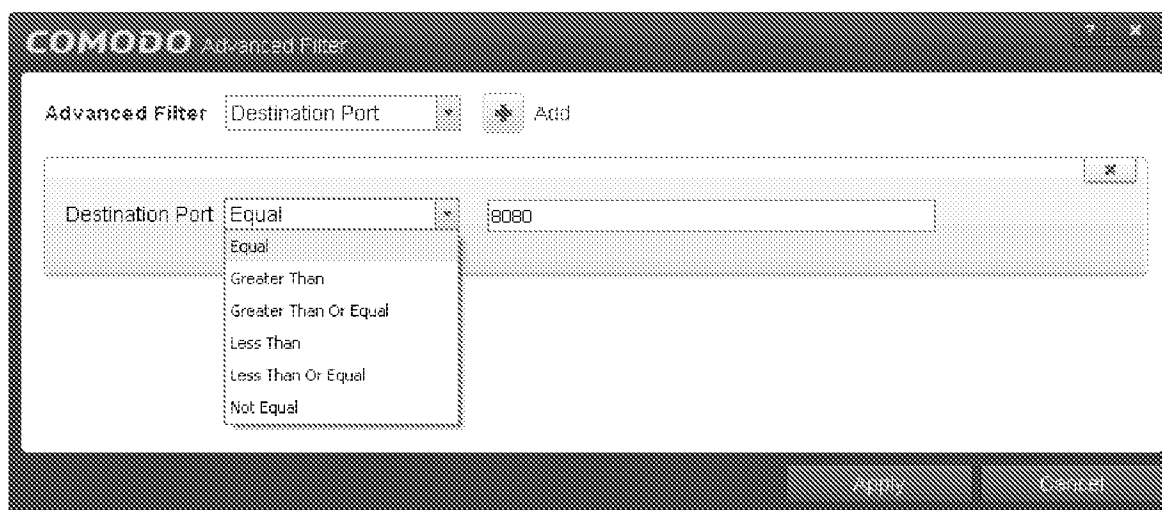
iii. **Destination IP:** Selecting the 'Destination IP' option displays two drop-down boxes and a text entry field.



- a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b) Select 'IPv4' or 'IPv6' from the drop-down box.
- c) Enter the destination system's IP address that needs to be filtered.

For example, if you choose 'Contains' option from the drop-down, select IPv4 and enter 192.168.111.111 in the text field, then all events containing the entry '192.168.111.111' in the 'Destination IP' column will be displayed.

iv. **Destination Port:** Selecting the 'Destination Port' option displays a drop-down box and text entry field.



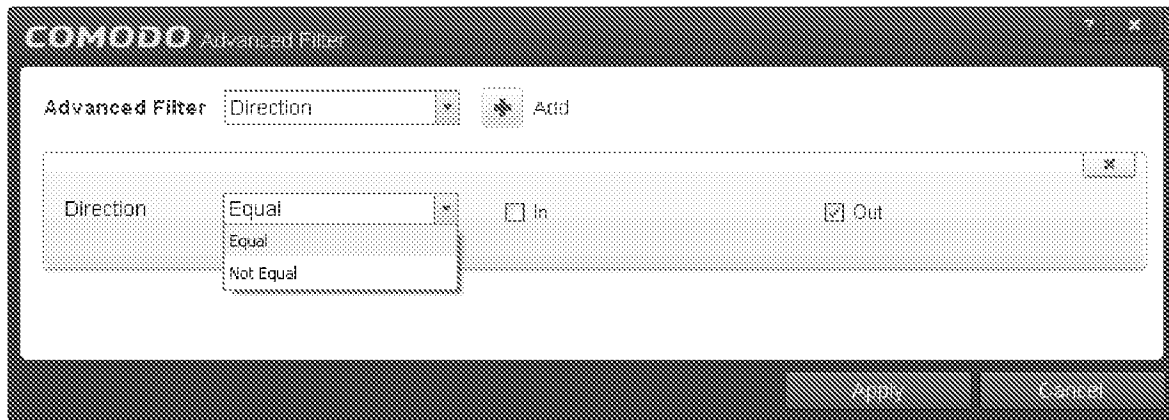
- a) Select any one of the following option the drop-down box.

- Equal
- Greater than
- Greater than or Equal
- Less than
- Less than or Equal
- Not Equal

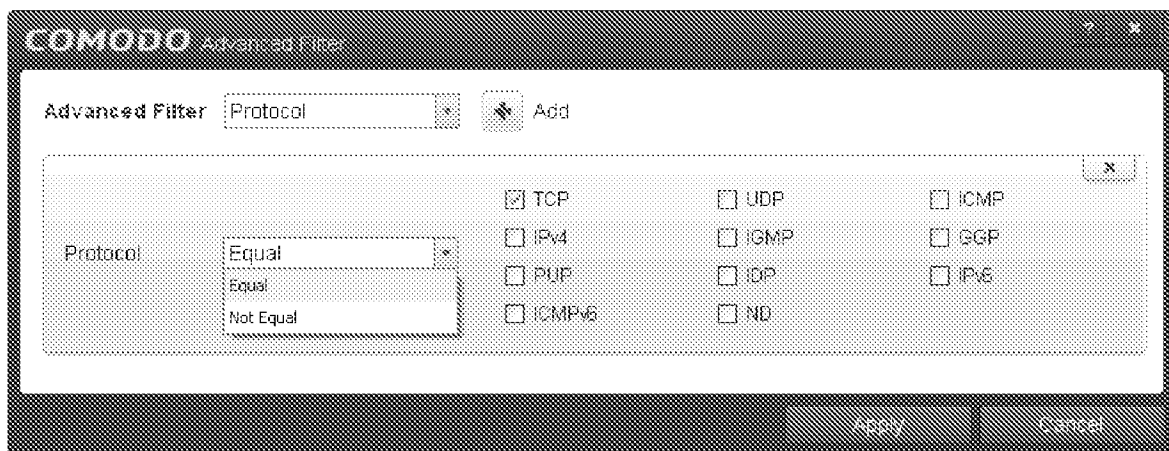
- b) Now enter the destination port number in the text entry field.

For example, if you choose 'Equal' option from the drop-down and enter 8080 in the text field, then all events containing the entry '8080' in the 'Destination Port' column will be displayed.

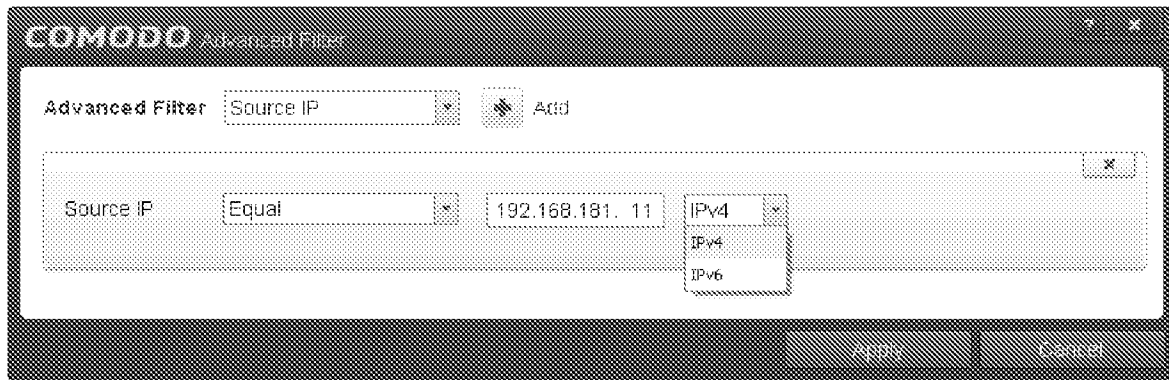
- v. **Direction:** Selecting the 'Direction' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



- a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
 - b) Now select the check box of the specific filter parameters to refine your search. The parameter available are:
 - In: Displays a list of events that were directed into the system
 - Out: Displays a list of events that were directed out of the system
- vi. **Protocol:** Selecting the 'Protocol' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

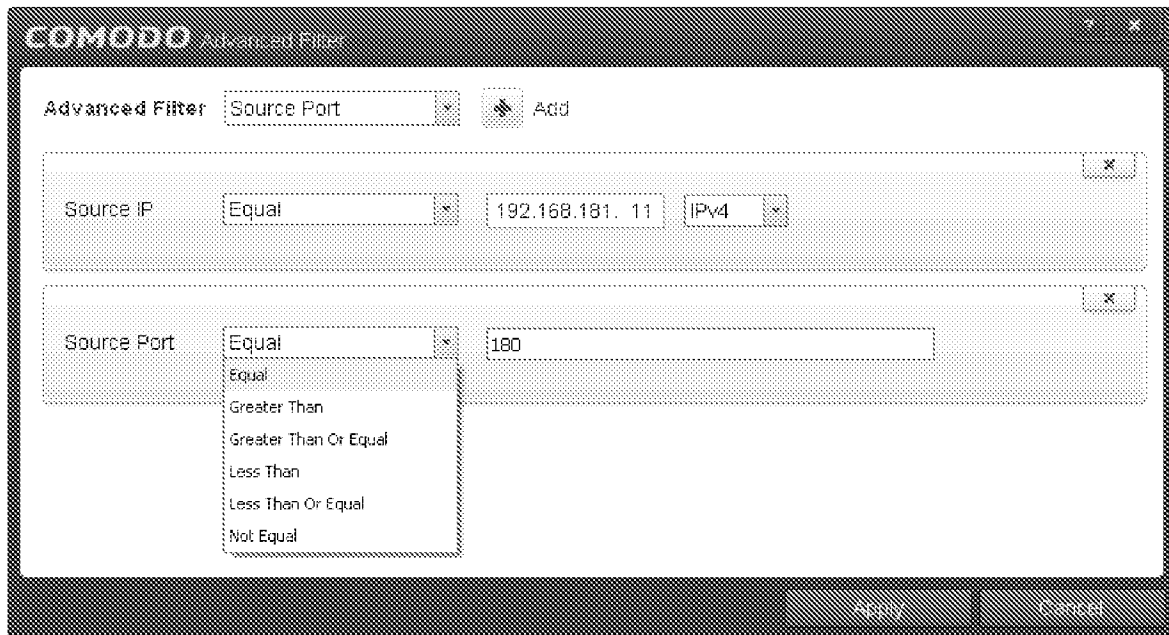


- a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
 - b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
 - TCP
 - UDP
 - ICMP
 - IPV4
 - IGMP
 - GGP
 - PUP
 - IDP
 - IPV6
 - ICMPV6
 - ND
- vii. **Source IP:** Selecting the 'Source IP' option displays two drop-down boxes and a set specific filter parameters that can be selected or deselected.



- a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b) Select 'IPv4' or 'IPv6' from the drop-down box.
- c) Enter the source system's IP address that needs to be filtered.

viii. **Source Port:** Selecting the 'Status' option displays a drop-down box and a set specific filter parameters that can be selected or deselected.



- a) Select any one of the following option the drop-down box.
 - Equal
 - Greater than
 - Greater than or Equal
 - Less than
 - Less than or Equal
 - Not Equal
- b) Now enter the source port number in the text entry field.

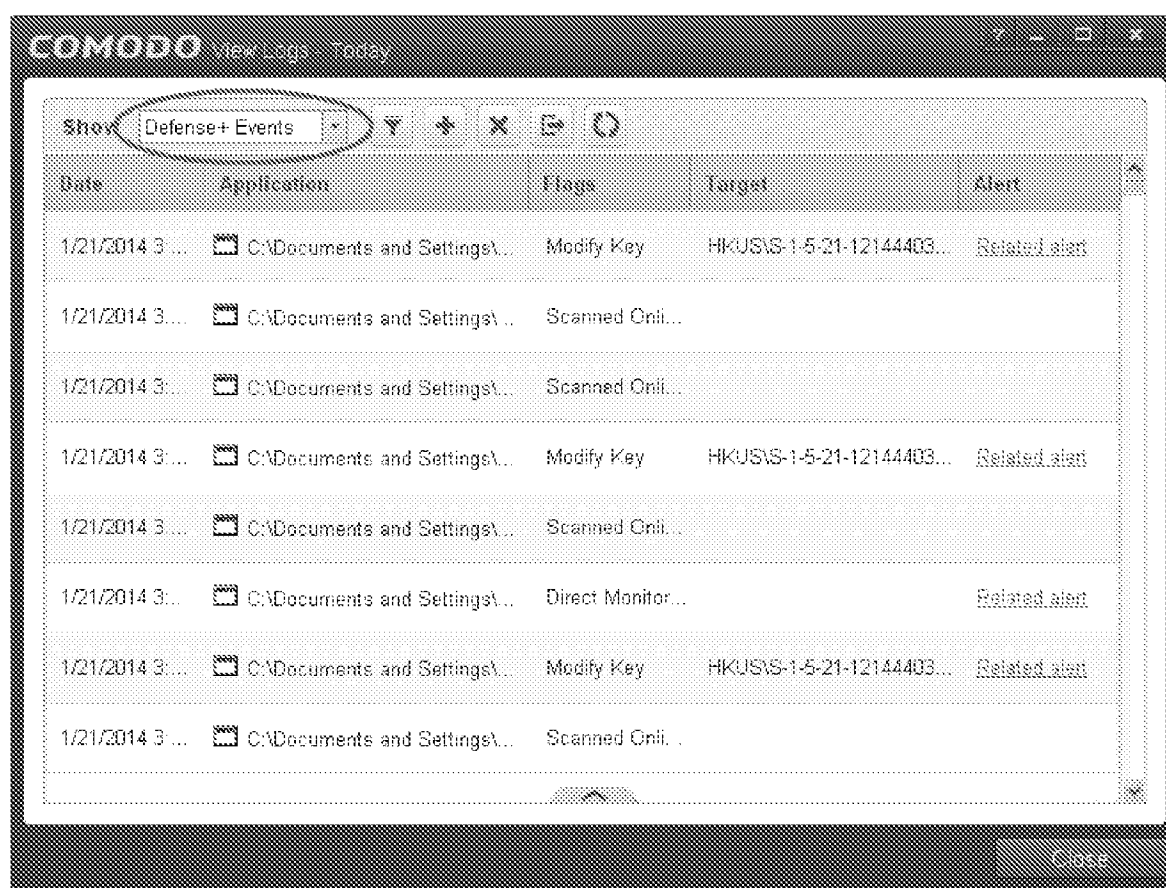
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the Firewall log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.6.3. Defense+ Logs

Comodo Internet Security records a history of all actions taken by Defense+. Defense+ 'Events' are generated and recorded for various reasons. Examples include changes in HIPS settings, when an application is auto-sandboxed by Behavior Blocker, when an application or process attempts to access restricted areas or when an action occurs that contravenes your HIPS Rulesets.

The Defense+ logs can be viewed by selecting 'Defense+ Events' tab from the 'Show' drop-down of the log viewer interface. Alternatively, the Defense+ log screen can be accessed by clicking the number beside 'Blocked Intrusions' in the Advanced View of the Home screen in the Auto-Sandbox pane.



Column Descriptions

- Date** - Contains precise details of the date and time of the access attempt.
- Application** - Indicates which application or process propagated the event. If the application has no icon, the default system icon for executable files are used.
- Flags** - Indicates flags set for the kinds of actions against the event triggered by the file.
- Target** - Represents the location of the target file.
- Alert** - Gives the details of the alert displayed for the event

- To export the Defense+ logs as a HTML file click the 'Export' button  or right click inside the log viewer and

choose 'Export' from the context sensitive menu.

- To open a stored CIS log file, click the 'Open' button .
- To refresh the Defense+ logs, click the 'Refresh' button  or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
- To clear the Defense+ logs click the 'Clear' button .

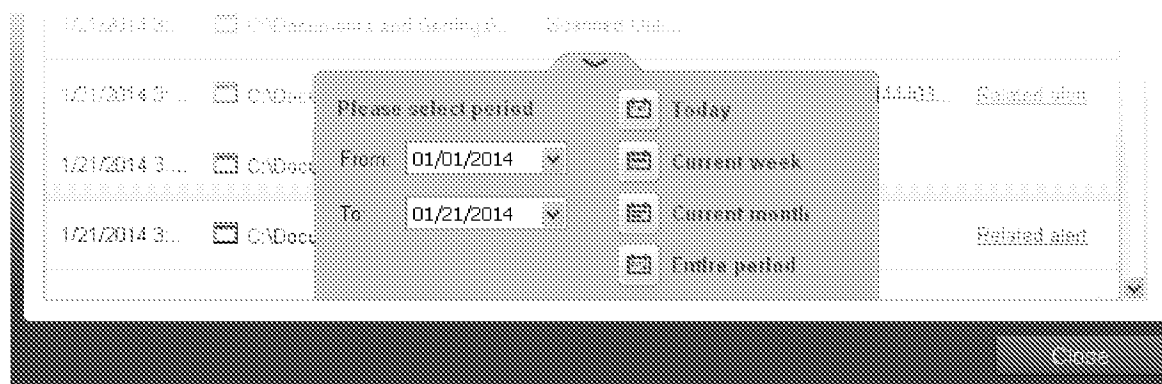
2.6.3.1. Filtering Defense+ Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- Preset Time Filters
- Advanced Filters

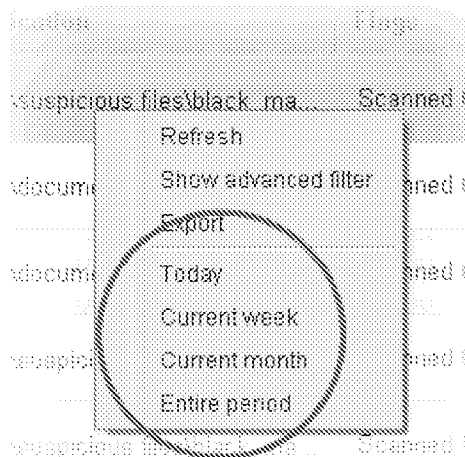
Preset Time Filters

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Internet Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



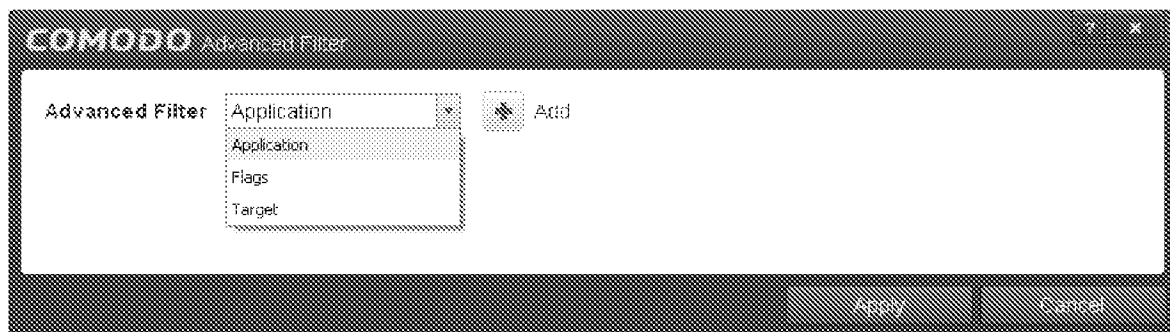
Advanced Filters

Having chosen a preset time filter from the top panel, you can further refine the displayed events according to specific filters. Following are available filters for Defense+ logs and their meanings:

- **Application** - Displays only the events propagated by a specific application
- **Flags** - Displays events according to the response (or action taken) by Defense+
- **Target** - Displays only the events that involved a specified target application

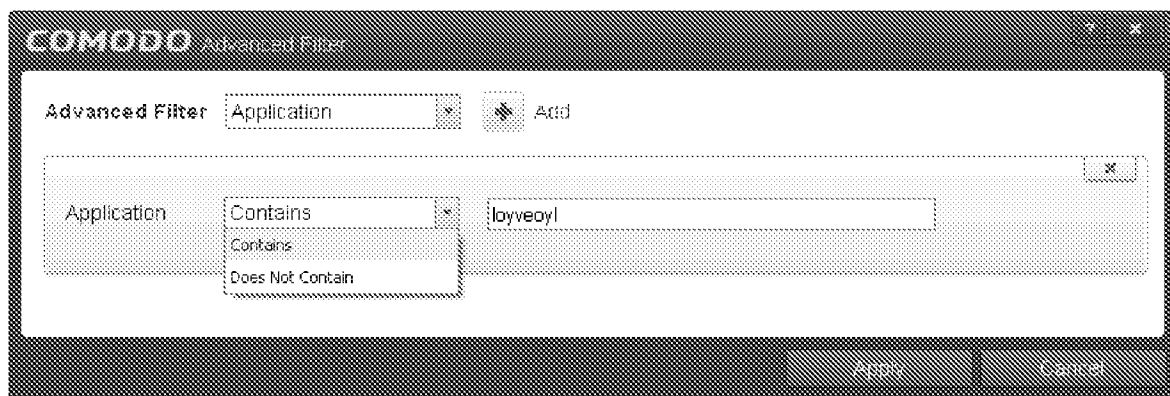
To configure Advanced Filters for Defense+ events

1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for Defense+ events will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



You have 3 categories of filter that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. Following are the options available in the 'Advanced Filter' drop-down:

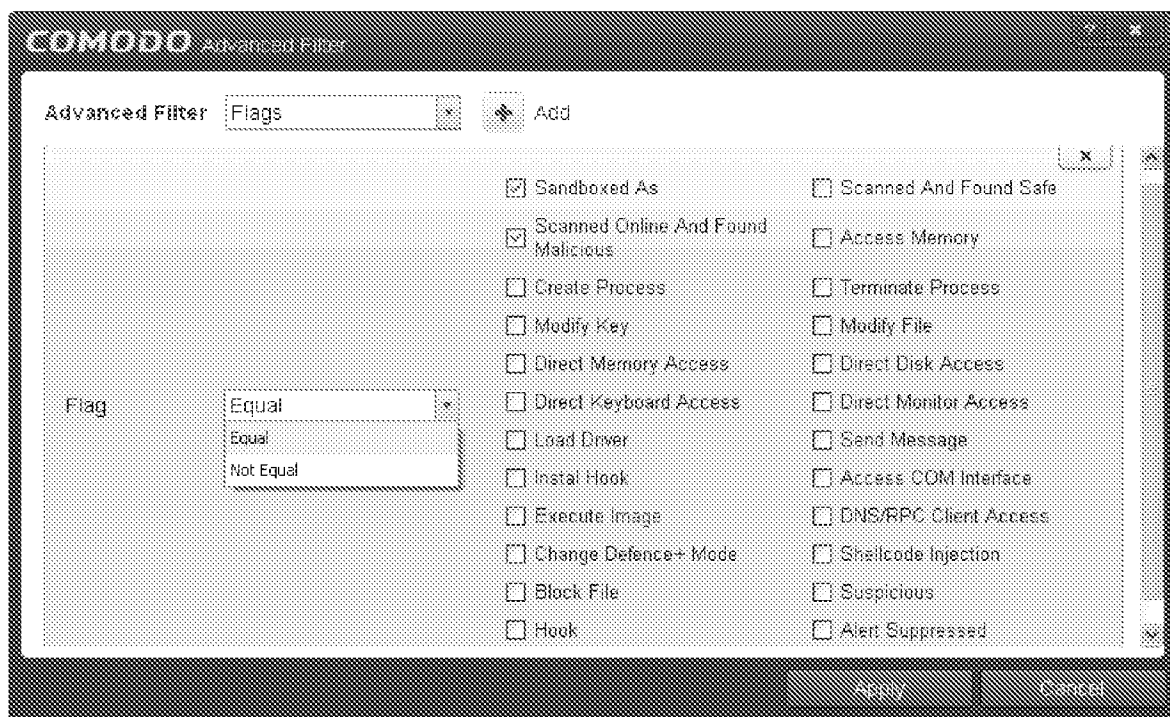
- i. **Application:** Adding the 'Application' option displays a drop-down field and text entry field.



- a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b) Enter the text or word that needs to be filtered.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'loyveoyl' in the text field, then all events containing the entry 'loyveoyl' in the 'Application' column will be displayed. If you choose 'Does Not Contain' option from the drop-down and enter the phrase 'loyveoyl' in the text field, then all events that do not have the entry 'loyveoyl' in the 'Application' column will be displayed.

- ii. **Flags:** Selecting the 'Flags' option displays a drop down menu and a set of specific filter parameters that can be selected or deselected.



- a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:

- Sandboxed As
- Scanned Online and Found Safe
- Scanned Online and Found Malicious
- Access Memory
- Create Process
- Terminate Process

- Modify Key
- Modify File
- Direct Memory Access
- Direct Disk Access
- Direct Keyboard Access
- Direct Monitor Access
- Load Driver
- Send Message
- Install Hook
- Access COM Interface
- Execute Image
- DNS/RPC Client Access
- Change Defense+ Mode
- Shellcode Injection
- Block File
- Suspicious
- Hook
- Alert Suppressed

For example, if you choose 'Equal' from the drop-down and select 'Sandboxed as' from the checkboxes, only the events of applications auto-sandboxed by Behavior Blocker will be displayed. If you choose 'Not Equal' from the drop-down field and select 'Modify Key' check box, then all events that do not have the entry 'Modify Key' in the 'Flags' column will be displayed. You can select more than one check box options from this interface, as required.

iii. **Target:** Selecting the 'Target' option displays a drop-down menu and text entry field.



- Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- Enter the text or word that needs to be filtered from the Target column.

For example, if you choose 'Contains' from the drop-down and enter the phrase 'svchost.exe' in the text field, then all events containing the entry 'svchost.exe' in the 'Target' column will be displayed. If you choose 'Does Not Contain' from the drop-down and enter the phrase 'svchost.exe' in the text field, then all events that do not have the entry 'svchost.exe' in the 'Target' column will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

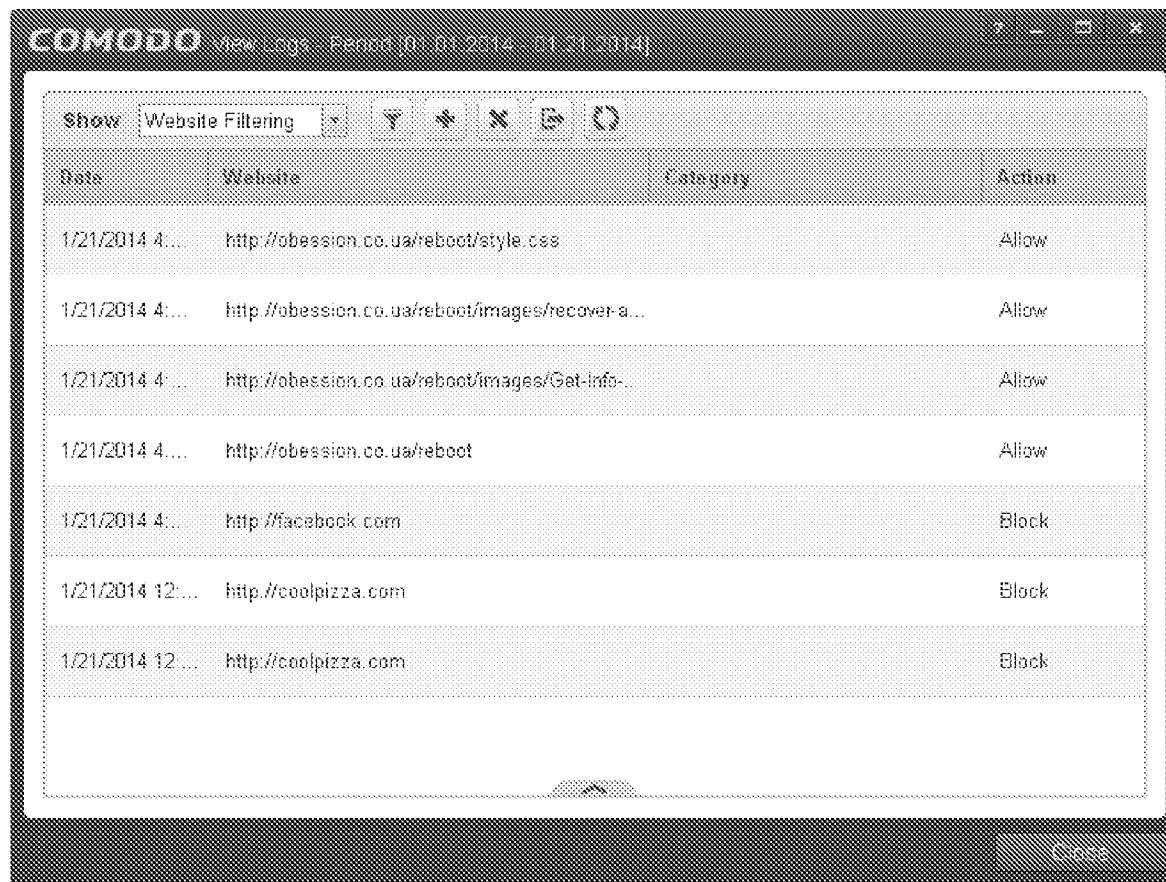
- Click 'Apply' for the filters to be applied to the Firewall log viewer. Only those Defense+ entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.6.4. 'Website Filtering' Logs

Comodo Internet Security maintains a log of Websites allowed or blocked to specific users by the 'Website Filter'.

You can configure rules to allow or block access to specific websites for particular users of your computer under Advanced Settings > Security Settings > Firewall Settings > Website Filtering. For more details on configuring the Website Filter, refer to the section Website Filtering. The Website Filtering log enables you to analyze the attempts made by the other users to access the blocked or allowed websites.

The 'Website Filtering' logs can be viewed by choosing the 'Website Filtering' from the 'Show' drop-down of the log viewer interface.



Column Descriptions

1. **Date** - Contains precise details of the date and time of the event.
 2. **Website** - Shows the url of the website that was blocked or allowed as per the rules configured in the Website Filtering interface.
 3. **Category** - Indicates the predefined category to which the website belongs.
 4. **Action** - Indicates whether the access to the website was allowed or blocked to the user.
- To export the 'Website Filtering' logs as a HTML file click the 'Export' button  or right click inside the log viewer and choose 'Export' from the context sensitive menu.
 - To open a stored CIS log file, click the 'Open' button .
 - To refresh the Alerts logs, click the 'Refresh' button  or right click inside the log viewer and choose 'Refresh' from the context sensitive menu..

- To clear the Alerts logs click the 'Clear' button .

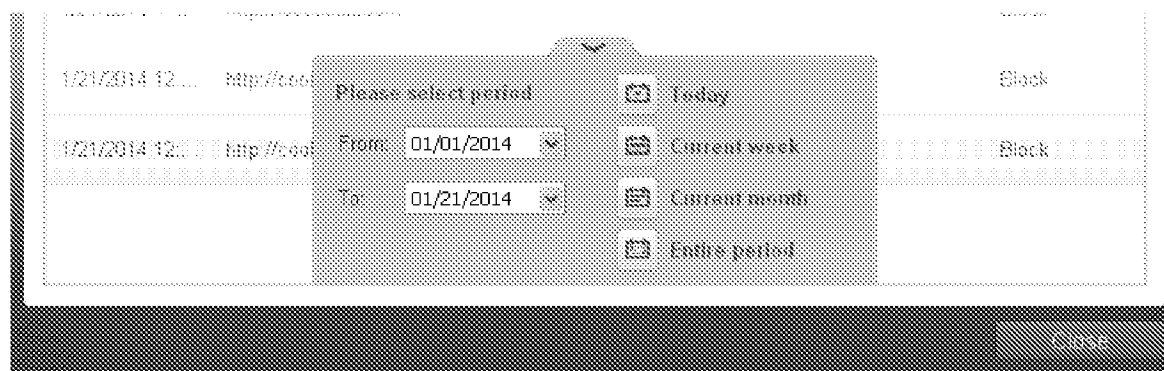
2.6.4.1. Filtering 'Website Filtering' Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- Preset Time Filters
- Advanced Filters

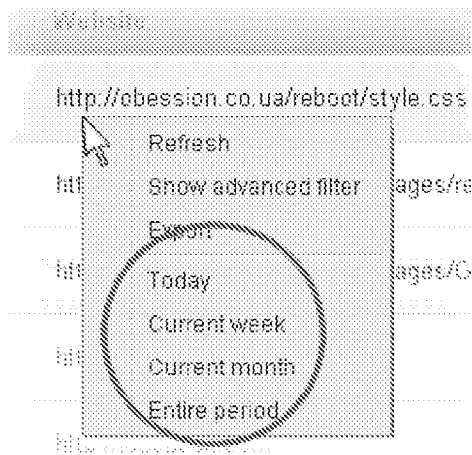
Preset Time Filters

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Internet Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



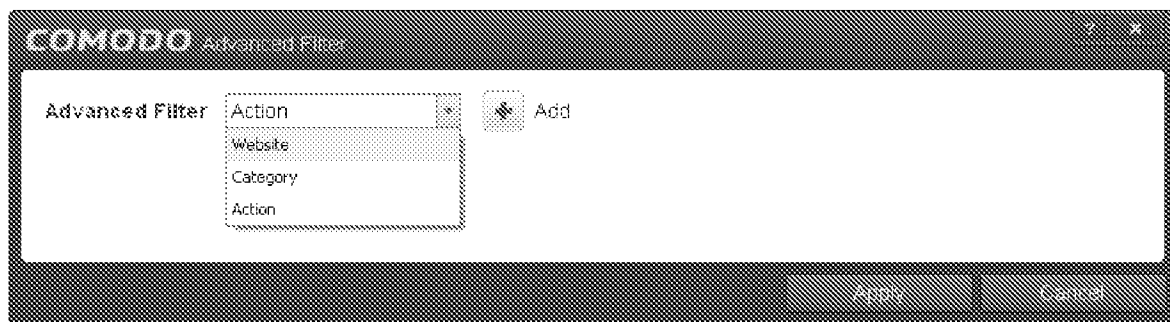
Advanced Filters

Having chosen a preset time filter from the top panel, you can further refine the displayed events according to specific filters. Following are available filters for Defense+ logs and their meanings:

- **Website** - Displays only the events that involve a specific website
- **Category** - Displays only the events that involve attempts to access the websites of the specified category
- **Action** - Displays only the events that involved the specified action

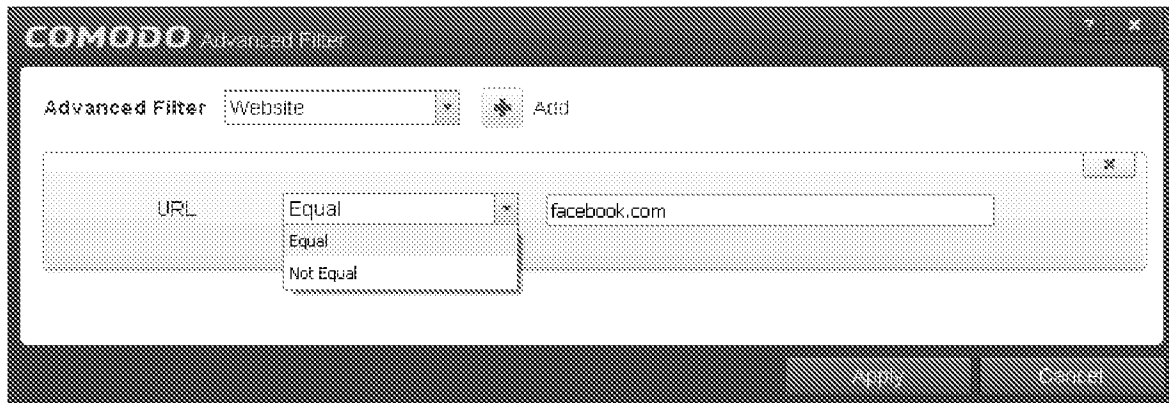
To configure Advanced Filters for Defense+ events

1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for 'Website Filtering' events will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



You have 3 categories of filter that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. Following are the options available in the 'Advanced Filter' drop-down:

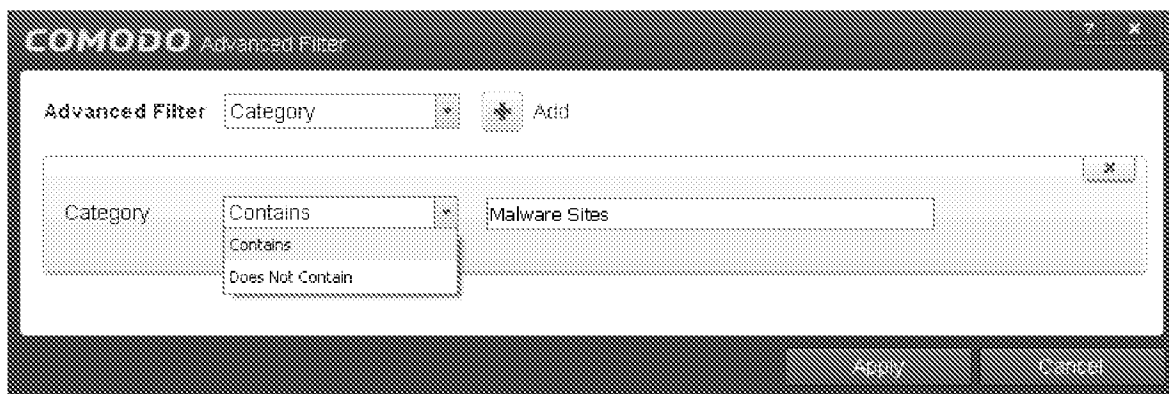
- i. **Website:** Adding the 'Website' option displays a drop-down menu and text entry field.



- a) Select 'Equal' or 'Not Equal' option from the drop-down menu.
- b) Enter the url of the website that needs to be filtered.

For example, if you choose 'Equal' option from the drop-down and enter the phrase 'facebook.com' in the text field, then all events that involve the website 'facebook.com' in the 'Website' column will be displayed. If you choose 'Not Equal' option from the drop-down and enter the phrase 'facebook.com' in the text field, then all events that do not involve 'facebook.com' will be displayed.

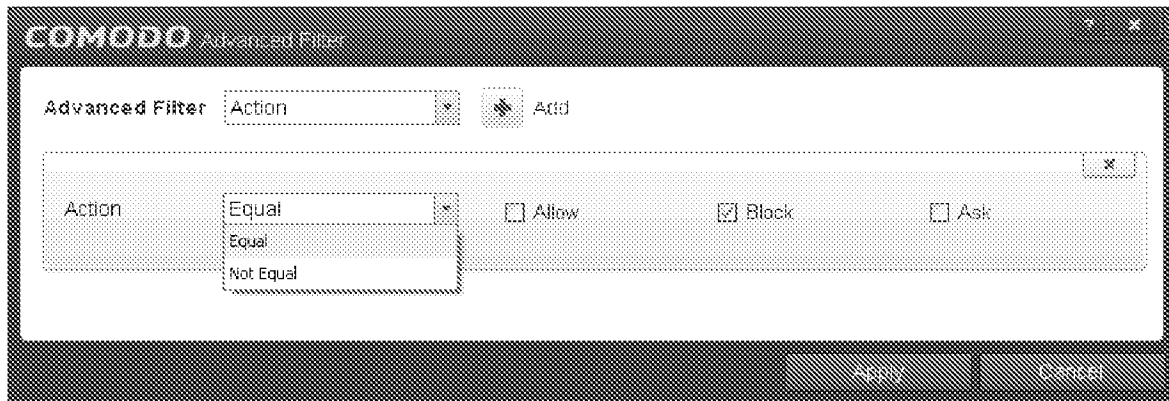
- ii. **Category:** Selecting the 'Category' option displays a drop down menu and text entry field.



- a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b) Enter the predefined category of websites that needs to be filtered from the Category column.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'Malware Sites' in the text field, then all events that involve the websites falling within the category will be displayed. If you choose 'Does Not Contain' option from the drop-down and enter the phrase 'Malware Sites' in the text field, then all events that do not involve the websites defined within the Malware Sites category will be displayed.

- iii. **Action:** Selecting the 'Action' option displays a drop-down menu and a set of specific filter parameters that can be selected or deselected.



- a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:
 - Allow
 - Block
 - Ask

For example, if you choose 'Equal' option from the drop-down and select 'Block' from the checkboxes, only the events that involve blocking the access to the websites to the users will be displayed. If you choose 'Not Equal' option from the drop-down and select 'Block' check box, all the events that do not involve blocking the websites will be displayed. You can select more than one check box options from this interface, as required.

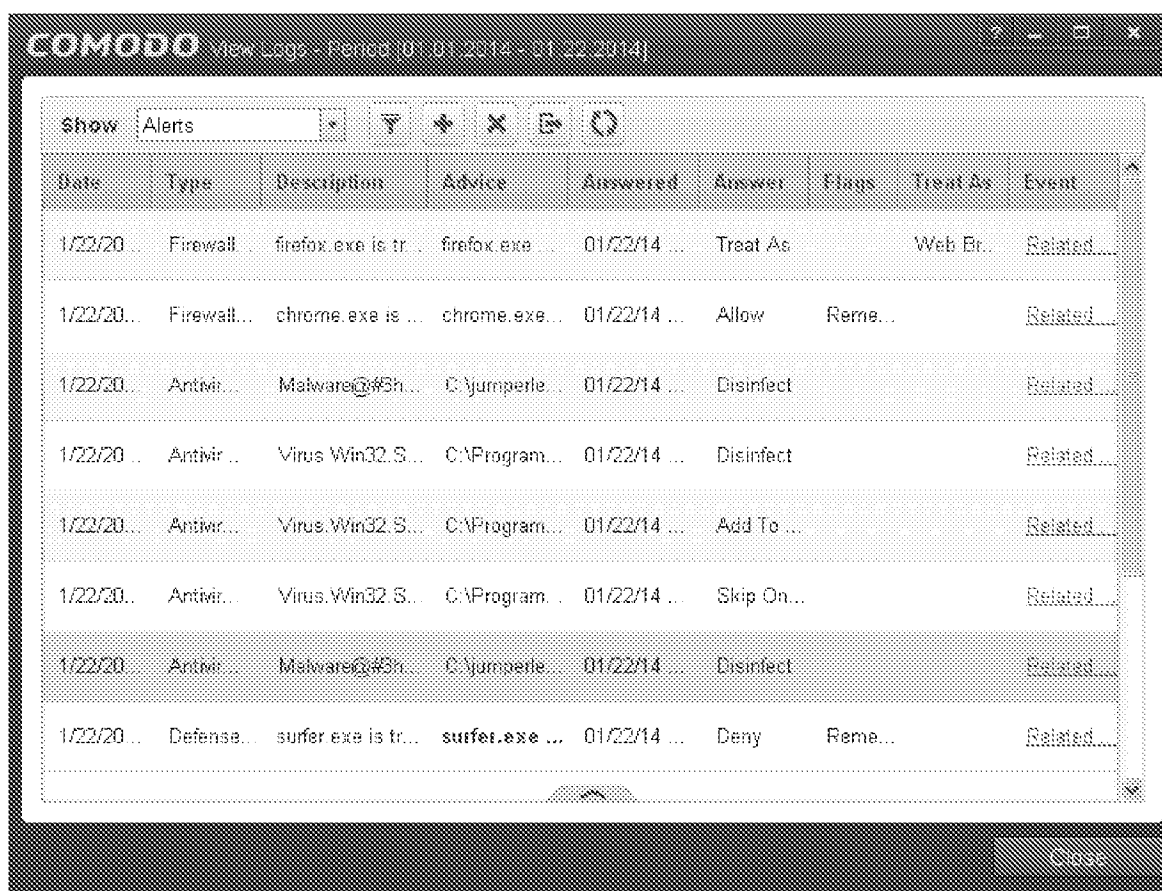
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the Website Filtering log viewer. Only those 'Website Filtering' log entries selected based on your filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.6.5. 'Alerts' Logs

CIS maintains a history of pop-up security alerts generated by its Antivirus, Firewall and Defense+ components and the actions taken against the threats discovered, depending on the response to the alerts by the user.

The Alerts logs can be viewed by selecting 'Alerts' from the 'Show' drop-down of the log viewer interface.



Column Descriptions

1. **Date** - Contains precise details of the date and time of the alert generation.
2. **Type** - Indicates the type of the alert, whether it is a, Antivirus, Firewall or Defense+ (HIPS, Behavior Blocker or Auto-Sandbox) alert.
3. **Description** - Brief description of the file or the event that triggered the alert.
4. **Advice** - Advice offered by CIS on how to respond for the alert.
5. **Answered** - Indicates whether the alert has been answered by the user and if answered, contains precise details of the date and time of response from the user.
6. **Answer** - Indicates the response given by the user.
7. **Flags** - Indicates flags set for the kinds of actions against the event triggered by the file.
8. **Treat As** - Based on the response how the file is treated, whether it is treated as a safe application, installer and so on.
9. **Event** - Clicking 'Related Event' opens the details of the event that has triggered the alert.

- To export the Alerts logs as a HTML file click the 'Export' button  or right click inside the log viewer and choose 'Export' from the context sensitive menu.

- To open a stored CIS log file, click the 'Open' button .

- To refresh the Alerts logs, click the 'Refresh' button  or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.

- To clear the Alerts logs click the 'Clear' button .

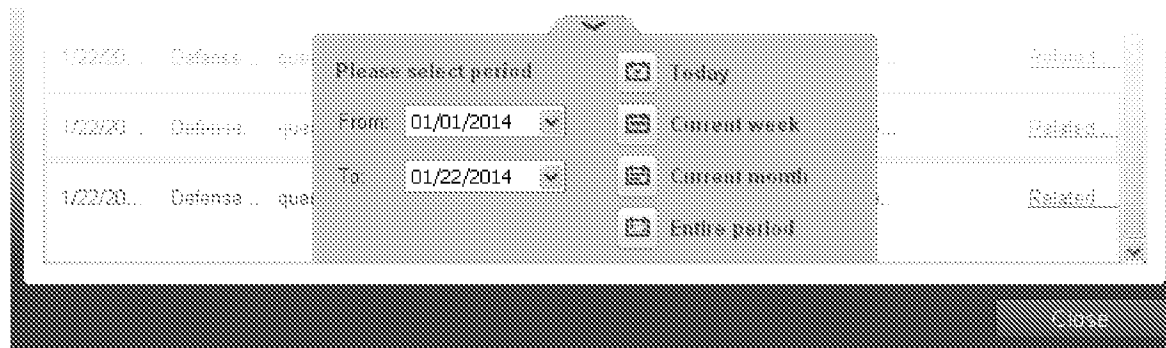
2.6.5.1. Filtering 'Alerts Displayed' Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- Preset Time Filters
- Advanced Filters

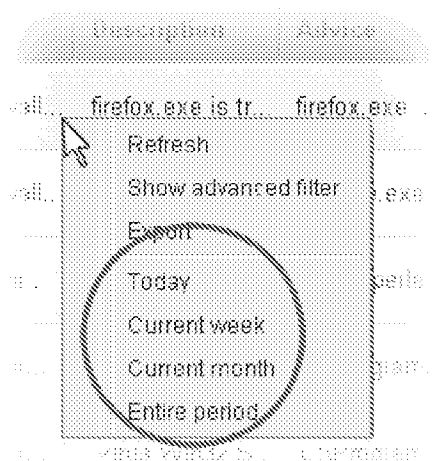
Preset Time Filters

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Internet Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



Advanced Filters

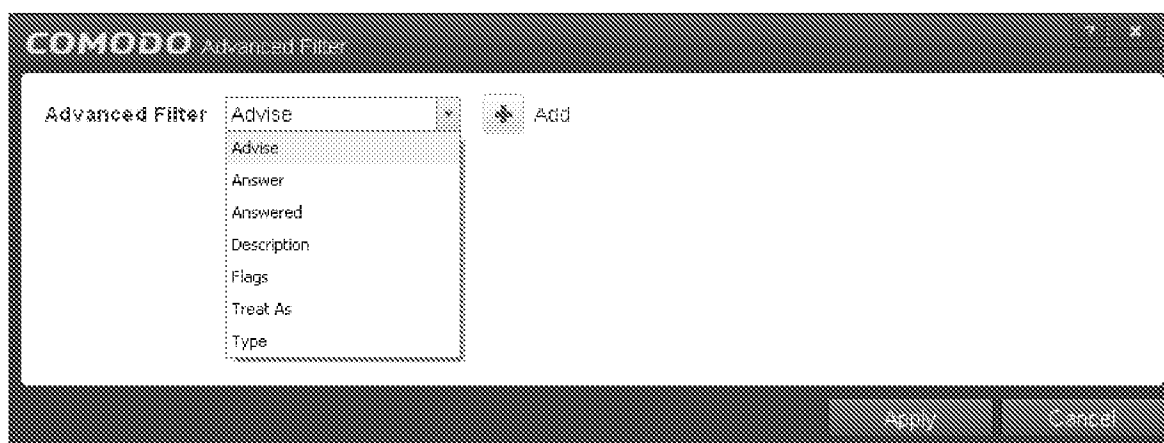
You can further refine the displayed events according to specific filters. Following are available filters for 'Alerts' logs and their meanings:

- **Advice**: Displays only the log of alerts that matches the advice entered

- **Answer:** Displays only the log of alerts that were answered by you with the selected response
- **Answered** Displays only the log of alerts that were answered on a selected date and time
- **Description:** Displays only the log of alerts that matches the description entered
- **Flags:** Displays only the log of alerts based on the selected flags set for the corresponding events
- **Treat As:** Displays only the log of alerts based on their 'Treat As' response you entered in the pop-up alert
- **Type:** Displays only the log of alerts of selected type. They can be Antivirus, Firewall or Defense+ (HIPS, Behavior Blocker or Auto-Sandbox) alerts.

To configure Advanced Filters for Alerts Displayed

1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for 'Alerts' logs will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



You have 7 categories of filters that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are the options available in the 'Add' drop down menu:

- i. **Advice:** The 'Advice' option enables you to filter the alerts based on advices given by CIS in the alert. Selecting the 'Advice' option displays a drop-down field and text entry field.

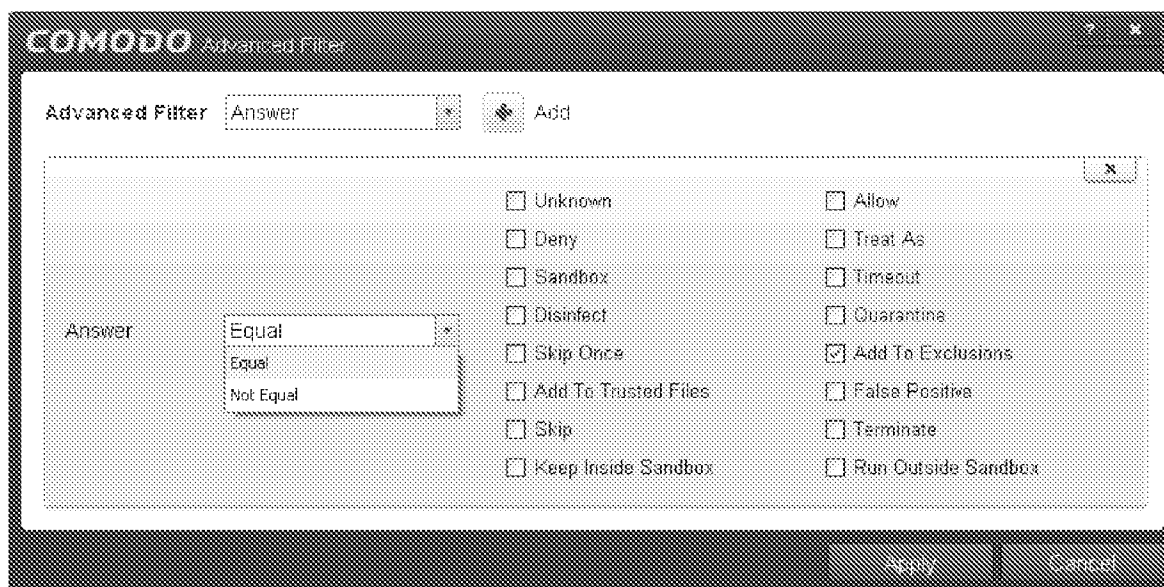


- a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b) Enter the text or word as your filter criteria.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'you can safely allow this request' in the text field, then only the entries containing 'you can safely allow this request' in the 'Advice' column will

be displayed.

- ii. **Answer:** The 'Answer' option enables you to filter the alerts based on how you answered for the alerts. Selecting the 'Answer' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

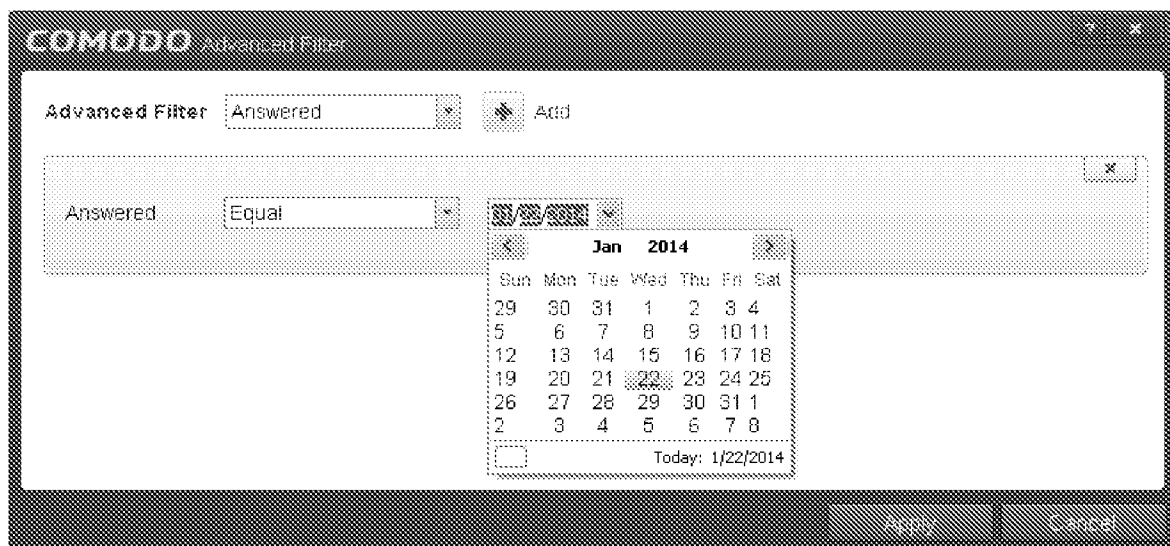


- a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:

- Unknown
- Allow
- Deny
- Treat As
- Sandbox
- Time-out
- Disinfect
- Quarantine
- Skip Once
- Add to Exclusions
- Add to Trusted Files
- False Positive
- Skip
- Terminate
- Keep inside Sandbox
- Run outside Sandbox

For example, if you choose 'Equal' from the drop-down and select 'Add to Exclusions' checkbox, only the log of Antivirus alerts for which you answered as 'Ignore' > 'Ignore and Add to Exclusions' will be displayed.

- iii. **Answered:** The Answered option enables you to filter the log based on the date you answered the alerts. Selecting the 'Answered' option displays a drop-down box and date entry field.



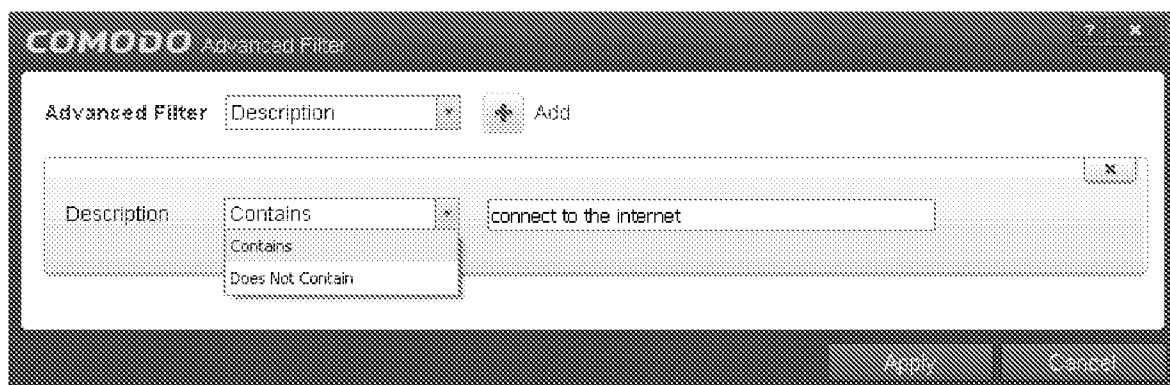
a) Select any one of the following option the drop-down box.

- Equal
- Not Equal

b) Enter the date by selecting it from the calender displayed by clicking the drop-down arrow.

For example, if you select 'Equal' from the drop-down and select '01/22/2014', only the log of alerts answered on 01/22/2014 will be displayed.

iv. **Description:** The Description option enables you to filter the log based on the description of the attempt displayed in the alert. Selecting the 'Description' option displays a drop-down field and text entry field.

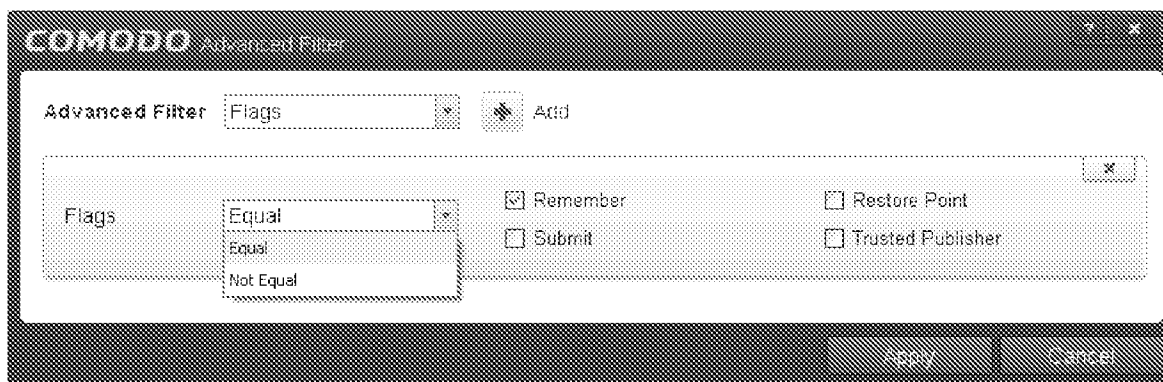


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the text or word as your filter criteria.

For example, if you select 'Contains' from the drop-down and enter 'connect to the Internet', only the log entries of Firewall alerts that contain the phrase 'connect to the Internet' in the description, will be displayed.

v. **Flags:** The 'Flags' option enables you filter the entries based on the flags set for the kinds of actions against the event triggered by the file. Selecting the 'Flags' option displays a drop down menu and a set of specific filter parameters that can be selected or deselected.

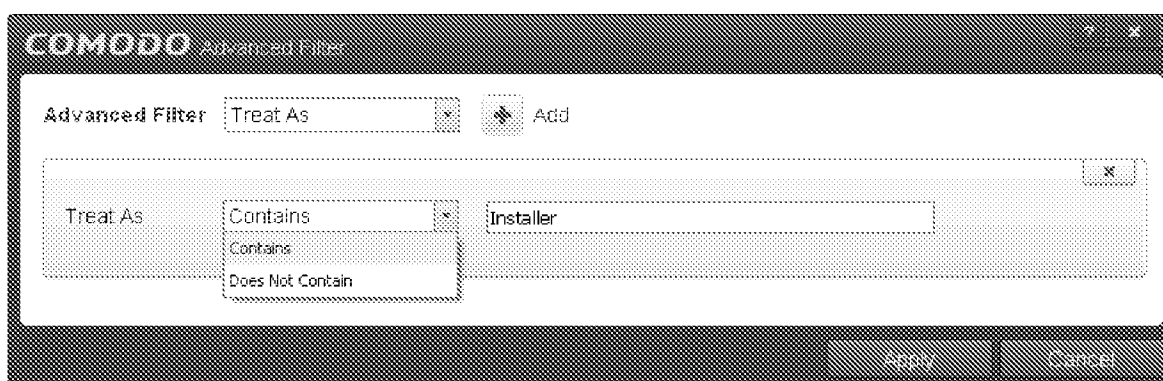


- a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:

- Remember
- Restore Point
- Submit
- Trusted Publisher

For example, if you choose 'Equal' from the drop-down and select 'Remember' from the checkbox options, only the log entries of alerts for which 'Remember my answer' option was selected will be displayed.

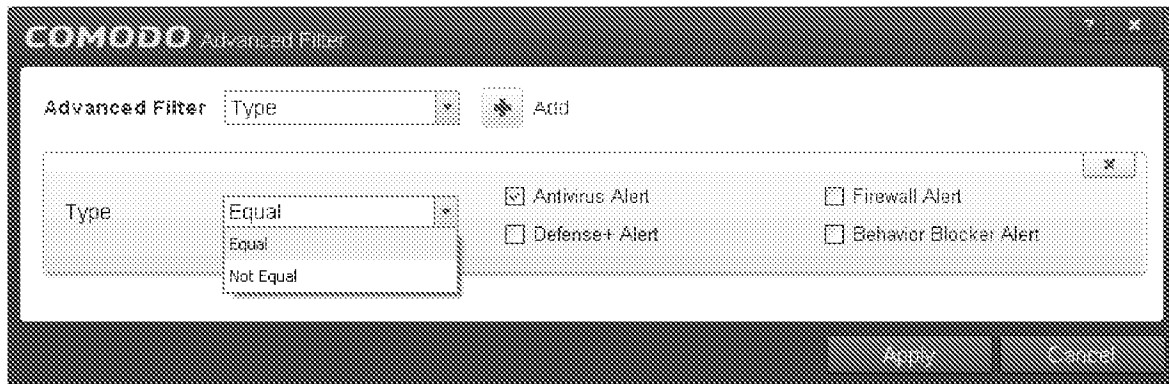
- vi. **Treat As:** The 'Treat As' enables you to filter the log entries based on their 'Treat As' response you entered in the pop-up alert. Selecting the 'Treat As' option displays a drop-down menu and text entry field.



- a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b) Enter the text or word as your filter criteria

For example, if you have chosen 'Contains' from the drop-down and entered 'Installer' in the text field, only the log entries containing the phrase 'Installer' in the 'Treat As' column will be displayed.

- vii. **Type:** The 'Type' option enables you to filter the entries based on the component of CIS that has triggered the alert. Selecting the 'Type' option displays a drop down menu and a set of specific alert types that can be selected or deselected.



- a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:

- Antivirus Alert
- Firewall Alert
- Defense+ Alert
- Behavior Blocker Alert

For example, if you select 'Equal' from the drop-down and select 'Antivirus Alert' checkbox, only the log of Antivirus alerts will be displayed.

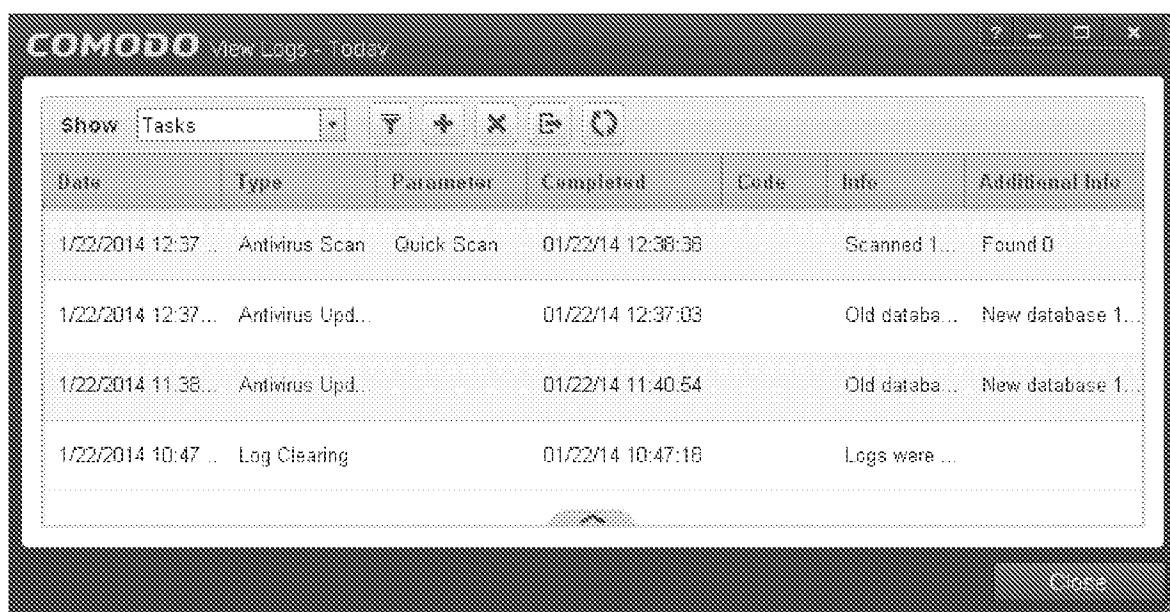
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'Alerts' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.6.6. Tasks

Comodo Internet Security records a history of all the CIS tasks like virus signature database updates, scans run and so on. The 'Tasks Launched' log window displays a list of tasks launched at various time points with their completion status and other details.

The 'Tasks' logs can be viewed by selecting 'Tasks' from the 'Show' drop-down of the log viewer interface.



Column Descriptions

1. **Date** - Contains precise details of the date and time when the task is launched.
 2. **Type** - Indicates the type of the task.
 3. **Parameter** - Indicates the parameter (like scan type) associated with the task.
 4. **Completed** - Contains precise details of the date and time of the completion of the task.
 5. **Code** - Indicates the code of the task as assigned by CIS.
 6. **Info & Additional Info** - Provides additional information of the task.
- To export the Tasks logs as a HTML file click the 'Export' button  or right click inside the log viewer and choose 'Export' from the context sensitive menu.
 - To open a stored CIS log file, click the 'Open' button .
 - To refresh the Tasks logs, click the 'Refresh' button  or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
 - To clear the Tasks logs click the 'Clear' button .

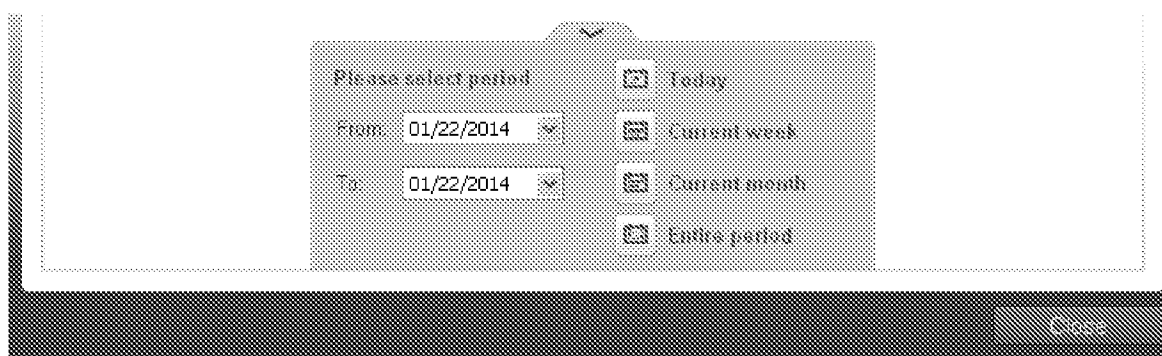
2.6.6.1. Filtering 'Tasks Launched' Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- Preset Time Filters
- Advanced Filters

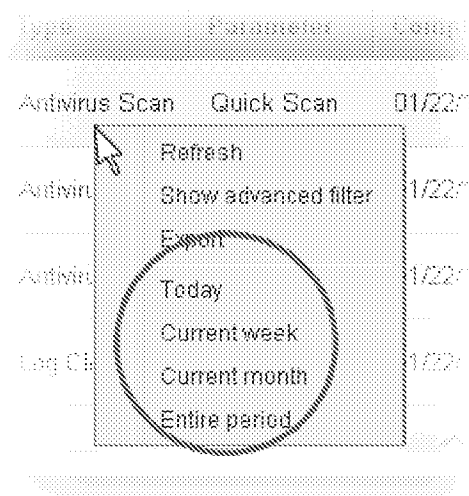
Preset Time Filters

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



- **Today** - Displays all logged tasks for today.
- **Current Week** - Displays all logged tasks during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged tasks during the month that holds the current date.
- **Entire Period** - Displays every task logged since Comodo Internet Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



Advanced Filters

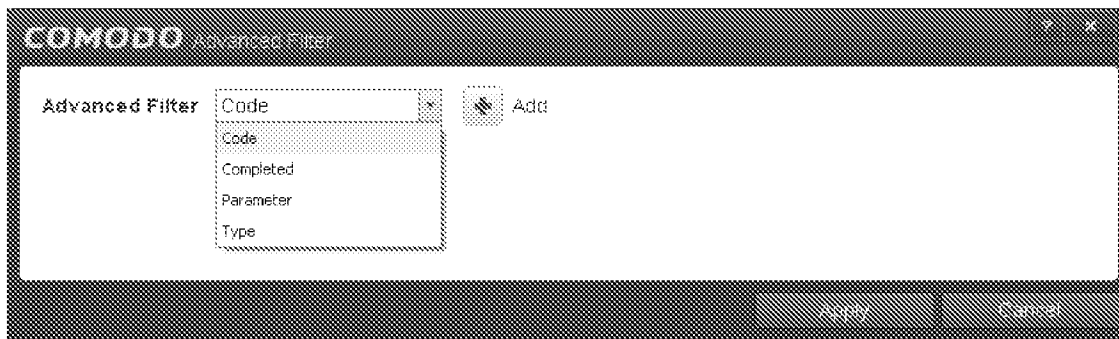
You can further refine the displayed events according to specific filters. Following are available filters for 'Tasks' logs and their meanings:

- **Code** - Displays the tasks based on the entered code value
- **Completed** - Displays the tasks completed on entered date.
- **Parameter** - Displays only the tasks launched that include the selected parameter, like scan profile or the locations scanned during custom scans.
- **Type** - Displays only the selected type of tasks launched. They can be a AV Update, AV Scan, Clearing logs and Guarantee Activation.

To configure Advanced Filters for 'Tasks' logs

1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for Tasks log viewer will open.

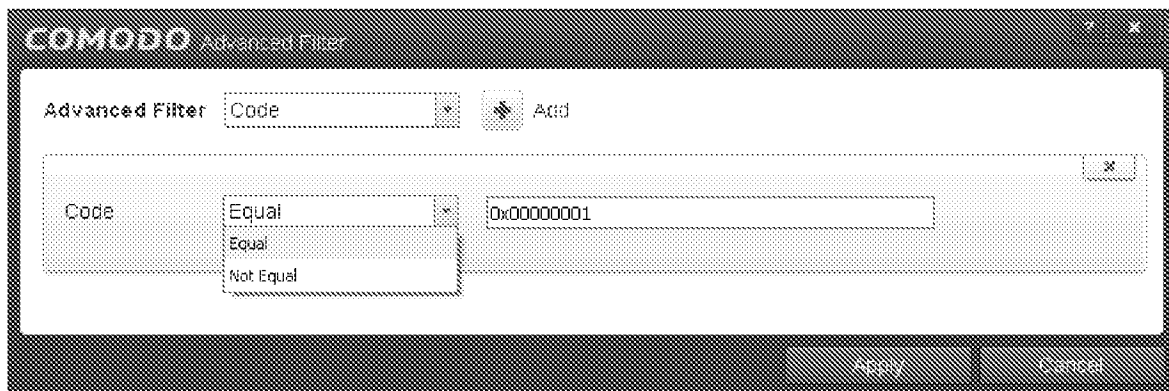
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



You can choose the category of filter from a drop down box. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided.

Following are the options available in the 'Advanced Filter' drop down menu:

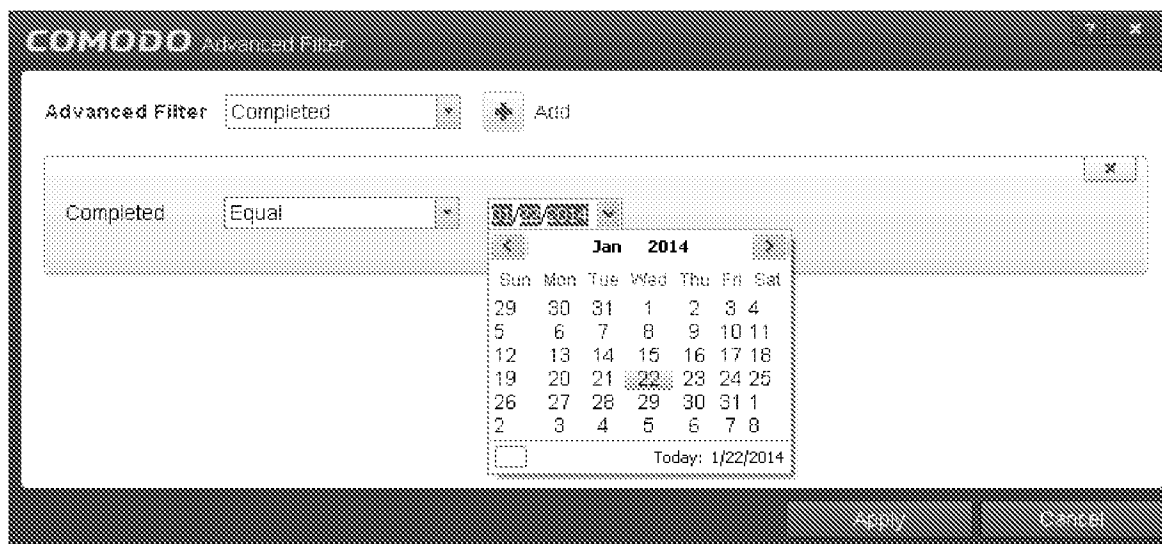
- i. **Code:** The Code option enables you to filter the tasks based on their code value. Selecting the 'Code' option displays a drop-down field and text entry field.



- a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b) Enter the code or a part of it as your filter criteria in the text field.

For example if you have chosen 'Equal' from the drop-down and entered '0x00000001' in the text field, then only the log entries with the value 0x00000001 in the code column will be displayed.

- ii. **Completed:** The 'Completed' option enables you to filter the log entries based on the completion dates of the Tasks. Selecting the 'Completed' option displays a drop-down box and date entry field.



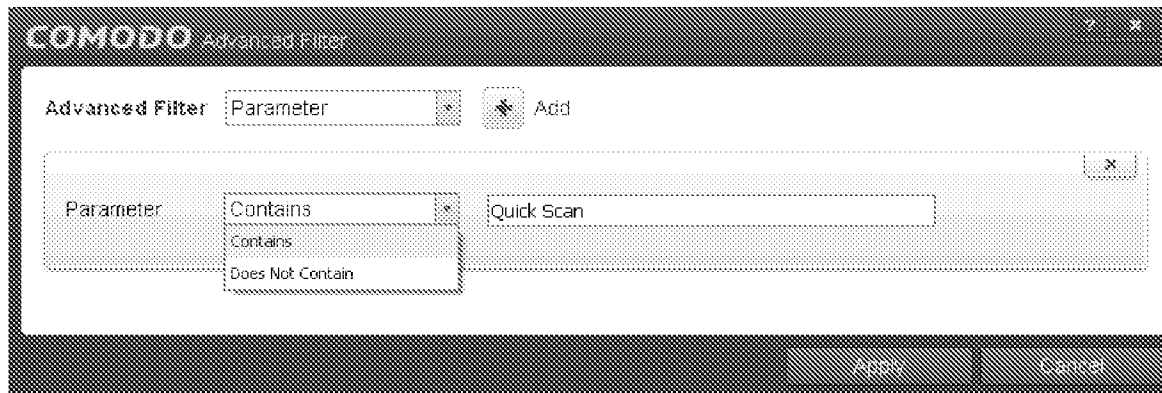
a) Select any one of the following option the drop-down box.

- Equal
- Not Equal

b) Enter the date by selecting it from the calender displayed by clicking the drop-down arrow.

For example, if you select 'Equal' from the drop-down and select '01/22/2014' , only the log of Tasks completed on 01/22/2014 will be displayed.

iii. **Parameter:** The Parameter option enables you to filter the entries based on the parameters like scan locations, associated with the Task. Selecting the 'Parameter' option displays a drop-down field and text entry field.

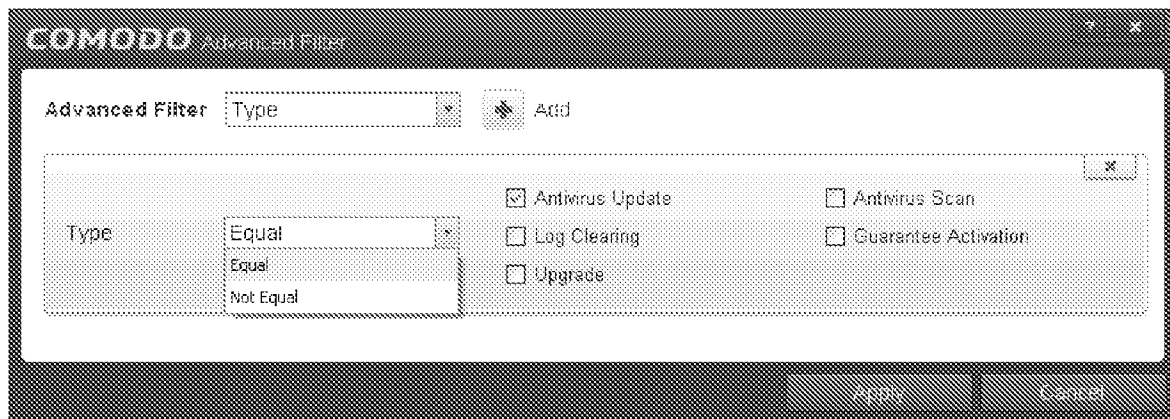


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the text or word as your filter criteria.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'Quick Scan' in the text field, then only the entries of Antivirus Scan Tasks with the scan parameter 'Quick Scan' will be displayed.

iv. **Type:** The 'Type' option enables you to filter the entries based on the type of Tasks launched. Selecting the 'Type' option displays a drop down menu and a set of specific task types that can be selected or deselected.



- a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:
 - Antivirus update
 - Antivirus Scan
 - Clearing Logs
 - Activation of guarantee
 - Version upgrade

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the Tasks log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.6.7. Configuration Changes

CIS keeps track of all the changes made to its configuration since its installation. The 'Configuration Changes' log viewer displays a list of changes to various options and other configuration changes made to the application.

The 'Configuration Changes' logs can be viewed by selecting 'Configuration Changes' from the 'Show' drop-down of the log viewer interface.

- To export the Configuration Changes logs as a HTML file click the 'Export' button  or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the 'Open' button .
- To refresh the Configuration Changes logs, click the 'Refresh' button  or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
- To clear the Configuration Changes logs click the 'Clear' button .

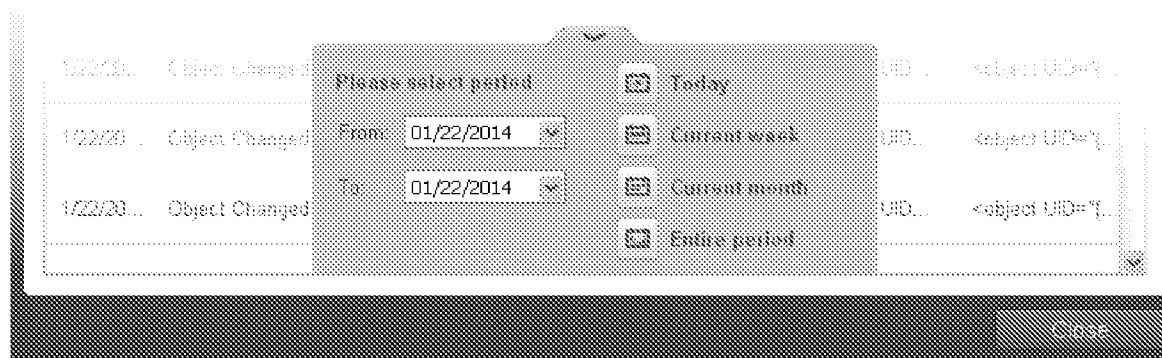
2.6.7.1. Filtering 'Configuration Changes' Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- Preset Time Filters
- Advanced Filters

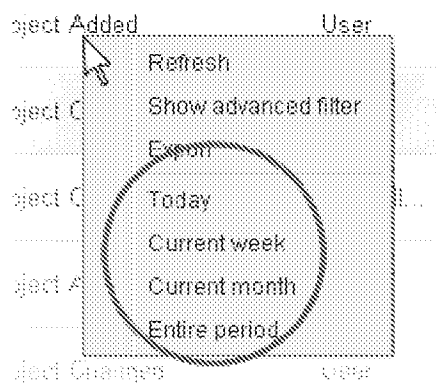
Preset Time Filters

Clicking on the handle at the bottom enables you to filter the log entries for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Internet Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



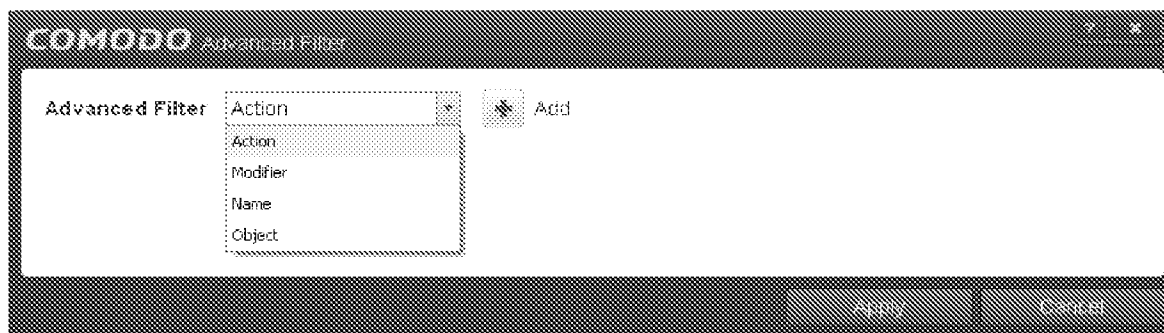
Advanced Filters

You can further refine the displayed events according to specific filters. Following are available filters for 'Configuration Changes' logs and their meanings:

- **Action:** Displays only the selected type of configuration change(s) like change in options, addition of objects, strings and so on.
- **Modifier:** Displays only the configuration changes effected by the selected entity like the user, response to Antivirus, Firewall or Defense+ Alerts and so on.
- **Name:** Displays only the configuration change with the name entered as search criteria.
- **Object:** Displays only the configuration changes on addition or removal of selected objects

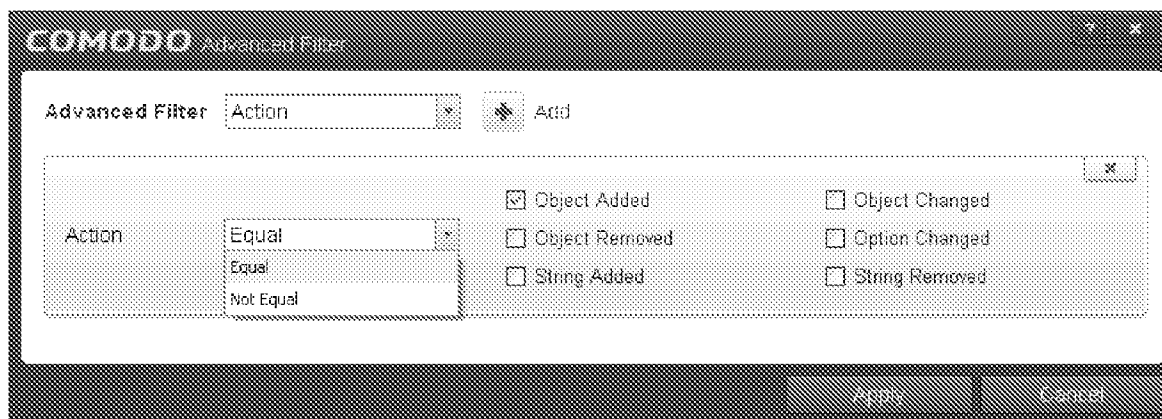
To configure Advanced Filters for Configuration Changes Logs

1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for 'Configuration Changes' logs will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



You can choose the category of filter from the 'Advanced Filter' drop-down. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. Following are the options available in the 'Add' drop down menu:

- i. **Action:** The 'Action' option allows you to filter the log entries based on the actions executed like change in options, addition of objects, strings and so on. Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

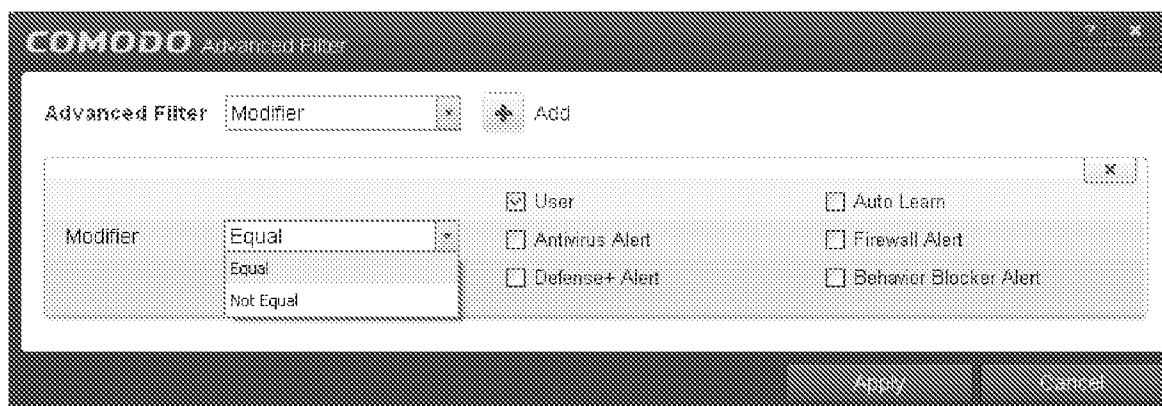


- a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b) Now select the checkboxes of the specific filter parameters to refine your search. The parameters available are:

- Object Added
- Object Changed
- Object Removed
- Option Changed
- String Added
- String Removed

For example, if you choose Equal in the drop-down and select 'Object Added' checkbox, then, only the log entries with the value 'Object Added' in the 'Action' column will be displayed.

- ii. **Modifier:** The 'Modifier' option allows you to filter the log entries based on the entity that is responsible for the configuration change. It can be the user or the response given to an alert. Selecting the 'Modifier' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



- a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b) Now select the checkboxes of the specific entities that has effected the change, to refine your search. The parameters available are:

- User
- Auto Learn
- Antivirus Alert
- Firewall Alert
- Defense+ Alert
- Behavior Blocker Alert

For example, if you have chosen Equal in the drop-down and selected 'Antivirus Alert' checkbox, then, only the log

entries related to the configuration changes effected by responses to Antivirus Alerts will be displayed.

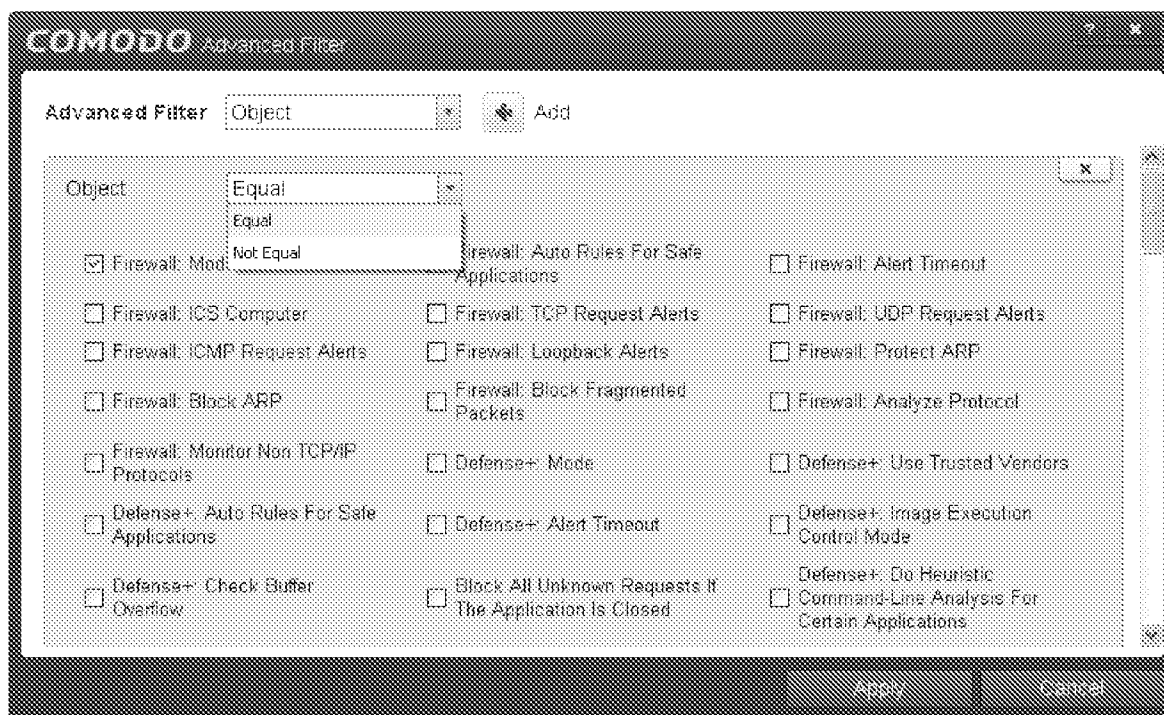
- iii. **Name:** The 'Name' option allows you to filter the log entries by entering the name of the parameter changed. Selecting the 'Name' option displays a drop-down field and text entry field.



- a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b) Enter the name of the change, partly or fully as filter criteria in the text box.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'surfer.exe' in the text field, then only the log entries containing the surfer.exe in the name column will be displayed.

- iv. **Object:** The 'Object' option enables you to filter the log entries related to the objects modified during the configuration change. Selecting the 'Object' option displays a drop down menu and the objects of CIS configuration, that can be selected or deselected.



- a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific objects as filter parameters to refine your search. Scroll down the window to see all the parameters options.

For example, if you have chosen 'Equal' from the drop-down and selected 'Firewall: Mode' checkbox, only the log entries related to the change of Firewall mode will be displayed.

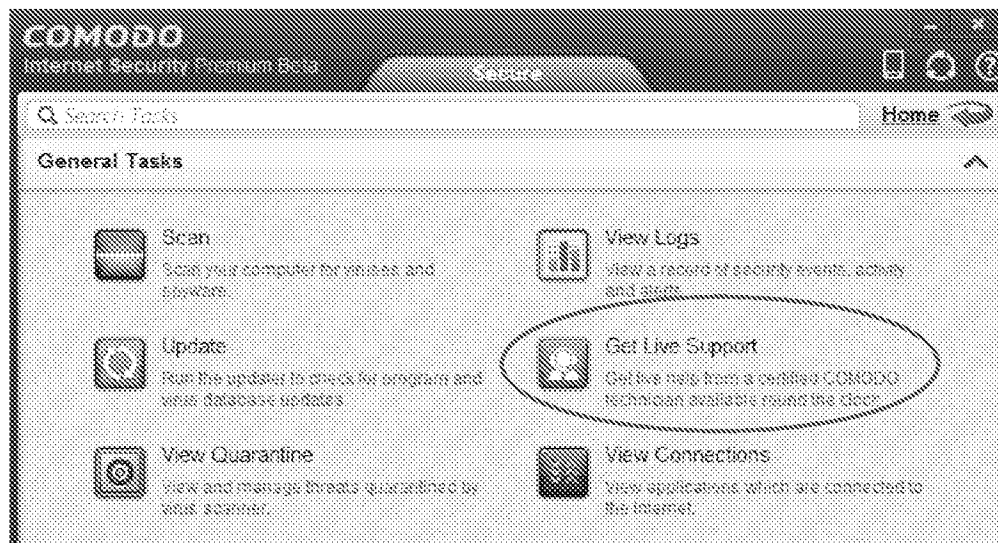
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and

click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the Configuration Changes log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.7. Get Live Support

Opens the GeekBuddy instant-chat client and connects you to a Comodo support technician.



GeekBuddy technicians can help solve most computer issues that you are experiencing. Do you need help to get rid of a particularly nasty virus? Has your computer slowed down to a crawl for no apparent reason? Are you having trouble setting up that wireless router you just bought? GeekBuddy techs can offer you expert guidance and, with your permission, can even remote-desktop into your computer and fix your problems while you sit back and watch. For more details about this service, please refer to Comodo GeekBuddy.

2.8. View Active Internet Connections

The 'View Connections' interface displays an at-a-glance summary of all currently active Internet connections on a per-application basis. You can view all the applications that are connected; all the individual connections that each application is responsible for; the direction of the traffic; the source IP and port and the destination IP and port. You can also see the total amount of traffic that has passed in and out of your system over each connection.

This list is updated in real time whenever an application creates a new connection or drops an existing connection. The 'View Connections' is an extremely useful aid when testing firewall configuration; troubleshooting new firewall policies and rules; monitoring the connection activity of individual applications and your system as a whole and for terminating any unwanted connections.

The 'View active Connections' interface can be accessed by clicking 'View Connections' from the 'General Tasks' interface. Alternatively, this screen can be accessed by clicking the number above Inbound or Outbound in the Advanced View of the Home screen in the Firewall pane.



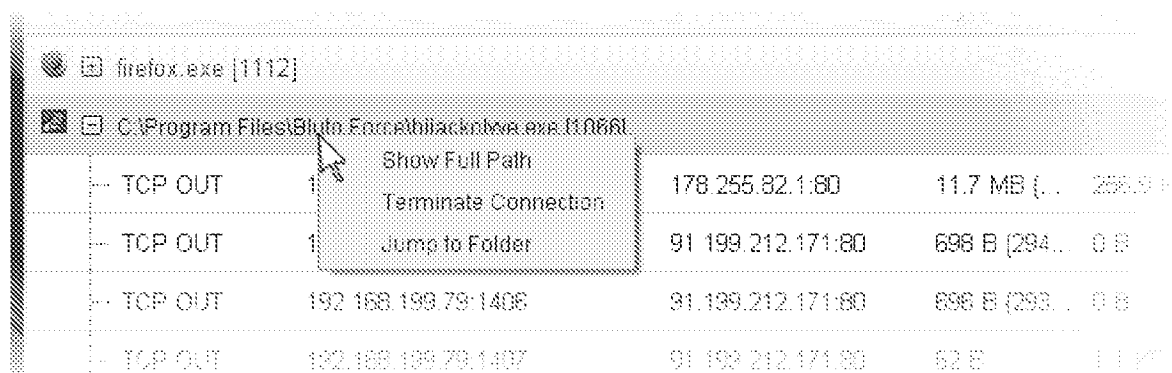
The 'View Connections' interface displays list of all the currently active Internet connections by initiated by various applications as a Tree structure.

Column Descriptions

- **Protocol** - Shows the application that is making the connection, the protocol it is using and the direction of the traffic. Each application may have more than one connection at any time. Clicking + at the left of the application name expands the list of connections made by it.
- **Source (IP : Port)** - The source IP Address and source port that the application is connecting through. If the application is waiting for communication and the port is open, it is described as 'Listening'.
- **Destination (IP : Port)** - The destination IP Address and destination port address that the application is connecting to. This is blank if the 'Source' column is 'Listening'.
- **Bytes In** - Represents the total bytes of incoming data since this connection was first allowed.
- **Bytes Out** - Represents the total bytes of outgoing data since this connection was first allowed.

Context Sensitive Menu

- Right click on an item in the list to see the context sensitive menu.



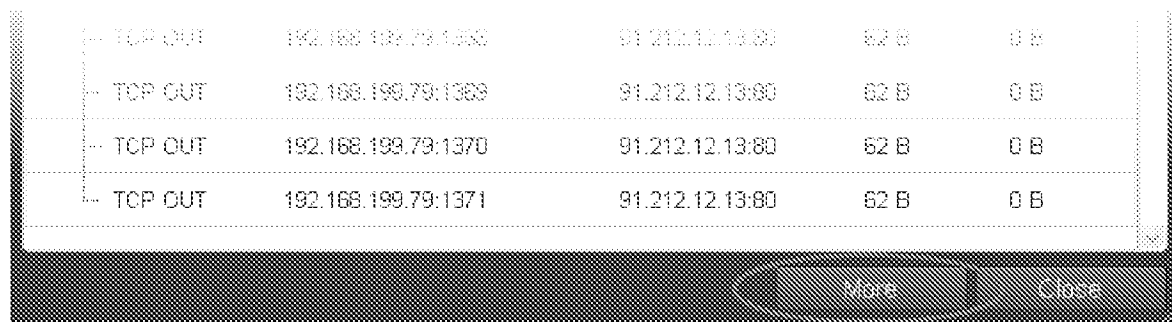
- If you wish to view the full path of the application, right click on the application name and select 'Show Full Path'.
- If you wish to terminate a connection belonging to an application, right click on the specific connection and click 'Terminate Connection'.
- If you wish to open the folder containing the executable file of the application, click 'Jump to Folder'.

Identify and Kill Unsafe Network Connections

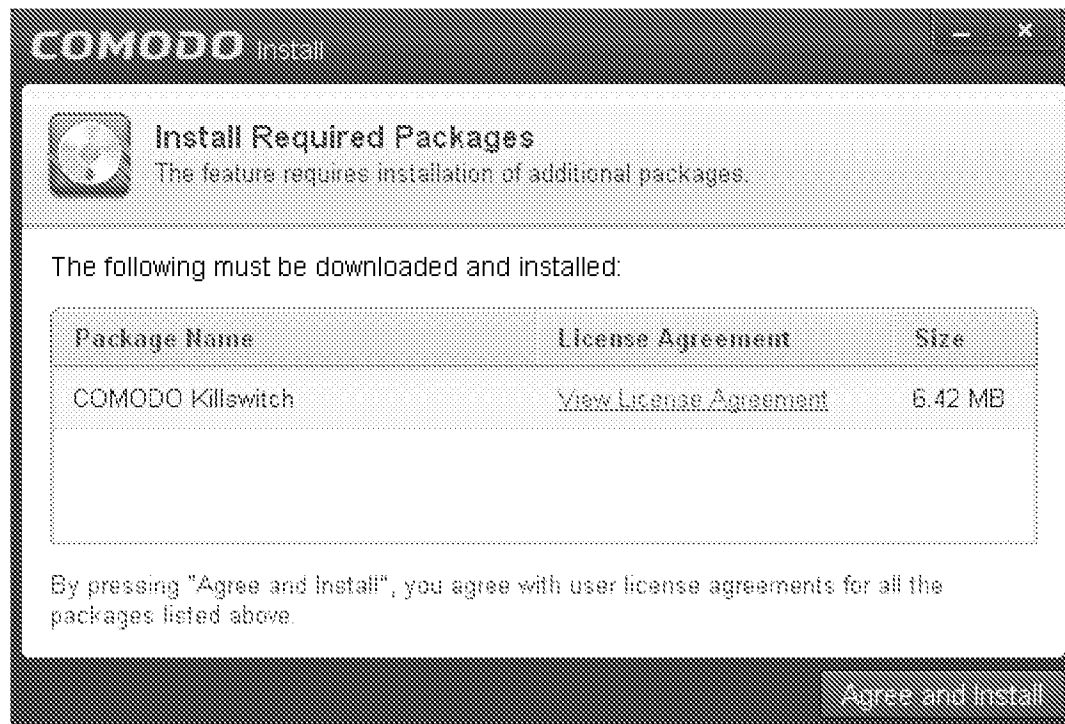
KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate unsafe processes and network connections that are running on their computer. Apart from offering unparalleled insight and control over computer processes and connections, KillSwitch provides you with yet another powerful layer of protection for Windows computers.

Comodo KillSwitch can show ALL running processes in granular detail— exposing even those that were invisible or very deeply hidden. You can simultaneously shut down every unsafe process with a single click and can even trace the process back to the parent malware.

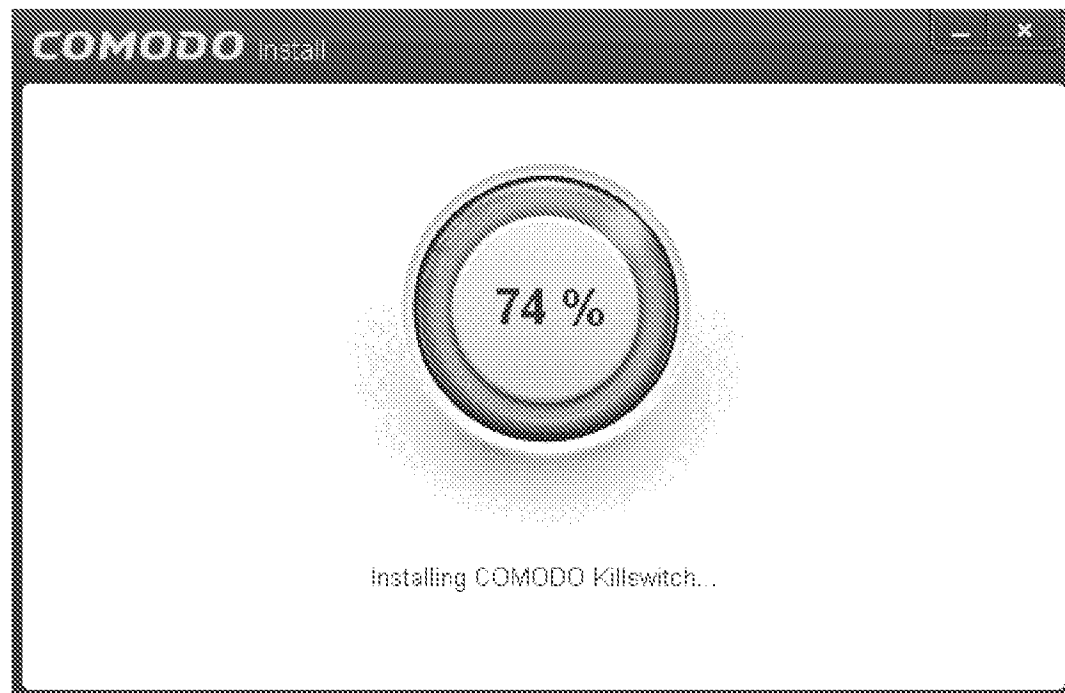
Comodo KillSwitch can be directly accessed from the 'View Connections' by clicking the 'More' button.



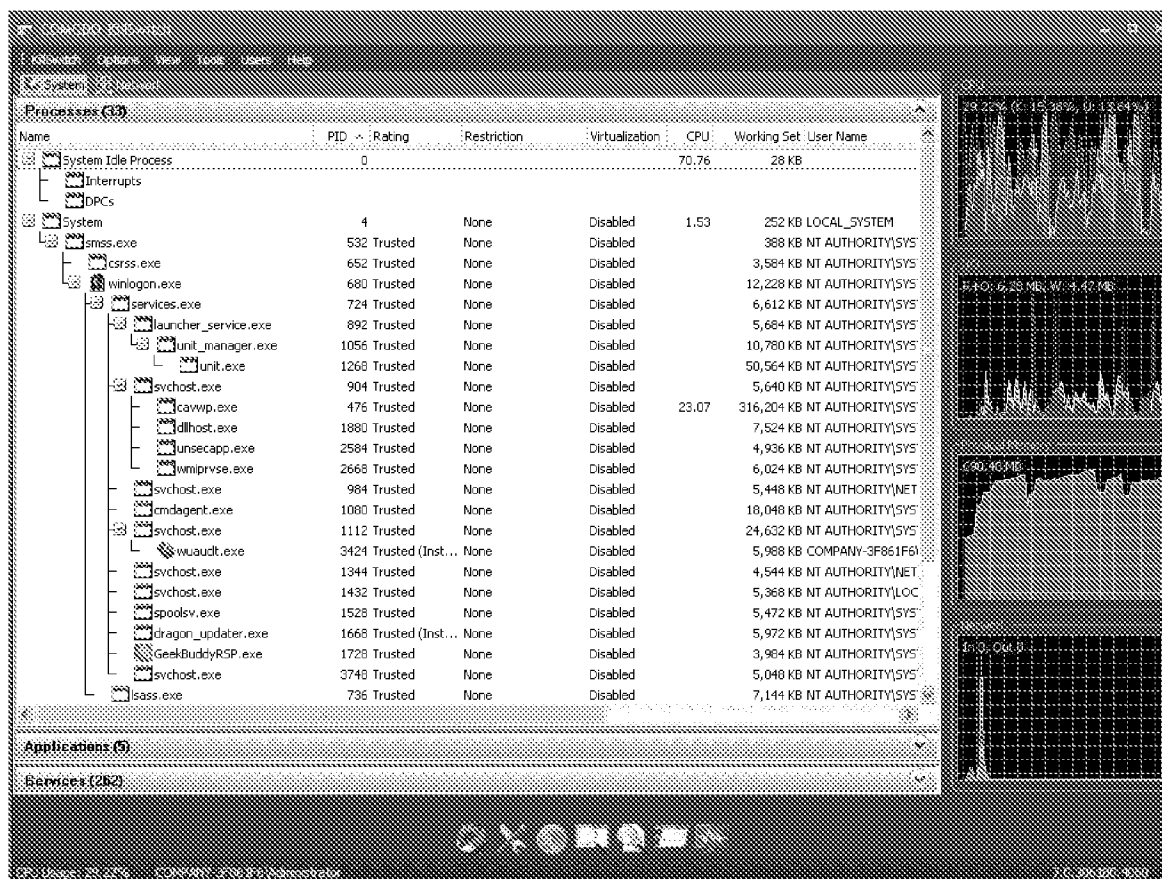
If Comodo KillSwitch is already installed in your computer, clicking 'More' will open the application. If not, CIS will download and install Comodo Killswitch. Once installed, clicking this button in future will open the Killswitch interface.



- Read the license agreement by clicking 'View License Agreement' and click 'Agree and Install'. CIS will download and install the application.



On completion of installation, the Comodo KillSwitch main interface will be opened. Clicking the Network tab will display the the Network Connections and Network Utilization panes.



- Details of how to use KillSwitch to view granular details on current network connections and terminate unsafe connections can be found at <http://help.comodo.com/topic-119-1-328-3577-Viewing-and-Handling-Network-Connections-and-Usage.html>.
- The complete user guide for Comodo KillSwitch is available at <http://help.comodo.com/topic-119-1-328-3518-Introduction-to-KillSwitch.html>

2.9. View Active Process List

The Active Process List interface displays all currently active processes initiated by applications that are currently running in the sandbox environment. By tracing an application's parent process, CIS can detect whether a non-trusted application is attempting to spawn an already trusted application and thus deny access rights for that trusted application. This system provides the very highest protection against Trojans, malware and rootkits that try to use trusted software to launch an attack. By default, the list displays the processes of sandboxed applications only, but can be made to display all the processes from the right-click options.

The processes of sandboxed applications include:

- Auto-Sandbox - Unrecognized applications are run inside the auto sandbox with access restriction as selected in the 'Auto-sandbox unknown applications as' drop down in Behavior Blocker.
- Run Virtual - Applications that are selected and run in Sandbox. Refer to 'Run an Application in the Sandbox' for more details.
- Applications that are run inside the sandbox using the context sensitive menu - Click here for more details.
- Running browsers inside the sandbox from the Widget - Click here for more details.
- Drag-and-drop applications on to CIS Home Screen - Click here for more details.

- Programs that are added manually - Refer to the section 'Configure the Sandbox' for more details.

To view Active Process list

- Click the first box in the status pane (third row) in the CIS Widget.

Note: The Status Pane is not displayed by default in the widget. To enable the Status Pane, right click on the CIS tray icon and select 'Show Status Pane' from the options.



- Alternatively, the screen can be accessed by clicking the number beside 'Sandboxed Apps' in the Advanced View of the Home screen in the Defense+ and Sandbox pane.

The Active Processes List (Sandboxed Only) screen will be displayed by default.

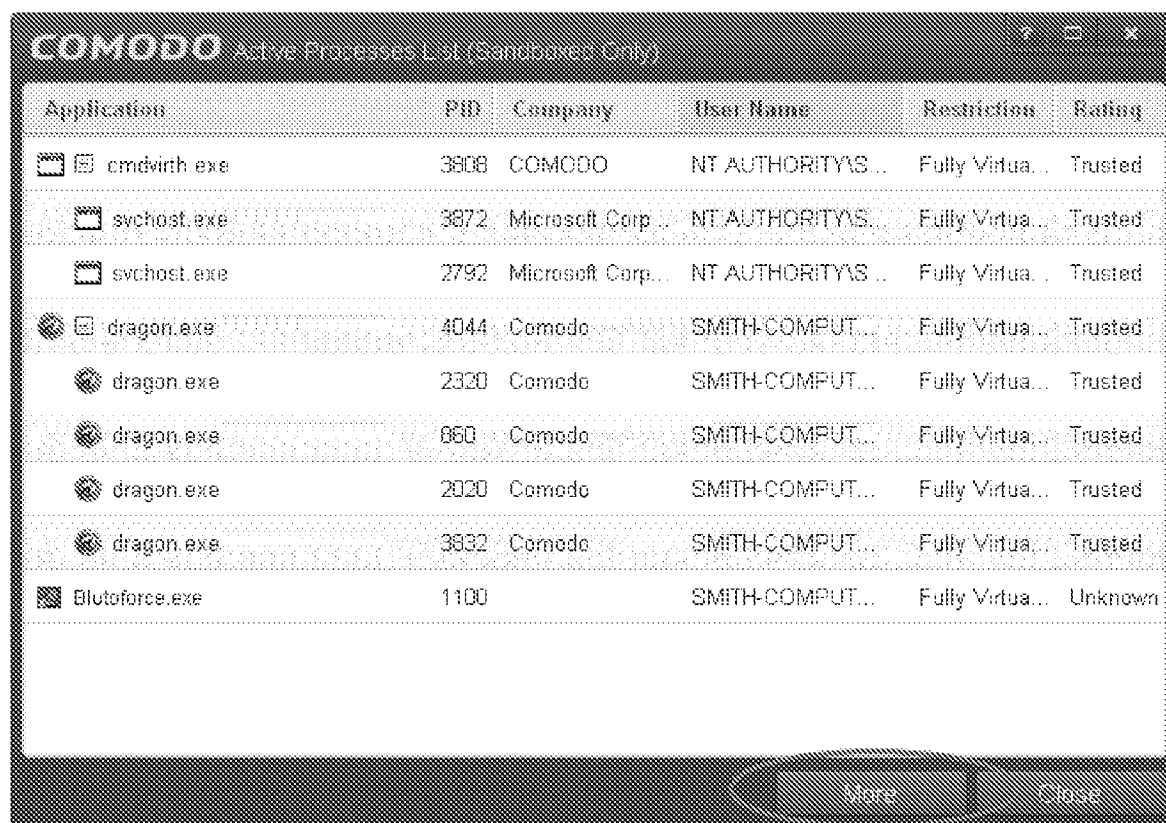
Column Descriptions

- Application - Displays the names of applications that are currently running.
- PID - Process Identification Number.
- Company - Displays the name of the software developer.
- User Name - The name of the user that started the process.
- Restriction - Displays the level of sandbox setting selected for the program.
- Rating - Displays the rating of the application whether trusted or unknown.

Right-click on any process to:

- Show full path: Displays the location of the the executable in addition to it's name.
- Show Sandboxed Only: Displays the details of the sandboxed programs only. Disable this option to view all the current active process list.
- Add to Trusted Files: The selected unknown program is added to Trusted Files list.
- Online Lookup: The selected program is compared with the Comodo database of programs and results declared whether it is safe or not.
- Submit: The selected application will be sent to Comodo for analysis.
- Jump to Folder: The folder containing the executable file of the application will open.
- Show Activities: Opens the Process Activities List dialog. The Process Activities dialog will display the list activities of the processes run by the application. The 'Show Activities' option is available only if Viruscope is enabled under Advanced Settings > Defense* > Behavior Blocker Settings.

Clicking the 'More' button at the bottom of the screen will open the Comodo KillSwitch application - an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes that are running on your system.



If KillSwitch is not yet installed, clicking this button will prompt you to download the application. Refer to the section [Identify and Kill Unsafe Processes](#) for more details.

3.Firewall Tasks - Introduction

The Firewall component of Comodo Internet Security (hereafter known simply as Comodo Firewall) offers the highest levels of security against inbound and outbound threats, stealths your computer's ports against hackers and blocks malicious software from transmitting your confidential data over the Internet. Comodo Firewall makes it easy for you to specify exactly which applications are allowed to connect to the Internet and immediately warns you when there is suspicious activity.

It can be accessed at all times by clicking on the 'Firewall Tasks' band from the 'Tasks' interface.

The Firewall Tasks area provides easy access to all major features and settings. From here, you can configure Internet access rights per-application, stealth your computer ports, manage available networks and even block all network traffic in and out of your computer. In 'Advanced Settings' you'll be able to specify overall firewall behavior and configure advanced settings such as application rules, rulesets, network zones and port sets.



Click the links below to see detailed explanations of each area in this section:

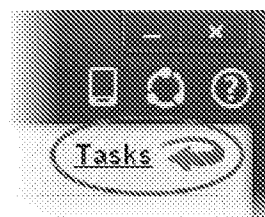
- [Allow or block Internet access to applications selectively](#)
- [Stealth your computer ports](#)
- [Manage network connections](#)
- [Stop all network activity](#)
- [Advanced firewall settings](#)

3.1. Allow or Block Internet Access to Applications Selectively

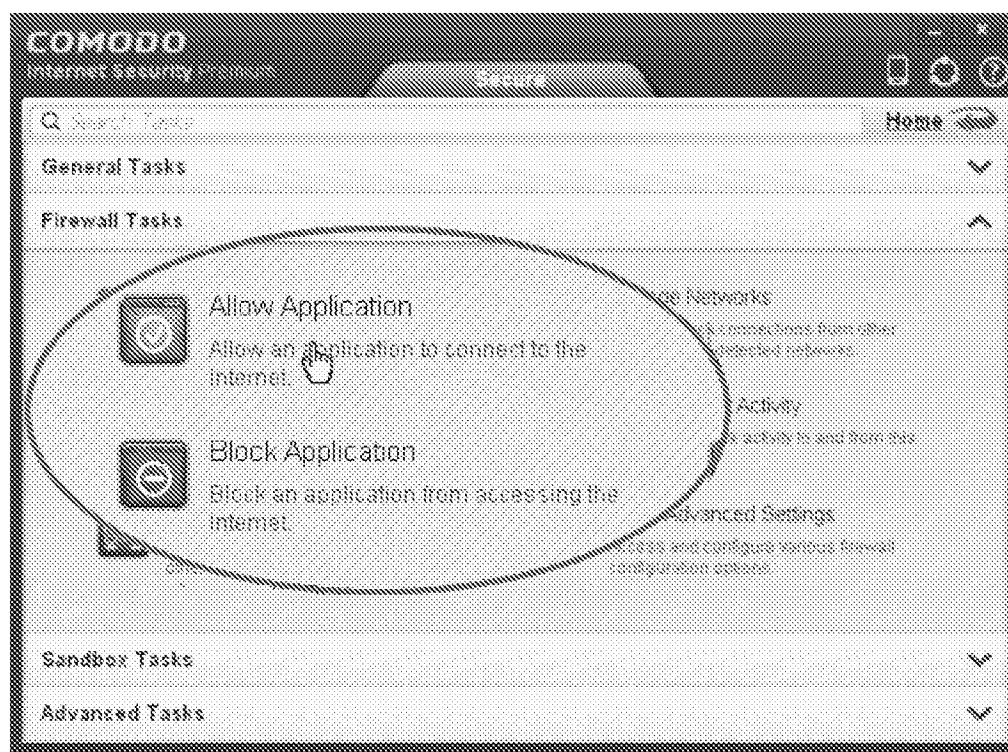
The Firewall Tasks interface allows you to selectively allow or block certain applications from accessing the Internet. These shortcuts represent a convenient way to create an automatic 'Allow Requests' rule or 'Block Requests' rule for individual applications - meaning that inbound and outbound connections are automatically permitted or not permitted to these applications respectively.

To open the 'Firewall Tasks' interface:

- Click the 'Tasks' arrow from the CIS home screen:



- Click on the 'Firewall Tasks' band from the 'Tasks' interface:



To allow an application to access to the Internet:

- Click the 'Allow Application' button from the 'Firewall Tasks' interface.
- Navigate to the main executable of the application in the 'Open' dialog.
- Click 'Open'. A rule will be created to allow Internet access to the selected application.

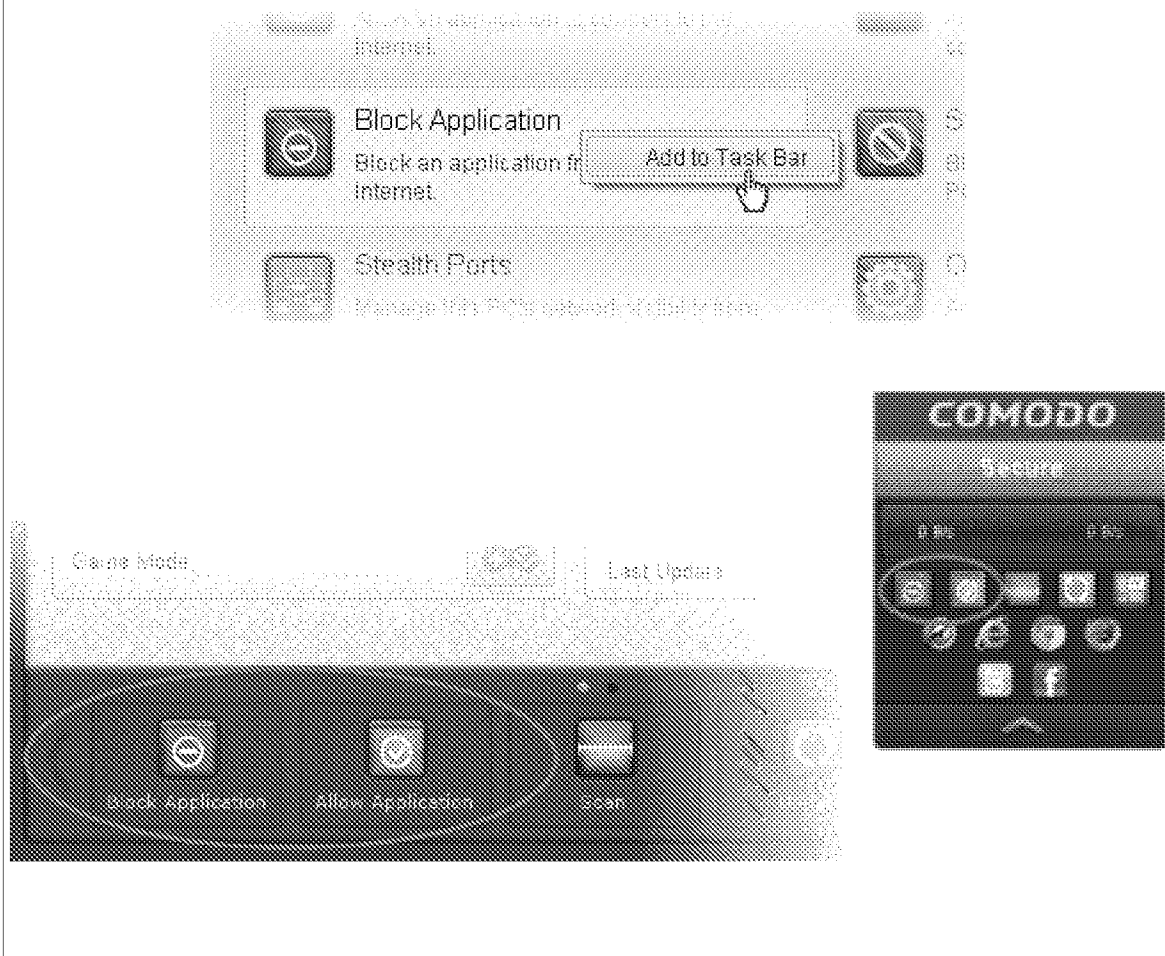
To block an application's Internet access rights

- Click the 'Block Application' button from the 'Firewall Tasks' interface.
- Browse to the main executable of the application in the 'Open' dialog.
- Click 'Open'. A rule will be created to prohibit Internet access to the selected application.

The advanced application rules interface can be accessed by clicking 'Tasks' from the CIS home screen > Firewall Tasks > Open Advanced Settings > Application rules. The application you just allowed or blocked should be listed here. For further information

on application rules governing internet access rights, see Application Rules.

Tip: If you plan to regularly allow/block applications, you can right click on the appropriate button and select 'Add to Taskbar'. It will then be quickly accessible from both the CIS home screen and the widget:



3.2. Stealth your Computer Ports

Port Stealthing is a security feature whereby ports on an Internet connected PC are hidden from sight, evoking no response to opportunistic port scans.

General Note: Your computer sends and receives data to other computers and to the Internet through an interface called a 'port'. There are over 65,000 numbered ports on every computer - with certain ports being traditionally reserved for certain services. For example, your machine almost definitely connects to Internet using port 80 and port 443. Your e-mail application connects to your mail server through port 25. A 'port scanning' attack consists of sending a message to each of your computer ports, one at a time. This information gathering technique is used by hackers to find out which ports are open and which ports are being used by services on your machine. With this knowledge, a hacker can determine which attacks are likely to work if used against your machine.

Stealthing a port effectively makes it invisible to a port scan. This differs from simply 'closing' a port as NO response is given to any connection attempts ('closed' ports respond with a 'closed' reply- revealing that there is actually a PC in existence.) This provides an extremely high level of security to your PC. If a hacker or automated scanner cannot 'see' your computers ports then they presume it is offline and move on to other targets. You can still be able to connect to Internet and transfer information as usual but remain invisible to outside threats.

- Click on 'Stealth Ports' link in Firewall Tasks



You have two options to choose from:

Block incoming connections

Selecting this option means your computer's ports are invisible to all networks, irrespective of whether you trust them or not. The average home user (using a single computer that is not part of a home LAN) finds this option the more convenient and secure. You are not alerted when the incoming connection is blocked, but the rule adds an entry in the firewall event log file. Specifically, this option adds the following rule in the 'Global Rules' interface:

Block And Log| IP | In| From Any IP Address| To Any IP Address | Where Protocol is Any

 Block IP In From MAC Any To MAC Any Where Protocol is Any

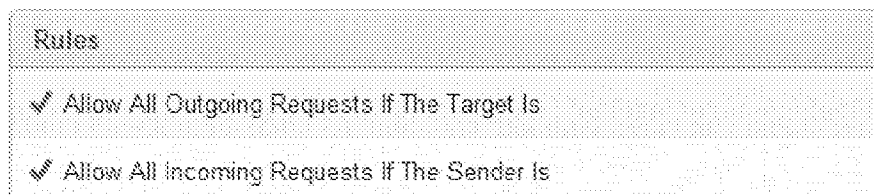
If you would like more information on the meaning and construction of rules, please [click here](#).

Alert incoming connections

You see a firewall alert every time there is a request for an incoming connection. The alert asks your permission on whether or not you wish the connection to proceed. This can be useful for applications such as Peer to Peer networking and Remote desktop applications that require port visibility in order to connect to your machine.

Specifically, this option adds the following rule in the 'Global Rules' interface:

Block | ICMP | In | From Any IP Address | To Any IP Address | Where Message is ECHO REQUEST

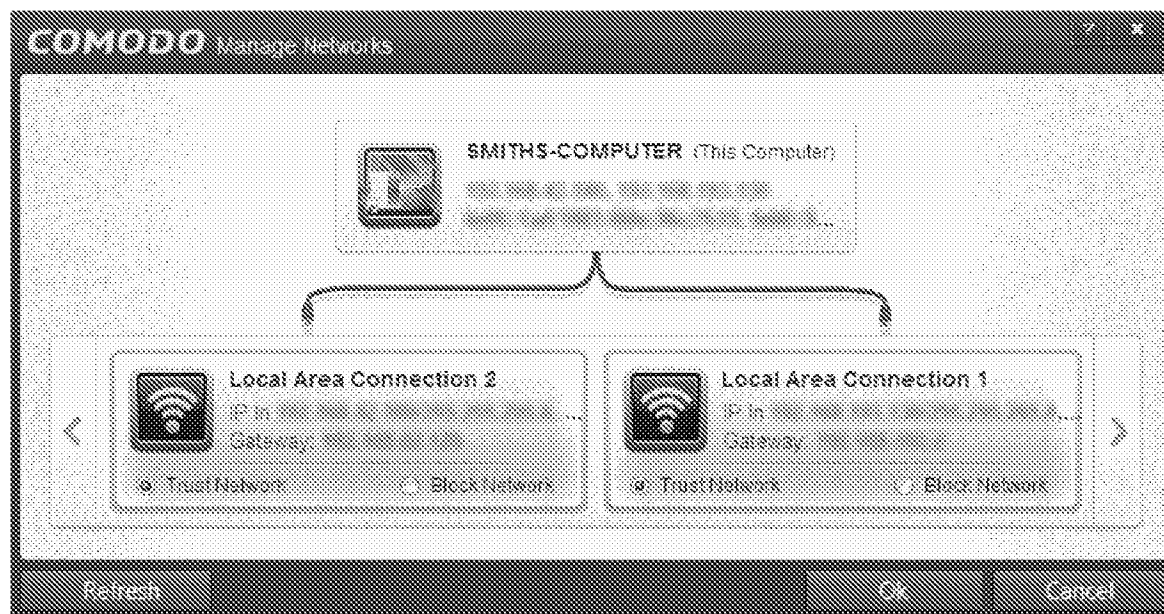


If you would like more information on the meaning and construction of rules, please [click here](#).

3.3. Manage Network Connections

The 'Manage Network Connections' interface allows you to quickly view all wired and wireless networks to which your computer is connected. The lower half of the panel displays details about each network including its name, IP address and gateway.

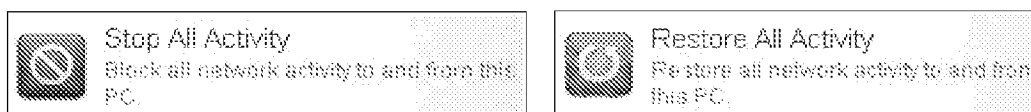
- You can choose to trust or block a network by selecting the appropriate radio button under the network in question. You will not be able to receive any inbound or outbound traffic from blocked networks.
- Use the handles (< >) to scroll through all available networks or computers
- Use the refresh button if you have recently made network changes and these are not yet visible in the interface.



- The 'Manage Networks' interface can be opened by clicking 'Tasks > Firewall Tasks > Manage Networks'.
- To view, create or block Network Zones, click 'Tasks > Firewall Tasks > Open Advanced Settings > Network Zones'.

3.4. Stop all Network Activities

As the name suggests, the 'Stop all network activity' button instructs the firewall to immediately cut-off all inbound/outbound communication between your computer and all available networks (including the Internet). Connections will remain closed until you re-enable them by clicking the button a second time. This allows you to quickly take your computer offline without having to delve into Windows network settings and without having to unplug any network cables.



- Access the network activity 'on/off' button by clicking Tasks > Firewall Tasks
- Disconnect your computer from all networks by clicking 'Stop All Activity' (button will be red)
- Re-enable connectivity by clicking 'Restore All Activity' (button will be green)
- Restoring activity just re-enables your existing firewall rules. Therefore, any networks that you have previously blocked in 'Manage Network Connections' or 'Network Zones' will remain blocked.
- You can assign networks into network zones in the 'Network Zones' area
- You can configure rules per network zone in the 'Global Rules' area
- You can view all network connections and enable/disable connectivity on a per-network basis in the 'Manage Network Connections' area

3.5. Advanced Firewall Settings

The 'Advanced Settings' area is the nerve center of Comodo Firewall and allows advanced users to configure and deploy traffic filtering rules and policies on an application specific and global basis. To open the interface, click 'Tasks' on the home screen followed by 'Open Advanced Settings' then 'Firewall Settings':



The interface is divided into six main sections - Firewall Settings, Application Rules, Global Rules, Rulesets, Network Zones and Portsets. Click the links below to jump to more details on each section:

- The Firewall Settings area allows you to configure the security of your computer and the frequency of alerts that are generated.
- The Application Rules area allows users to view, manage and define the network and Internet access rights of applications on your system.
- The Global Rules area allows users view, manage and define overall Firewall ruleset that applies to your computer and is independent of application rules.
 - Both application rules and global rules are consulted when the firewall is determining whether or not to allow or block a connection attempt.
 - For Outgoing connection attempts, the application rules are consulted first and then the global rules.
 - For Incoming connection attempts, the global rules are consulted first and then application specific rules.
- The Rulesets area contains a list of preset Firewall rules that can be re-used and applied to multiple applications. For example, there is a 'Browser' rule, an 'Email Client' rule and rules for 'Trusted' and 'Blocked' applications.
- The Network Zones area allows you to group IP addresses and ranges into named zones. Once defined, privileges and rules can be applied to these zones in other areas of CIS. For example, global and application rules can be applied to network zones. This interface also allows you to block network zones.
- The Portsets area contains groups of important / regularly used port numbers that can be easily selected as part of a global or application rule.
- The Website Filtering area allows you to create website filtering rules which let you determine which sites certain

users can or cannot access.

4. Sandbox Tasks - Introduction

Comodo Internet Security features a fully functional sandbox called the 'Virtual Desktop' - an isolated operating environment for running unknown, untrusted and suspicious applications. Applications executed inside the sandbox/virtual Desktop will not affect other processes, programs or data on your real computer. In addition to running suspicious applications inside the sandbox on an ad-hoc basis, you can create a specific list of programs that should always run in the sandbox.



Note: The sandbox referred to here is a full environment and is distinct to the 'auto-sandbox' configured under behavior blocker. Users can, however, enable 'Full Virtualization' of auto-sandboxed files in the Behavior Blocker settings.

The Sandbox Tasks interface has shortcuts for the following tasks:

- **Run Virtual Desktop** - Starts the Virtual Desktop
- **Open Shared Space** - Opens the folder 'Shared Space' which is shared by your host operating system and the Virtual Desktop. The folder is created by the Virtual Desktop at the location 'C:\Documents and Settings\All Users\Application Data\Shared Space'. The folder can be opened in both your host operating system and inside the Virtual Desktop, and enables to share files and applications between the OS and the Virtual Desktop.
- **Run Virtual** - Allows you to run individual applications in the sandbox
- **Reset Sandbox** - Allows you to clear all data written by programs run inside the sandbox
- **Open Advanced Settings** - Add programs that should always run inside the sandbox and access advanced sandbox settings. This is covered in the 'Configure the Sandbox' section of 'Advanced Settings'

The Virtual Desktop is a sandboxed operating environment inside of which you can run programs and browse the Internet without fear that those activities will damage your real computer. Applications running in the Virtual Desktop also leave no cookies or history behind on your real system, making it a secure environment for Internet banking and online shopping. It is also ideal for visiting any risky websites/links and for testing out beta/unstable software.



- The Virtual Desktop can run any program that you can run in regular Windows and is particularly useful for browsing the Internet in a secure manner.
- Any changes made to files and settings in the Virtual Desktop will not affect the original versions on your host system. Changes will only be visible in the Virtual System itself.
- Similarly, any changes made by malicious programs or unstable beta software will not damage your real computer.
- Any files you wish to keep and access from your host operating system can be saved to 'Shared Space'.
- The Virtual Desktop can be password-protected for added privacy.
- The virtual keyboard allows you to securely enter confidential passwords without fear of key-logging software.
- The Virtual Desktop UI can be used in both 'Classic' (Windows style) and 'Tablet' modes by selecting the mode from Settings.
- You can reset the Virtual Desktop and clear shared space at any time. We recommend that you do this regularly to maximize your privacy and security. Please note that all settings, stored data and any applications installed sandboxed will be deleted.

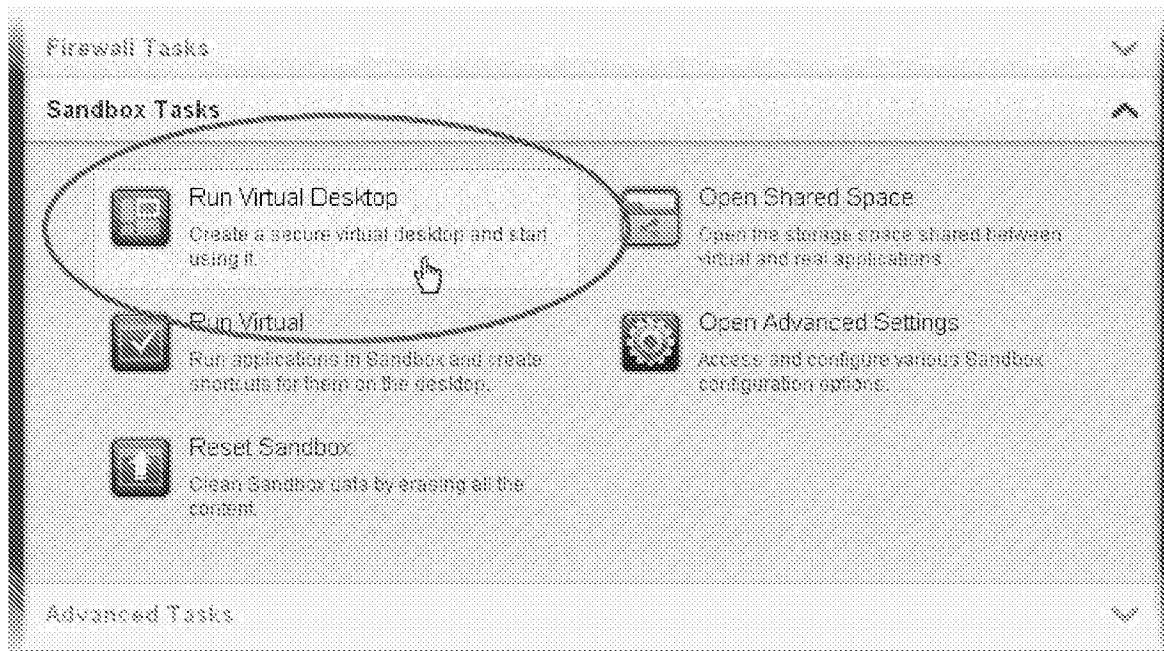
- Starting the Virtual Desktop
- The Main Interface

- Run Browsers inside Virtual Desktop
- Open Files and Run Applications inside Virtual Desktop
- Configuring the Virtual Desktop
- Closing the Virtual Desktop

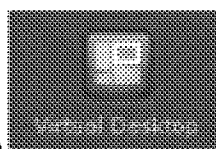
4.1.1. Starting the Virtual Desktop

The Virtual Desktop can be started by:

- Clicking Tasks > Sandbox Tasks > Run Virtual Desktop



OR



- by clicking the Virtual Desktop shortcut button from the task bar at the bottom of Home Interface

OR

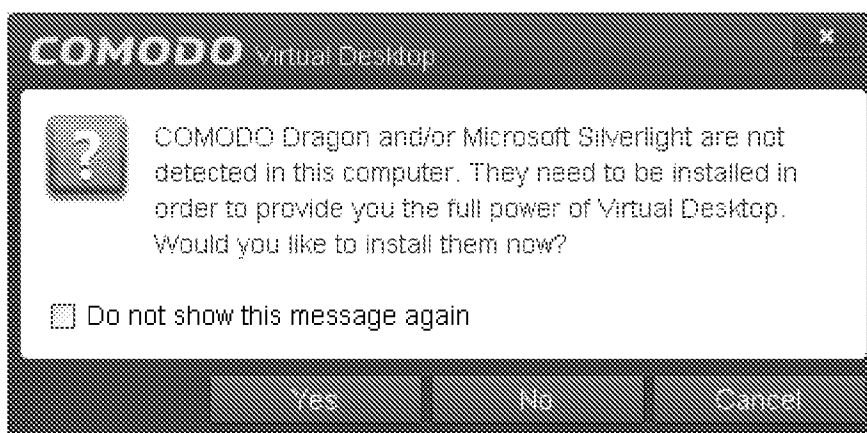
- By clicking the Virtual Desktop shortcut button from the CIS widget



The following software is needed to utilize the Virtual Desktop to its full potential:

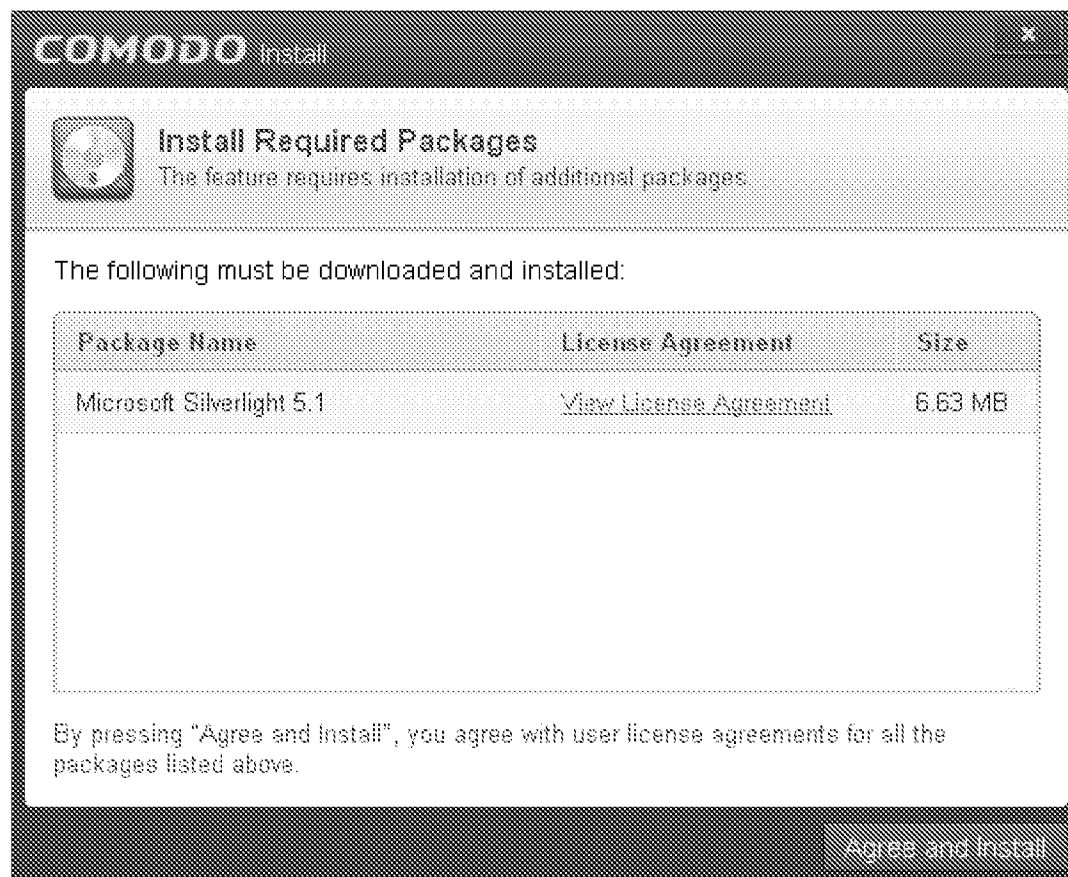
- Comodo Dragon Browser
- Microsoft Silverlight

Whenever you run the Virtual Desktop, Comodo Internet Security checks whether these components are installed. If they aren't, you will be prompted to install them.



- If you want Comodo Dragon and/or Microsoft Silverlight to be installed this time, click 'Yes'. If not, click 'Cancel'. You will be prompted to install them, next time when you start the Virtual Desktop.
- If you do not want the applications to be installed at all, click 'No'.
- Click 'Yes' to download and install the software.

The 'Install Required Packages' dialog will be displayed.



- Click 'View License Agreement' to read the license agreement of the additional software to be installed
- Click Agree and Install to download and install the required software

The software package(s) will be downloaded and installed automatically.

4.1.2. The Main Interface

The Virtual Desktop is presented with two switchable interfaces:

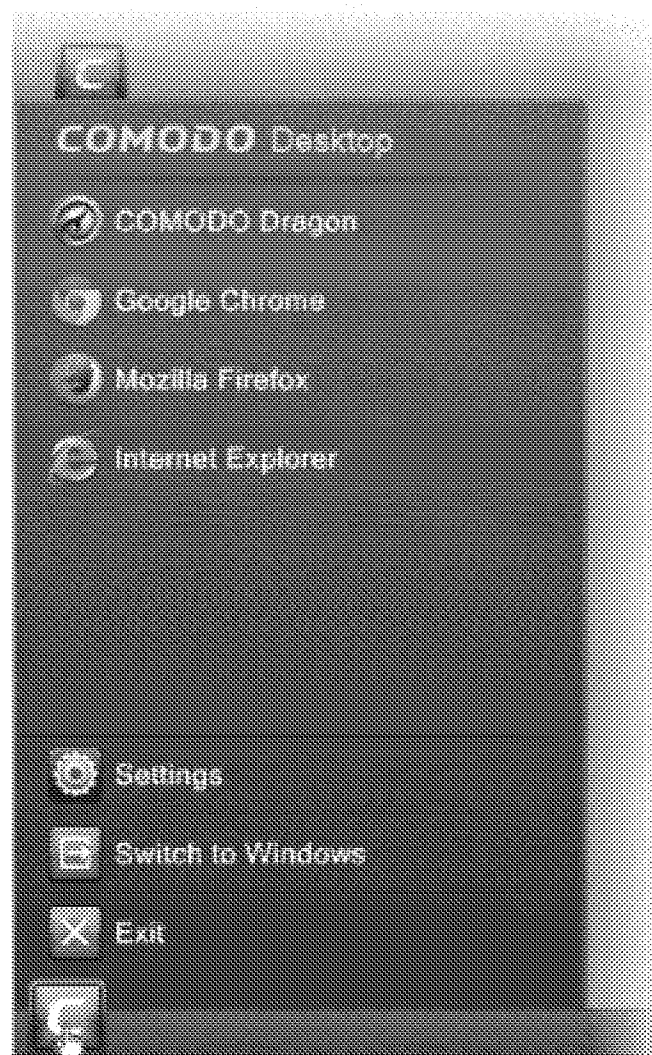
- Classic Windows style Desktop mode
- Tablet mode

You can switch between these two modes by clicking the green 'C' button at bottom-left then 'Settings' (C Button > Settings > 'Mode' tab.). Refer to the table below for a comparison of different modes of the Virtual Desktop main interface.



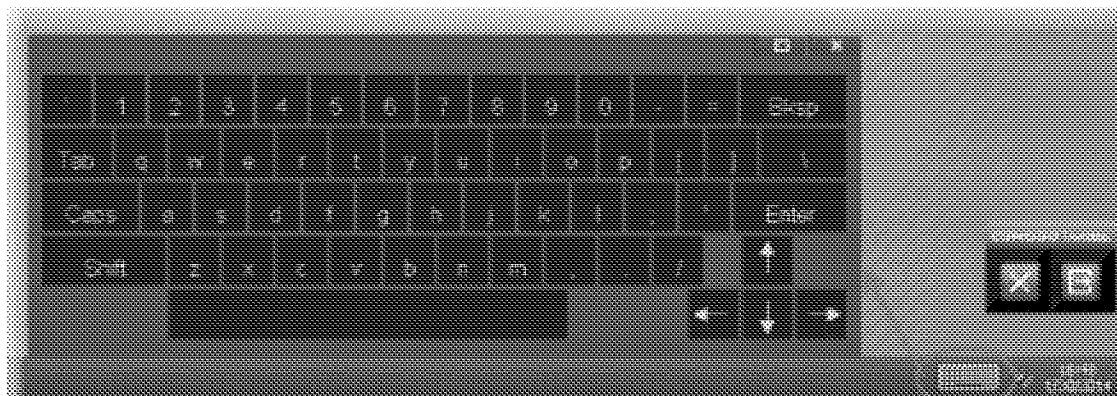
In 'Classic' mode,

- All items on your real desktop are displayed. Clicking the shortcuts on the Virtual Desktop will run the program or file inside the virtual computer system.
- Clicking the green 'C' button at bottom-left will open a Windows-style 'Start Menu'.

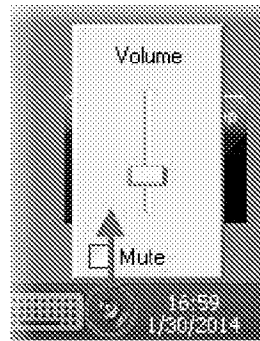


The start menu allows you to:

- Run browsers that are installed on your system. Refer to [Running Browsers inside the Virtual Desktop](#) for more details.
- Configure the Virtual Desktop by clicking 'Settings'. Refer to [Configuring the Virtual Desktop](#) for more details.
- Clicking the keyboard icon on the system tray opens a virtual keyboard that can be used to input confidential data like website user-names, passwords and credit card numbers.



- Clicking the 'Volume Control' icon at the system tray enables you to control the system volume.



- Right-clicking on the task bar and selecting 'Watch Activity' opens the 'Windows Task Manager' to view your computer's performance, close unresponsive programs and to troubleshoot problems with Windows.



Tablet Mode



To switch to 'Tablet' mode from 'Classic' mode, click the green 'C' button at bottom left followed by Settings > Mode and select 'Tablet Mode'.

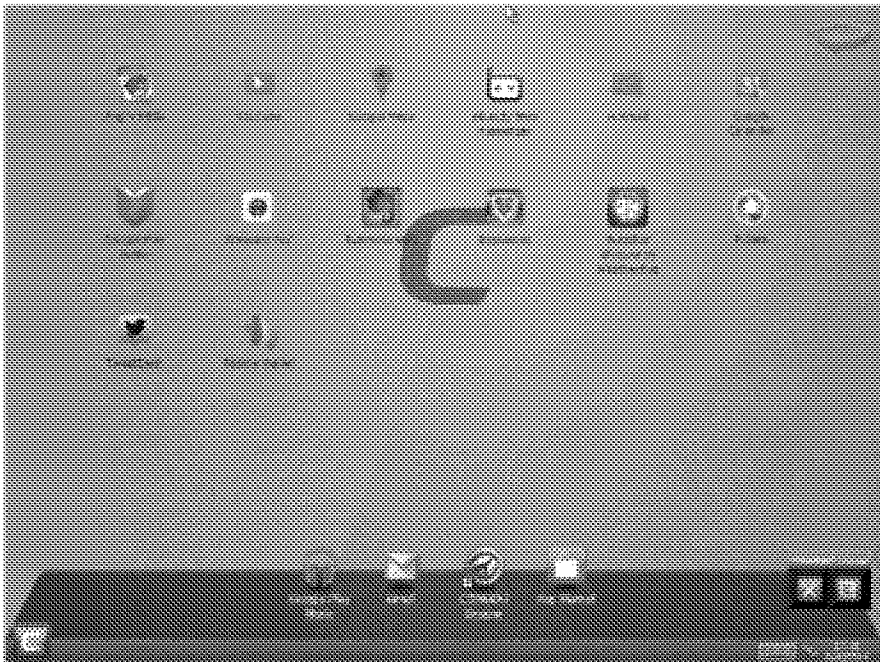
There are two variations of this mode:

- Mode A - Pure Tablet device - A touch-screen interface that will be familiar to users of modern smart devices. The home page displays a set of popular apps covering games, social media and networking. You can, of course, install your own apps from the app market.
 - To install your own apps, click the App Market icon from the launch bar. You will be taken to https://chrome.google.com/webstore/category/home?utm_source=COMODO-Kiosk. Select the apps you want to install from the web-store.
- Mode B - Tablet device + Windows - The home page displays the desktop items from your real system. The task bar from classic mode is present along with the green 'C' button and the virtual keyboard. The launch strip will display all installed browsers.

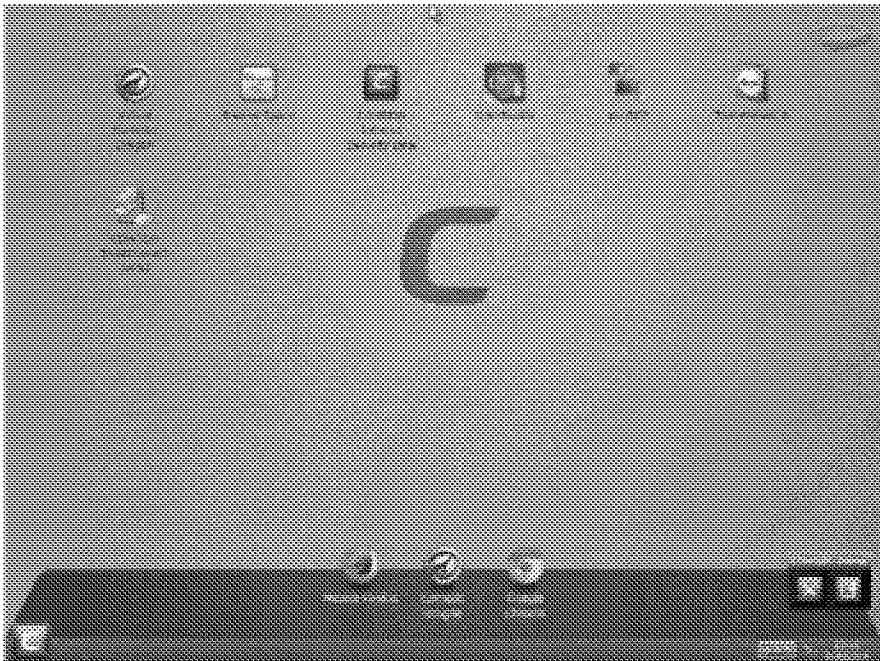


You can swap between the two modes by clicking the green arrow at the top right corner.

You can swipe the home screen in both left and right directions to navigate between successive home pages.



Tablet Mode A - Pure Tablet



Tablet Mode B - Tablet + Windows

The following table gives a comparison of the classic and tablet modes of the main interface:

Classic Mode	Mode A - Pure Tablet	Mode B - Tablet + Windows
Windows desktop style interface.	Tablet style interface.	Tablet style interface.
Your real desktop shortcuts and files are displayed	Shortcut icons of the apps installed on the tablet are displayed	Your real desktop shortcuts and files are displayed
Shortcuts and files are laid out vertically as they would be on a Windows desktop	Shortcuts are laid out horizontally	Shortcuts and files are laid out horizontally

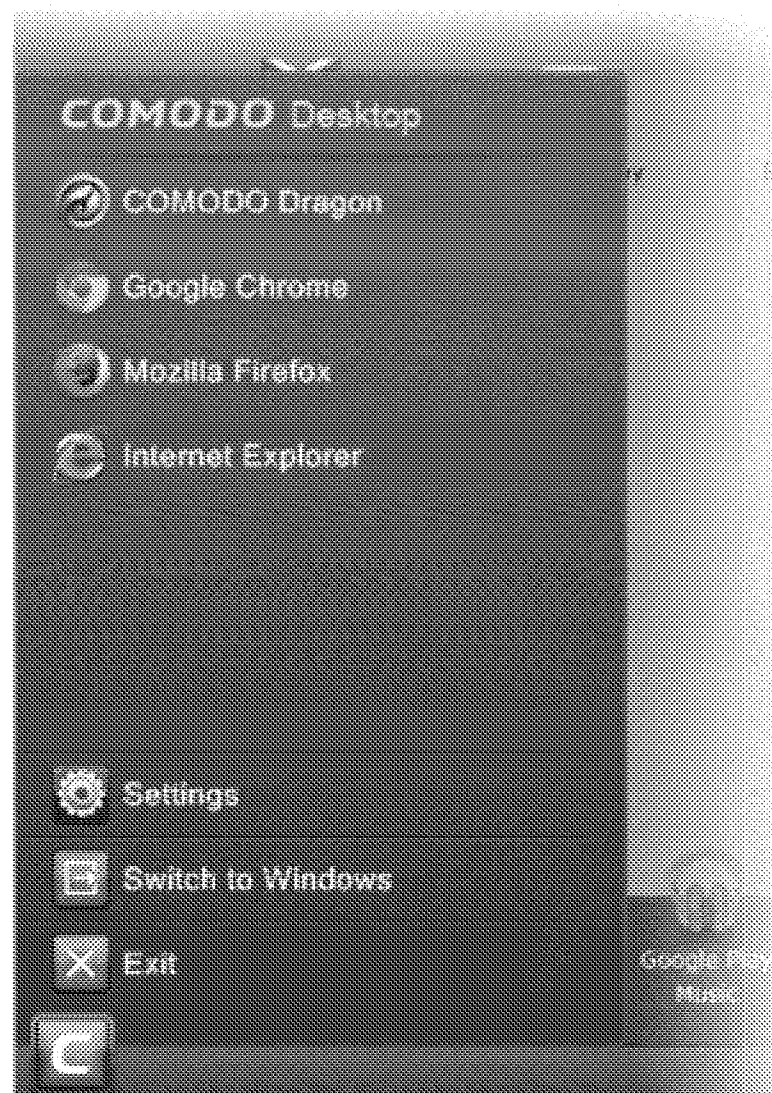
No Launch Bar	Browser shortcuts are displayed on the launch bar at the bottom	Browser shortcuts are displayed on the launch bar at the bottom
Cannot have multiple home screens	Can have multiple home screens	Can have multiple home screens if you have many shortcuts and files
Cannot swipe the screen to move between home screens	Can swipe the screen to move between home screens	Can swipe the screen to move between home screens

4.1.3. Running Browsers inside the Virtual Desktop

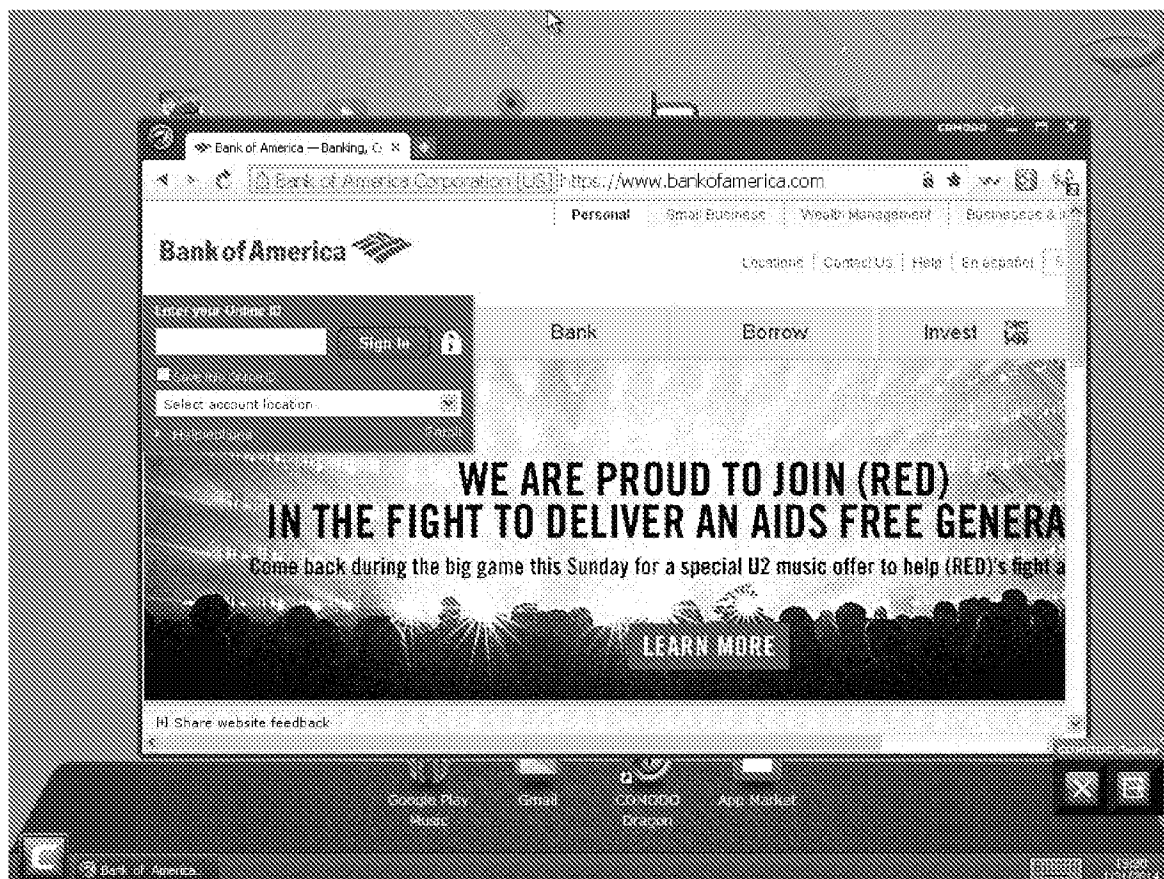
The Virtual Desktop provides an extremely secure environment for internet related activities because it isolates your browser from the rest of your computer. Just by visiting them, malicious websites can install viruses malware, rootkits and spyware onto your computer that can allow hackers to steal confidential information. Surfing the 'net from inside the virtual computer system removes this threat by preventing websites from installing applications on your real computer. Furthermore, the Virtual Keyboard allows you to securely enter user-names, credit card numbers and passwords without fear of key-logging software recording your physical keystrokes.

To run a browser inside the Virtual Desktop

1. Click the 'C' button at bottom left
2. Select the browser you want to run:



Your choice of browser will open inside the virtual desktop, ready for secure surfing:



Browsing history and other records of your internet activity will not be stored on your computer when your session is finished.

4.1.4. Opening Files and Running Applications inside the Virtual Desktop

Applications installed or the files stored in your system can be opened inside the Virtual Desktop by the following methods:

- Opening the applications/files from the desktop shortcuts
- Sharing the application/files through the Shared Space folder

Desktop Shortcuts

You can copy the files or create shortcuts for the applications/files to be opened in Virtual Desktop, in the desktop of your real system. The shortcuts of your real desktop will be available in the Virtual Desktop. You can double click on the icon to open the respective application or file inside the Virtual Desktop.

Note: The real computer desktop icons will be available only in the Classic Windows Mode and Tablet + Classic Mode.

Shared Space

The Virtual Desktop creates a folder Shared Space in the location "C:\Documents and Settings\All Users\Application Data\Shared Space". The 'Shared Space' folder can be shared by your host operating system and the Virtual Desktop.

The Shared Space can be accessed in the following ways:

- Click 'Open Shared Space' under 'Sandbox' Tasks in the Tasks Interface
- Click the 'Shared Space' shortcut icon from the home screen of CIS
- Click the 'Shared Space' shortcut icon from the CIS widget

- Click the 'Shared Space' desktop shortcut icon

To open an application or file from your host system in the Virtual Desktop

1. Open the 'Shared Space' as mentioned above
2. Copy/Move the application or the file to be opened into the Shared Space
3. Start 'Virtual Desktop'
4. Open Shared Space inside the Virtual Desktop by clicking the 'Shared Space' icon in the home screen.

Note: The Shared space home screen icon will be available only in the Classic Windows Mode and Tablet + Classic Mode.

5. Double click on the application/file in the shared space to open it inside the Virtual Desktop.

The changes you make to the file will be stored to the file only inside the Virtual Desktop and not in the real computer system.

4.1.5. Configuring the Virtual Desktop

The settings panel allows you to specify the Virtual Desktop operational mode and to modify its look and feel.

To open the settings panel:

1. Click the 'C' button at bottom left.
2. Select 'Settings' from the start menu. The Settings panel will open.

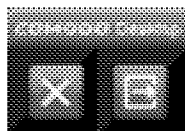


The Settings panel has two tabs:

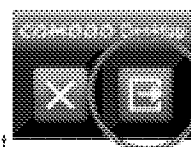
- **Mode** - Allows you to select the display mode of the Virtual Desktop between Classic Windows mode and Tablet Mode (Default)
 - **Themes** - Allows you to choose the appearance of the Virtual Desktop
3. Click OK for your settings to take effect

4.1.6. Closing the Virtual Desktop

The shortcuts at the bottom right of the Virtual Desktop, allow you to temporarily switch to your real computer system, if you plan to continue using the virtual desktop at a later time, or to fully exit the Virtual Desktop.



To temporarily switch to your real Windows system



- Click the right button from the shortcuts pane at the bottom right
- Alternatively, Click the 'C' button at bottom left and choose 'Switch to Windows' from the Virtual Desktop Start Menu.

The Virtual Desktop will be temporarily closed. You can quickly return to it by clicking the right switch from the Virtual Desktop

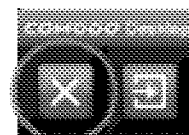
shortcut buttons displayed at the bottom right of your Windows Desktop



or by clicking 'Run Virtual

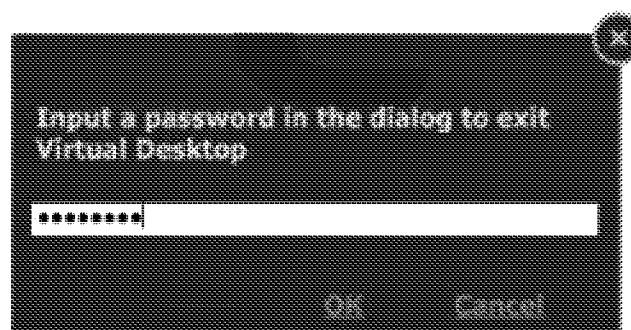
Desktop' from the 'Sandbox Tasks' interface.

To close the Virtual Desktop



- Click the X button from the Virtual Desktop shortcuts pane at the bottom right
- Alternatively, Click the 'C' button at bottom left and choose 'Exit' from the Virtual Desktop Start Menu.

In either case, if password protection is enabled under Advanced Settings > Security Settings > Defense+ > Sandbox Settings, you will be prompted to enter the password. Else the Virtual Desktop will be closed.



- Enter the password and click OK.

Notes: Remember to save the changes before you exit the Virtual Desktop. Your changes will be lost if you exit the Virtual Desktop.

4.2.Run an Application in the Sandbox

Comodo Internet Security allows you to run programs inside the Sandbox on a 'one-off' basis. This is helpful to test the behavior of new executables that you have downloaded or for applications that you are not sure that you trust. Adding a program in this way means that it will run in the Sandbox this time only. On subsequent executions it will not run in the sandbox (presuming it passes the sandboxing process).

You can also create a desktop shortcut to run the application inside the sandbox on future occasions. The following image shows how a 'virtual' shortcut will appear on your desktop:



Note: If you wish to run an application in the sandbox on a long-term/permanent basis then add the file to the Sandbox.

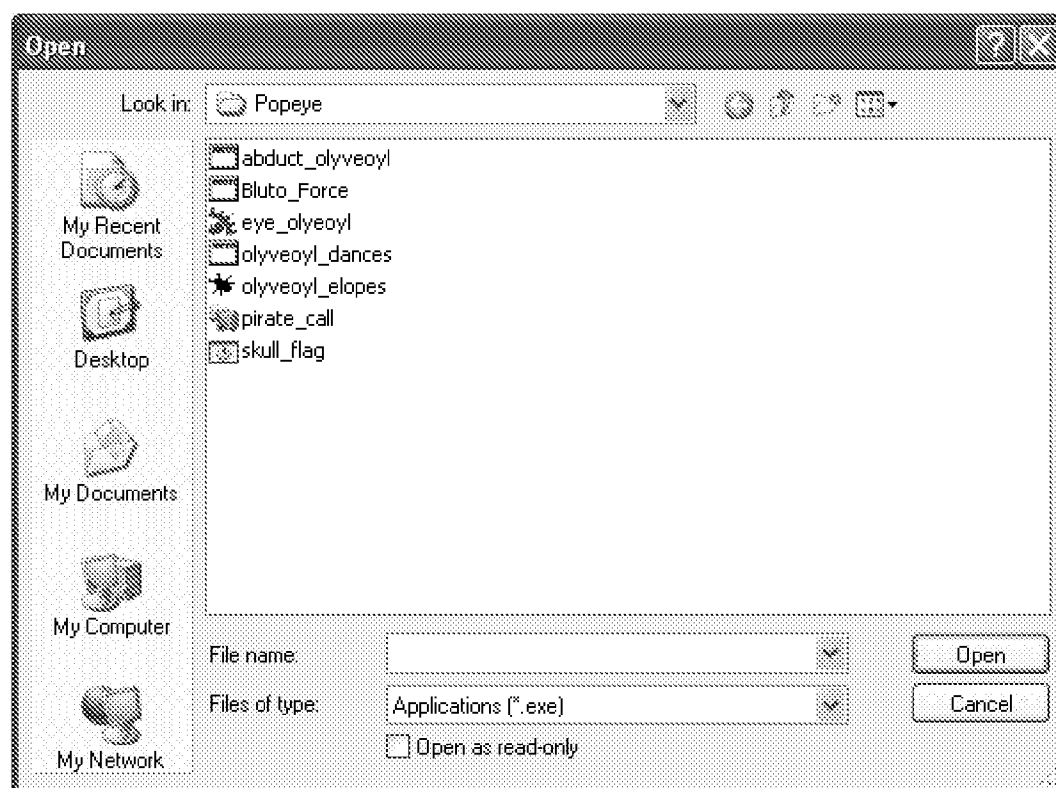
To run an application in the Sandbox

1. Open the Sandbox Tasks interface and Click 'Run Virtual'.



The 'Run Virtual' dialog will be displayed.

2. To run an application inside the sandbox, click 'Choose and Run' then browse to the application. The application will run with a green border indicating that it is sandboxed. If you wish to run the application in the sandbox in future, then select 'Create a virtual desktop shortcut'.



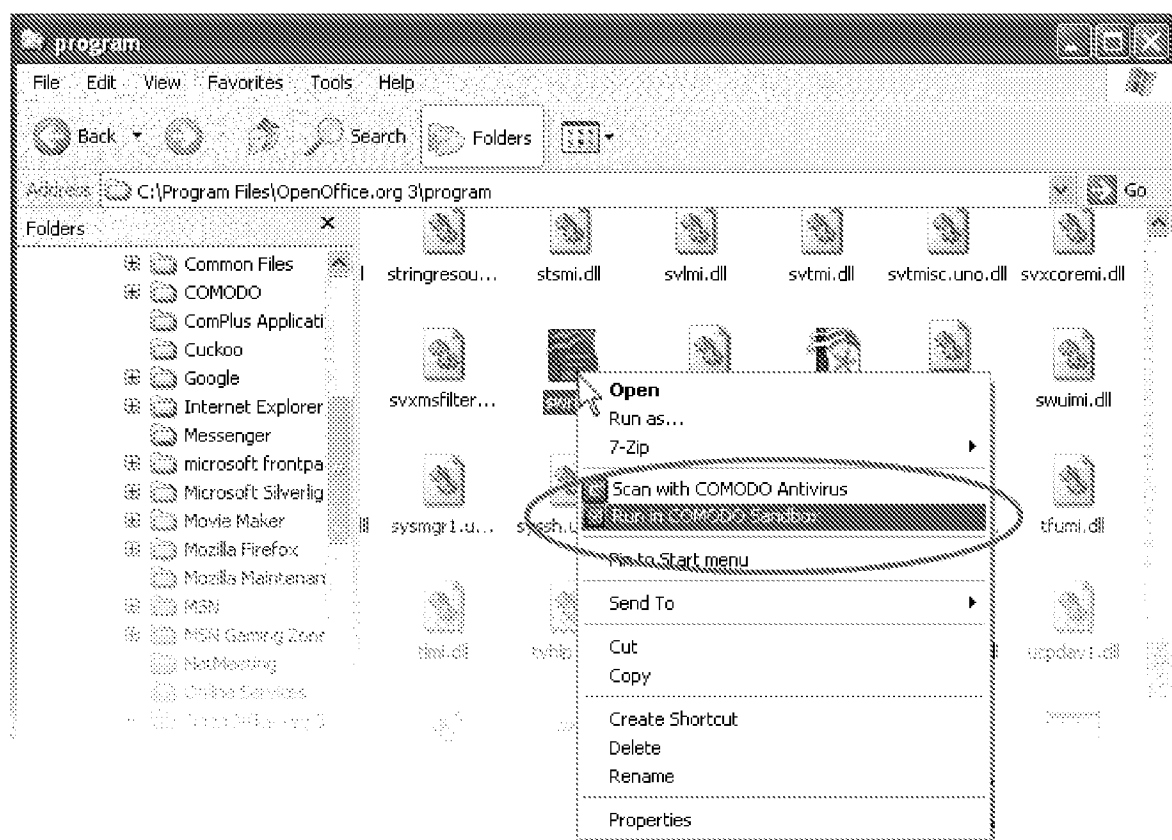
3. Browse to the application and click 'Open'. In the example above, Open Office Writer is chosen.

Alternatively, you can run an application inside the sandbox by the following shortcut methods:

- From the context sensitive menu
- Running browsers inside sandbox

Running a program from the context sensitive menu

- Navigate to the program in your system that you want to run in sandboxed environment and right click on it



- Choose 'Run in Comodo Sandbox' from the context sensitive menu

Running Browsers inside the Sandbox

The CIS Desktop Widget displays shortcut icons of the browsers installed in your computer.



- Clicking on a browser icon will start the browser inside the sandbox.

The browser will be started and executed inside the sandbox at 'Fully Virtualized' level. CIS displays a green border around the windows of programs to indicate that they are running inside the sandbox, if the setting 'Show highlight frame for virtualized programs' is enabled in Sandbox Settings.



The application will run in the Sandbox on this occasion only. If you often want the browser to run sandboxed then create a 'virtual shortcut' for the application by selecting the check-box 'Create a virtual desktop shortcut' in step 2. If you wish to run an application in the sandbox on a long-term/permanent basis then add the file to the Sandbox.

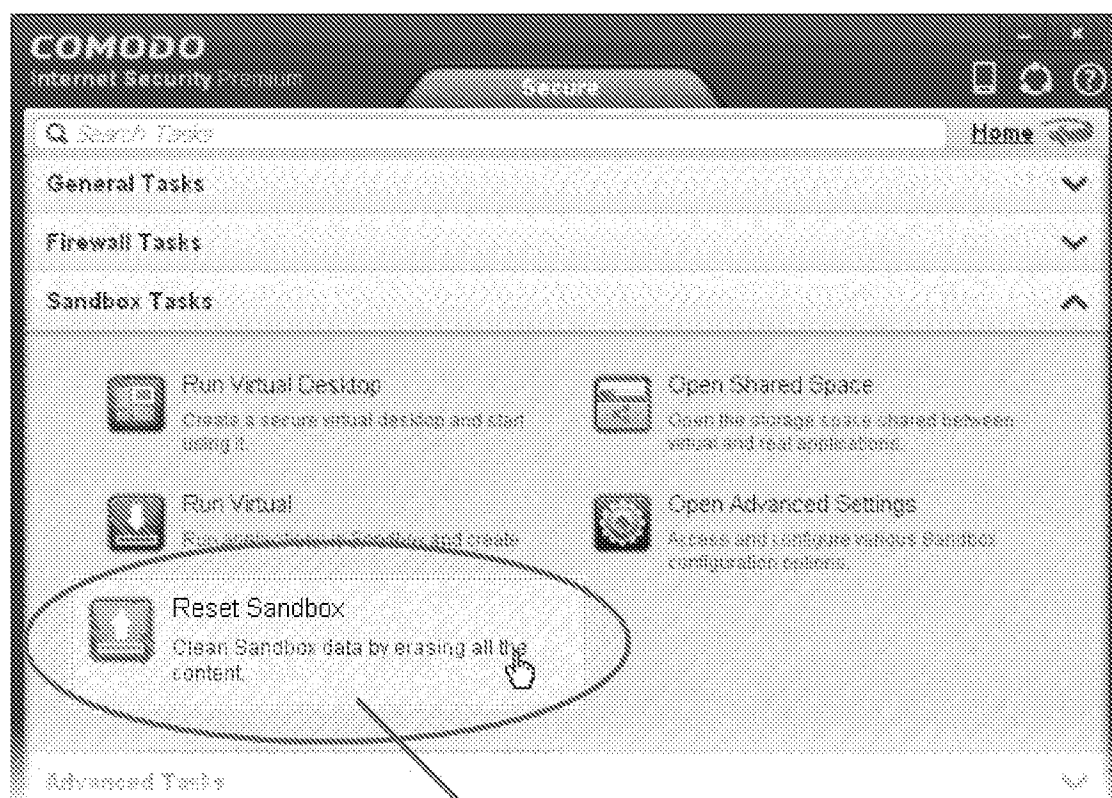
4.3. Reset the Sandbox

Programs running inside the Virtual Desktop store the changes to the files accessed by them inside the sandbox so that the changes do not affect the real computer system. Items stored in the sandbox/ Virtual Desktop could, depending on your usage patterns, contain malware downloaded from websites or private data in your browsing history. Periodically resetting the sandbox will clear all this data and help protect your privacy and security. If data has accumulated over a long period of time, then resetting the sandbox will also help the Virtual Desktop operate more smoothly.

The Reset Sandbox option under the Sandbox Tasks allows you to delete all the items stored in the sandbox.

To clear the sandbox

- Click on the 'Sandbox Tasks' bar from the Tasks interface and then click 'Reset Sandbox'



The 'Reset Sandbox' dialog will appear.

- Click 'Erase Changes'. The contents in the sandbox will be deleted immediately.



5. Advanced Tasks - Introduction

The 'Advanced Tasks' area allows you modify the overall configuration of CIS, manage CIS tasks like AV scans and updates currently running in the background or in minimized window and to take advantage of several other Comodo utilities. Click the following links to find out more about each item:

- [Create Rescue Disk](#) - Burn a bootable ISO that lets you run virus scans in pre-boot environments
- [Submit Files](#) - Directly Submit unknown/suspicious files to Comodo for analysis
- [Watch Activity](#) - Use Comodo Killswitch to identify unsafe processes and manage system activity
- [Clean Endpoint](#) - Deploy Comodo Cleaning Essentials to eradicate persistent infections from your PC
- [Task Manager](#) - Manage priorities of, stop, pause and resume currently running CIS tasks like Antivirus scans and updates
- [Open Advanced Settings](#) - Configure overall behavior, define custom rulesets and much more

Some of these utilities require the download and installation of additional setup files. After installation, the utility will start directly next time you click the button.



5.1. Create a Rescue Disk

Comodo Rescue Disk (CRD) is a bootable disk image that allows users to run virus scans in a pre-boot environment (before Windows loads). CRD runs Comodo Cleaning Essentials on a lightweight distribution of the Linux operating system. It is a powerful virus, spyware, rootkit scanner and cleaner which works in both GUI and text mode. The tool can provide a more comprehensive and thorough scan than regular malware cleaning applications because it cleans your system before Windows is loaded. CRD is intended to be used when malware embeds itself so deeply into your system that regular AV software cannot remove it. The rescue disk is also very effective at removing infections that are preventing Windows from booting in the first place. Apart from the virus scanner, CRD also provides tools to explore files in your hard drive, take screen-shots and browse web pages.

- Clicking the 'Create Rescue Disk' button in CIS 'Advanced Settings' opens a utility that allows you to download and burn the CRD iso to a CD/DVD, USB or other drive. [Click here](#) to jump to a walk-through of this process



After you have burned the ISO, you need to boot your system to the rescue disk in order to use the scanner in your pre-boot environment.

- Details of how to change boot order on your computer can be found in the Rescue Disk user guide at <http://help.comodo.com/topic-170-1-493-5227-Changing-Boot-Order.html>
- Details of how to initiate CRD after booting can be found at <http://help.comodo.com/topic-170-1-493-5228-Booting-to-and-Starting-Comodo-Rescue-Disk.html>
- Details of how to start running scans on your pre-boot environment are available at <http://help.comodo.com/topic-170-1-493-5216-Starting-Comodo-Cleaning-Essentials.html> and <http://help.comodo.com/topic-170-1-493-5217-CCE-interface.html>

5.1.1. Downloading and Burning Comodo Rescue Disk

To create a Comodo Rescue Disk, Click 'Create Rescue Disk' button from the Advanced Tasks interface.



The Comodo Rescue Disk interface will open. The interface displays the steps involved in creation of a new Rescue Disk on a CD/DVD or in a USB drive.

Step 1- Select the ISO file

This step allows you to select the Comodo Rescue Disk image file in .iso format stored in your hard drive, if you have already downloaded the same from Comodo servers or copied from another computer. Pre-storing the .iso file and burning the rescue disk from it conserves your Internet connection bandwidth usage. This step is optional. If you haven't downloaded the iso file, it will be automatically downloaded from Comodo Servers prior to execution of Step 3 - Burning the Rescue Disk.

- Click Select ISO File (Optional) and navigate to the comodo_rescue_disk.iso file

Step 2 Select target drive

This step allows you to select the CD/DVD drive or the USB drive to burn the Rescue Disk.

To burn the Rescue disk on a CD or a DVD

- Label a blank CD or DVD as "Comodo Rescue Disk - Bootable" and load it to the CD/DVD drive in your system
- Click 'Select Target Drive' from the 'Comodo Rescue Disk' interface and select the drive from the Select Disk dialog



To burn the Rescue disk on a USB Drive

- Insert a formatted USB memory to a free USB port on your computer
- Click 'Select Target Drive' from the 'Comodo Rescue Disk' interface and select the drive from the Select Disk dialog

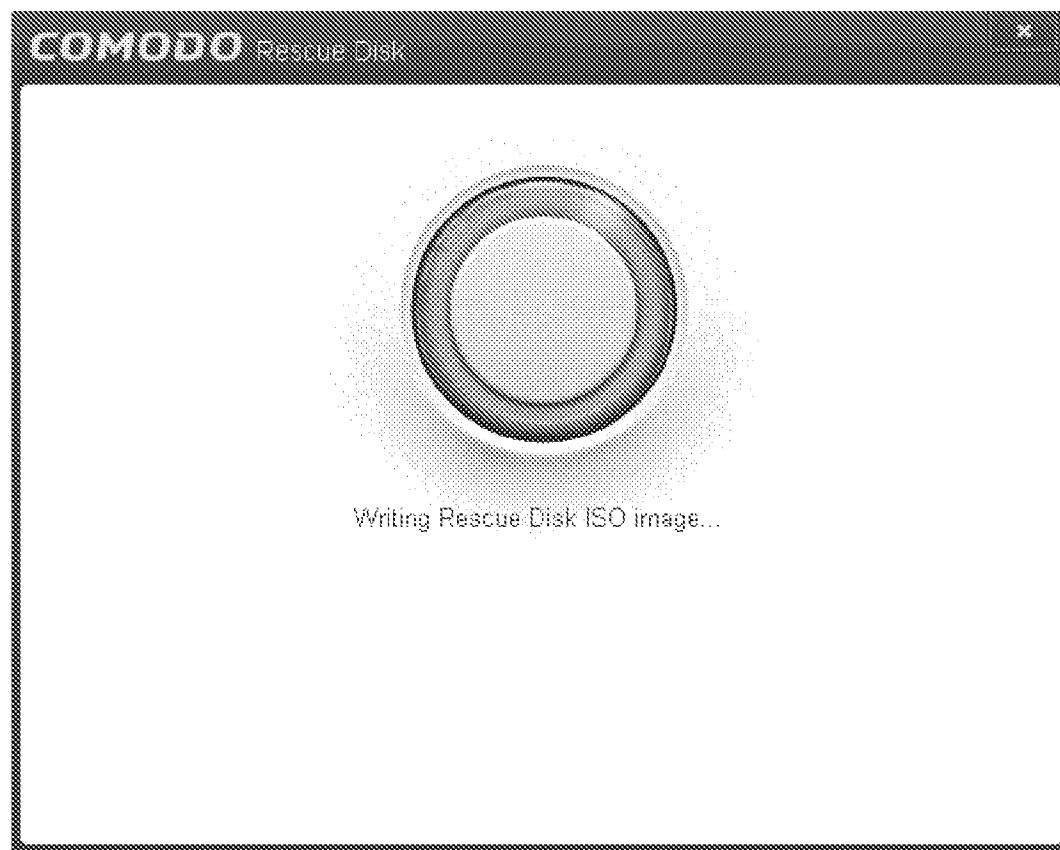


Step 3 - Burn the Rescue Disk

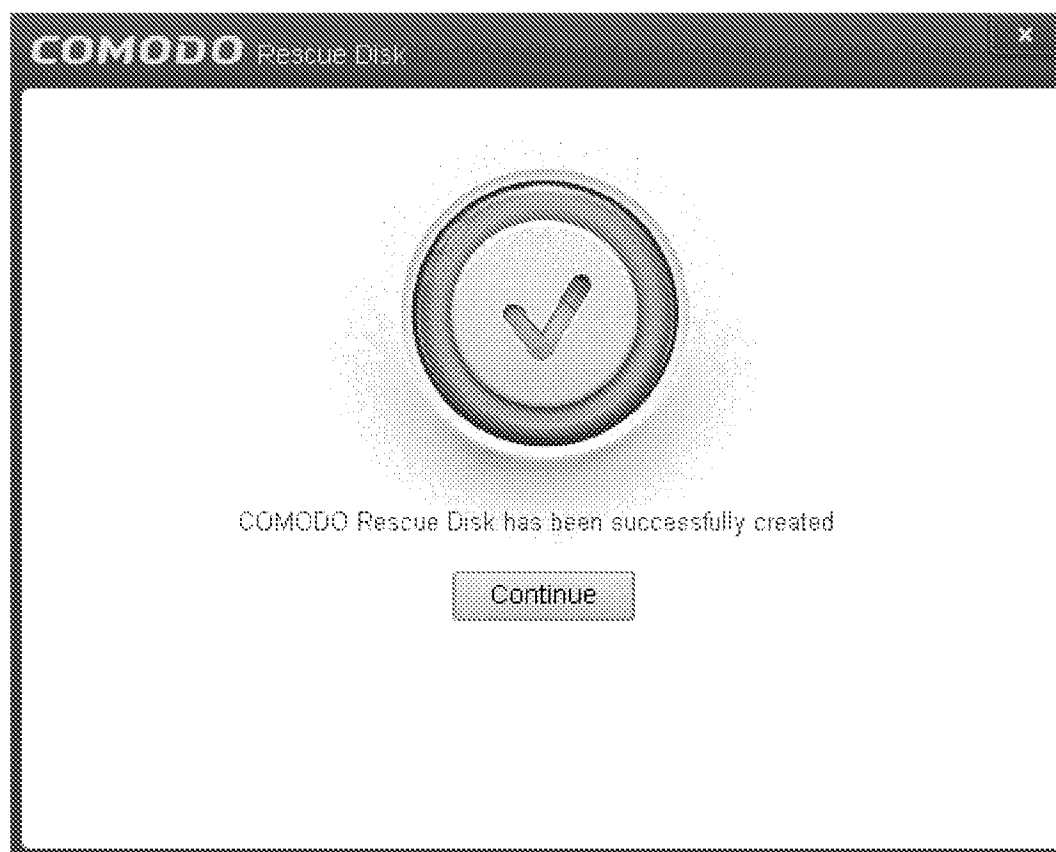
- After you selected the target drive, click 'Start'. If you have selected an .iso file from your hard disk, the burning of the disk will start immediately. Else, the .iso file will be downloaded from Comodo Servers.



On completion, the files will be written on to the CD/DVD or the USB Drive.



- Wait till the completion of the process. Do not eject the CD/DVD or the USB drive. On completion of the process, the CD/DVD will be ejected automatically.



Your Bootable Comodo Rescue Disk is created. Click 'Continue' to go back to CIS interface.

5.2. Remove Deeply Hidden Malware

Comodo Cleaning Essentials (CCE) is a set of computer security tools designed to help users identify and remove malware and unsafe processes from infected computers.

Major features include:

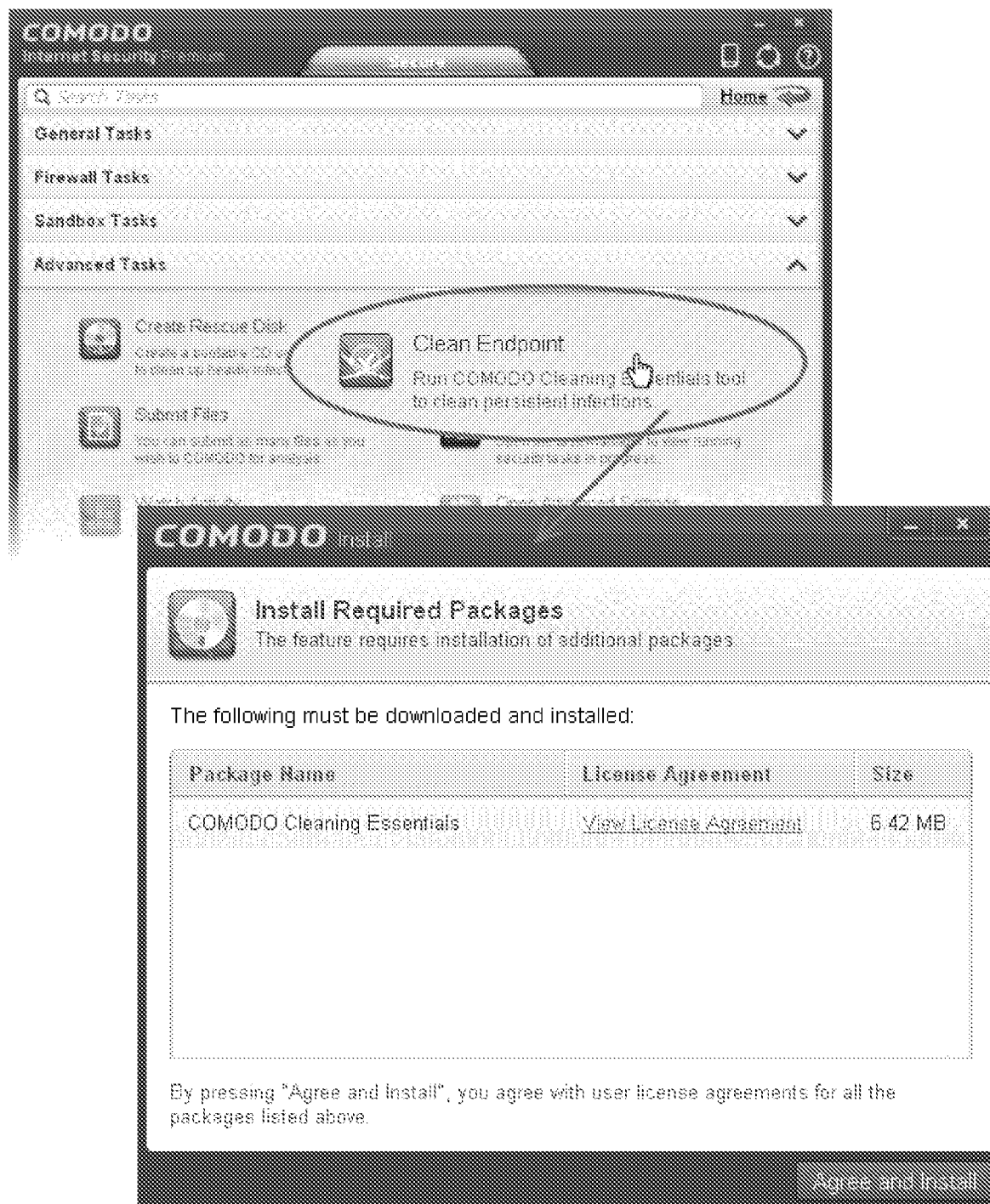
- **KillSwitch** - an advanced system monitoring tool that allows users to identify, monitor and stop any unsafe processes that are running on their system.
- **Malware scanner** - Fully customizable scanner capable of unearthing and removing viruses, rootkits, hidden files and malicious registry keys hidden deep in your system.
- **Autorun Analyzer** - An advanced utility to view and handle services and programs that were loaded when your system booted-up.

CCE enables home users to quickly and easily run scans and operate the software with the minimum of fuss. More experienced users will enjoy the high levels of visibility and control over system processes and the ability to configure customized scans from the granular options menu.

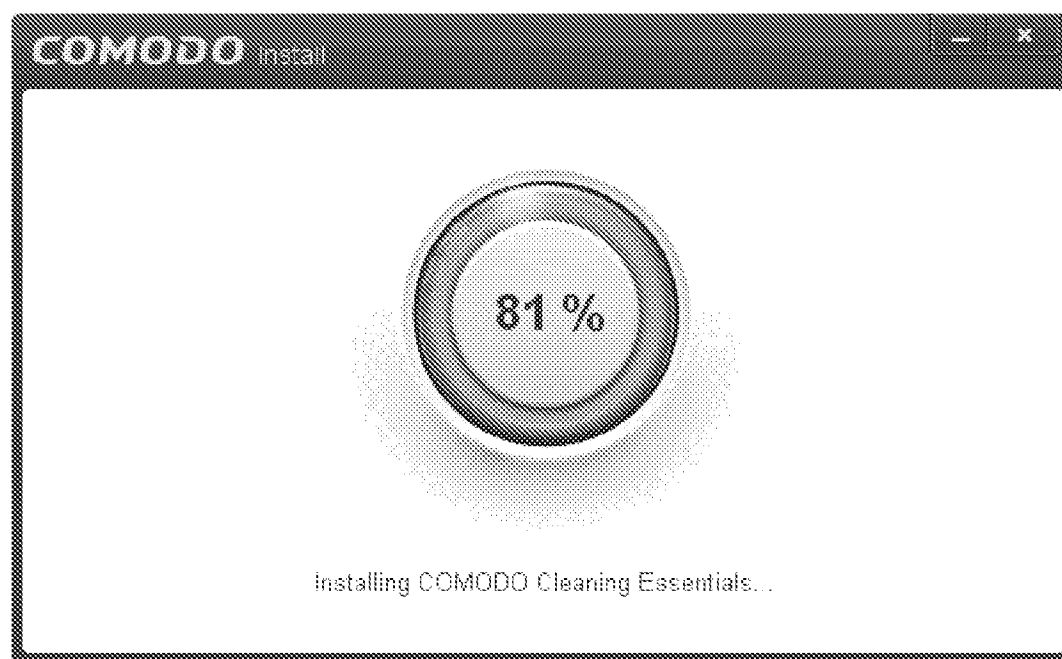
For more details on the features and usage of the application, please refer to the online guide at <http://help.comodo.com/topic-119-1-328-3516-introduction-to-Comodo-Cleaning-Essentials.html>.

Comodo Cleaning Essentials can be directly accessed from the CIS interface by clicking the 'Clean Endpoint' button in the 'Advanced Tasks' interface.

- Clicking the 'Clean Endpoint' for the first time, CIS will download and install Comodo Cleaning Essentials. Once installed, clicking this button in future will open the CCE interface.



- Read the license agreement by clicking 'View License Agreement' and click 'Agree and Install'. CIS will download and install the application.



On completion of installation, the Comodo Cleaning Essentials main interface will be opened.



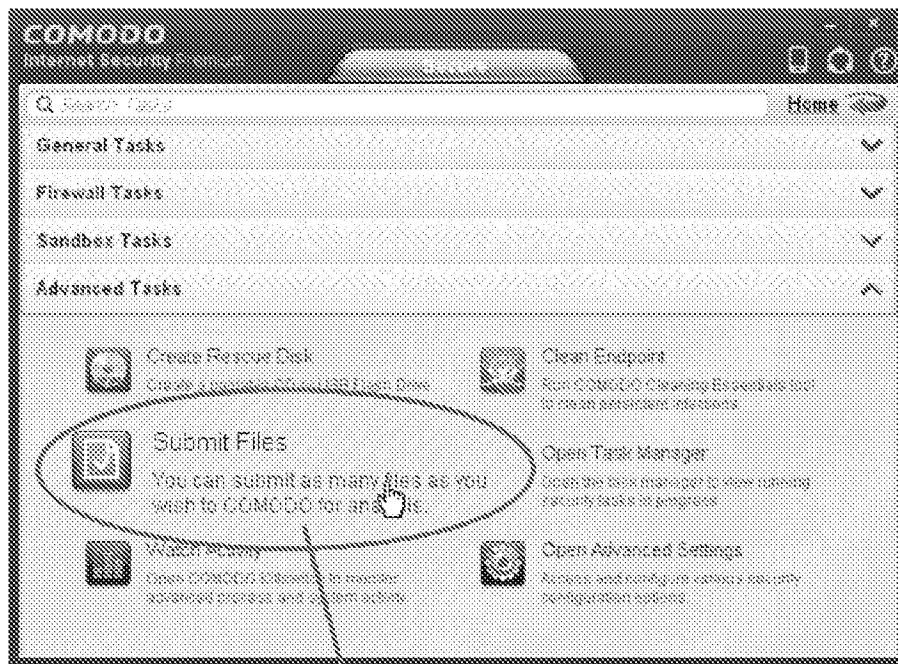
- Details of how to use KillSwitch to monitor and terminate unsafe process from the main interface can be found at <http://help.comodo.com/topic-119-1-328-3525-The-Main-Interface.html>
- On clicking the 'Clean Endpoint' button from next time onwards, Comodo Cleaning Essentials will be opened.

5.3. Submit Files

As the name suggests, the 'Submit Files' interface allows you to send as many files as you wish to Comodo for analysis. Files which CIS classifies as 'Unknown' or 'Unrecognized' are not in the Comodo safe list but have also not been identified as known malware. By sending these files to Comodo, you allow our team to analyze them and classify them as either 'Safe' or 'Malicious'. You can also submit files you suspect of being 'false positives' (those files that you feel CIS has incorrectly identified as malware). Subsequent to classification, they will be added to the white or black list accordingly.

Note: Unrecognized files can also be submitted from the 'Unrecognized Files' interface should you prefer.

To open the 'Submit Files' interface, click 'Tasks' on the home screen followed by 'Advanced Tasks' > 'Submit Files'

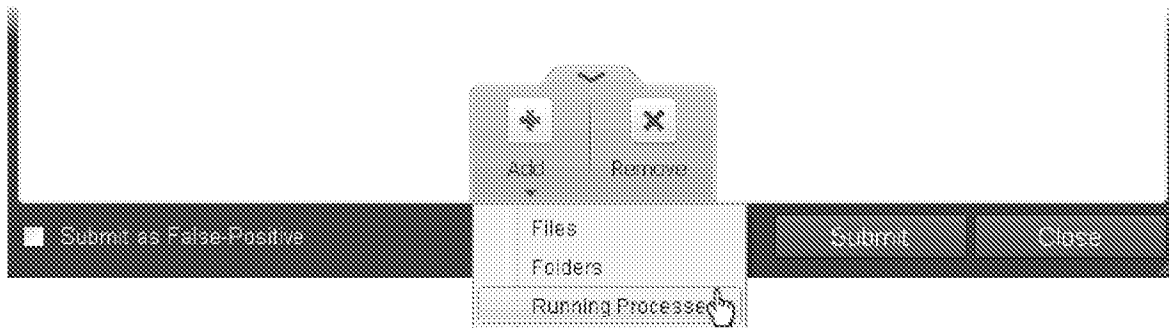


Clicking the handle at the bottom center of the panel opens the following options:

- Add - Allows you to add files to the 'Submit Files' list
- Remove - Allows you to remove files from the 'Submit Files' list

To add new file(s) to 'Submit Files' list

- Click the handle from the bottom center and choose 'Add'



You can add files to the Submit Files list by three ways:

- **Files** - Allows you to navigate to the file or executable of the program you wish to add.
- **Folders** - Allows you to navigate to the folder you wish to add. All the files in the folder will be added to the 'Trusted Files' list.
- **Running Processes** - Allows you to select a currently running process. On selecting a process, the parent application, which invoked the process will be added to 'Trusted Files' list.
- Repeat the process to add more files and to submit them at-once.

To remove the files from 'Submit Files' list

- Select the file from the list
- Click the handle from the bottom center and select Remove

After adding the files you want to submit, click 'Submit' button. If you want to submit the files as False Positives to Comodo, select the 'Submit as False-Positive check' box.

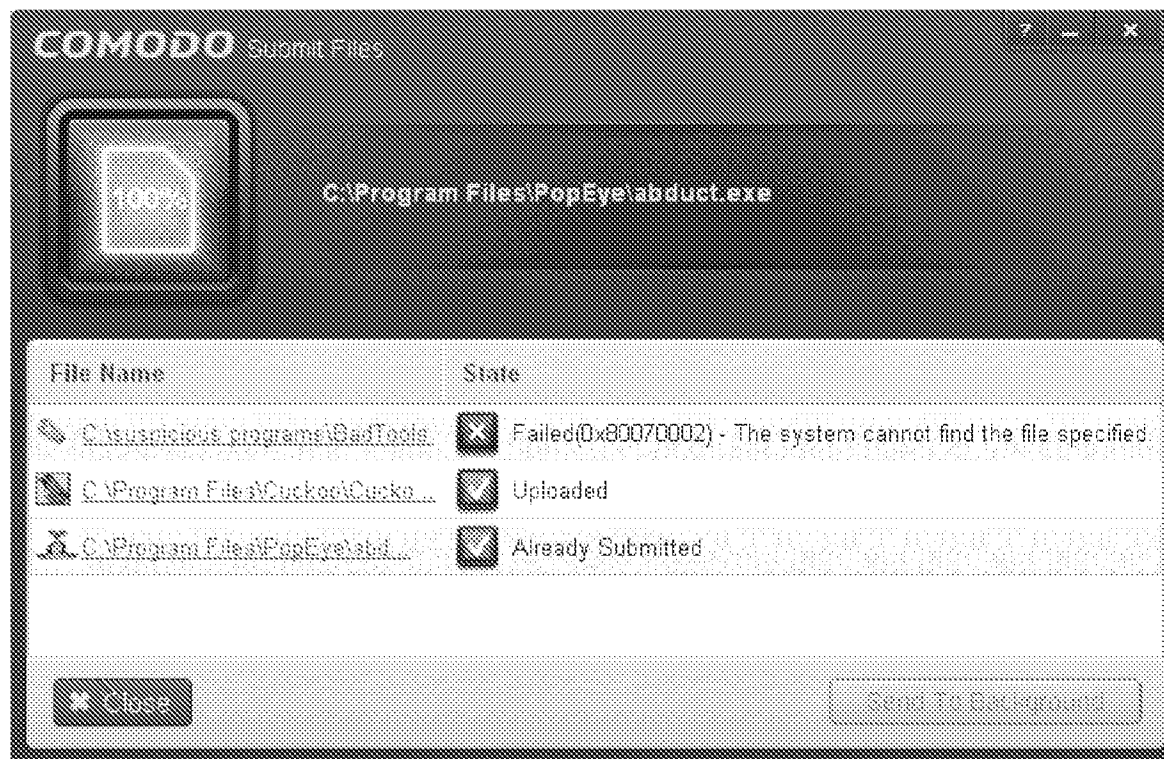
The files will be submitted and the progress will be displayed



You can stop, pause/resume or send the submission process to background by clicking respective buttons.

When a file is first submitted, Comodo's online file look-up service will check whether the file is already queued for analysis by

our technicians. The results screen displays these results on completion.



- 'Uploaded' - The file's signature was not found in the list of files that are waiting to be tested and was therefore uploaded from your machine to our research labs.
- 'Already submitted' - The file has *already* been submitted to our labs by another CIS user and was not uploaded from your machine at this time.

Comodo will analyze all submitted files. If they are found to be trustworthy, they will be added to the Comodo safe list (i.e. white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (i.e. black-listed).

The list of files submitted from your computer can be viewed from the Submitted Files interface.

5.4. Identify and Kill Unsafe Running Processes

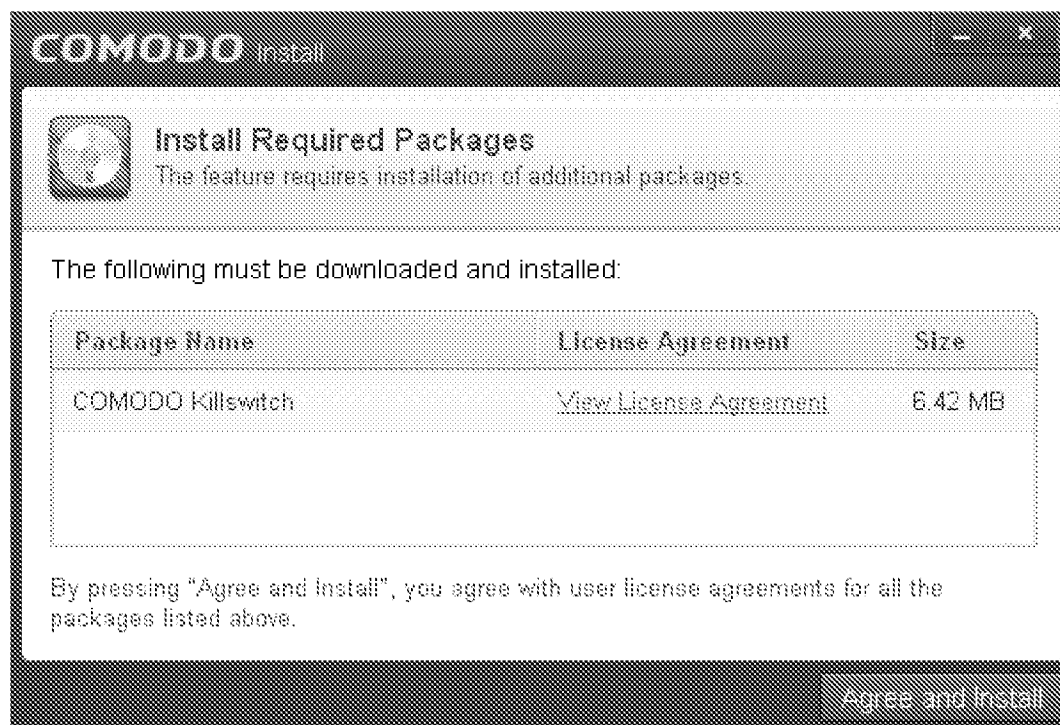
Comodo KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes that are running on their system. Apart from offering unparalleled insight and control over computer processes, KillSwitch provides you with yet another powerful layer of protection for Windows computers.

KillSwitch can show ALL running processes - exposing even those that were invisible or very deeply hidden. It allows you to identify which of those running processes are unsafe and to shut them all down with a single click. You can also use Killswitch to trace back to the malware that generated the process.

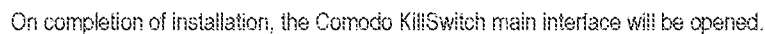
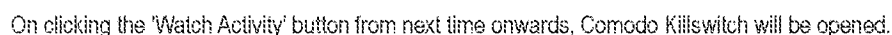
Comodo KillSwitch can be directly accessed from the CIS interface by clicking the 'Watch Activity' button in the 'Advanced Tasks' interface.



- Killswitch is a component of Comodo Cleaning Essentials. If you have already installed Comodo Cleaning Essentials by clicking 'Clean Endpoint' from the 'Advanced Tasks' interface, clicking the 'Watch Activity' will open the KillSwitch interface directly. Refer to the section Remove Deeply Hidden Malware for more details on installing Cleaning Essentials.
- Otherwise, on clicking the 'Watch Activity' for the first time, CIS will download and install Comodo Killswitch. Once installed, clicking this button in future will open the Killswitch interface.



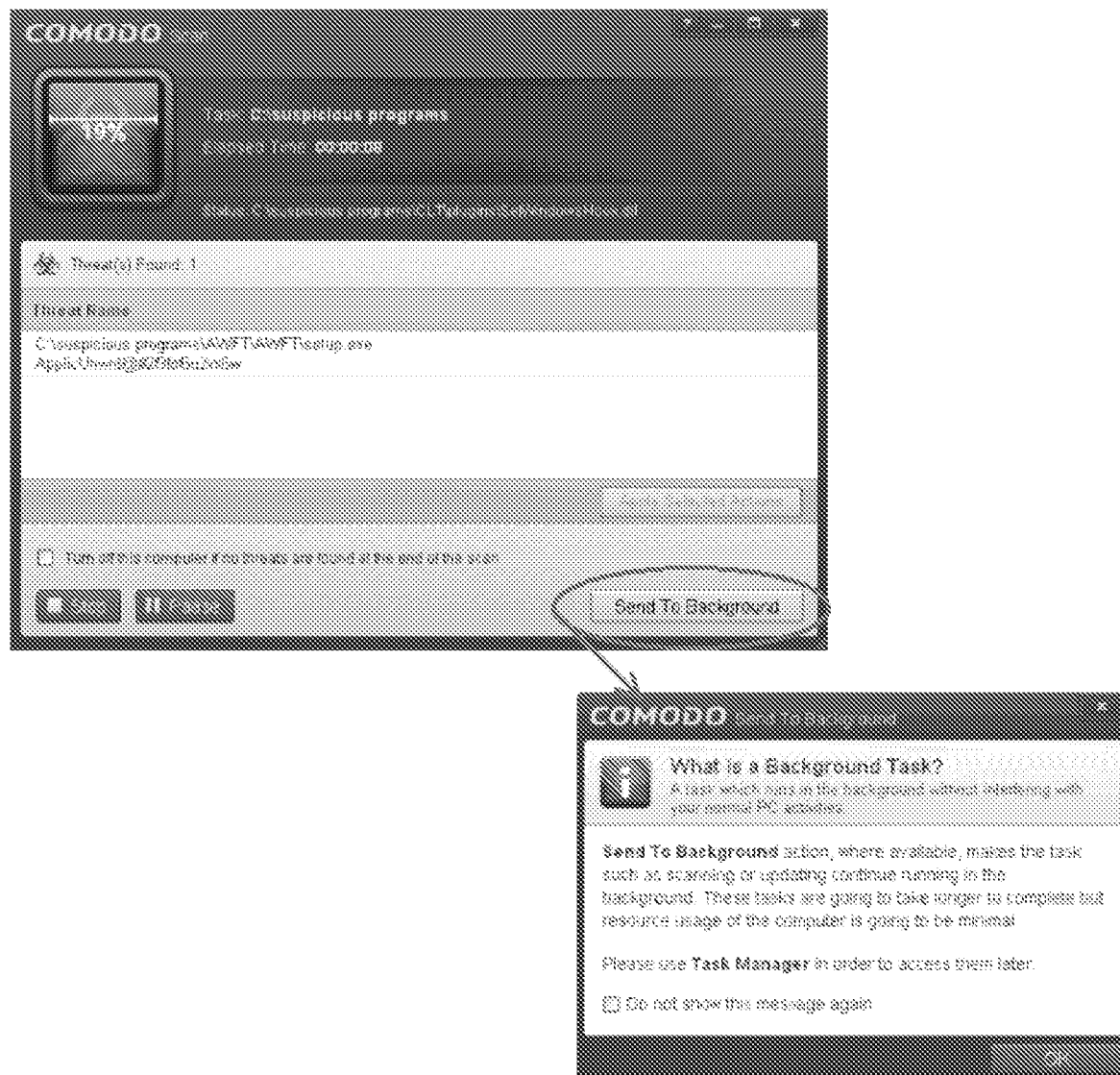
- Read the license agreement by clicking 'View License Agreement' and click 'Agree and Install'. CIS will download and install the application.



- IBM - Ex. 1002-Part 1 of 10, Page 554
IPR2025-00379 (IBM v. Croga)

5.5. Manage CIS Tasks

Comodo Internet Security has the ability to concurrently run several tasks like on-demand or scheduled scans, virus signature database updates and so on. The tasks that are currently run, can be sent to background from the progress interface, by clicking Send to Background as shown in the example below.



These tasks can be managed, through the Task manager interface that can be accessed at anytime by clicking Open Task Manager from the 'Advanced Tasks' interface.



Tip: The Task Manager can also be opened by clicking on the center tab in the Status row of the widget, that displays the number of tasks that are currently running.

The Task Manager window displays a list of background tasks that are currently running with the details of time elapsed on each task, status and priority.

From the Task Manager interface, you can:

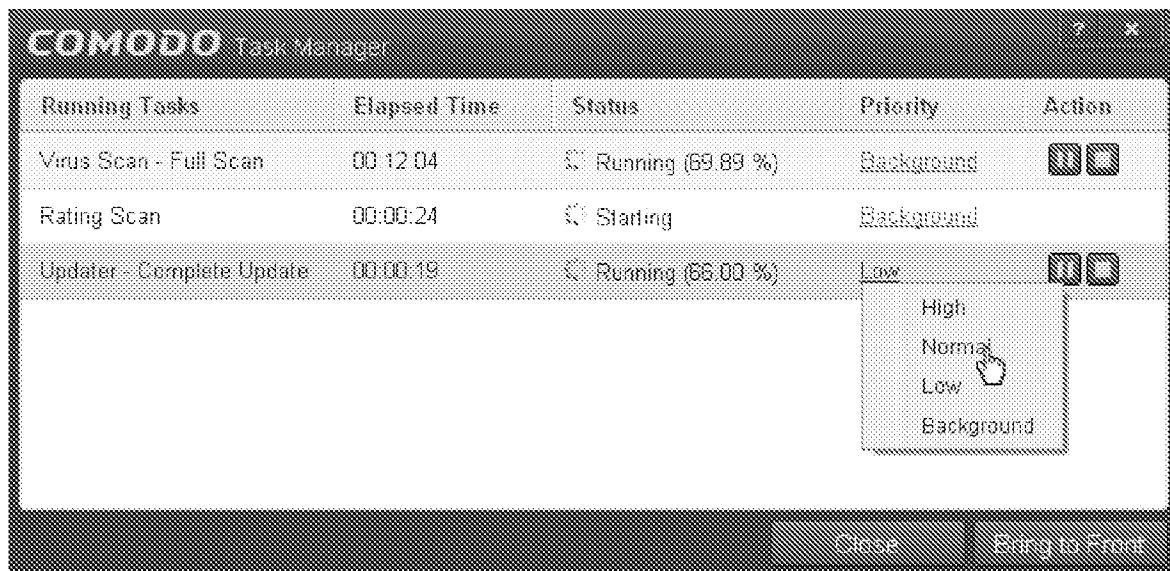
- Reassign priorities to the tasks
- Pause/Resume or Stop a running task
- Bring a selected task to foreground

Reassigning Priorities for a task:

The Priority column in the Task Manager interface displays the current priority assigned for each task.

To change the priority for a task

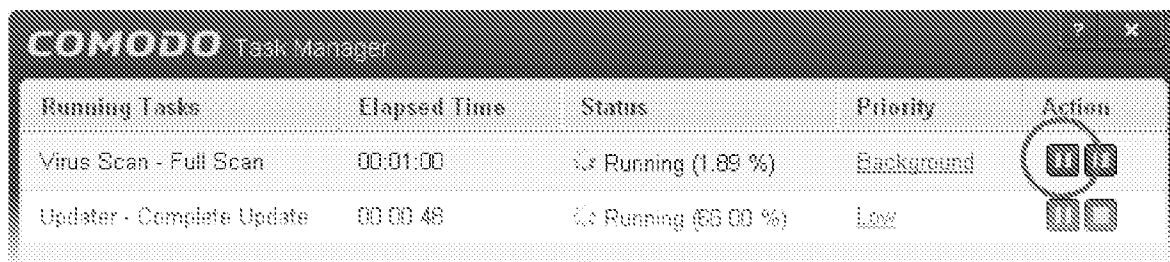
- Click on the current priority and select the priority you want to assign from the options.



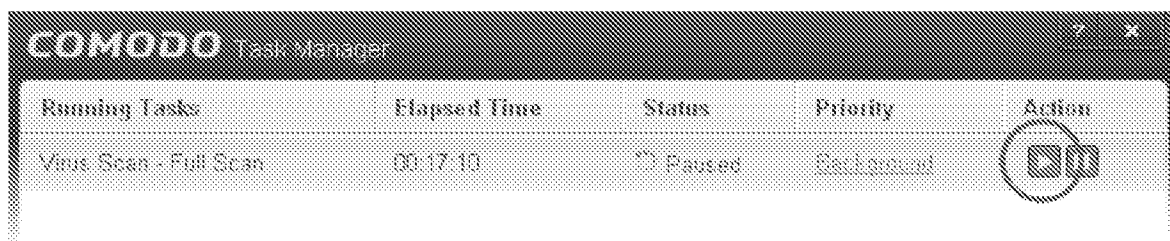
Pausing/Resuming or Stopping running tasks

The Action column displays the Pause/Resume and Stop buttons

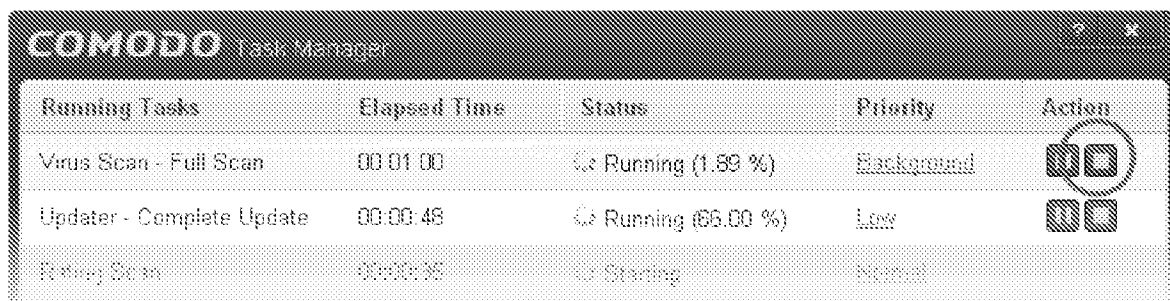
- To pause a running task, click the Pause button



- To resume a paused task, click the Resume button



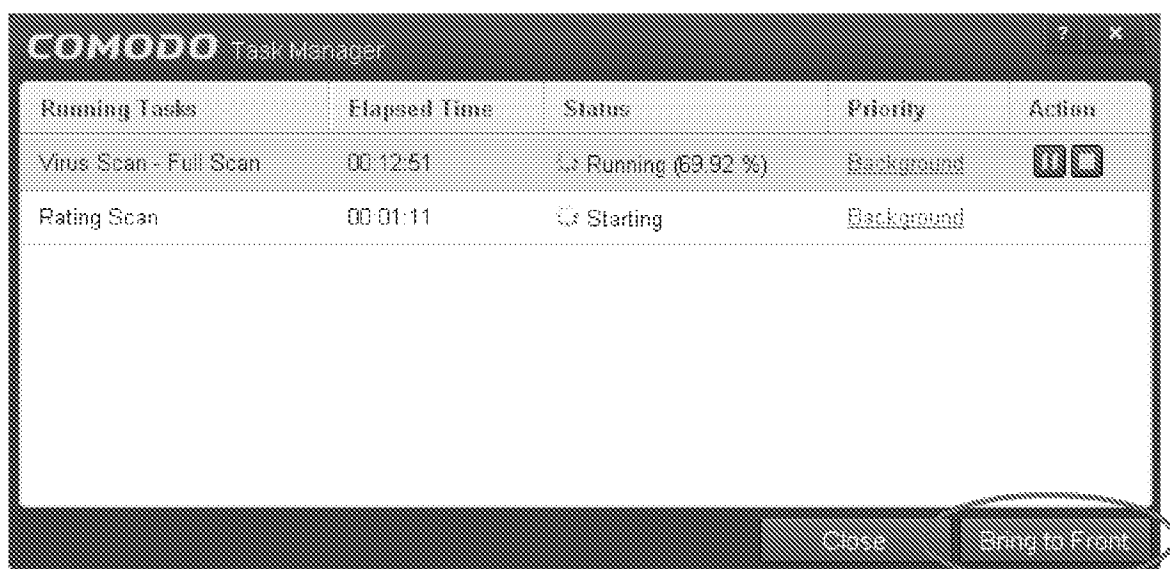
- To stop a running task, click the stop button



Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:01:00	Running (1.89 %)	Background	
Updater - Complete Update	00:00:48	Running (66.00 %)	Low	
Rating Scan	00:00:35	Starting	Normal	

Bringing a running task to foreground

- To view the progress of a background task, select the task and click 'Bring to Front'



Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:12:51	Running (69.92 %)	Background	
Rating Scan	00:01:11	Starting	Background	

Close
Bring to Front

The progress window of the task will be displayed. If the task is completed, the results window will be displayed.



6. Advanced Settings

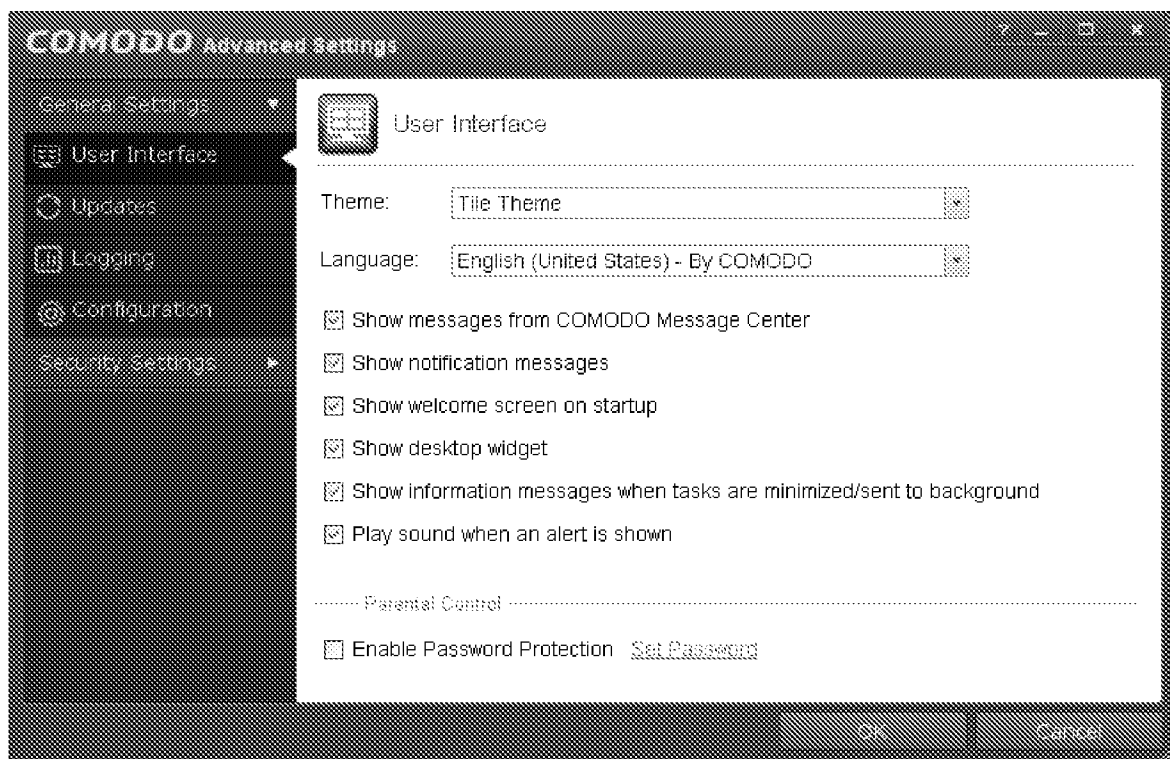
The 'Advanced Settings' area allows you to configure every aspect of the operation, behavior and appearance of Comodo Internet Security. The 'General Settings' section lets you specify top-level preferences regarding the interface, updates and event logging. The 'Security Settings' section lets advanced users delve into granular configuration of the Antivirus, Firewall, Defense+ and File Ratings modules. For example, the 'Security Settings' area allows you to create custom virus scan schedules, create virus exclusions, create Firewall and HIPS rules, modify sandbox behavior, define network zones and specify how the file rating system deals with trusted and untrusted files.

To open 'Advanced Settings':

- Click the 'Tasks' arrow if you are on the CIS home screen
- Click 'Advanced Tasks' then 'Open Advanced settings'



The 'Advanced Settings' panel will open:



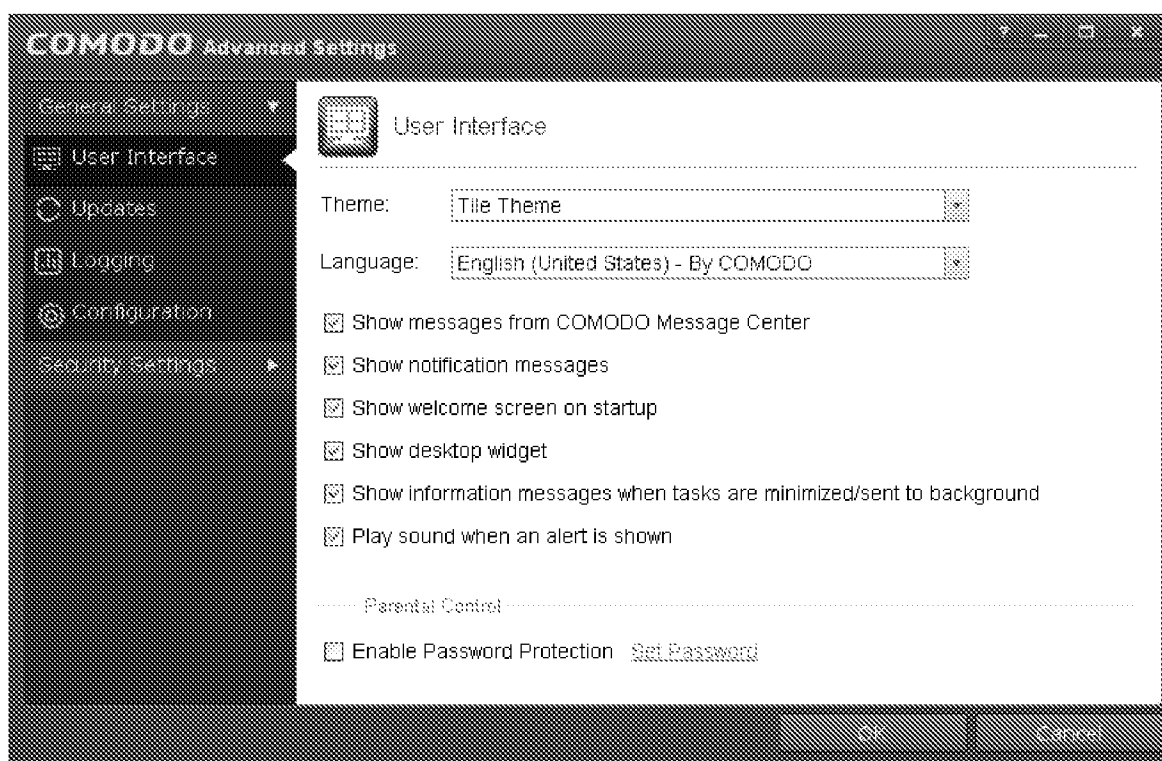
Please click the links below to find out more about each section:

- **General Settings** - Allows you to configure the appearance and behavior of the application

- Customize User Interface
 - Configure Program and database Updates
 - Log Settings
 - Manage CIS Configurations
- Security Settings - Advanced configuration of Antivirus, Firewall, Defense+ and File Ratings modules
 - Antivirus Settings
 - Defense+ Settings
 - Firewall Settings
 - File Ratings

6.1. General Settings

The 'General Settings' area enables you to customize the appearance and overall behavior of Comodo Internet Security. You can configure general properties like the interface language, notification messages, automatic updates, logging and more.



The category has the following settings:

- User Interface
- Updates
- Logging
- Configuration

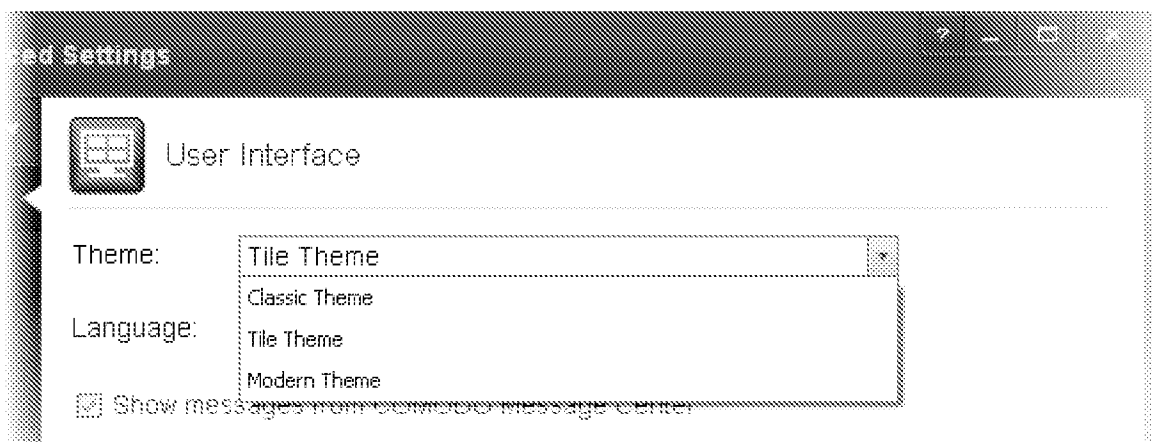
6.1.1. Customize User Interface

The 'User Interface' tab lets you choose the display theme, interface language and customize the look and feel of Comodo Internet Security according to your preferences. You can also configure how messages are displayed and enable password protection for your settings.

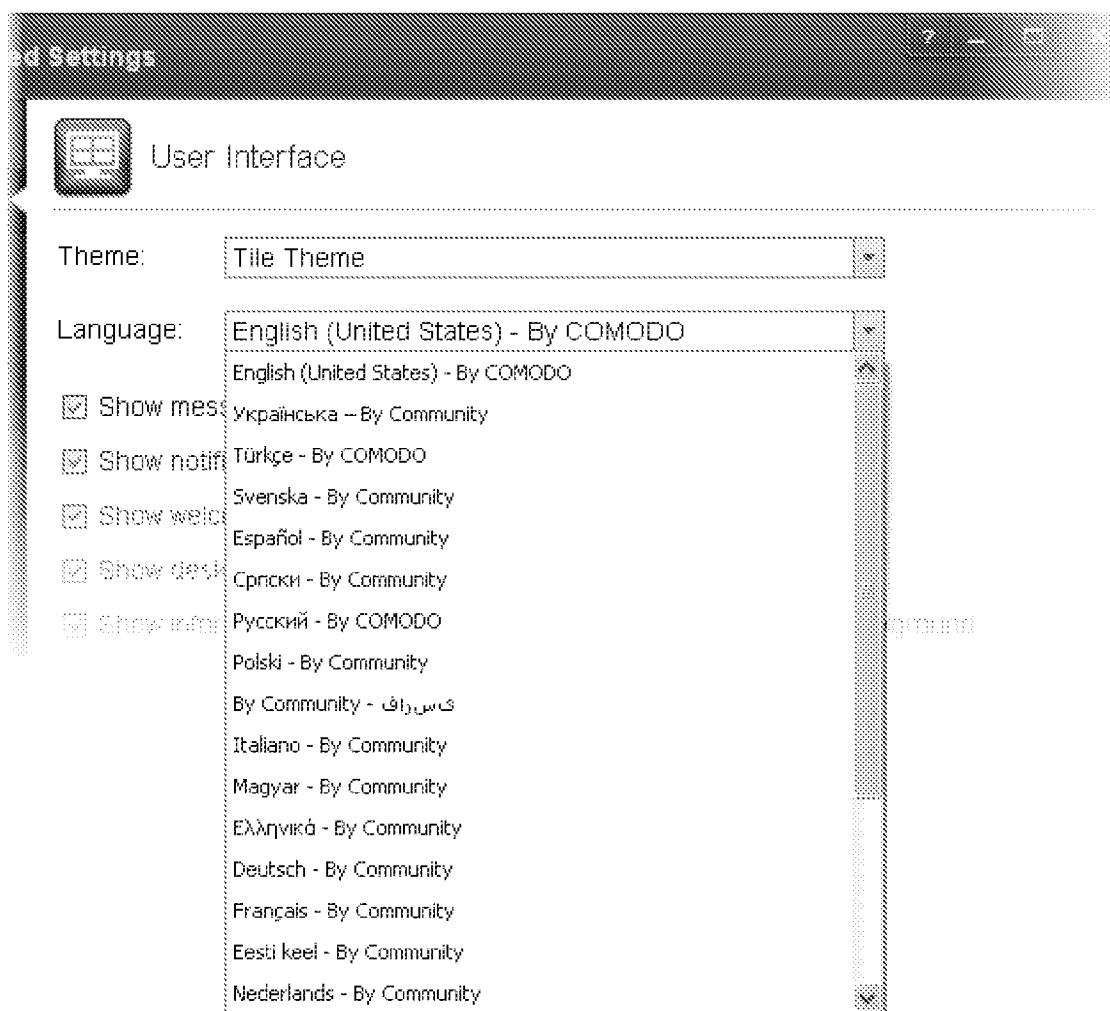


The User Interface Settings allows you configure the following:

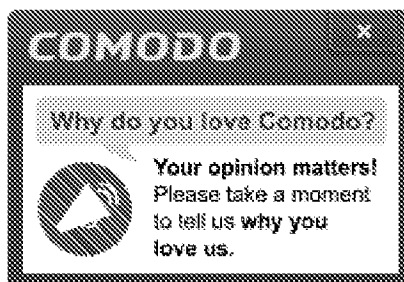
- Themes
- Language
- Show messages from COMODO Message Center
- Show notification messages
- Show Welcome screen on start up
- Show desktop widget
- Show information messages when tasks are minimized/sent to background
- Play sound when an alert is shown
- Enable Password Protection
- **Theme** - The 'Themes' drop-down allows you to choose the colors and appearance of the GUI as you prefer (**Default = Tile Theme**).



- **Language Settings** - Comodo Internet Security is available in multiple languages. You can switch between installed languages by selecting from the 'Language' drop-down menu (**Default = English (United States)**).



- **Show messages from COMODO Message Center** - If enabled, Comodo Message Center messages will periodically appear to keep you abreast of news in the Comodo world.



They contain news about product updates, occasional requests for feedback, info about other Comodo products you may be interested to try and other general news. (**Default = Enabled**).

- **Show notification messages** - These are the CIS system notices that appear in the bottom right hand corner of your screen (just above the tray icons) and inform you about the actions that CIS is taking and any CIS status updates. For example 'Comodo Firewall is learning' or 'Defense+ is learning' are generated when these modules are learning the activity of previously unknown components of trusted applications. Antivirus notifications will also be displayed if you have selected 'Do not show antivirus alerts' check box in Antivirus > Real-time Scan settings screen. Clear this check box if you do not want to see these system messages (**Default = Enabled**).
- **Show Welcome Screen on start up** - If enabled, CIS will display a welcome screen when the application first starts.

(Default = Enabled):



Tip: You can disable the Welcome Screen by selecting the checkbox 'Do not show this window again' in the window itself.

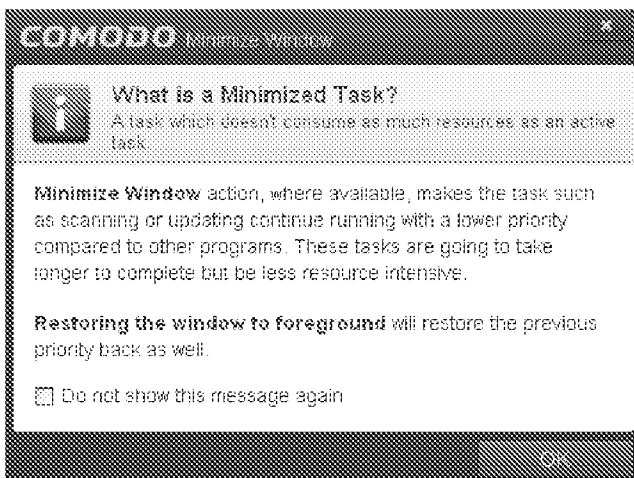
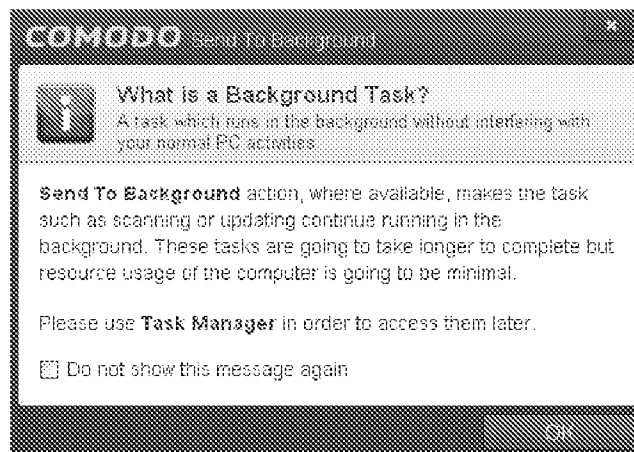
- **Show desktop widget** - The CIS desktop widget displays at-a-glance information about CIS security status, speed of outgoing and incoming traffic, number of background tasks and links to social networking sites.



The widget also acts as a shortcut to open the CIS main interface, the Task Manager, your browsers and so on. If you do not want the widget to be displayed on your desktop, clear this checkbox. (Default = Enabled).

Tip: You can disable the widget from the CIS system tray icon. Right click on the CIS system tray icon and deselect the 'Show' option that appears on hovering the mouse cursor on 'Widget'.

- **Show information messages when tasks are minimized/sent to background** - CIS displays messages explaining the effects of minimizing or moving a running task like an AV scan to the background.



If you do not want these messages to be displayed, clear this check-box (**Default = Enabled**).

Tip: You can also disable these messages in the message window itself by selecting 'Do not show this message again'

- **Play sound when an alert is shown** - CIS generates a chime whenever it raises a security alert to grab your attention. If you do not want the sound to be generated, clear this check box (**Default = Enabled**).
- **Enable Password Protection** - Enforces password protection for all important configuration sections and wizards within the interface. If you enable this feature, you must first specify and confirm a password by clicking the 'Set Password' link. You will then be asked for this password whenever you try to access important configuration areas (for example, all sections in the General Tasks, Firewall Tasks, Sandbox Tasks and Advanced Tasks will request the password).

This setting is of particular value to parents, network administrators and administrators of shared computers to prevent other users from modifying critical settings and exposing the machine to threats (**Default = Disabled**).

To enable password protection

- Select the 'Enable Password Protection' check-box then click 'Set Password'. The Change password dialog will appear.

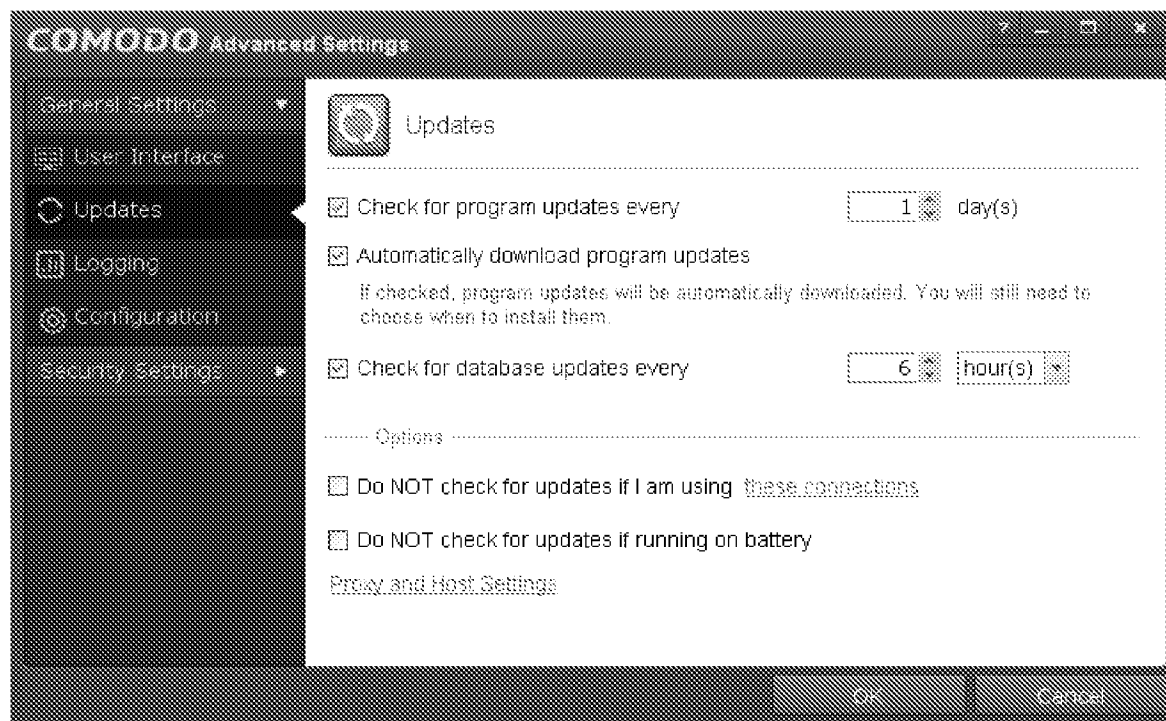


- Enter and confirm your password then click OK. Make sure to create a strong password containing a mixture of uppercase and lowercase characters, numbers and symbols so that it cannot be easily guessed by others.

6.1.2. Configure Program and Virus Database Updates

The 'Updates' area allows you to configure settings that govern CIS program and virus database updates.

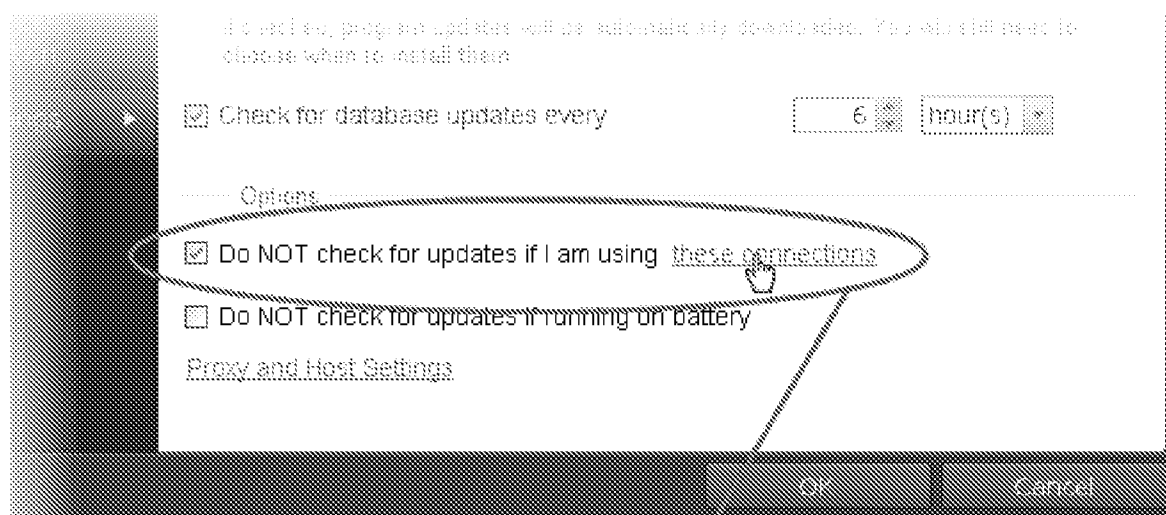
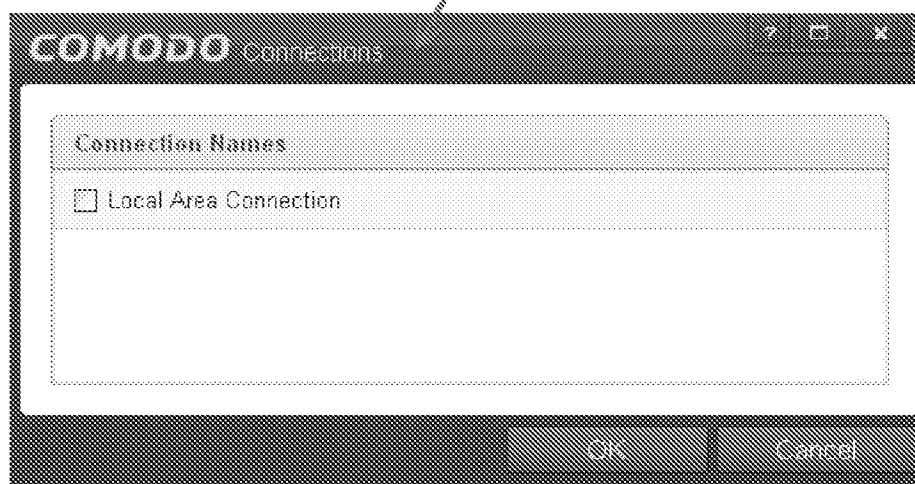
This screen can be accessed by clicking 'Updates' under the 'General Settings' section of 'Advanced Settings':



- **Check program updates every NN day(s)** - Enables you to set the interval at which CIS will check for program updates. Select the interval in days from the drop-down combo box. **(Default = 1 day)**
- **Automatically download program updates** - Instructs CIS to automatically download program updates as soon as they are available. **(Default=Enabled)**
- **Check for database updates every NN hour(s)/day(s)** - Enables you to set the interval at which CIS will check for virus signature database updates. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. **(Default and recommended = 6 hours)**
- **Do NOT check updates if am using these connections** - Enables you to restrict CIS from checking for updates if you use certain types of Internet connection. For example, you may not wish to check updates if using a wireless connection you know to be slow or not secure **(Default = Disabled)**

To do this:

- Select the 'Do NOT check updates if am using these connections' check-box
- Then click the 'these connections'. The connections dialog will appear with the list of connections you use.

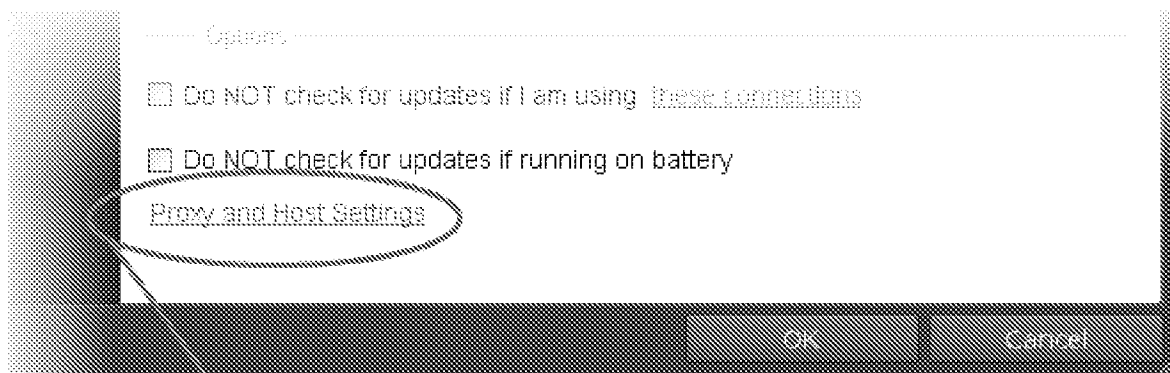


- Select the connection through which you do not want CIS to check for updates and click OK.
- **Do NOT check for updates if running on battery** - If enabled, CIS will not download updates if it detects your computer is running from battery power. This is intended to extend battery lifetime on laptops. **(Default = Enabled)**
- **Proxy and Host Settings** - Allows you to select the host from which updates are downloaded. By default, CIS will directly download updates from Comodo servers. However, advanced users and network admins may wish to first download updates to a proxy/staging server and have individual CIS installations collect the updates from there. The 'Proxy and Host Settings' interface allows you to point CIS at this proxy/staging server. This helps conserve overall bandwidth consumption and accelerates the update process when large number of endpoints are involved.

Note: You first need to install Comodo Offline Updater in order to download updates to your proxy server. This can be downloaded from <http://enterprise.comodo.com/security-solutions/endpoint-security/endpoint-security-manager/free-trial.php>

To configure updates via proxy server

- Click 'Proxy and Host Settings' at the bottom of the 'Updates' interface. The 'Proxy and Host Settings' interface will open.



- Select the 'Use Proxy' check-box.
- Enter the host name and port numbers. If the proxy server requires access credentials, select the 'Use Authentication' check-box and enter the login / password accordingly.
- You can add multiple servers from which updates are available. To do this, click the handle at the bottom center of the 'Servers' panel, click the 'Add' button then enter the host name in the 'Edit Property' dialog.

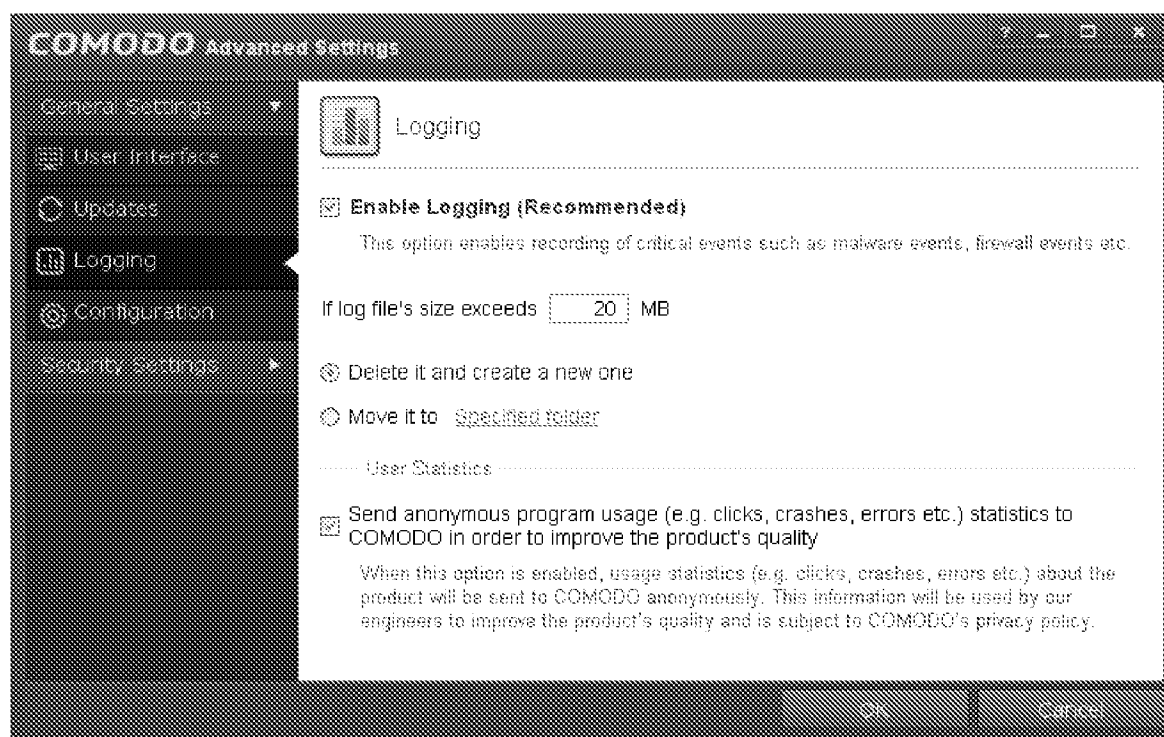


- If you specify multiple servers:
 - Activate or deactivate each update server using the 'Active' toggle switch alongside it
 - Use the 'Move Up' and 'Move Down' buttons to specify the order in which each server should be consulted for updates. CIS will commence downloading from the first server that contains new updates.
- Click 'OK' for your settings to take effect.

6.1.3. Log Settings

By default, Comodo Internet Security maintains detailed logs of all Antivirus, Firewall and Defense+ events. Logs are also created for 'Alerts Displayed', 'Tasks Launched' and 'Configuration Changes'.

- This 'Logging' interface allows you to specify whether you want to enable logging; the maximum size of the log file and how CIS should react if the maximum file size is exceeded.
- Note: If you wish to actually view, manage and export logs, then you need to open the 'View Logs' interface under 'General Settings' (Tasks > General Settings > View Logs)

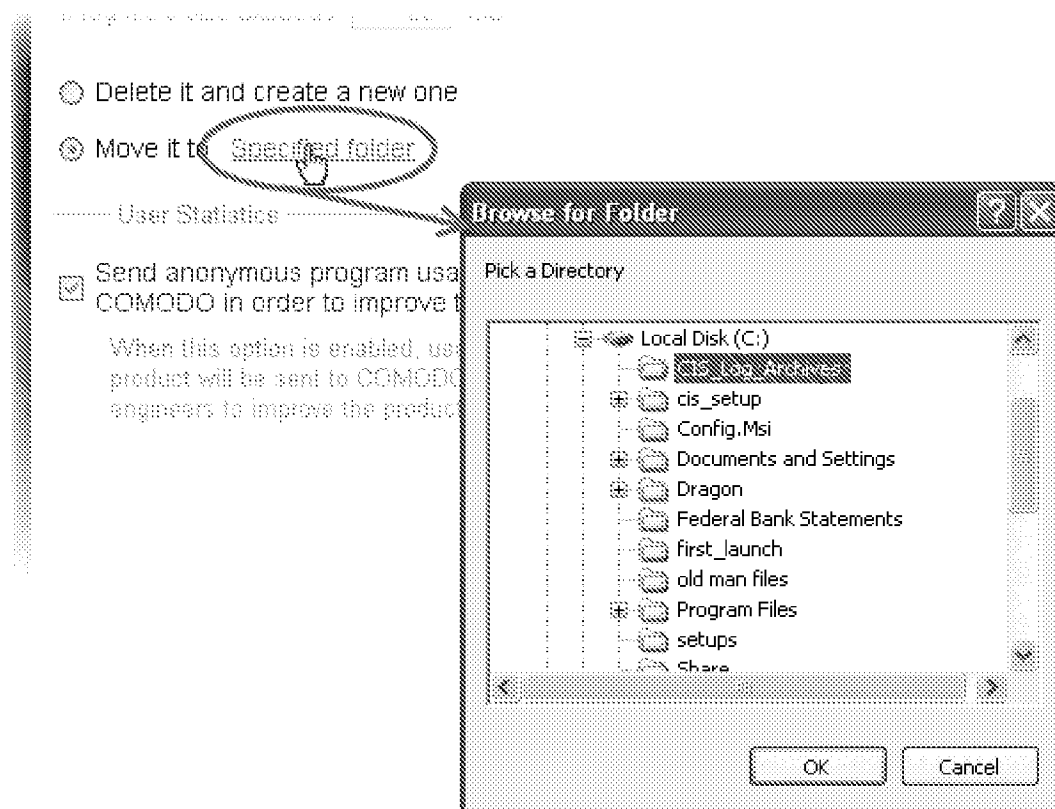


- **Enable Logging** - CIS logs events only if this setting is enabled. (**Default = Enabled**)
- **If the log file's size exceeds (Mb(s))** - Enables you to specify behavior when the log file reaches a certain size. You can decide on whether to maintain log files of larger sizes or to discard them depending on your future reference needs and the storage capacity of your hard drive.
 - Specify the maximum limit for the log file size (in MB) in the text box beside 'If the log file's size exceeds'

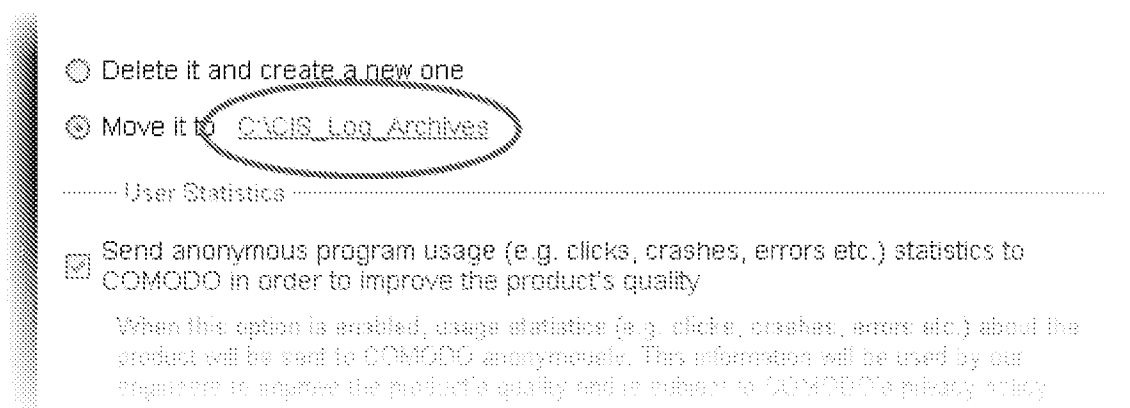
(MB)' (Default = 20MB).

If you want to discard the log file if it reaches the maximum size, select **'Delete it and create a new one'**. Once the log file reaches the specified maximum size, it will be automatically deleted from your system and a new log file will be created with the log of events occurring from that instant **(Default = Enabled)**.

If you want to save the log file even if it reaches the maximum size, select **'Move it to'** and select a destination folder for the log file **(Default = Disabled)**.



The selected folder path will appear beside 'Move it to'.



Once the log file reaches the maximum size, it will be automatically moved to the selected folder and a new log file will be created with the log of events occurring from that instant.

- **Send anonymous program usage (e.g. clicks, crashes, errors etc) statistics to COMODO in order to improve the product's quality** - Comodo collects the usage details from millions of CIS users to analyze their usage patterns for the continual enhancement of the product. Your CIS installation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy

is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. **(Default = Enabled)**.

6.1.4. Manage CIS Configurations

Comodo Internet Security allows you to maintain, save and export multiple configurations of your security settings as configuration profiles. This is especially useful if you are a network administrator looking to roll out a standard security configuration across multiple computers. If you are upgrading your system and there is a need to uninstall and re-install Comodo Internet Security then it can be great time-saver to export your configuration settings beforehand. After re-installation, you can import your previous settings and avoid having to configure everything over again.

Note: Any changes you make over time will be automatically stored in the currently active profile. If you want to export your current settings then export the 'Active' profile.

This panel can be accessed by clicking 'Configuration' under the 'General Settings' section of 'Advanced Settings':



The currently active configuration is indicated under the 'Active' column. Click the following links for more details:

- [Comodo Preset Configurations](#)
- [Importing/Exporting and Managing Personal Configurations](#)

6.1.4.1. Comodo Preset Configurations

By default, CIS is installed with 'COMODO - Internet Security' as the active configuration. Reminder - the active profile is, in effect, your current CIS settings. Any changes you make to settings are recorded in the active profile. You can change the active profile at any time from the 'Configuration' panel.

Click the links below to find out more details on each configuration:

- [COMODO - Internet Security](#)
- [COMODO - Proactive Security](#)
- [COMODO - Firewall Security](#)

COMODO - Internet Security - This configuration is activated by default, when both Antivirus and Firewall components are installed (i.e. the complete installation). The firewall is always set to 'Safe mode' but, according to the results of the malware scan performed during the setup process, the HIPS setting may vary. If no malware is found, HIPS is set to Clean PC mode. Otherwise, the default is 'Safe Mode'.

- Behavior Blocker is Enabled.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- Defense+ is tuned to prevent infection of the system.

If you wish to switch to Internet Security option, you can select the option from the 'Configuration' panel.

COMODO - Proactive Security - This configuration turns CIS into the ultimate protection machine. All possible protections are activated and all critical COM interfaces and files are protected. During the setup, if only Comodo Firewall installation option is selected, the next screen allows users to select this configuration as default CIS configuration. If selected, Firewall is always set to Safe mode. But according to the malware scanning results performed during the setup process, if no malware is found, HIPS is set to Clean PC mode. Otherwise, the default is Safe mode.

If you wish to switch to Proactive Security option, you can select the option from the 'Configuration' panel.

COMODO - Firewall Security - This configuration is activated when the user chooses to install Firewall only and selects optimum protection settings for HIPS. Firewall is always set to Safe mode. But according to the malware scanning results performed during the setup process, if no malware is found, HIPS is set to Clean PC mode. Otherwise, the default is Safe mode.

- Behavior Blocker is disabled.
- Computer Monitor and Keyboard are NOT monitored.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- HIPS is tuned to prevent infection of the system and detect Internet access request leaks even if it is infected.

If you wish to switch to Firewall Security option, you can select the option from the 'Configuration' panel.

6.1.4.2. Importing/Exporting and Managing Personal Configurations

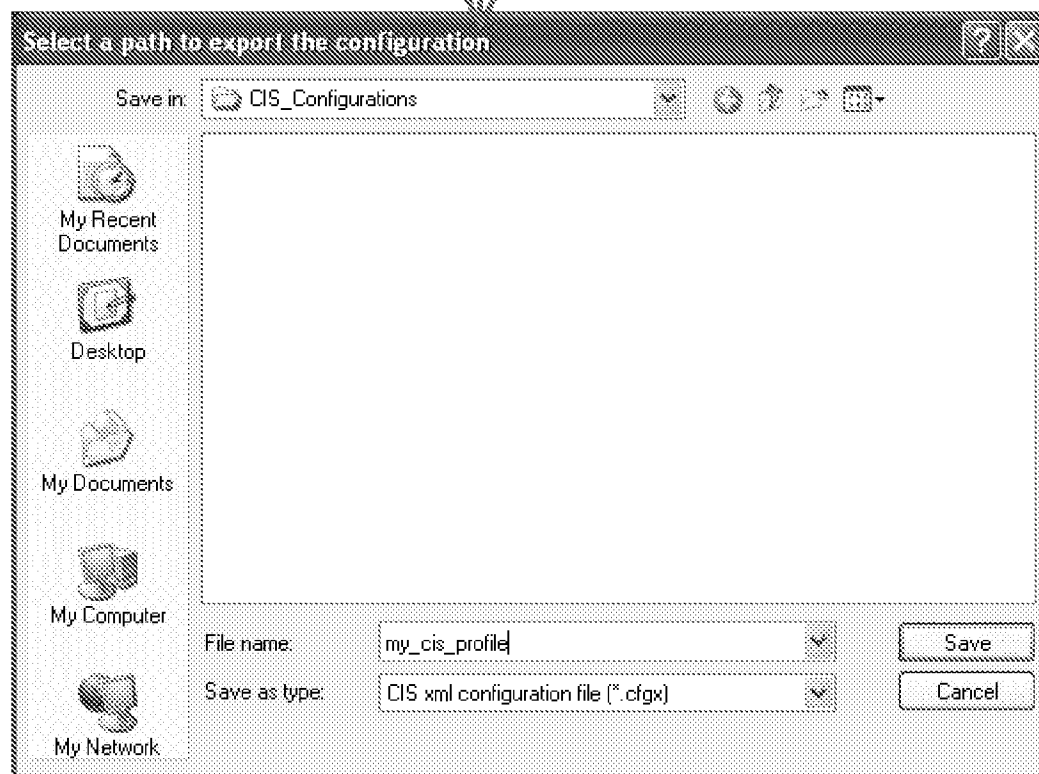
The CIS configurations can be exported/imported, activated and managed through the Configuration panel accessible by clicking 'Configuration' tab under 'General Settings' in 'Advanced Settings' interface.

Click the area on which you would like more information:

- Export a stored configuration to a file
- Import a saved configuration from a file
- Select a different active configuration setting
- Delete a inactive configuration profile

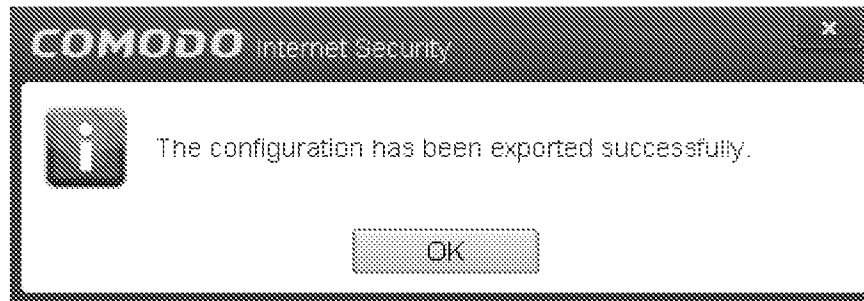
Exporting a stored configuration to a file

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface
2. Select the configuration, click the handle at the foot of the interface and choose 'Export'. The 'Select a path to export the configuration' dialog will open.



3. Navigate to the location where you want to save the configuration file, type a name (e.g., 'My CIS Profile') for the file to be saved in .cfgx format and click 'Save'.

A confirmation dialog will appear on successful export of the configuration.

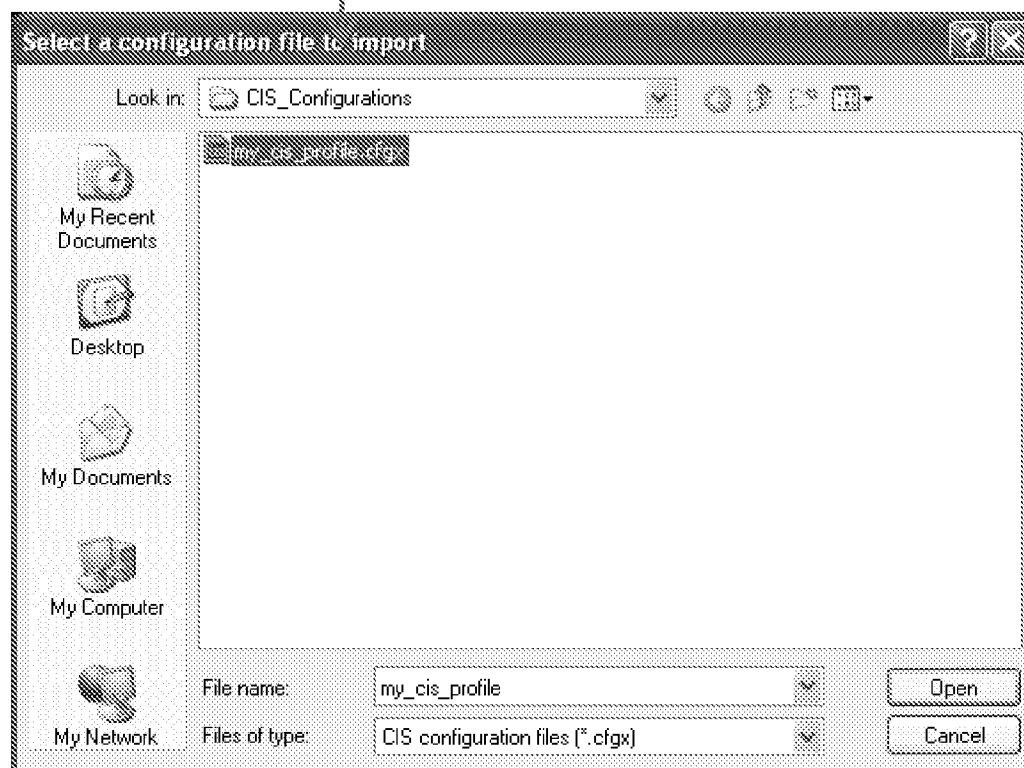


Importing a saved configuration from a file

Importing a configuration profile allows you to store any profile within Comodo Internet Security. Any profiles you import do not become active until you select them for use.

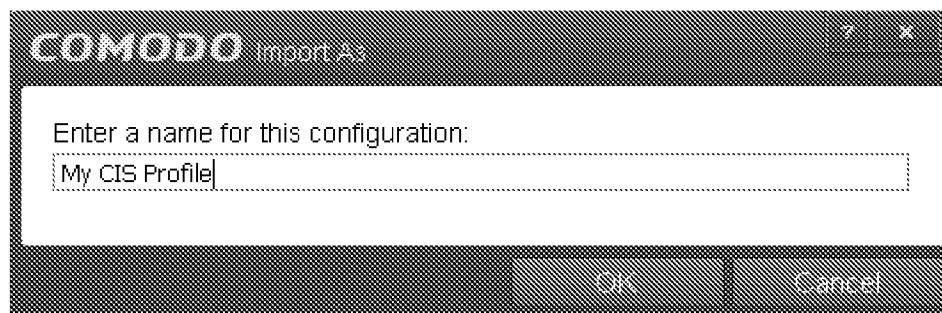
To import a profile

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface, click the handle at the foot of the interface and choose Import from the options.

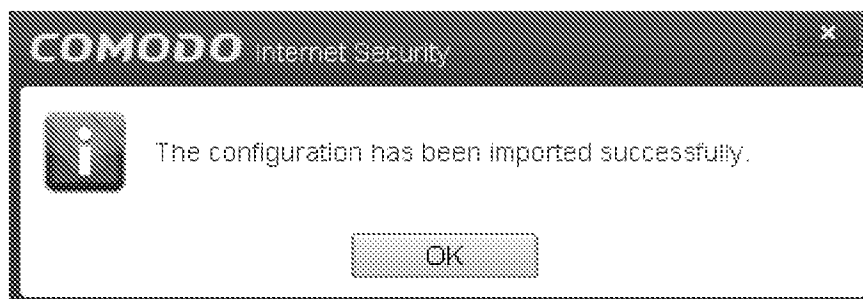


The 'Select a configuration file to import' dialog will open.

2. Navigate to the location of the saved profile and click 'Open'.
3. The 'Import As' dialog will appear. Enter a name for the profile you wish to import and click 'OK'.



A confirmation dialog will appear indicating the successful import of the profile.



Once imported, the configuration profile is available for deployment by selecting it.

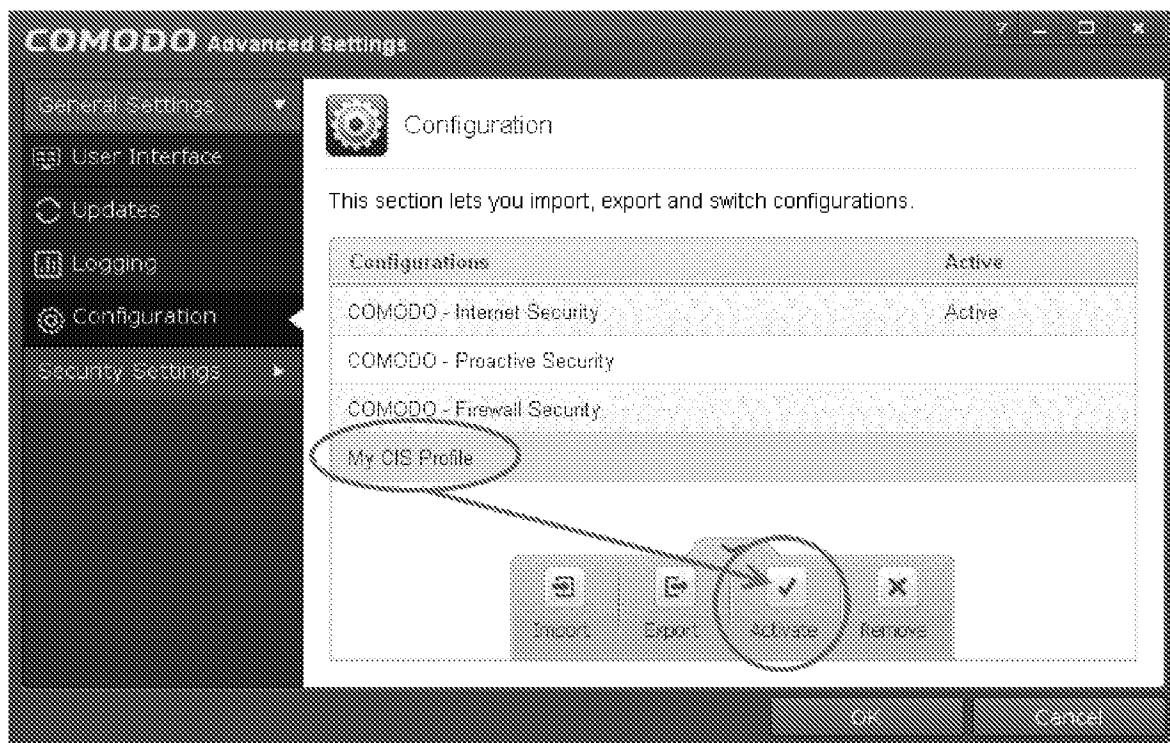


Selecting and Implementing a different configuration profile

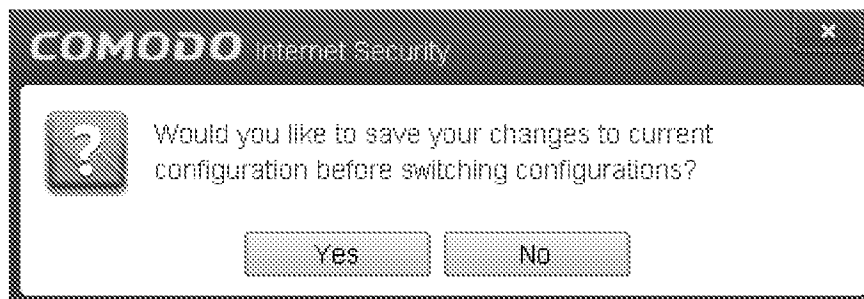
You can change the configuration profile active in CIS at any time from the 'Configurations' panel

To change the active configuration profile

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface
2. Select the configuration profile you want to activate, click the handle at the foot of the interface and choose Activate from the options.

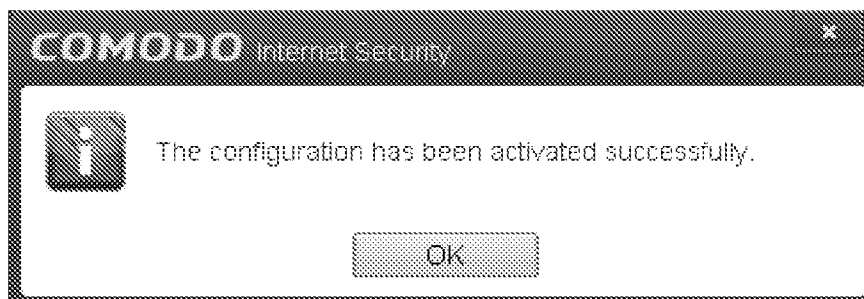


You will be prompted to save the changes to the settings in you current profile before the new profile is deployed.



- Click 'Yes' to save any setting changes in the current configuration, else click 'No'.

An activation confirmation dialog will be displayed. But the new profile will be implemented only on the next restart of the computer.



A 'Restart Computer' alert will appear at the bottom right of the screen.



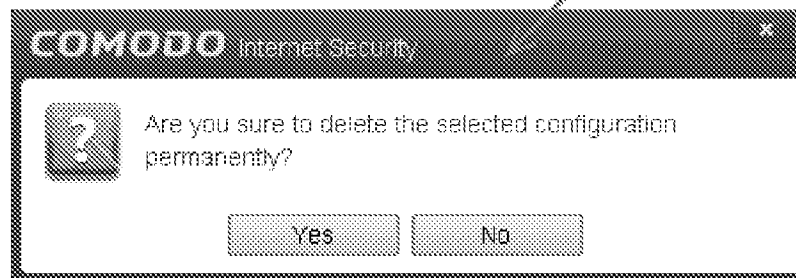
- If you want to restart the computer immediately, save all your work and click 'Restart Now'.
- If you want to restart the computer at a later time, select when you need to be reminded from the drop-down and click 'Postpone'.

Deleting an inactive configuration profile

You can remove any unwanted configuration profiles from the list of stored configuration profiles. You cannot delete the profile that Comodo Internet Security is currently using - only the inactive ones. For example if the COMODO - Internet Security is the active profile, you can only delete the inactive profiles, 'COMODO - Proactive Security', 'My_CIS_Configuration' and so on.

To remove an unwanted profile

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface
2. Select the configuration profile you want to delete, click the up arrow from the bottom center and choose 'Remove' from the options. A confirmation dialog will be displayed.

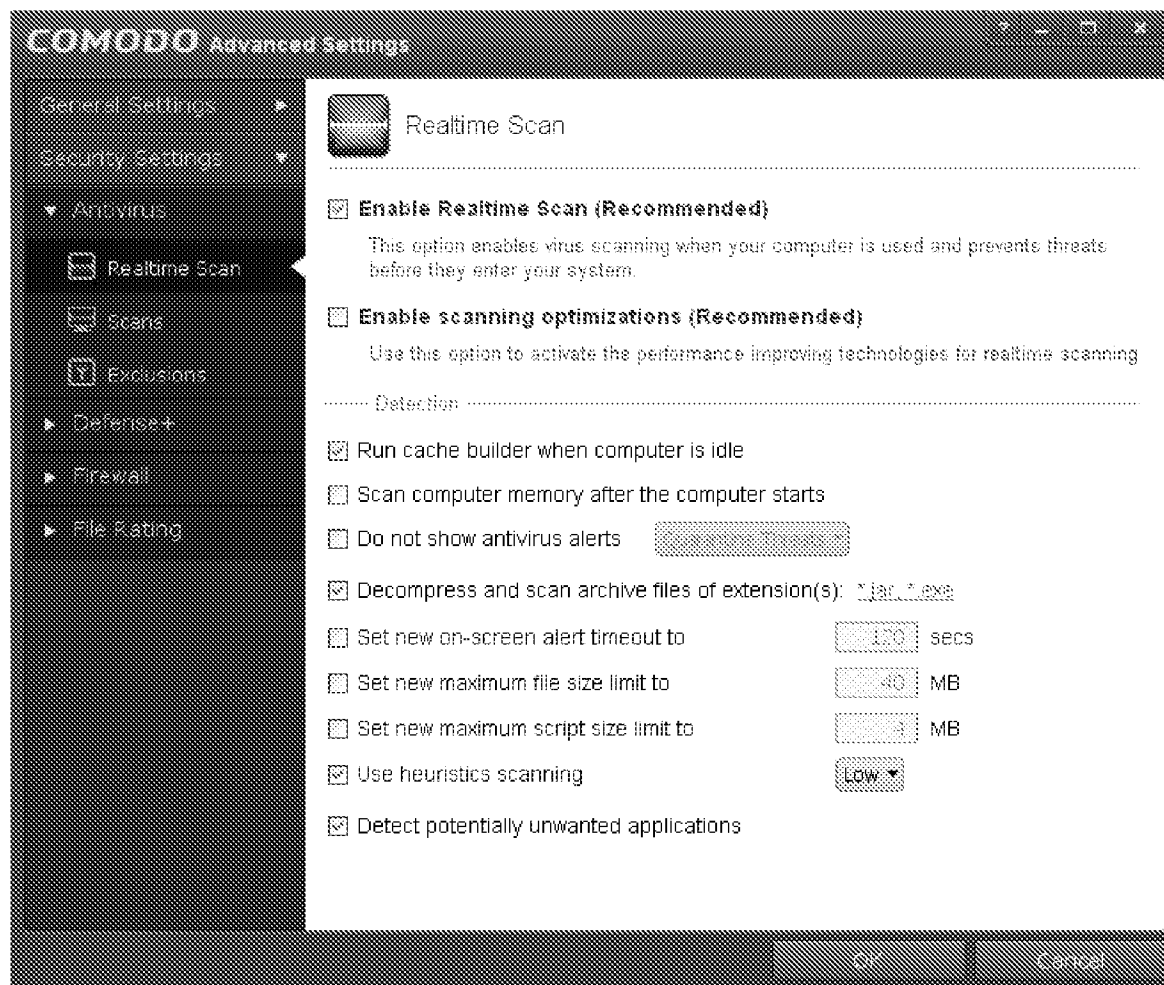


- Click 'Yes'. The configuration profile will be deleted from your computer.



6.2. Security Settings

The Security Settings area enables you to perform granular configuration of the Antivirus, Firewall, Defense+ and File ratings components of Comodo Internet Security. Although these settings play a large part in governing the level of security offered by the application, Comodo Internet Security 6.2 does ship with secure defaults for all major settings so provides 'out-of-the-box' protection for all users.



Click the following links to go straight to the topic that explains the respective settings screen:

- [Antivirus Settings](#)
 - [Real-time Scanner Settings](#)
 - [Custom Scan Settings](#)
 - [Exclusions](#)
- [Defense+ Settings](#)
 - [HIPS Behavior Settings](#)
 - [Active HIPS Rules](#)
 - [Predefined HIPS Rule Sets](#)
 - [Protected Objects](#)
 - [Behavior Blocker](#)
 - [Sandbox Settings](#)
- [Firewall Settings](#)
 - [Firewall Behavior Settings](#)

- Application Rules
- Global Rules
- Predefined Rule Sets
- Network Zones
- Port Sets
- Website Filtering
- Manage File Rating
 - File Rating Settings
 - Trusted Files
 - Unrecognized Files
 - Submitted Files
 - Trusted Vendors List

6.2.1. Antivirus Settings

The Antivirus Settings category has sub-sections that allow you to configure Real Time Scans (a.k.a 'On-Access' scanning), Custom Scans, and Exclusions (a list of the files you consider safe).

Click the following links to jump to each section:

- [Real Time Scan](#) - To set the parameters for on-access scanning;
- [Custom Scan](#) - To create scan profiles and run custom scans, schedule custom scans and set the parameters for custom scans;
- [Exclusions](#) - To see the list of ignored threats and to set the parameters for Exclusions.

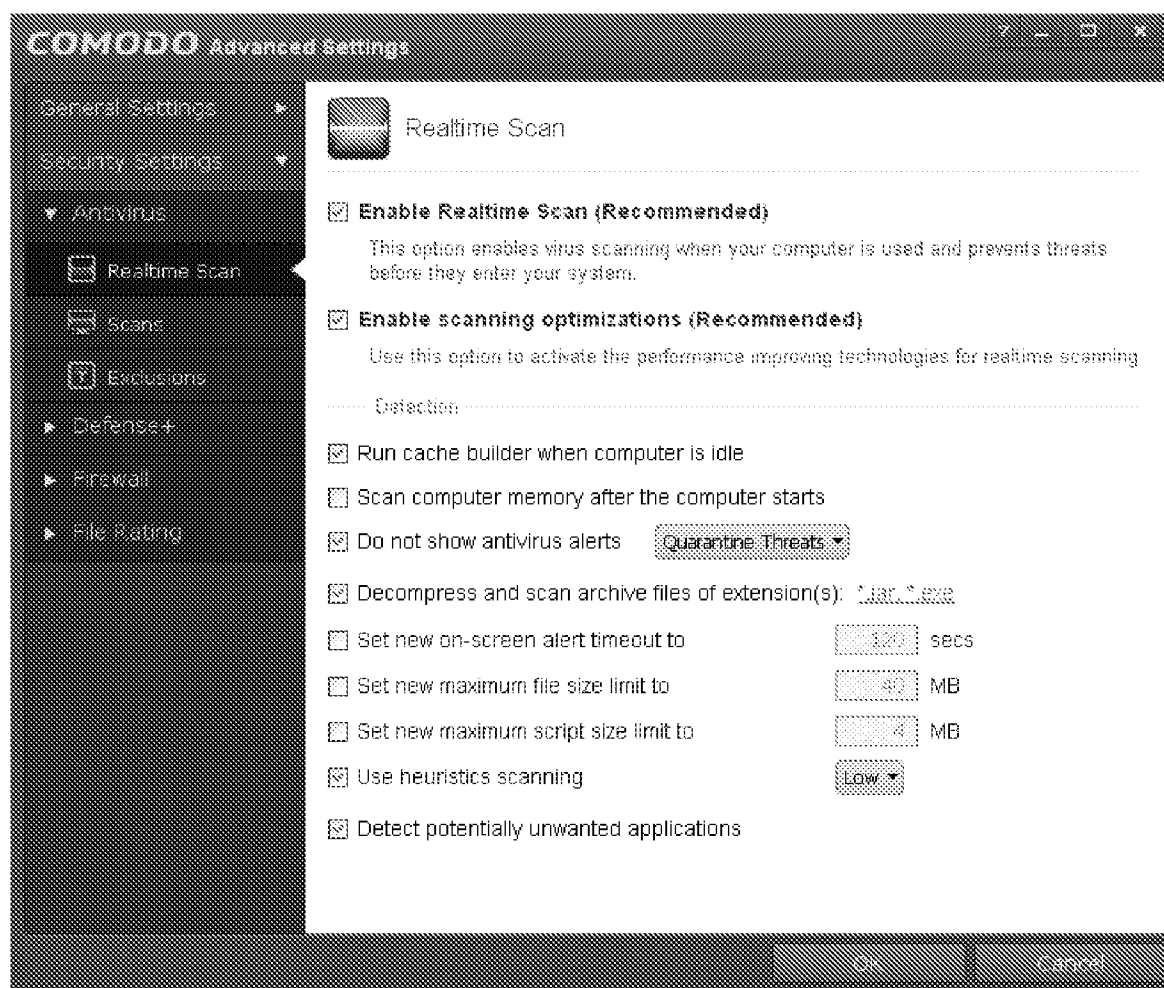
6.2.1.1. Real-time Scanner Settings

The real-time scanner (aka 'On-Access Scan') is always ON and checks files in real time when they are created, opened or copied (as soon as you interact with a file, Comodo Antivirus checks it). This instant detection of viruses assures you, the user, that your system is perpetually monitored for malware and enjoys the highest level of protection.

The real-time scanner also scans system memory on start. If you launch a program or file which creates destructive anomalies, then the scanner blocks it and alerts you immediately. Should you wish, however, you can specify that CIS does not show you alerts if viruses are found but automatically deals with them (choice of auto-quarantine or auto-block/delete). It is highly recommended that leave the Real Time Scanner enabled to ensure your system remains continually free of infection.

To open the Real Time Scan settings panel

- Click 'Tasks > Advanced Tasks > Open Advanced Settings > Security Settings > Antivirus > Realtime Scan':



- **Enable Realtime Scan** - Allows you to enable or disable real-time scanning. Comodo recommends to leave this option selected. (Default=Enabled)
- **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to reduce consumption of system resources and speed-up the scanning process (Default = Enabled)

Note: The above two settings can be modified from the 'Advanced View' of the Home screen by clicking the status link beside Antivirus. If you choose Disabled option, both 'Enable Realtime Scan' and 'Enable scanning optimizations' will be disabled. If you choose 'Stateful', both the settings will be enabled and on choosing 'On Access', only 'Enable Realtime Scan' will be enabled.

Detection Settings

- **Run cache builder when computer is idle** - CIS runs the Antivirus Cache Builder whenever the computer is idle, to boost the real-time scanning. If you do not want the Cache Builder to run, deselect this option (Default = Enabled).
- **Scan computer memory after the computer starts** - When this check box is selected, the Antivirus scans the system memory during system start-up (Default = Disabled)
- **Do not show antivirus alerts** - Allows you to configure whether or not to show antivirus alerts when malware is encountered. Choosing 'Do not show antivirus alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then you have a choice of default responses that CIS should automatically take - either 'Block Threats' or 'Quarantine Threats'. (Default = Enabled)
 - **Quarantine Threats** - Moves the detected threat(s) to quarantine for your later assessment and action. (Default)
 - **Block Threats** - Stops the application or file from execution, if a threat is detected in it.

Notes: If you deselect this option and thus enable alerts then your choice of quarantine/block is presented within the alert itself.

- **Decompress and scan archive files of extension(s)** - Comodo Antivirus can scan all types of archive files such as .jar, RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB if this option is left selected. You will be alerted to the presence of viruses in compressed files before you even open them. **(Default = Enabled)**

You can add the archive file types that should be decompressed and scanned by Comodo Antivirus.

- Click link on the file type displayed at the right end. The 'Manage Extensions' dialog will open.



You can use the search option to find a specific file extension in the list by clicking the search icon  at the far right in the column header.



- Enter the file extension to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the  icon in the search field to close the search option.

Adding a New File Type

- To add a file type, click the up arrow at the bottom center and click 'Add'.



- Enter the extension (e.x.: rar, msi, zip, 7z, cab and so on) to be included in the Edit property dialog and click OK.
- Repeat the process to add more extensions
- Click OK in the 'Manage Extensions' dialog
- **Set new on-screen alert timeout to** - This box allows you to set the time period (in seconds) for which the alert message should stay on the screen. (**Default = 120 seconds**)
- **Set new maximum file size limit to** - This box allows you to set a maximum size (in MB) for the individual files to be scanned during on-access scanning. Files larger than the size specified here, will not be scanned. (**Default = 40 MB**)
- **Set new maximum script size limit to** - This box allows you to set a maximum size (in MB) for the script files to be scanned during on-access scanning. Files larger than the size specified here, are not scanned. (**Default = 4 MB**)
- **Use heuristics scanning** - Allows you to enable or disable Heuristics scanning and define scanning level. (**Default = Enabled**)

Heuristic techniques identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that match a signature on the virus blacklist.

This is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

Leave this option selected to keep Heuristics scanning enabled. Else, deselect this checkbox. If enabled, you can select the level of Heuristic scanning from the drop-down:

- **Low** - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users. (**Default**)
- **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
- **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.
- **Detect potentially unwanted applications** - When this check box is selected, Antivirus scans also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet (**Default = Enabled**).

6.2.1.2. Scan Profiles

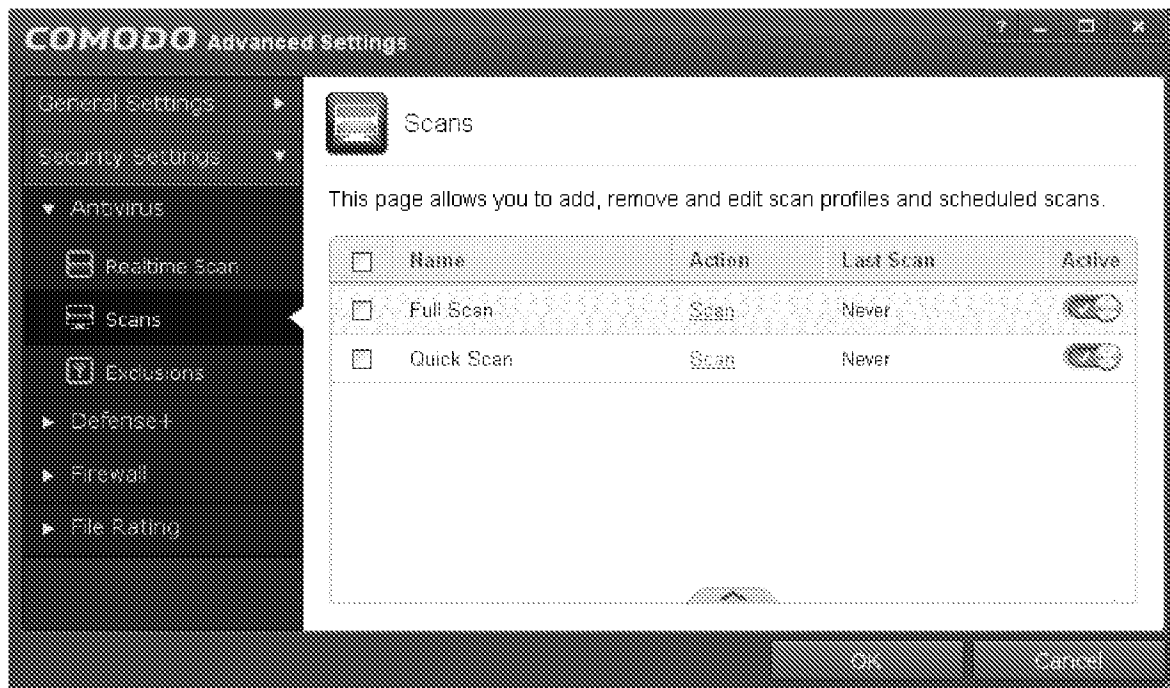
The Scan Profiles area allows you to view, edit, create and run custom virus scans. Each profile is a collection of scanner settings that tell CIS:

- Where to scan (which files, folders or drives should be covered by the scan)
- When to scan (you have the option to specify a schedule)

- How to scan (options that let you specify the behavior of the scan engine when running this profile)

To open the panel

- Click Security Settings > Antivirus > 'Scans' tab in the 'Advanced Settings' panel.



CIS ships with two predefined scan profiles:

- **Full Scan** - Covers every local drive, folder and file on your system.
- **Quick Scan** - Covers critical areas in your system which are highly prone to infection from viruses, rootkits and other malware. This includes system memory, auto-run entries, hidden services, boot sectors, important registry keys and system files. These areas are responsible for the stability of your computer and keeping them clean is essential.

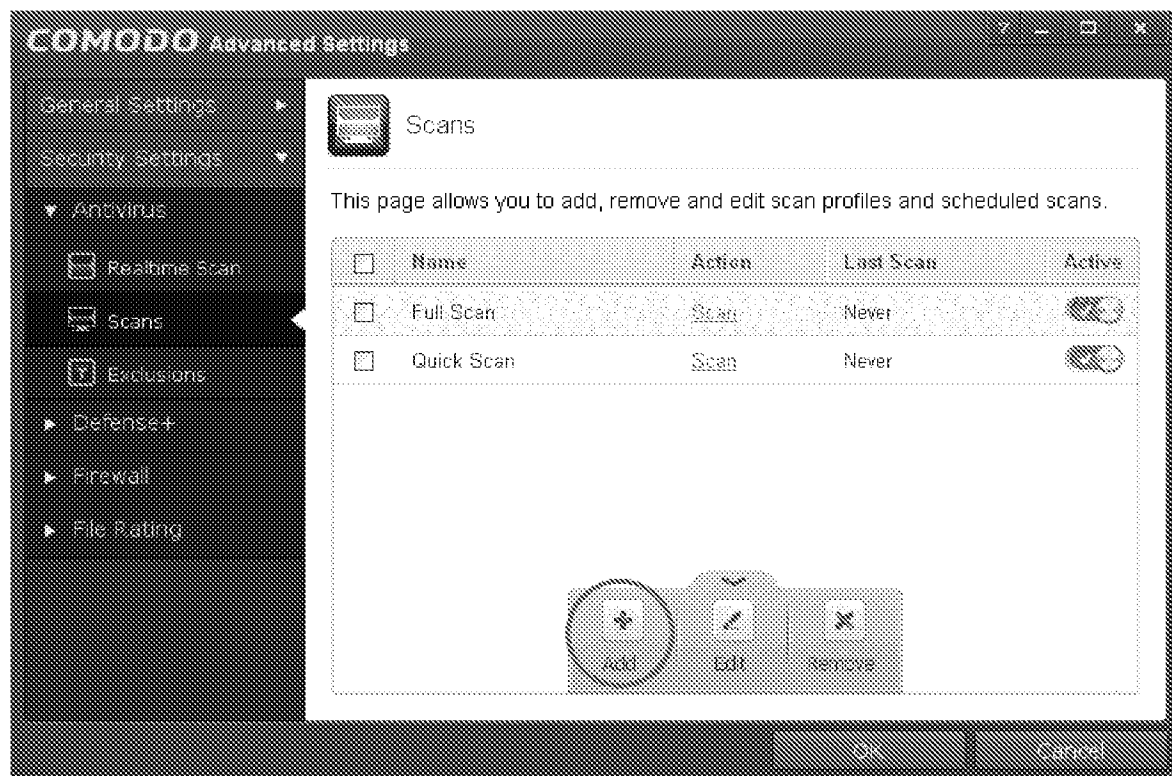
You can run a profile-scan immediately by clicking the 'Scan' link alongside it. Click the handle at the foot of the interface if you wish to edit, remove or add a profile.

Click the following links for more details on:

- [Creating a Scan Profile](#)
- [Running a custom scan](#)

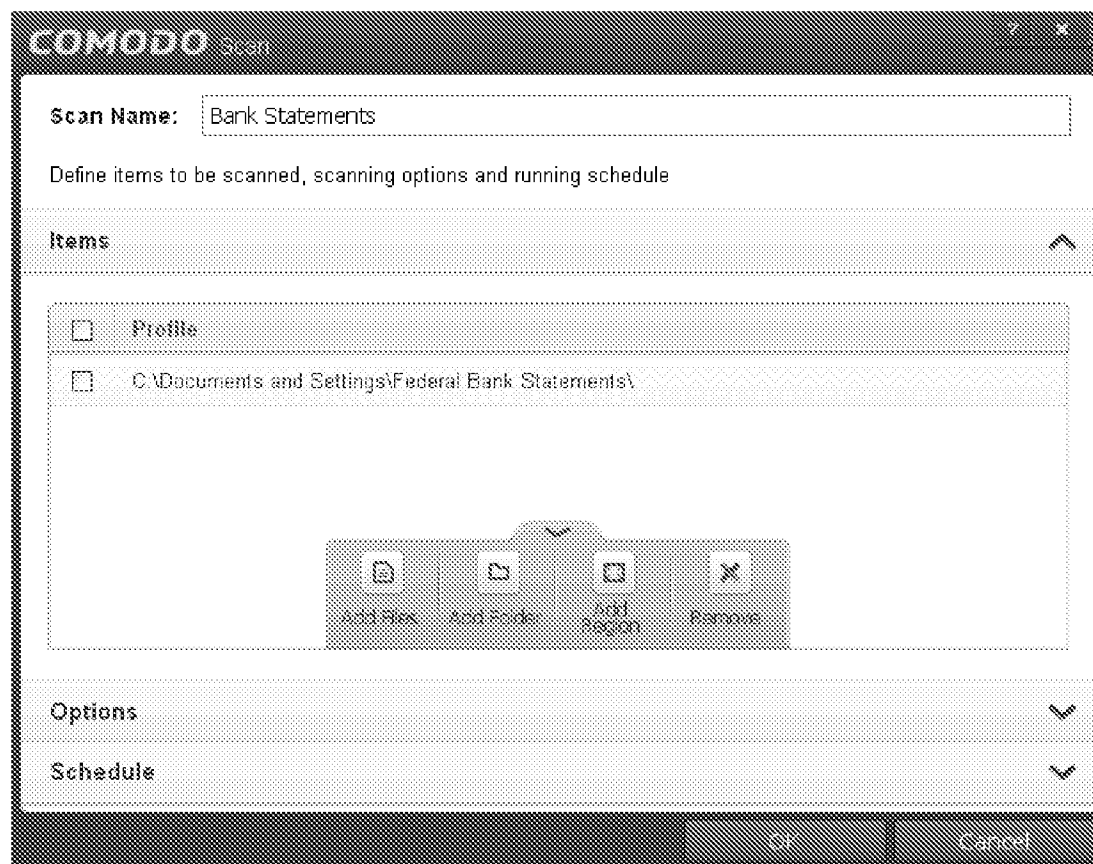
To create a custom profile

- Click the handle at the bottom of the interface then click the 'Add' button:

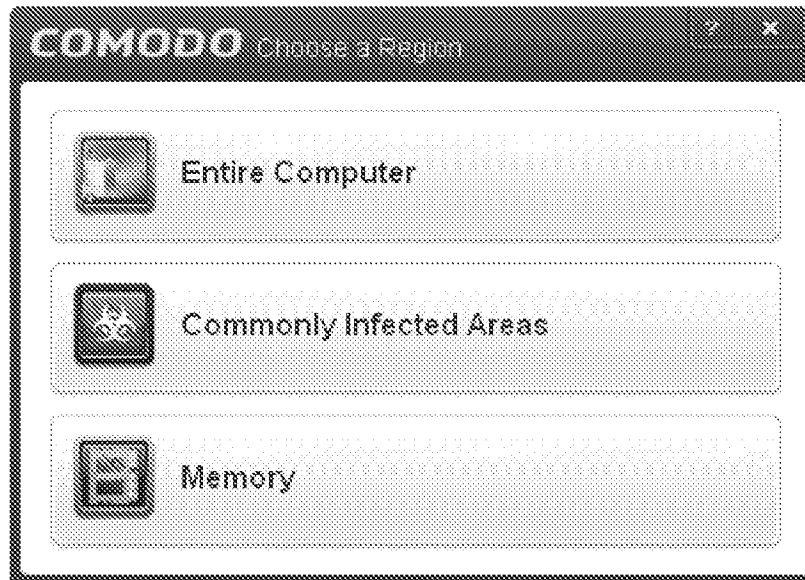


The scan profile interface will be displayed.

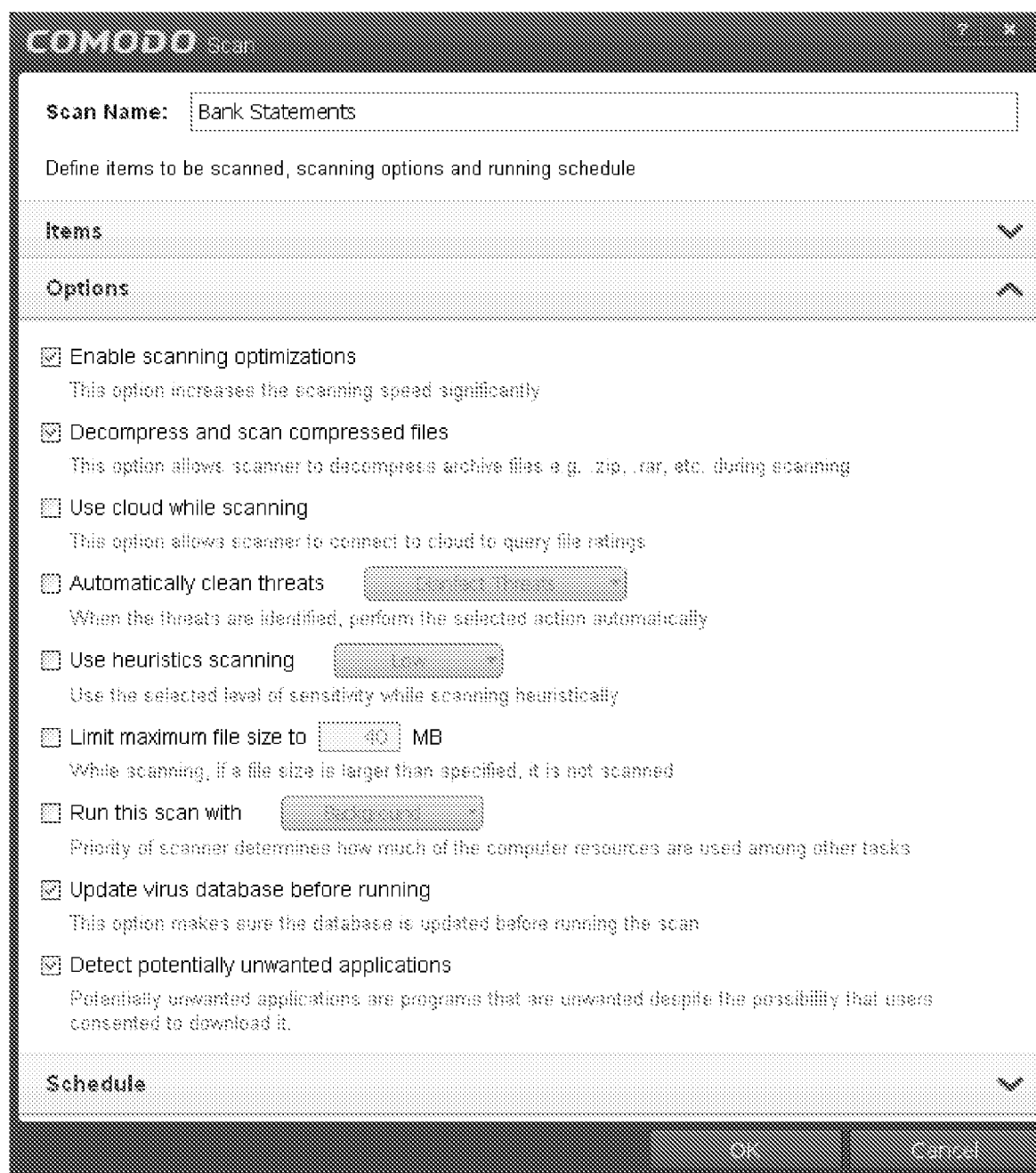
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items that should be included in the profile



- **Add Files** - Allows you to navigate to specific files that you wish to add to the profile
- **Add Folder** - Opens the 'Browse For Folder' window and allows you to select entire folders
- **Add Region** - Allows you to add predefined regions to the profile. For example, 'Full Computer', 'Commonly Infected Areas' and 'System Memory'.



- Repeat the process to add more items into the profile
- Click 'Options' to further customize the scan



- Options:

- **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process (**Default = Enabled**) .
- **Decompress and scan compressed files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (**Default = Enabled**) .
- **Use cloud while scanning** - Selecting this option enables the Antivirus to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local antivirus database is out-dated. (**Default = Disabled**).
- **Automatically clean threats** - Enables you to select the action to be taken against the detected threats and infected files automatically from disinfecting Threats and moving the threats to quarantine. (**Default = Disabled**).

- **Use heuristics scanning** - Enables you to select whether or not Heuristic techniques should be applied on scans in this profile. You are also given the opportunity to define the heuristics scan level. **(Default = Disabled).**

Background info: Comodo Internet Security employs various heuristic techniques to identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code patterns similar to those in known viruses. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting 'virus-like' traits or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist.

This allows CIS to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

- **Low** - Lowest sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users.
- **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
- **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.
- **Limit maximum file size to** - Select this option if you want to impose size restrictions on files being scanned. Files of size larger than that specified here, are not scanned, if this option is selected **(Default = 40 MB).**
- **Run Scan with** - Enables you to set the priority of the scanning from High to Low or to run at background. **(Default = Disabled).**

☐ Limit maximum file size to MB

While scanning, if a file size is larger than specified, it is not scanned.

☒ Run this scan with **Background**

Priority of scanner determined by the computer resource.

☒ Update virus database

This option makes sure the virus database is updated before running the scan.

☒ Detect potentially unwanted applications

This option makes sure the scan also includes potentially unwanted applications.

- **Update virus database before running** - Selecting this option makes CIS to check for virus database updates and if available, update the database before commencing the scan. **(Default = Enabled).**
- **Detect potentially unwanted applications** - When this check box is selected, Antivirus scans also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may have functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet. **(Default = Enabled).**
- If you want the scan to be performed periodically, set a Schedule for the custom scan by clicking 'Schedule'

COMODO Scan

Scan Name:

Define items to be scanned, scanning options and running schedule

Items ▼

Options ▼

Schedule ▲

Frequency:

☐ Do not schedule this task
☐ Every Day
☒ Every Week
☐ Every Month

Start Time:

Day(s) of Week

Sun	Mon	Tue	Wed	Thu	Fri	Sat

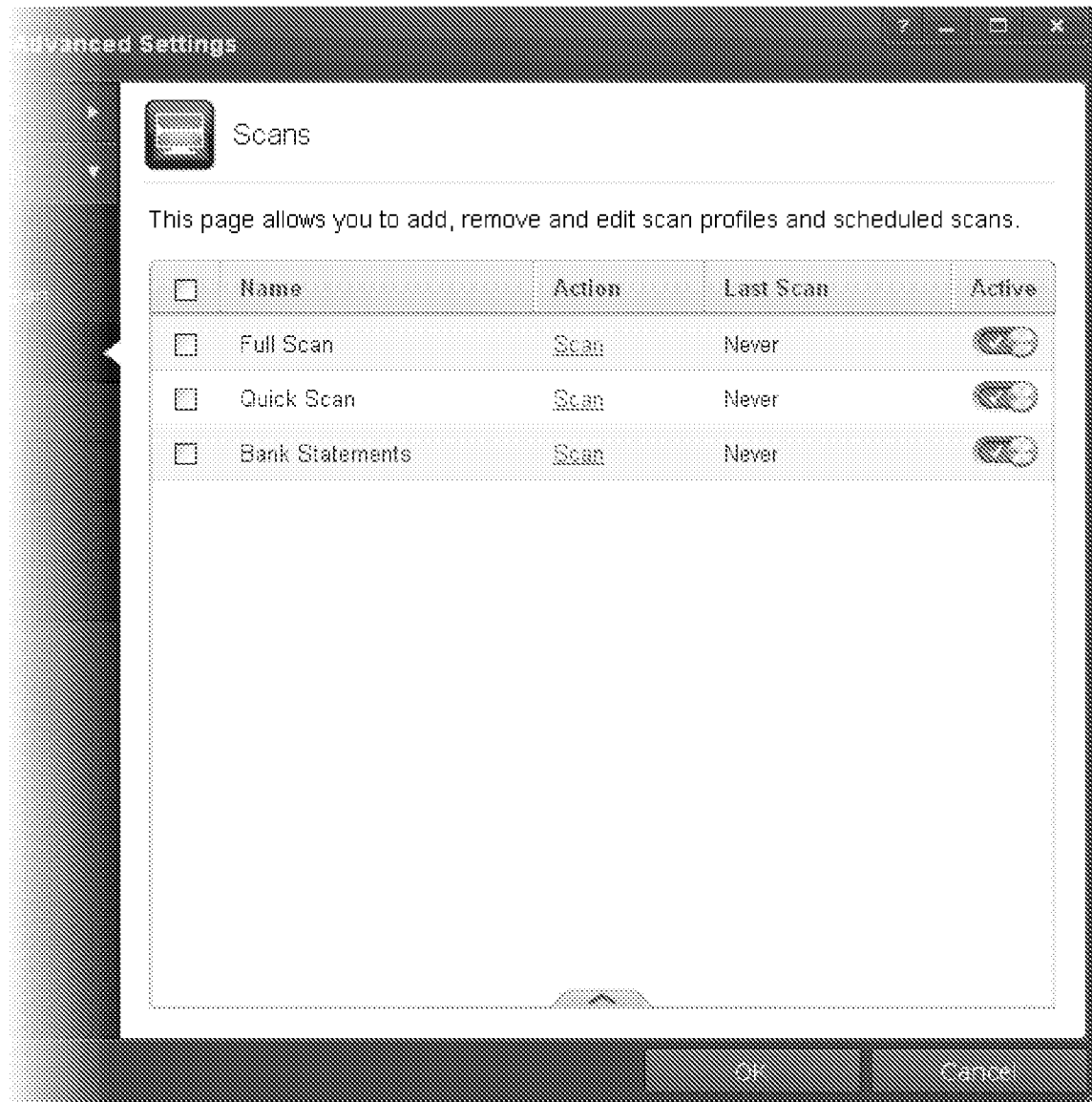
☐ Run only when computer is not running on battery
☐ Run only when computer is IDLE
☐ Turn off computer if no threats are found at the end of the scan

OK Cancel

- **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
- **Every Day** - Runs the scan every day at the time specified
- **Every Week** - Scans the areas defined in the scan profile on the day(s) of the week specified in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them.
- **Every Month** - Scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them.
- **Run only when computer is not running on battery** - This option is useful when you are using a laptop or any other battery driven portable computer. Selecting this option runs the scan only if the computer runs with the adapter connected to mains supply and not on battery.
- **Run only when computer is IDLE** - Select this option if you do not want to be disturbed when involved in computer related activities. The scheduled scan will run only if the computer is in idle state
- **Turn off computer if no threats are found at the end of the scan** - Selecting this option turns your computer off, if no threats are found during the scan. This is useful when you are scheduling the scans to run at nights.
- Click OK to save the profile.

Note: The scheduled scan will run only if it is enabled. Click the button under the Active column beside the respective profile row

to toggle between on and off status.



To run a custom scan as per scan profile

- Click Scan from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'More Scan Options' from the 'Custom Scan' pane
- The 'Advanced Settings' interface will be displayed with 'Scans' panel opened.
- Click Scan beside the required scan profile.



- The scan will be started and on completion the results will be displayed.



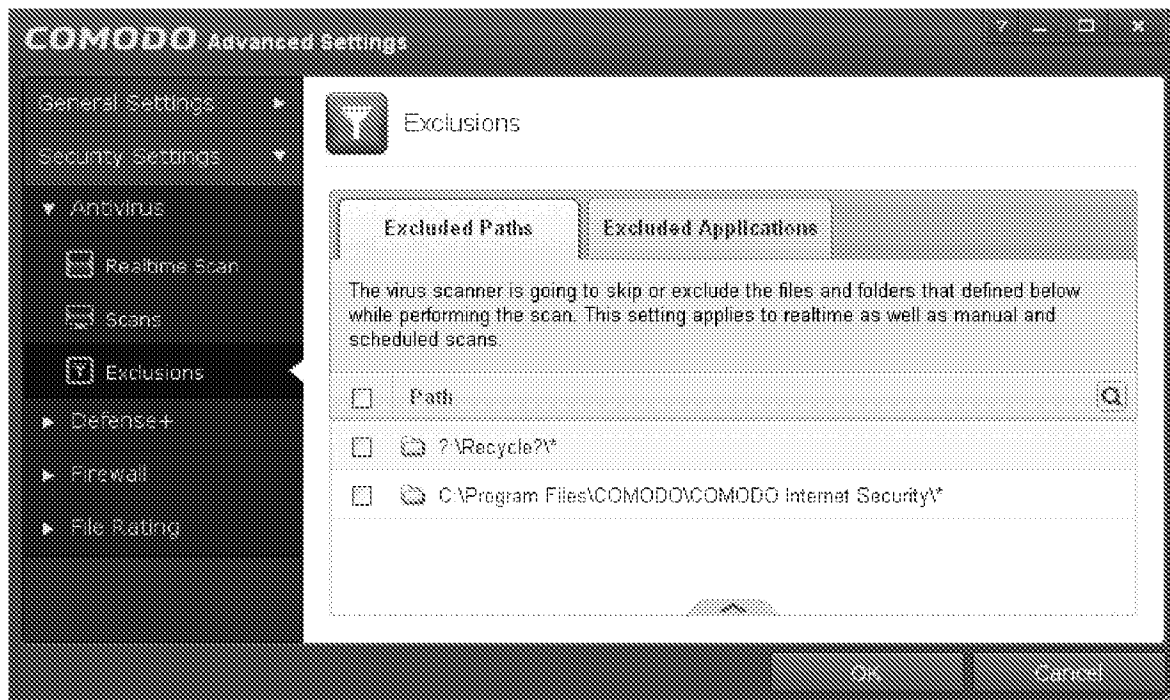
You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to [Processing the infected files](#) for more details.

6.2.1.3. Exclusions

The 'Exclusions' panel under the Antivirus Settings Settings displays a list of paths and applications/files for which you have selected **Ignore** from the Scan Results window of various scans or added to the Exclusions from an antivirus alert.

To open the Exclusions panel

- Click Security Settings > Antivirus > 'Exclusions' tab in the 'Advanced Settings' panel.

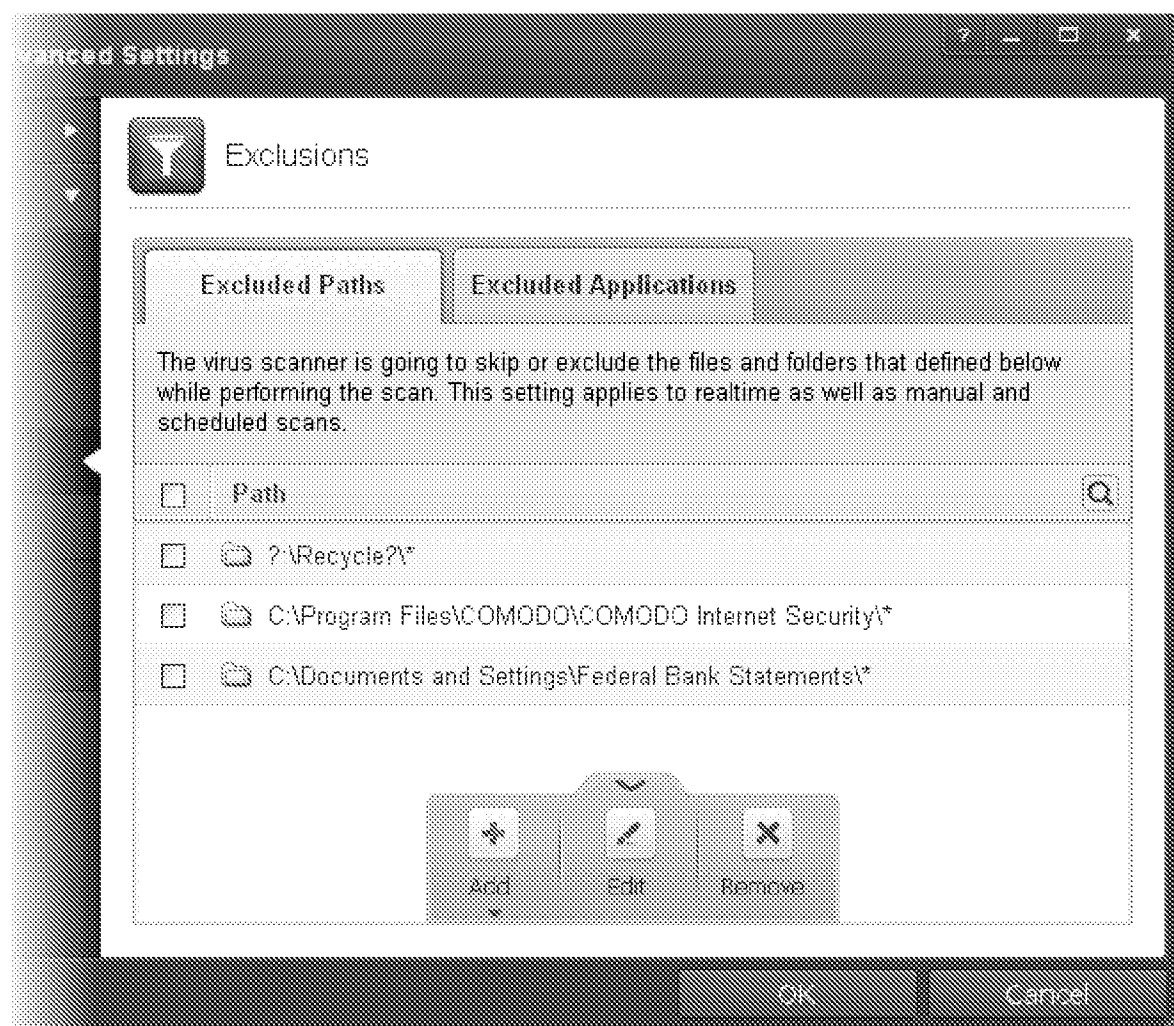


The 'Exclusions' panel has two tabs:

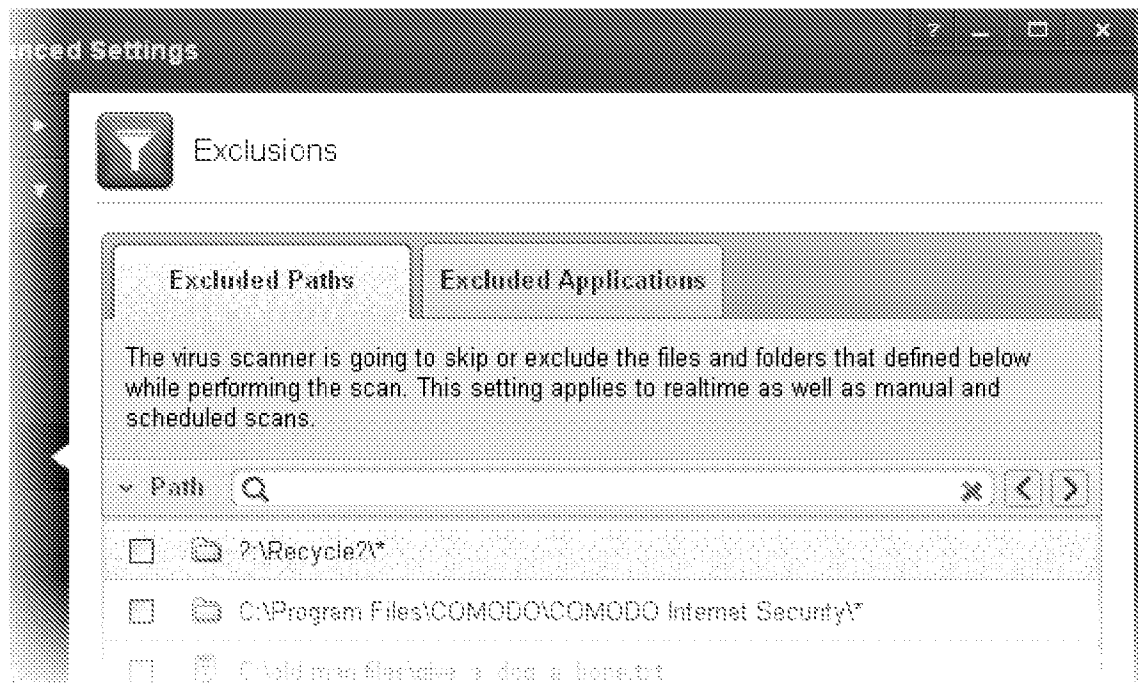
- **Excluded Paths** - Displays a list of paths/folders/files in your computer, which are excluded from both real-time and on-demand antivirus scans. Refer to the section [Excluding Drives/Folders/Files from all types of scans](#) for more details on adding and removing exclusion items in this interface.
- **Excluded Applications** - Displays a list of programs/applications in your computer, which are excluded from real-time antivirus scans. The items are included on clicking 'Ignore' from the Scan Results window of various scans and Antivirus Alerts or manually. Please note that these items are excluded only on real-time scans but will be scanned on running on-demand scans. Refer to the section [Excluding Programs/Applications from real-time scans](#) for more details on manually adding and removing exclusion items in this interface.

Excluding Drives/Folders/Files from all types of scans

You can exclude a drive partition, a folder, a sub-folder or a file from both the real-time and on-demand/custom scheduled antivirus scans at any time, by adding them to Excluded Paths.



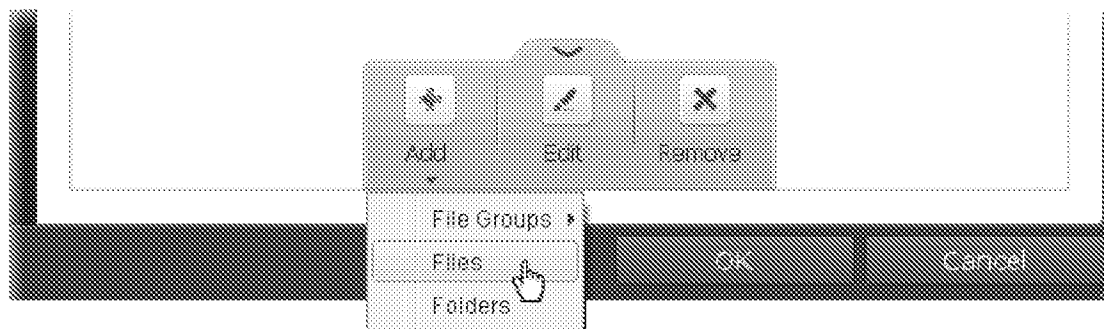
You can use the search option to find a specific excluded path, folder or file from the list by clicking the search icon  at the far right in the column header.



- Enter the path, folder name or file name to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the  icon in the search field to close the search option.

To add item(s) to excluded paths

- Click the handle from the bottom center and click on 'Add' from the options

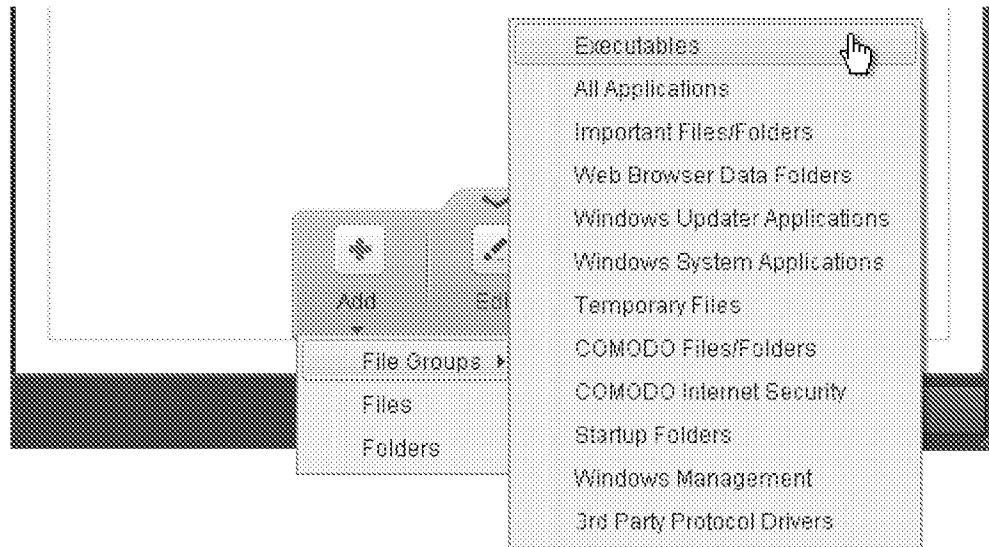


You can choose to add a:

- File Group
 - Drive partition/Folder
- or
- an individual file

Adding a File Group

- Choosing File Groups allows you to exclude a category of pre-set files or folders. For example, selecting 'Executables' would enable you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.

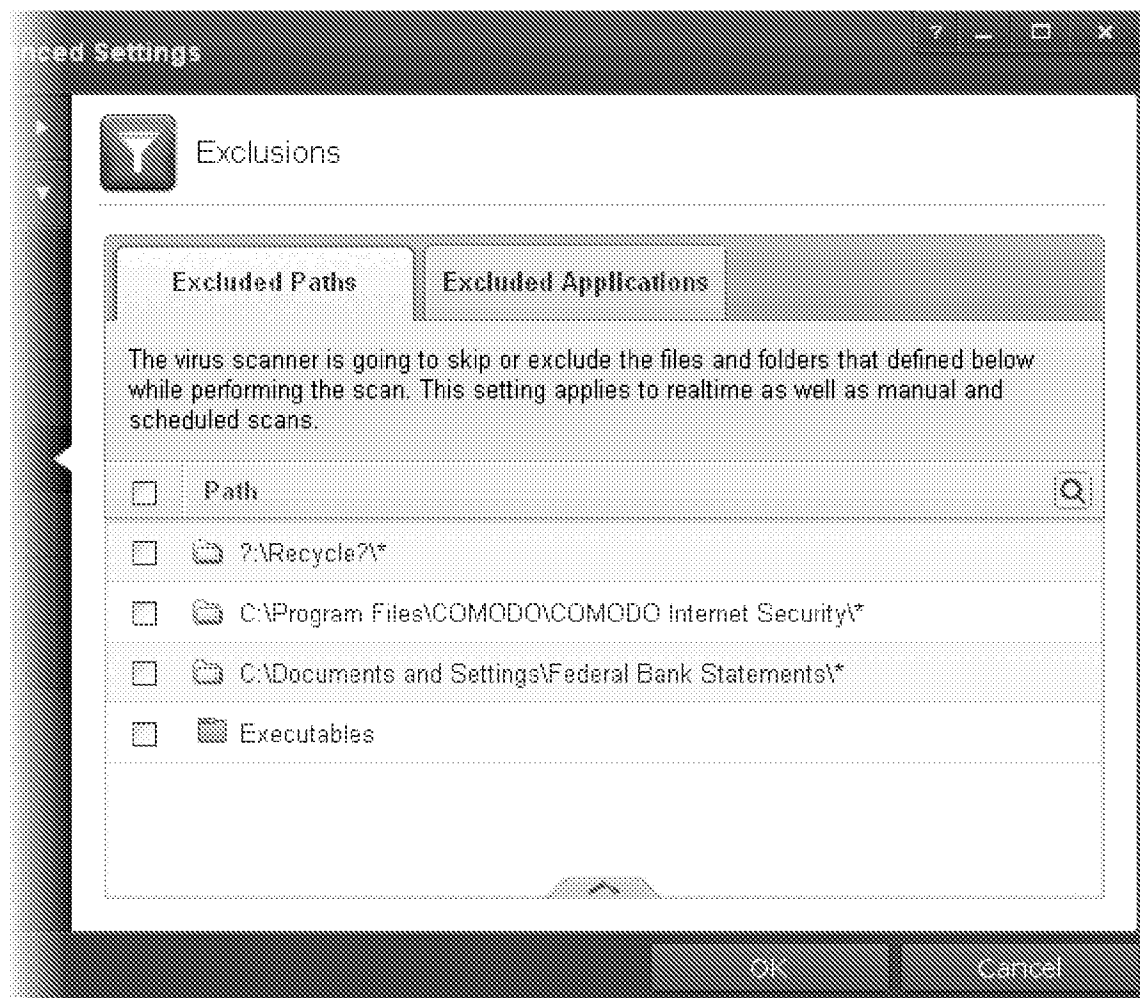


To view the file types and folders that are affected by choosing one of these options, you need to visit the 'File Groups' interface.

The 'File Groups' interface can be accessed by the following method:

- Navigate to **Advanced Settings > Defense > HIPS > Protected Files**, click the up arrow from the bottom of the interface and select 'Groups' from the options.

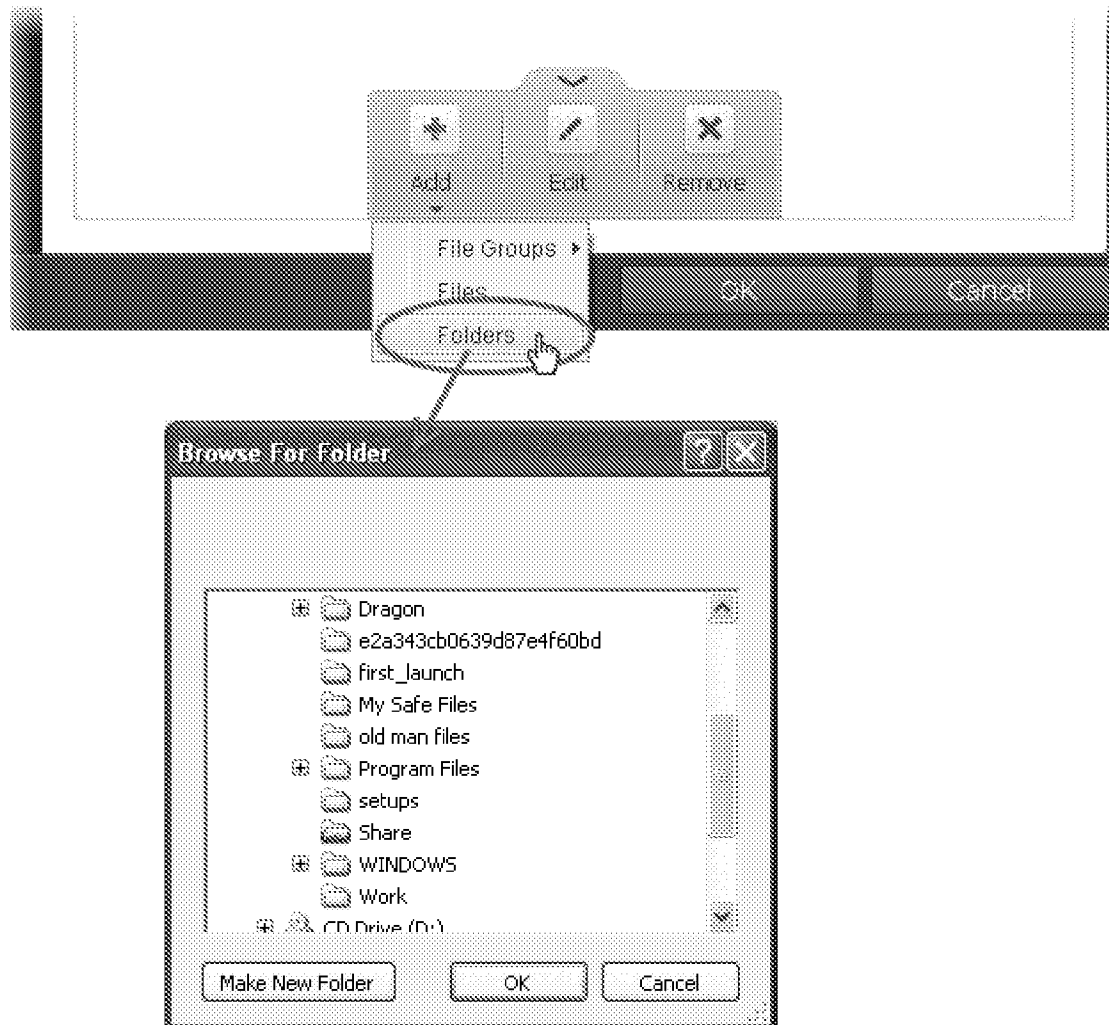
The file groups will be added to Excluded Paths.



- Repeat process to add more file groups. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

Adding a Drive Partition/Folder

- To add a folder, choose 'Folders' from the 'Add' drop-down.



The 'Browse for Folder' dialog will appear.

- Navigate to the drive partition or folder you want to add to excluded paths and click OK

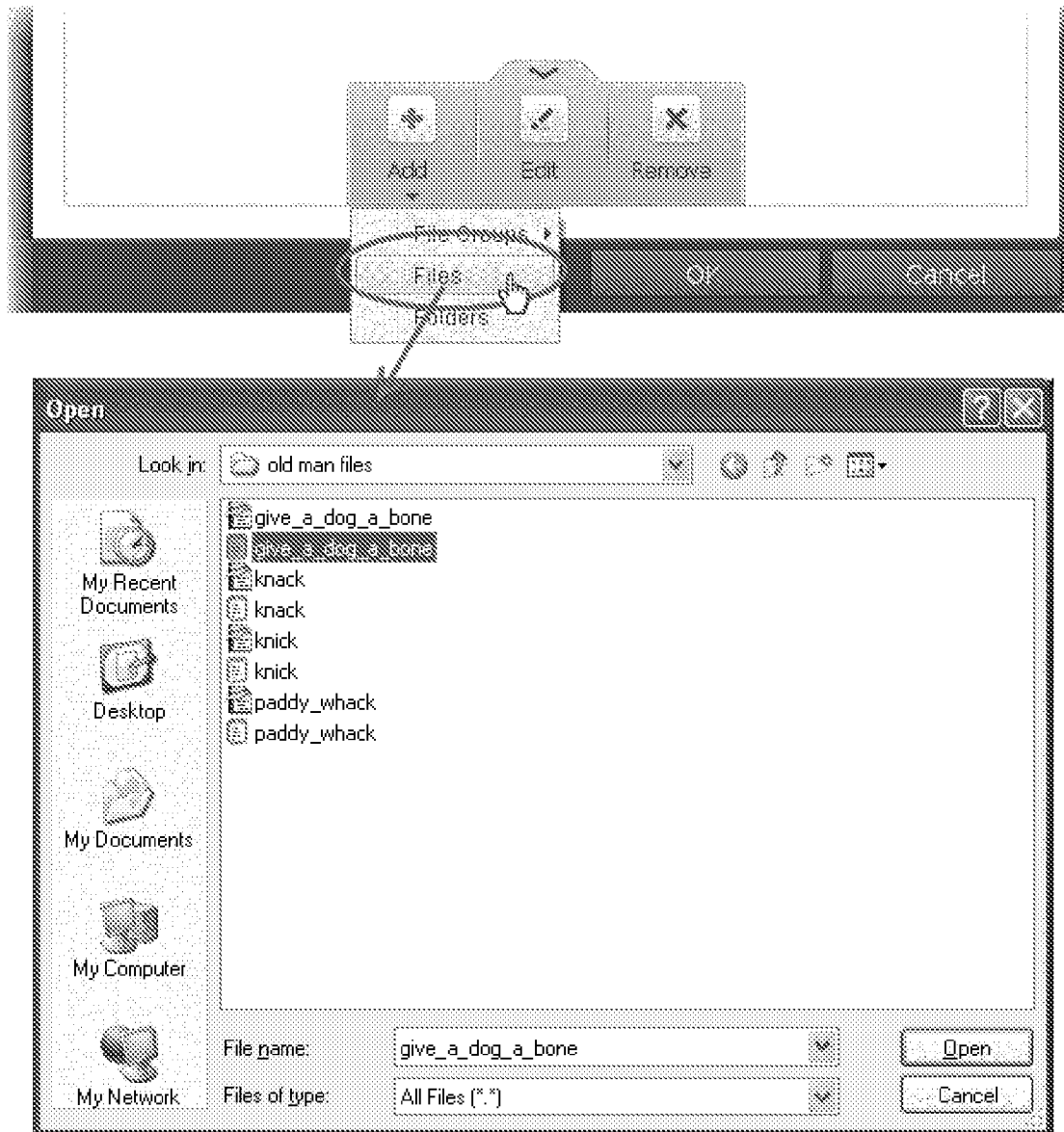
The drive partition/folder will be added to Excluded Paths.



- Repeat process to add more folders. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

Adding an individual File

- Choose 'Files' from the 'Add' drop-down.



- Navigate to the file you want to add to Excluded Paths in the 'Open' dialog and click 'Open'

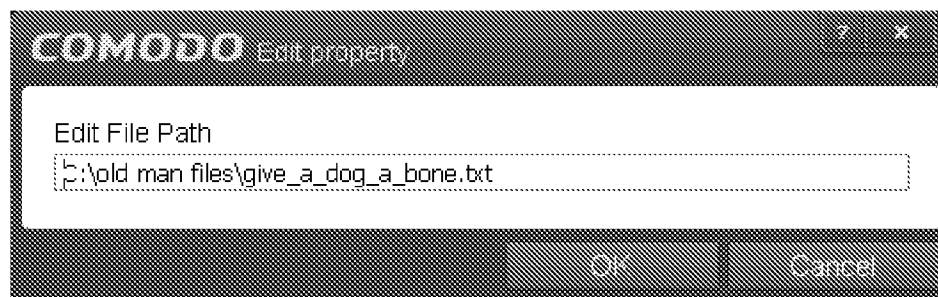


The file will be added to Excluded Paths.

- Repeat process to add more paths. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

To edit the path of an added item

- Select the item, click the handle from the bottom center and select 'Edit'.
- Make the required changes for the file path in the Edit Property dialog.



To remove an item from the Excluded Paths

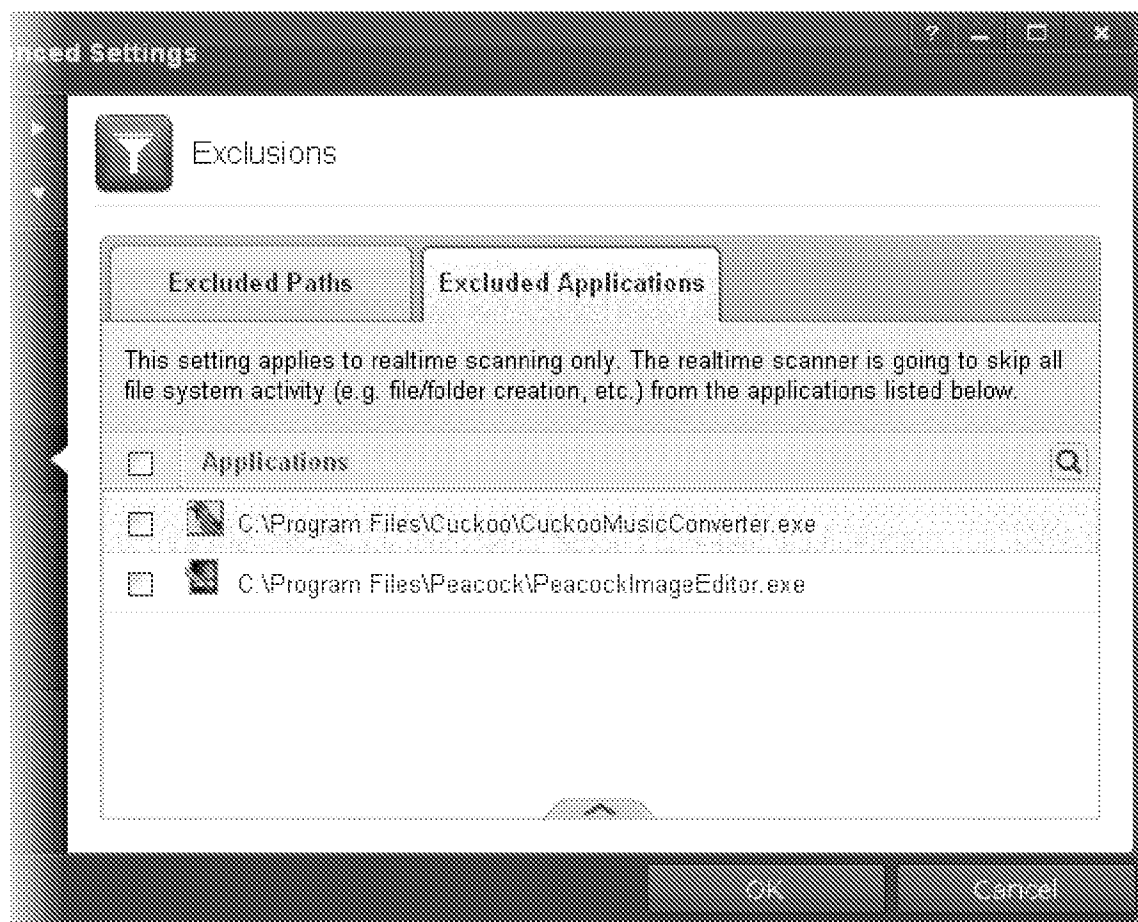
- Select the item, click the handle from the bottom center and select 'Remove'.



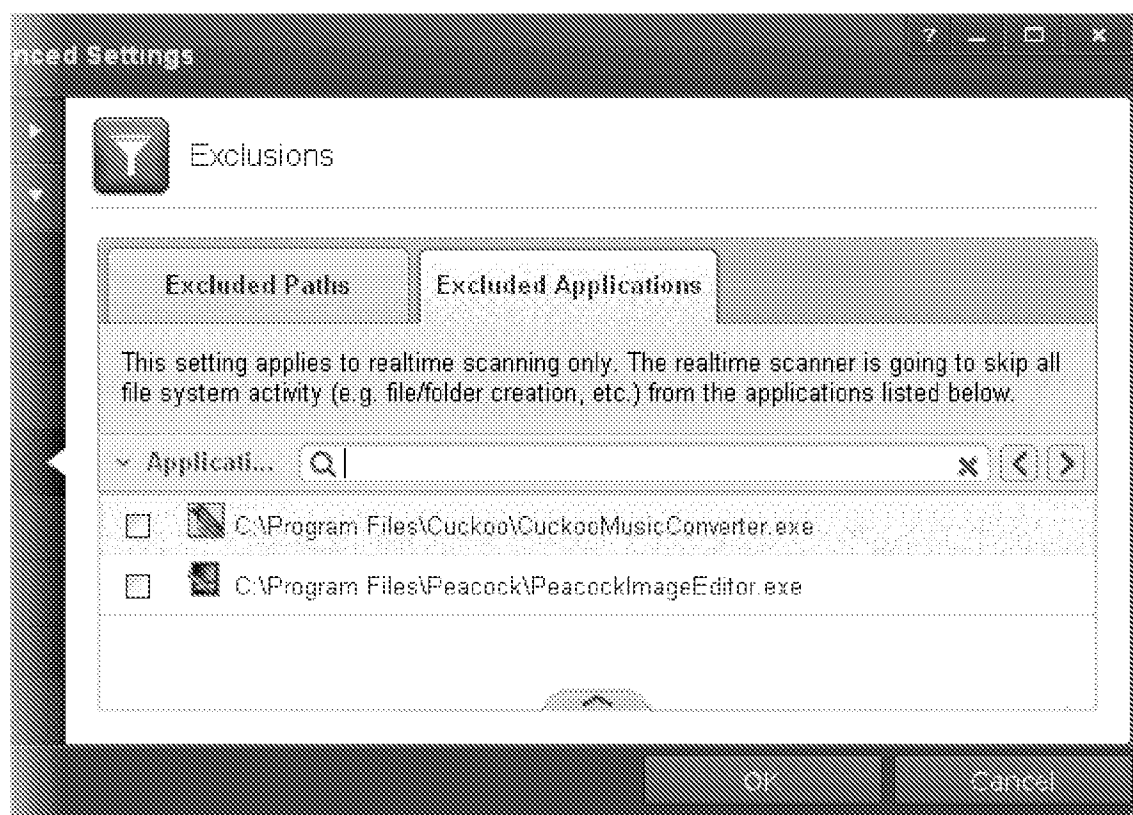
- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

Excluding Programs/Applications from Real-time Scans

The 'Excluded Applications' tab allows you to manually add programs, applications or files to Excluded Applications list for excluding them from real-time scans. Also you can remove the items from Excluded Applications that were added by mistake.



You can use the search option to find a specific excluded application from the list by clicking the search icon  at the far right in the column header.



- Enter the name of the application to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the icon in the search field to close the search option.

To add an item to Excluded Applications

- Click the handle from the bottom center and click on 'Add' from the options

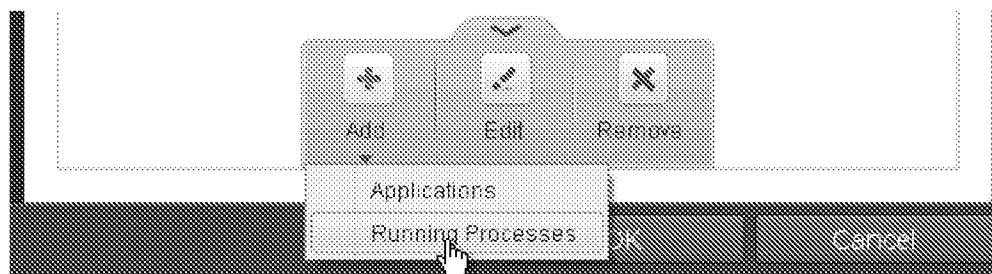


You can choose to add an application by:

- Selecting it from the running processes - This option allows you to choose the target application from the list of processes that are currently running on your PC.
- Browsing your computer for the application - This option is the easiest for most users and simply allows you to browse the files which you want to exclude from a virus scan.

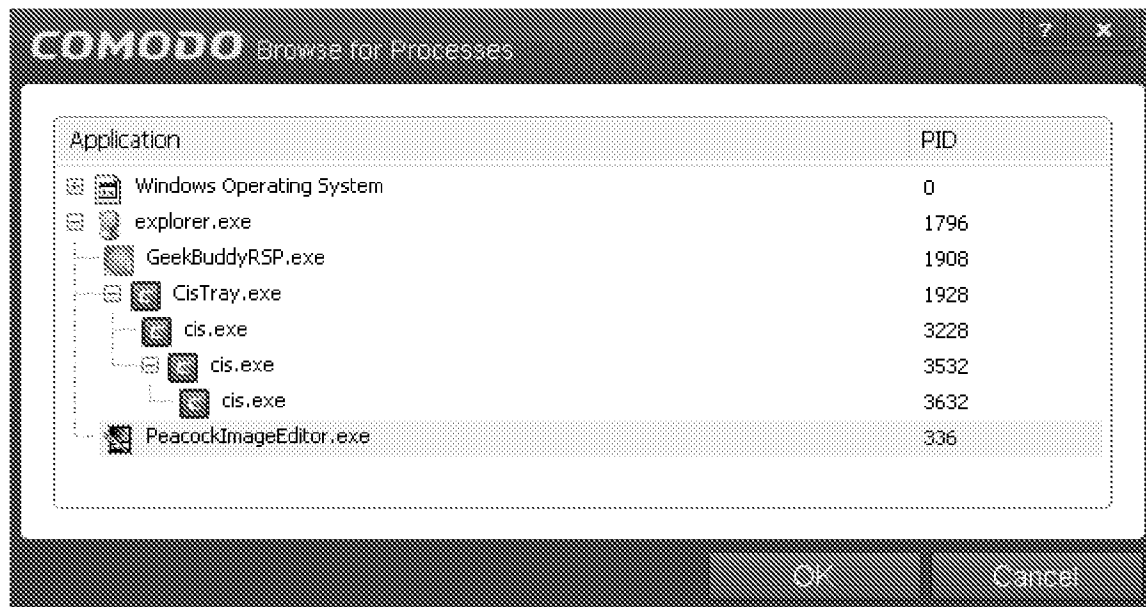
Adding an application from a running processes

- Choose 'Running Processes' from the 'Add' drop-down

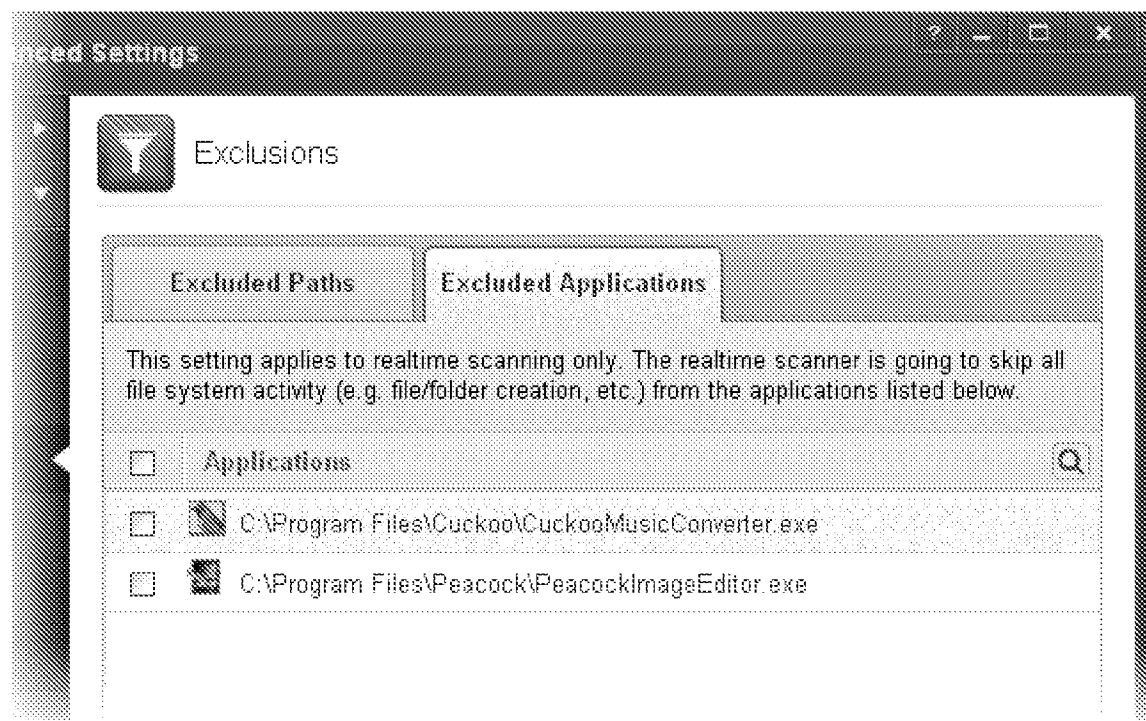


A list of currently running processes in your computer will be displayed

- Select the process, whose target application is to be added to excluded applications and click OK from the Browse for Process dialog.

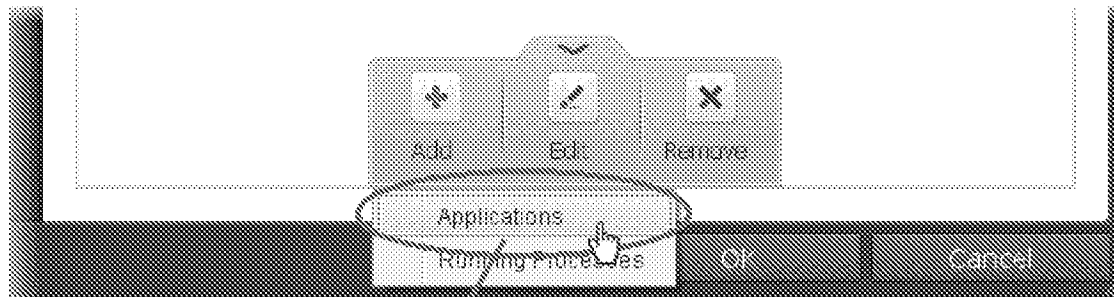
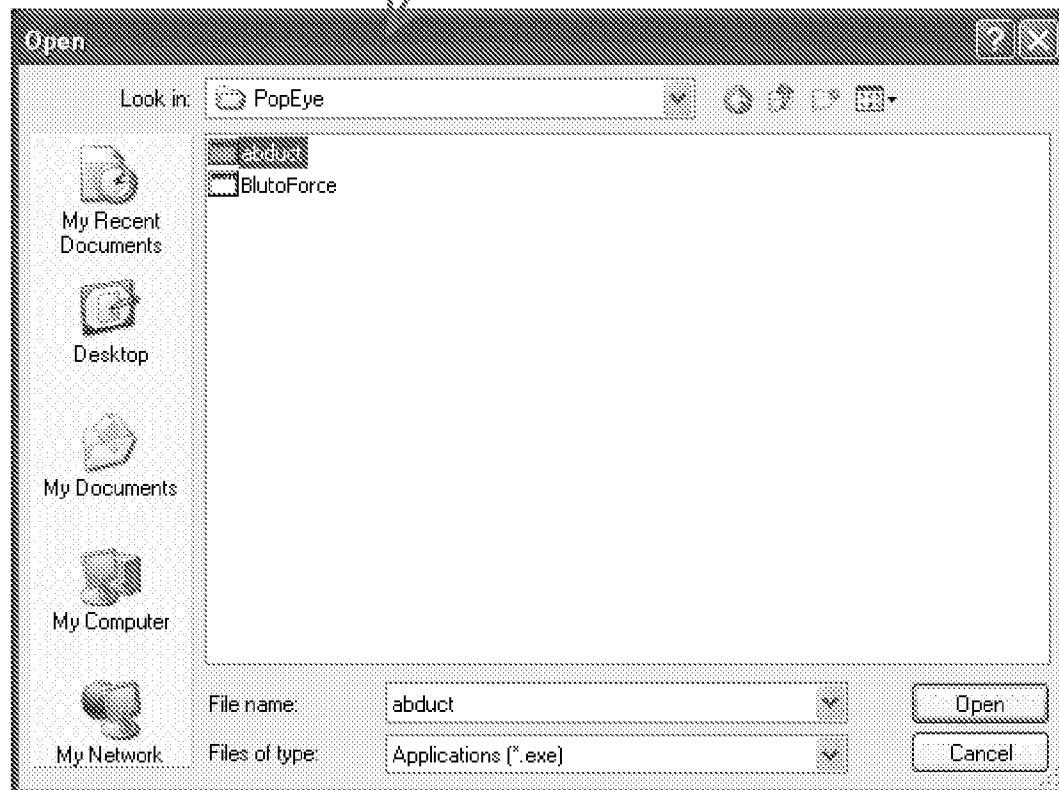


The application will be added to Excluded Applications.



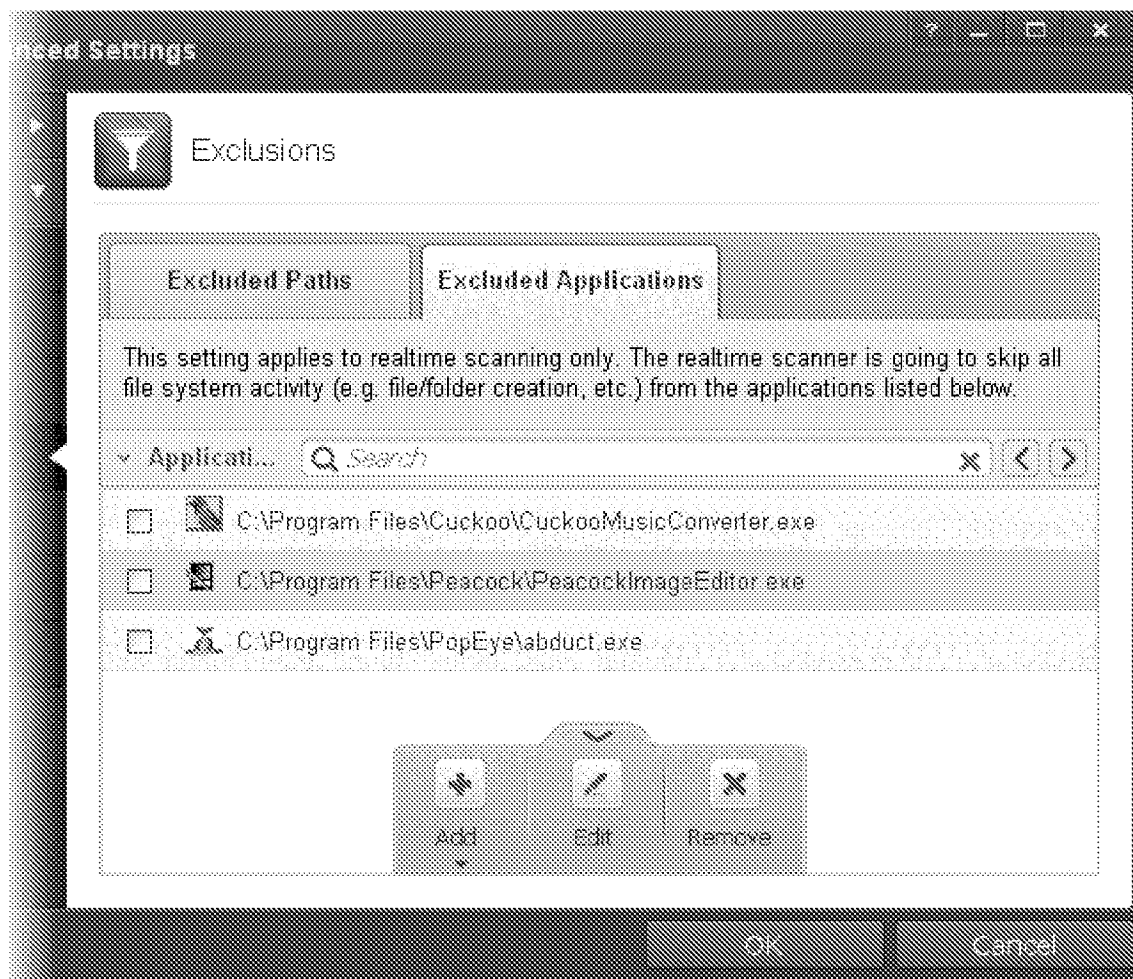
Browsing to the Application

- Choose 'Applications' from the 'Add' drop-down



- Navigate to the file you want to add to Excluded Applications in the 'Open' dialog and click 'Open'.

The file will be added to 'Excluded Applications'.



- Repeat process to add more items. The items will be skipped from future real-time scans.

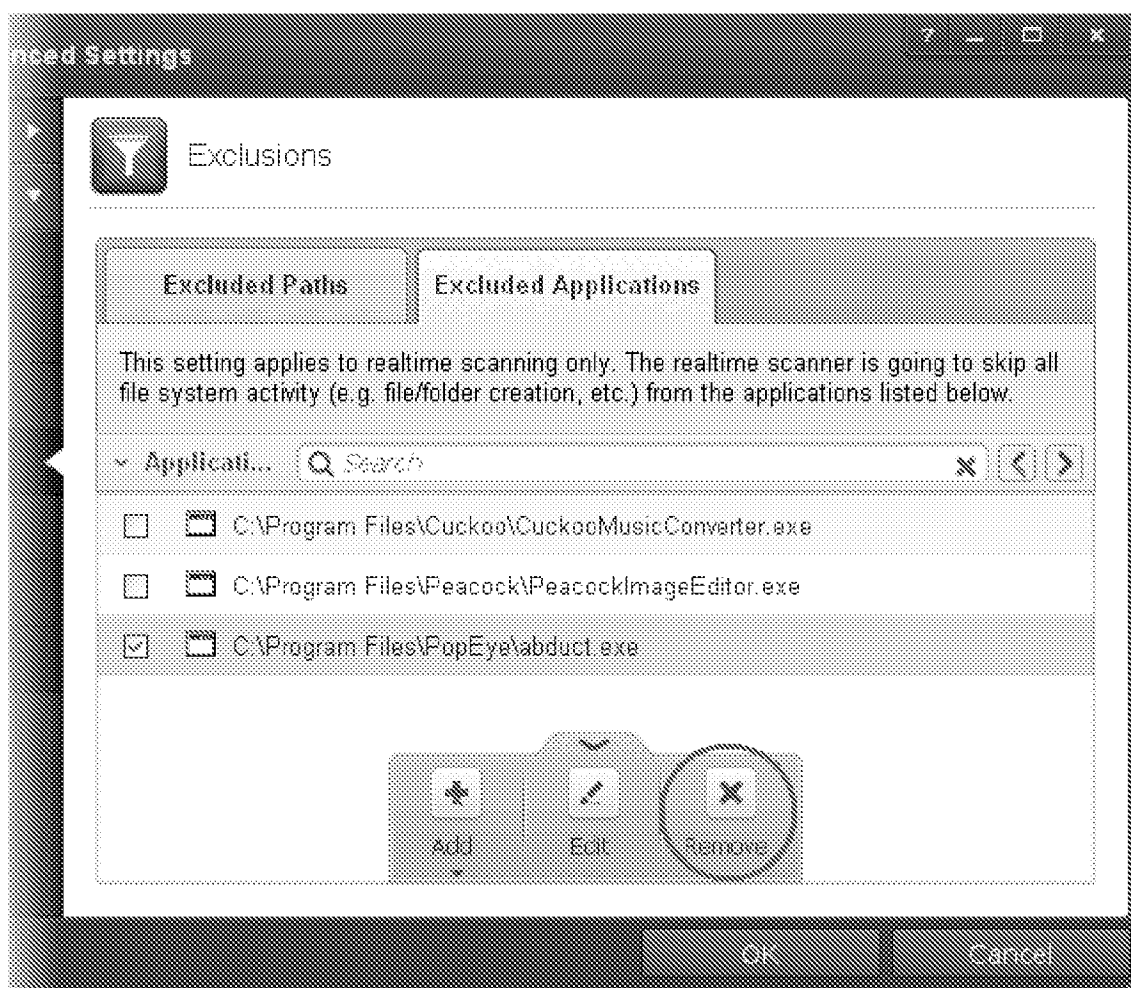
To edit the path of the application added to Excluded Application

- Select the application, click the handle from the bottom center and select 'Edit'.
- Make the required changes for the file path in the Edit Property dialog.



To remove an item from the Excluded Applications

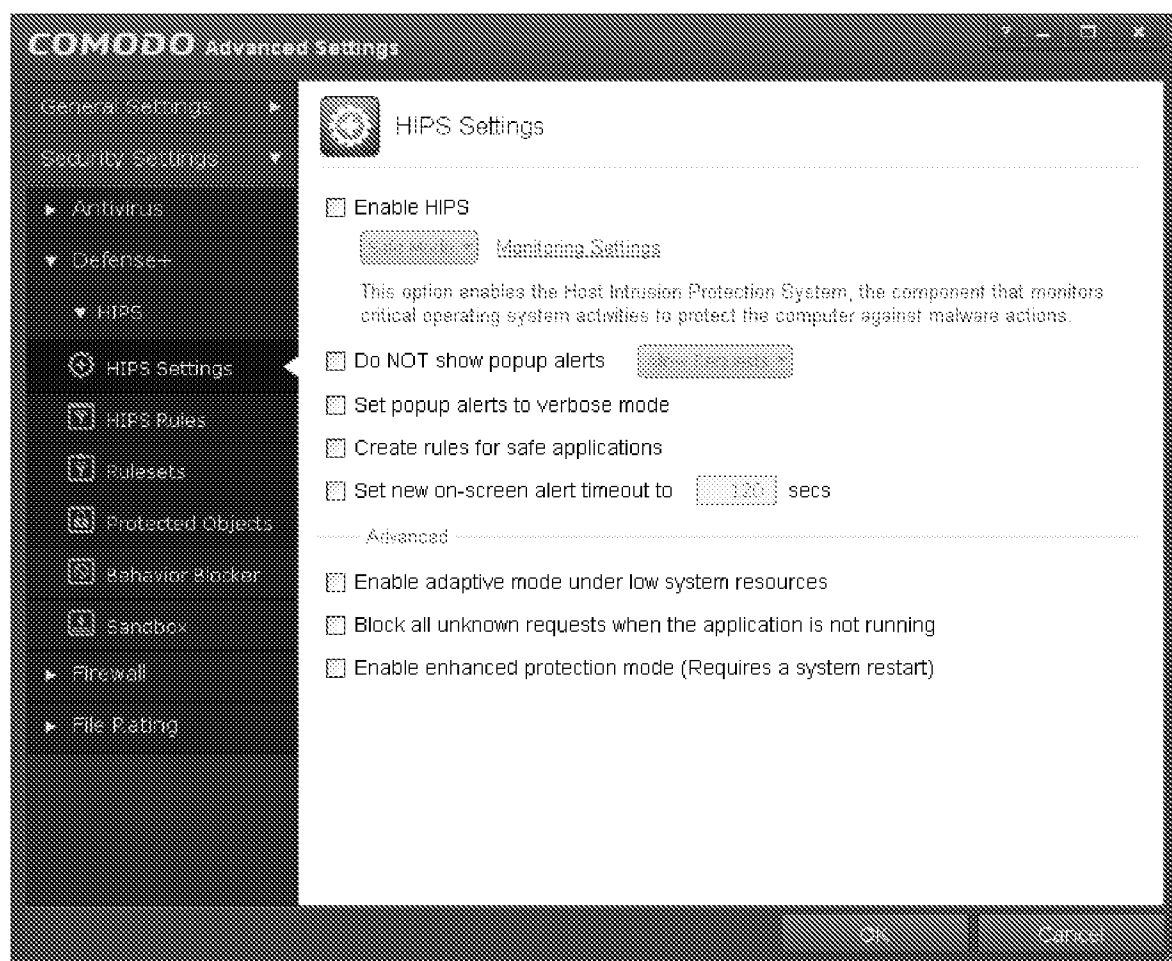
- Select the item, click the handle from the bottom center and select 'Remove'.



- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

6.2.2. Defense+ Settings

Defense+ is a collective term that covers the Host Intrusion Prevention (HIPS), sandboxing and behavior blocker components of Comodo Internet Security. Together, these technologies ensure all applications, processes and services on your PC behave in a secure manner - and are prevented from taking actions that could damage your computer or your data.



The Defense+ settings area allows you to configure the following:

- HIPS
 - HIPS Behaviour Settings
 - Active HIPS Rules
 - Predefined HIPS Rule Sets
 - Protected Objects
- Behavior Blocker
- Sandbox Settings

6.2.2.1. HIPS Behavior Settings

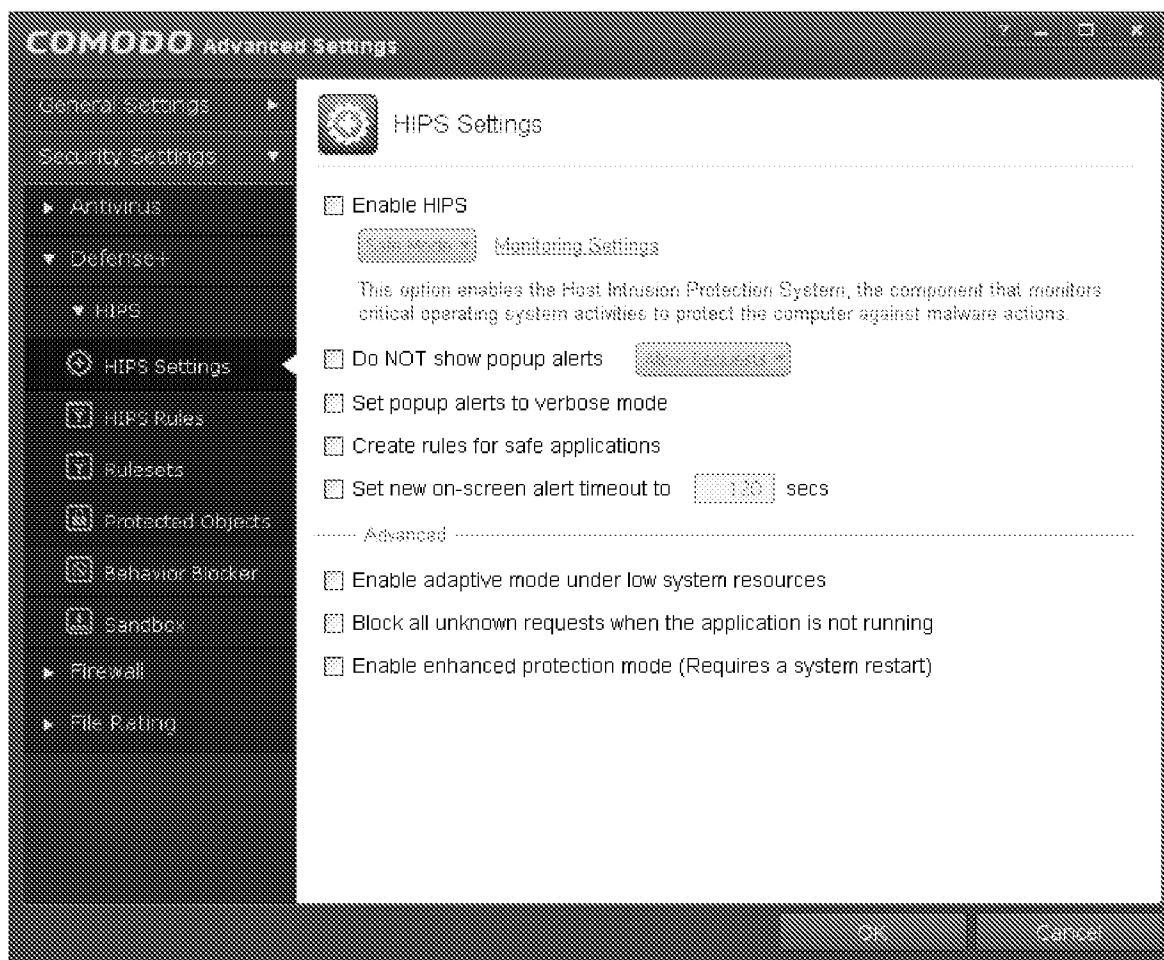
HIPS constantly monitors system activity and only allows executables and processes to run if they comply with the prevailing security rules that have been enforced by the user. For the average user, Comodo Internet Security ships with a default HIPS ruleset that works 'out of the box' - providing extremely high levels of protection without any user intervention. For example, HIPS automatically protects system-critical files, folders and registry keys to prevent unauthorized modifications by malicious programs. Advanced users looking to take a firmer grip on their security posture can quickly create custom policies and rulesets using the powerful rules interface.

Note for beginners: This page often refers to 'executables' (or 'executable files'). An 'executable' is a file that can instruct your computer to perform a task or function. Every program, application and device you run on your computer requires an executable file of some kind to start it. The most recognizable type of executable file is the '.exe' file. (e.g., when you start Microsoft Word, the executable file 'winword.exe' instructs your computer to start and run the Word application). Other types of

executable files include those with extensions .cpl, .dll, .drv, .inf, .ocx, .pf, .scr, .sys.

Unfortunately, not all executables can be trusted. Some executables, broadly categorized as malware, can instruct your computer to delete valuable data; steal your identity; corrupt system files; give control of your PC to a hacker and much more. You may also have heard these referred to as Trojans, scripts and worms.

- The HIPS Settings panel allows you to enable/disable HIPS, set its security level and configure its general behavior.
- The HIPS Settings panel can be accessed by clicking Security Settings > Defense+ > HIPS > 'HIPS Settings' tab from 'Advanced Settings' interface



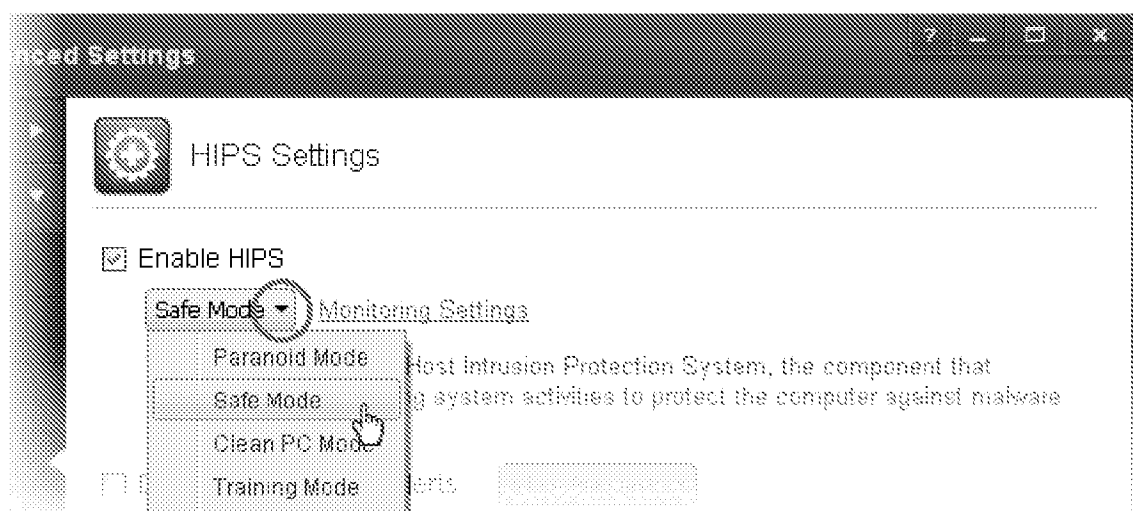
- **Enable HIPS** - Allows you to enable/disable the HIPS protection. *(Default=Disabled)*

Note: The HIPS settings can also be configured in the 'Advanced View' of the 'Home' screen by clicking the status link beside HIPS in the 'Defense+ and Sandbox' pane.

If enabled, you can choose the security level and configure the monitoring settings for the HIPS component.

Configuring Security Level of HIPS

The security level can be chosen from the drop-down that becomes active only on enabling HIPS:



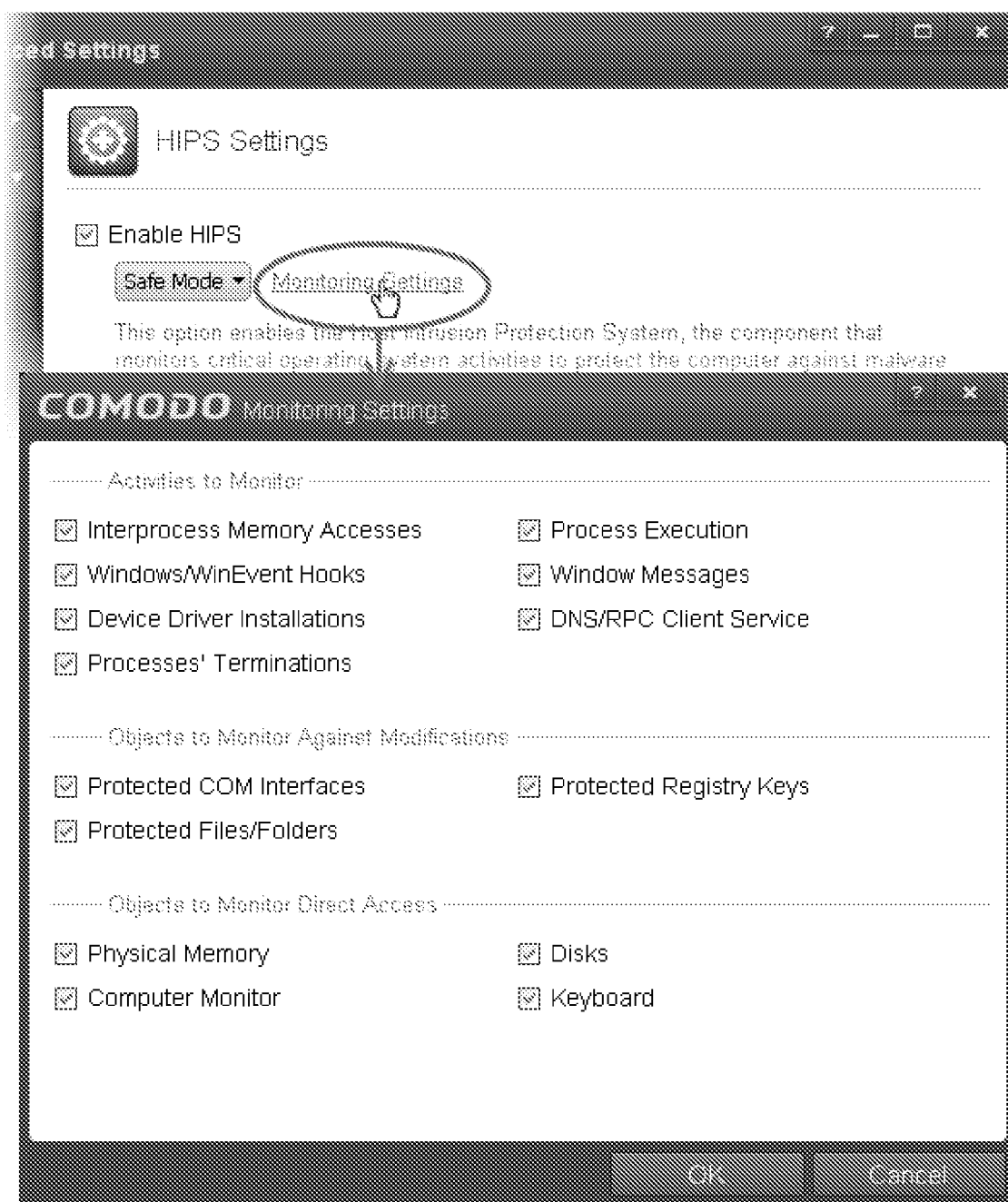
The choices available are:

- Paranoid Mode:** This is the highest security level setting and means that Defense+ monitors and controls all executable files apart from those that you have deemed safe. Comodo Internet Security does not attempt to learn the behavior of any applications - even those applications on the Comodo safe list and only uses *your* configuration settings to filter critical system activity. Similarly, the Comodo Internet Security does automatically create 'Allow' rules for any executables - although you still have the option to treat an application as 'Trusted' at the HIPS alert. Choosing this option generates the most amount of HIPS alerts and is recommended for advanced users that require complete awareness of activity on their system.
- Safe Mode:** While monitoring critical system activity, Defense+ automatically learns the activity of executables and applications certified as 'Safe' by Comodo. It also automatically creates 'Allow' rules these activities, if the checkbox 'Create rules for safe applications' is selected. For non-certified, unknown, applications, you will receive an alert whenever that application attempts to run. Should you choose, you can add that new application to the safe list by choosing 'Treat this application as a Trusted Application' at the alert. This instructs the Defense+ not to generate an alert the next time it runs. If your machine is not new or known to be free of malware and other threats as in 'Clean PC Mode' then 'Safe Mode' is recommended setting for most users - combining the highest levels of security with an easy-to-manage number of HIPS alerts.
- Clean PC Mode:** From the time you set the slider to 'Clean PC Mode', Defense+ learns the activities of the applications currently installed on the computer while all new executables introduced to the system are monitored and controlled. This patent-pending mode of operation is the recommended option on a new computer or one that the user knows to be clean of malware and other threats. From this point onwards HIPS alerts the user whenever a new, unrecognized application is being installed. In this mode, the files in 'Unrecognized Files' are excluded from being considered as clean and are monitored and controlled.
- Training Mode:** Defense+ monitors and learn the activity of any and all executables and create automatic 'Allow' rules until the security level is adjusted. You do not receive any HIPS alerts in 'Training Mode'. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications and executables installed on your computer are safe to run.

Configuring the Monitoring Settings

The activities, entities and objects that should be monitored by HIPS can be configured by clicking the [Monitoring Settings](#) link.

Note: The settings you choose here are universally applied. If you disable monitoring of an activity, entity or object using this interface it completely switches off monitoring of that activity on a *global* basis - effectively creating a universal '**Allow**' rule for that activity. This 'Allow' setting **over-rules** any Ruleset specific 'Block' or 'Ask' setting for that activity that you may have selected using the 'Access Rights' and 'Protection Settings' interface.



Activities To Monitor:

- Interprocess Memory Access** - Malware programs use memory space modification to inject malicious code for numerous types of attacks, including recording your keyboard strokes; modifying the behavior of the invaded application; stealing confidential data by sending confidential information from one process to another process etc. One of the most serious aspects of memory-space breaches is the ability of the offending malware to take the identity of the invaded process, or 'impersonate' the application under attack. This makes life harder for traditional virus scanning software and intrusion-detection systems. Leave this box checked and HIPS alerts you when an application attempts to modify the memory space allocated to another application (**Default = Enabled**).
- Windows/WinEvent Hooks** - In the Microsoft Windows® operating system, a hook is a mechanism by which a function can intercept events (messages, mouse actions, keystrokes) *before* they reach an application. The function can act on events and, in some cases, modify or discard them. Originally developed to allow legitimate software developers to develop more powerful and useful applications, hooks have also been exploited by hackers to create more powerful malware. Examples include malware that can record every stroke on your keyboard; record your mouse movements; monitor and modify all messages on your computer; take over control of your mouse and keyboard to remotely administer your computer. Leaving this box checked means that you are warned every time a hook is

executed by an untrusted application (**Default = Enabled**).

- **Device Driver Installations** - Device drivers are small programs that allow applications and/or operating systems to interact with a hardware device on your computer. Hardware devices include your disk drives, graphics card, wireless and LAN network cards, CPU, mouse, USB devices, monitor, DVD player etc.. Even the installation of a perfectly well-intentioned device driver can lead to system instability if it conflicts with other drivers on your system. The installation of a malicious driver could, obviously, cause irreparable damage to your computer or even pass control of that device to a hacker. Leaving this box checked means HIPS alerts you every time a device driver is installed on your machine by an untrusted application (**Default = Enabled**).
- **Processes' Terminations** - A process is a running instance of a program. (for example, the Comodo Internet Security process is called 'cis.exe'. Press 'Ctrl+Alt+Delete' and click on 'Processes' to see the full list that are running on your system). Terminating a process, obviously, terminates the program. Viruses and Trojan horses often try to shut down the processes of any security software you have been running in order to bypass it. With this setting enabled, Defense+ monitors and alerts you to all attempts by an untrusted application to close down another application (**Default = Enabled**).
- **Process Execution** - Typical malware like rootkits, keylogger etc. would often invoke by itself and runs its process mostly at the background. These processes, invisible at the foreground will act as agents for infecting your computer and to steal your confidential and sensitive information like your credit card details and passwords and pass to hackers. With this setting enabled, the HIPS monitors and alerts you to whenever a process is invoked by an untrusted application. (**Default = Enabled**).
- **Windows Messages** - This setting means Comodo Internet Security monitors and detects if one application attempts to send special Windows Messages to modify the behavior of another application (e.g. by using the WM_PASTE command) (**Default = Enabled**).
- **DNS/RPC Client Service** - This setting alerts you if an application attempts to access the 'Windows DNS service' - possibly in order to launch a DNS recursion attack. A DNS recursion attack is a type of Distributed Denial of Service attack whereby an malicious entity sends several thousand spoofed requests to a DNS server. The requests are spoofed in that they appear to come from the target or 'victim' server but in fact come from different sources - often a network of 'zombie' pc's which are sending out these requests without the owners knowledge. The DNS servers are tricked into sending all their replies to the victim server - overwhelming it with requests and causing it to crash. Leaving this setting enabled prevents malware from using the DNS Client Service to launch such an attack (**Default = Enabled**).

Background Note: DNS stands for Domain Name System. It is the part of the Internet infrastructure that translates a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the Internet routes messages to their destinations on the basis of this destination IP address, not the domain name. Whenever you type a domain name, your Internet browser contacts a DNS server and makes a 'DNS Query'. In simplistic terms, this query is 'What is the IP address of example.com?'. Once the IP address has been located, the DNS server replies to your computer, telling it to connect to the IP in question.

Objects To Monitor Against Modifications:

- **Protected COM Interfaces** enables monitoring of COM interfaces you specified from the COM Protection pane. (**Default = Enabled**)
- **Protected Registry Keys** enables monitoring of Registry keys you specified from the Registry Protection pane. (**Default = Enabled**).
- **Protected Files/Folders** enables monitoring of files and folders you specified from the File Protection pane. (**Default = Enabled**).

Objects To Monitor Against Direct Access:

Determines whether or not Comodo Internet Security should monitor access to system critical objects on your computer. Using direct access methods, malicious applications can obtain data from a storage devices, modify or infect other executable software, record keystrokes and more. Comodo advises the average user to leave these settings enabled:

- **Physical Memory:** Monitors your computer's memory for direct access by an applications and processes. Malicious programs attempt to access physical memory to run a wide range of exploits - the most famous being the 'Buffer Overflow' exploit. Buffer overruns occur when an interface designed to store a certain amount of data at a specific address in memory allows a malicious process to supply too much data to that address. This overwrites its internal structures and can be used by malware to force the system to execute its code (**Default = Enabled**).
- **Computer Monitor:** Comodo Internet Security raises an alert every time a process tries to directly access your computer monitor. Although legitimate applications sometimes require this access, there is also an emerging category

of spyware programs that use such access to monitor users' activities. (for example, to take screen shots of your current desktop; to record your browsing activities etc) **(Default = Enabled)**.

- **Disks:** Monitors your local disk drives for direct access by running processes. This helps guard against malicious software that need this access to, for example, obtain data stored on the drives, destroy files on a hard disk, format the drive or corrupt the file system by writing junk data **(Default = Enabled)**.
- **Keyboard:** Monitors your keyboard for access attempts. Malicious software, known as 'key loggers', can record every stroke you make on your keyboard and can be used to steal your passwords, credit card numbers and other personal data. With this setting checked, Comodo Internet Security alerts you every time an application attempts to establish direct access to your keyboard **(Default = Enabled)**.

Checkbox Options

- **Do NOT show popup alerts** - Configure whether or not you want to be notified when the HIPS encounters a malware. Choosing 'Do NOT show popup alerts' will minimize disturbances but at some loss of user awareness **(Default = Disabled)**.

If you choose not to show alerts then you have a choice of default responses that CIS should automatically take - either 'Block Requests' or 'Allow Requests'.

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

☒ Do NOT show popup alerts

☐ Set popup alerts to verbose mode

☐ Create rules for safe applications

☐ Set new on-screen alert timeout to secs

Advanced

☐ Enable adaptive mode under low system resources

☐ Block all unknown requests when the application is not running

☐ Enable enhanced protection mode (Requires a system restart)

- **Set popup alerts to verbose mode** - Enabling this option instructs CIS to display HIPS Alerts in verbose mode, providing more more informative alerts and more options for the user to allow or block the requests **(Default = Disabled)**.
- **Create rules for safe applications** - Automatically creates rules for safe applications in HIPS Ruleset **(Default = Disabled)**.

Note: HIPS trusts the applications if:

- The application/file is included in the Trusted Files list
- The application is from a vendor included in the Trusted Software Vendors list
- The application is included in the extensive and constantly updated Comodo safelist.

By default, CIS does not automatically create 'allow' rules for safe applications. This helps saving the resource usage, simplifies the rules interface by reducing the number of 'Allowed' rules in it, reduces the number of pop-up alerts and is beneficial to beginners who find difficulties in setting up the rules.

Enabling this checkbox instructs CIS to begin learning the behavior of safe applications so that it can automatically generate the 'Allow' rules. These rules are listed in the HIPS Rules interface. The Advanced users can edit / modify the rules as they wish.

Background Note: Prior to version 4.x, CIS would automatically add an allow rule for 'safe' files to the rules interface. This allowed advanced users to have granular control over rules but could also lead to a cluttered rules interface. The constant addition of these 'allow' rules and the corresponding requirement to learn the behavior of applications that are already considered 'safe' also took a toll on system resources. In version 4.x and above, 'allow' rules for applications considered 'safe' are not automatically created - simplifying the rules interface and cutting resource overhead with no loss in security. Advanced users can re-enable this setting if they require the ability to edit rules for safe applications (or, informally, if they preferred the way rules were created in CIS version 3.x).

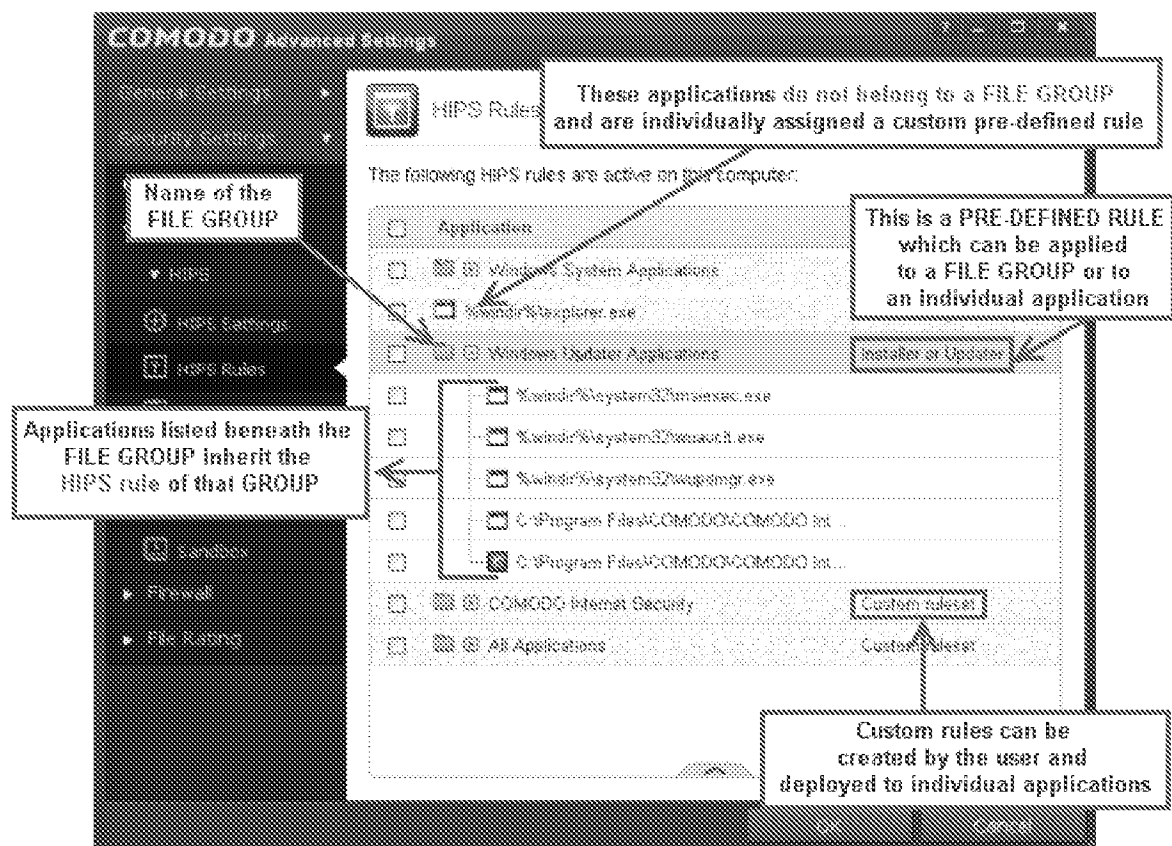
- **Set new on-screen alert time out to:** Determines how long the HIPS shows an alert for without any user intervention. By default, the timeout is set at 120 seconds. You may adjust this setting to your own preference.

Advanced HIPS Settings

- **Enable adaptive mode under low system resources** - Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CIS functions to fail. With this option enabled, CIS will attempt to locate and utilize memory using adaptive techniques so that it can complete its pending tasks. However, the cost of enabling this option may be reduced performance in even lightly loaded systems (**Default = Disabled**).
- **Block all unknown requests if the application is closed** - Selecting this option blocks all unknown execution requests if Comodo Internet Security is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know your machine is already 'clean' and are looking just to enable the highest CIS security settings then it is OK to leave this box unchecked. (**Default = Disabled**)
- **Enable enhanced protection mode** - On 64 bit systems, enabling this mode will activate additional host intrusion prevention techniques to countermeasure extremely sophisticated malware that tries to bypass regular countermeasures. Because of limitations in Windows 7/8 x64 systems, some HIPS functions in previous versions of CIS could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS. CIS requires a system restart for enabling enhanced protection mode. (**Default = Disabled**)

6.2.2.2. Active HIPS Rules

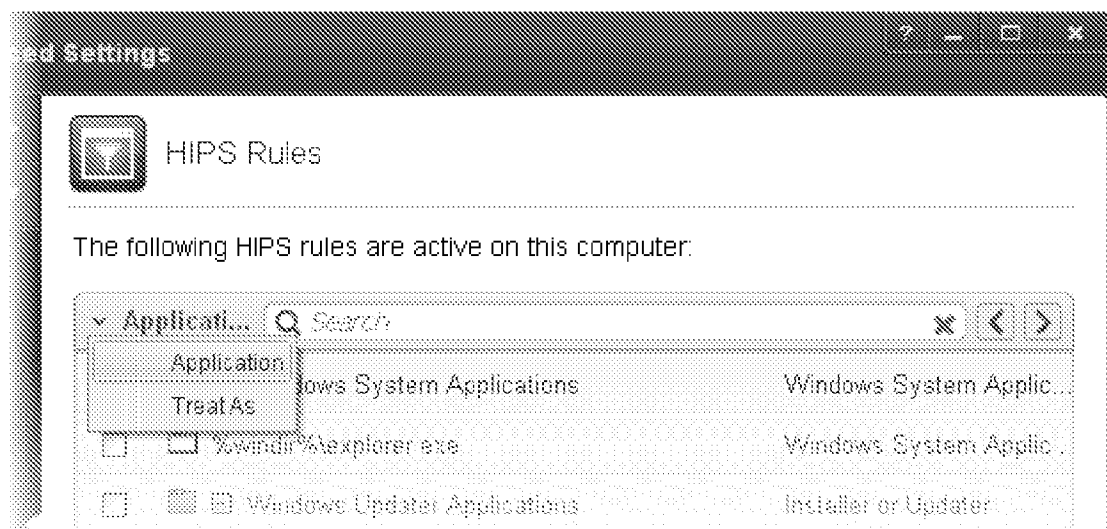
The HIPS rules tab lists the different groups of applications installed in your system and the Rulesets applied to them. You can change the ruleset applied to selected applications and also create custom rulesets to be applied to selected applications.



The first column, **Application Name**, displays a list of the applications on your system for which a HIPS ruleset has been deployed. If the application belongs to a file group, then all member applications assume the ruleset of the file group. The second column, **Treat as**, column displays the name of the HIPS ruleset assigned to the application or group of applications in column one.

You can use the search option to find a specific file or a company in the list.

To use the search option, click the search icon  at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the  icon in the search field to close the search option.

General Navigation:

Clicking the Up arrow at the bottom center of the interface opens an option panel with the following options:

- **Add** - Allows the user to Add a new Application to the list then create it's ruleset. See the section 'Creating or Modifying a HIPS Ruleset'.
- **Edit** - Allows the user to modify the HIPS rule of the selected application. See the section 'Creating or Modifying a HIPS Ruleset'.
- **Remove** - Deletes the selected ruleset.

Note: You cannot remove individual applications from a file group using this interface - you must use the 'File Groups' interface to do this.

- **Purge** - Runs a system check to verify that all the applications for which rulesets are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.

Users can re-order the priority of rules by simply selecting the application name or file group name in question, clicking the handle at the bottom center and selecting 'Move Up' or 'Move Down' from the options. To alter the priority of applications that belong to a file group, you must use the 'File Groups' interface.

Creating or Modifying a HIPS Ruleset

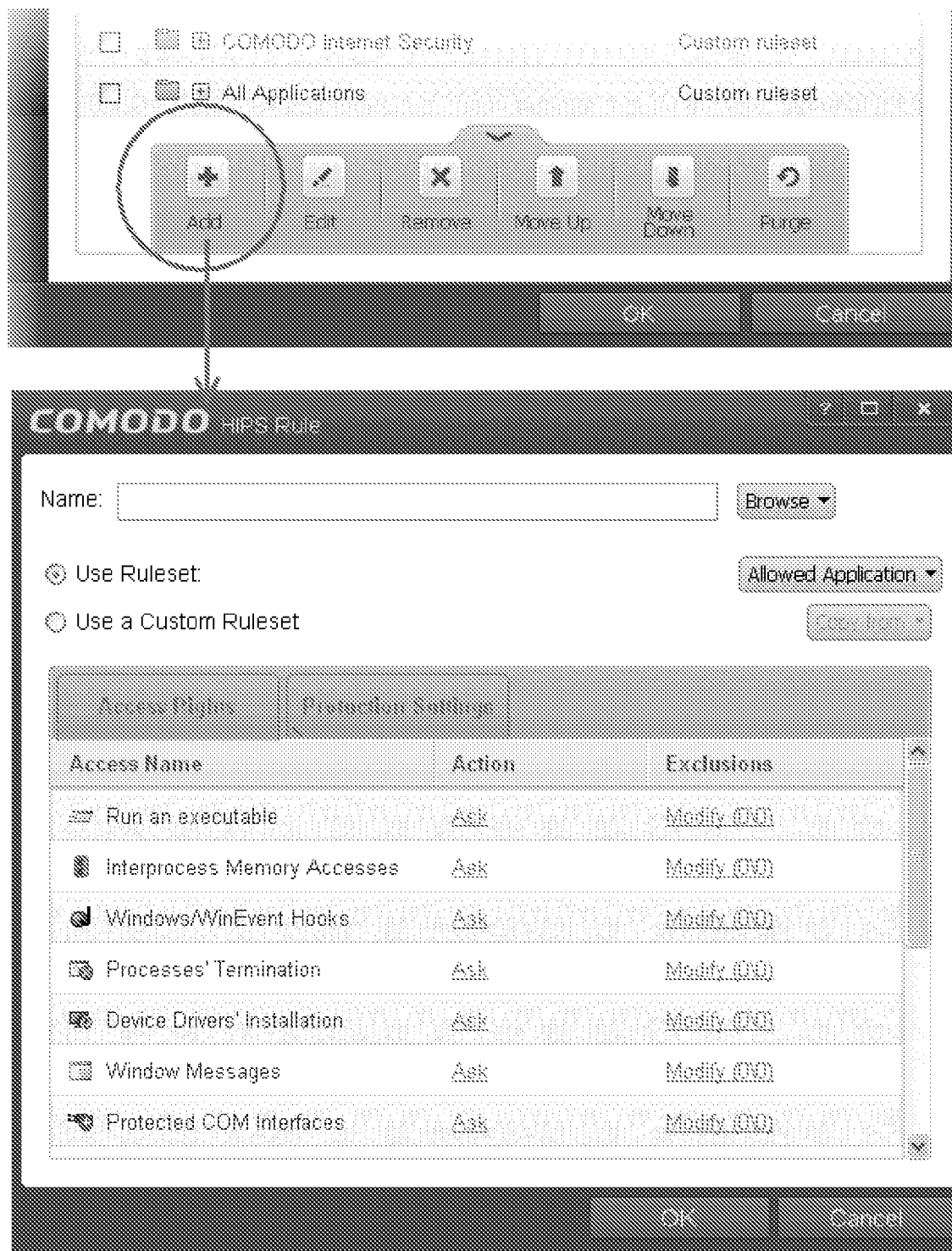
To begin defining an application's HIPS Ruleset

1. Select the application or file group that you wish the ruleset to apply to.

2. Configure the ruleset for this application.

Step 1 - Select the application or file group that you wish the ruleset to apply to

If you wish to define a rule for a new application (i.e. one that is not already listed), click the handle from the HIPS Rules pane and select 'ADD'. This brings up the 'HIPS Rule' interface as shown below.

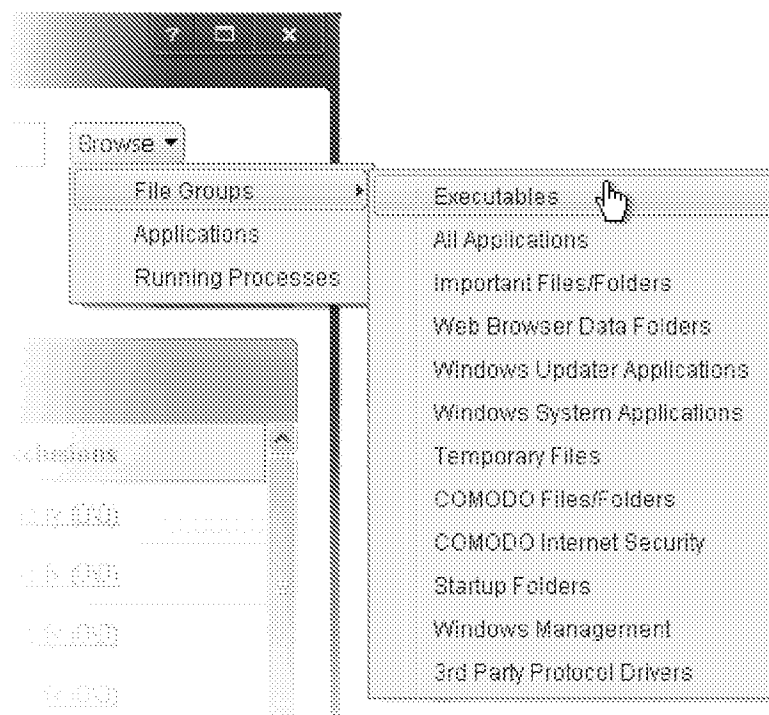


Because you are defining the HIPS rule settings for a new application, you can notice that the 'Name' box is blank. (If you were editing an existing rule instead, then this interface would show that application's name with installation path or application group's name.)

- Click 'Browse' to begin.

You now have 3 methods available to choose the application for which you wish to create a Ruleset - File Groups; Applications and Running Processes.

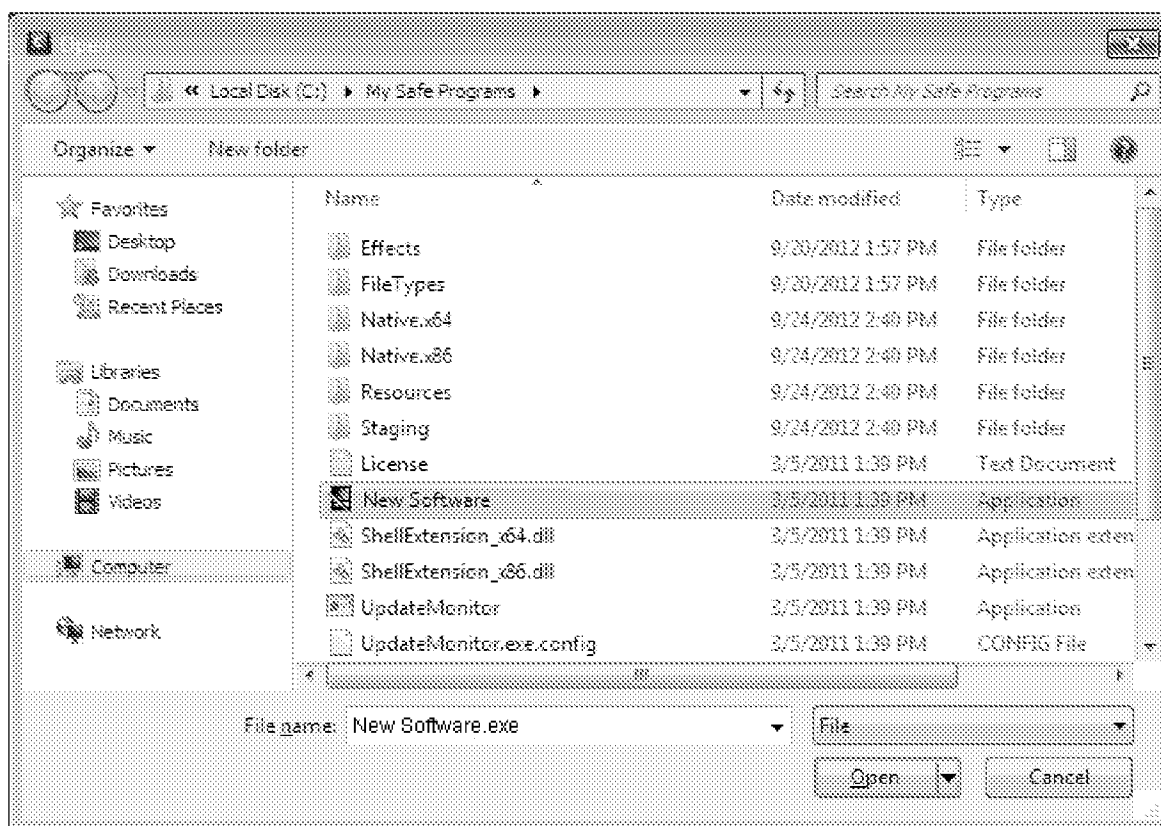
1. **File Groups** - Choosing this option allows you to create a HIPS ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.



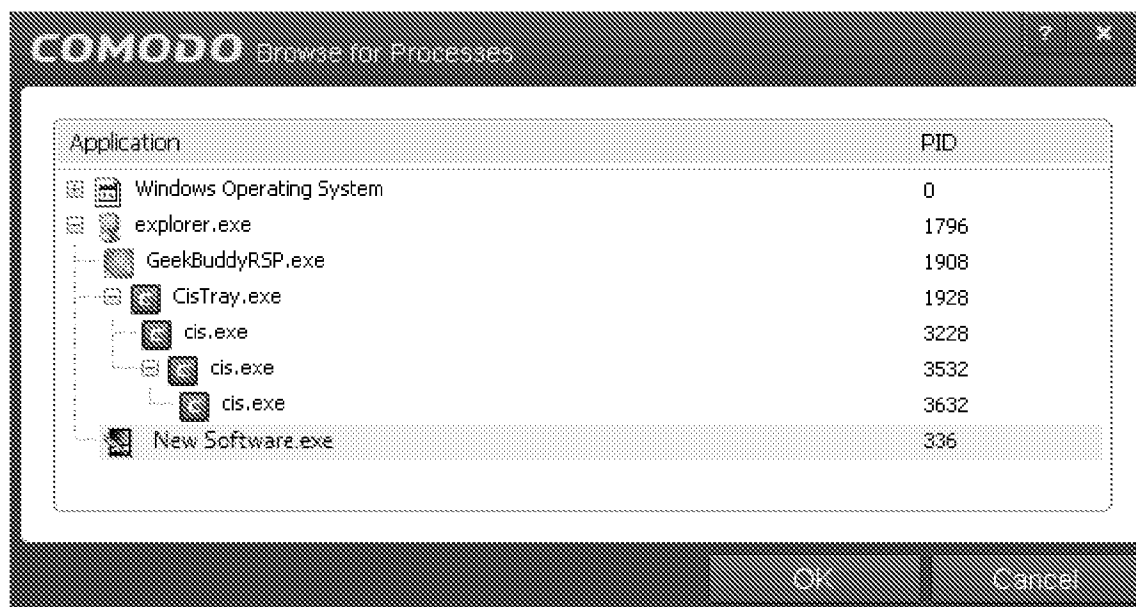
To view the file types and folders that are affected by choosing one of these options, you need to visit the 'File Groups' interface.

The 'File Groups' interface can be accessed by the following method:

- Navigate to Advanced Settings > Defense+ > HIPS > Protected Files, click the up arrow from the bottom of the interface and select 'Groups' from the options.
2. **Applications** - This option is the easiest for most users and simply allows you to browse to the location of the application for which you want to deploy the ruleset.



3. **Running Processes** - as the name suggests, this option allows you to create and deploy a ruleset for any process that is currently running on your PC.



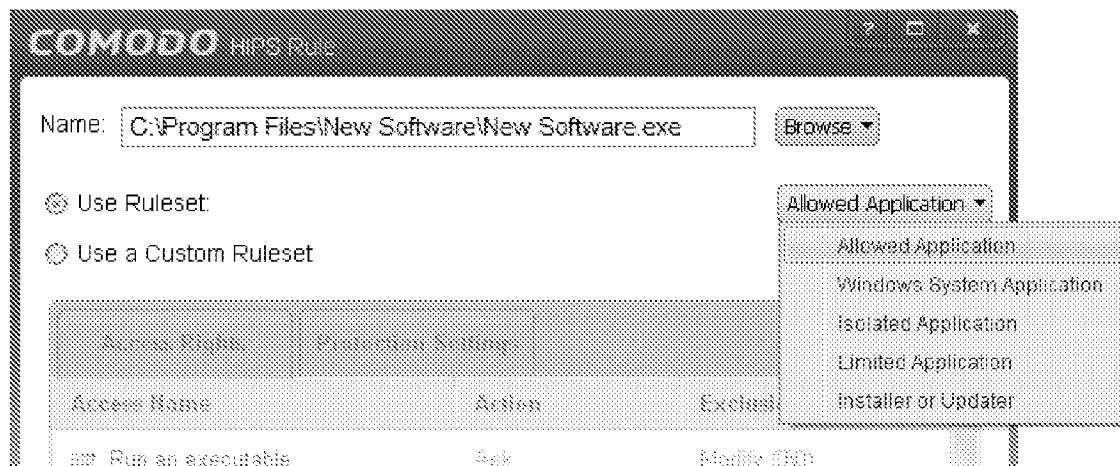
Having selected the individual application, running process or file group, the next stage is to Configure the rules for this ruleset.

Step 2 - Configure the HIPS Ruleset for this application

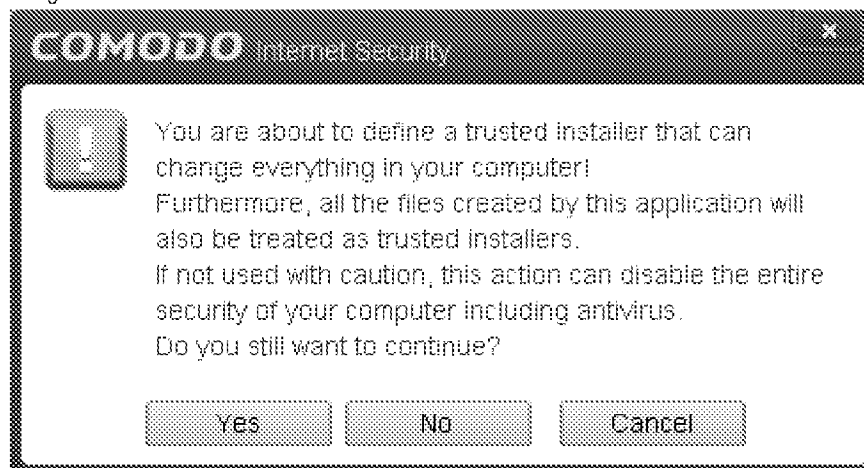
There are two broad options available for selecting a ruleset that applies to an application - Use Ruleset or Use a Custom Ruleset.

1. **Use Ruleset** - Selecting this option allows the user to quickly deploy an existing HIPS ruleset on to the target

application. Choose the ruleset you wish to use from the drop down menu. In the example below, we have chosen 'Allowed Application'. The name of the ruleset you choose is displayed in the 'Treat As' column for that application in the HIPS Rules interface (**Default = enabled**).



Note on 'Installer or Updater' Rule : Applying the Predefined Ruleset 'Installer or Updater' for an application defines it as a trusted installer and all files created by the application will also be considered as trusted files. Some applications may have hidden code that could impair the security of your computer if allowed to create files of their own. Comodo advises you to use this Predefined Ruleset - 'Installer or Updater' with caution. On applying this ruleset to any application, an alert dialog will be displayed, describing the risks involved.



General Note: Predefined Rulesets, once chosen, cannot be modified directly from this interface - they can only be modified and defined using the 'Rulesets' interface. If you require the ability to add or modify settings for an specific application then you are effectively creating a new, custom ruleset and should choose the more flexible Use a Custom Ruleset option instead.

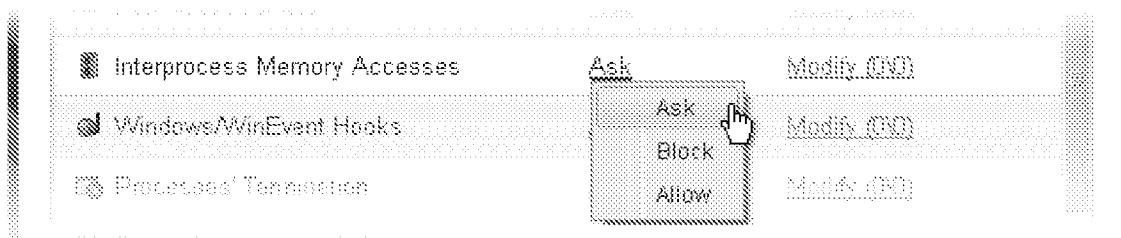
2. **Use a Custom Ruleset** - designed for more experienced users, the 'Custom Ruleset' option enables full control over the configuration specific security ruleset and the parameters of each rule within that ruleset. The Custom ruleset has two main configuration areas - Access Rights and Protection Settings (**Default = Disabled**).

In simplistic terms 'Access Rights' determine what the application *can do* to other processes and objects whereas 'Protection Settings' determine what the application *can have done to it* by other processes.

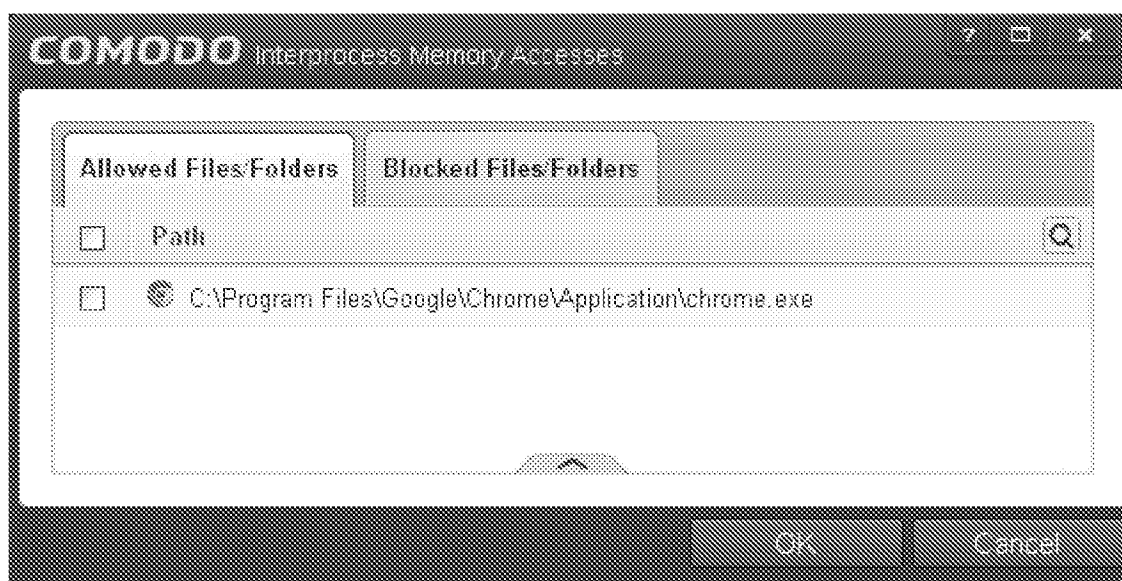
- i. **Access Rights** - The Process Access Rights tab allows you to determine what activities the applications in your custom ruleset are allowed to execute. These activities are called 'Access Names'.



Refer to the section **HIPS Behavior Settings > Activities to Monitor** to view a list of definitions of the Action Names listed above and the implications of choosing the action from 'Ask', 'Allow' or 'Block' for each setting as shown below:



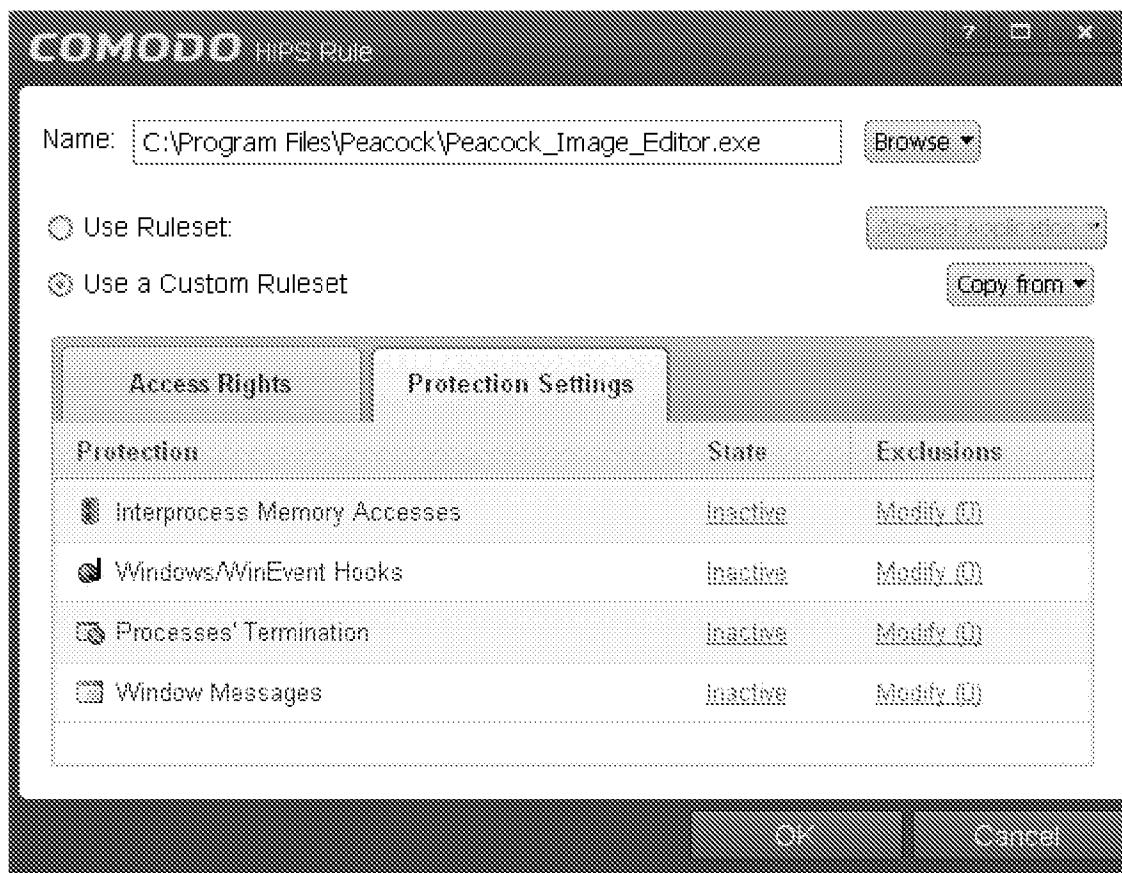
- Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the ruleset by clicking the 'Modify' link on the right.
- Select the 'Allowed Applications' or 'Blocked Applications' tab depending on the type of exception you wish to create.



Clicking the handle and selecting 'Add' allows you to choose which applications or file groups you wish this exception to apply to. (click [here](#) for an explanation of available options).

In the example above, the default action for 'Interprocess Memory Access' is 'Ask'. This means HIPS will generate an alert asking your permission if 'New Software.exe' tries to modify the memory space of any other program. Clicking 'Modify' then adding 'opera.exe' to the 'Allowed Applications' tab creates an exception to this rule. New Software.exe can now modify the memory space of opera.exe.

- ii. **Protection Settings** - Protection Settings determine how protected the application or file group in your ruleset is against activities by other processes. These protections are called 'Protection Types'.



- Select 'Active' to enable monitoring and protect the application or file group against the process listed in the 'Protection Type' column. Select 'Inactive' to disable such protection.

[Click here](#) to view a list of definitions of the 'Protection Types' listed above and the implications of activating each setting.

Exceptions to your choice of 'Active' or 'Inactive' can be specified in the application's Ruleset by clicking the 'Modify' link on the right.

3. Click 'OK' to confirm your settings.

6.2.2.3. HIPS Rule Sets

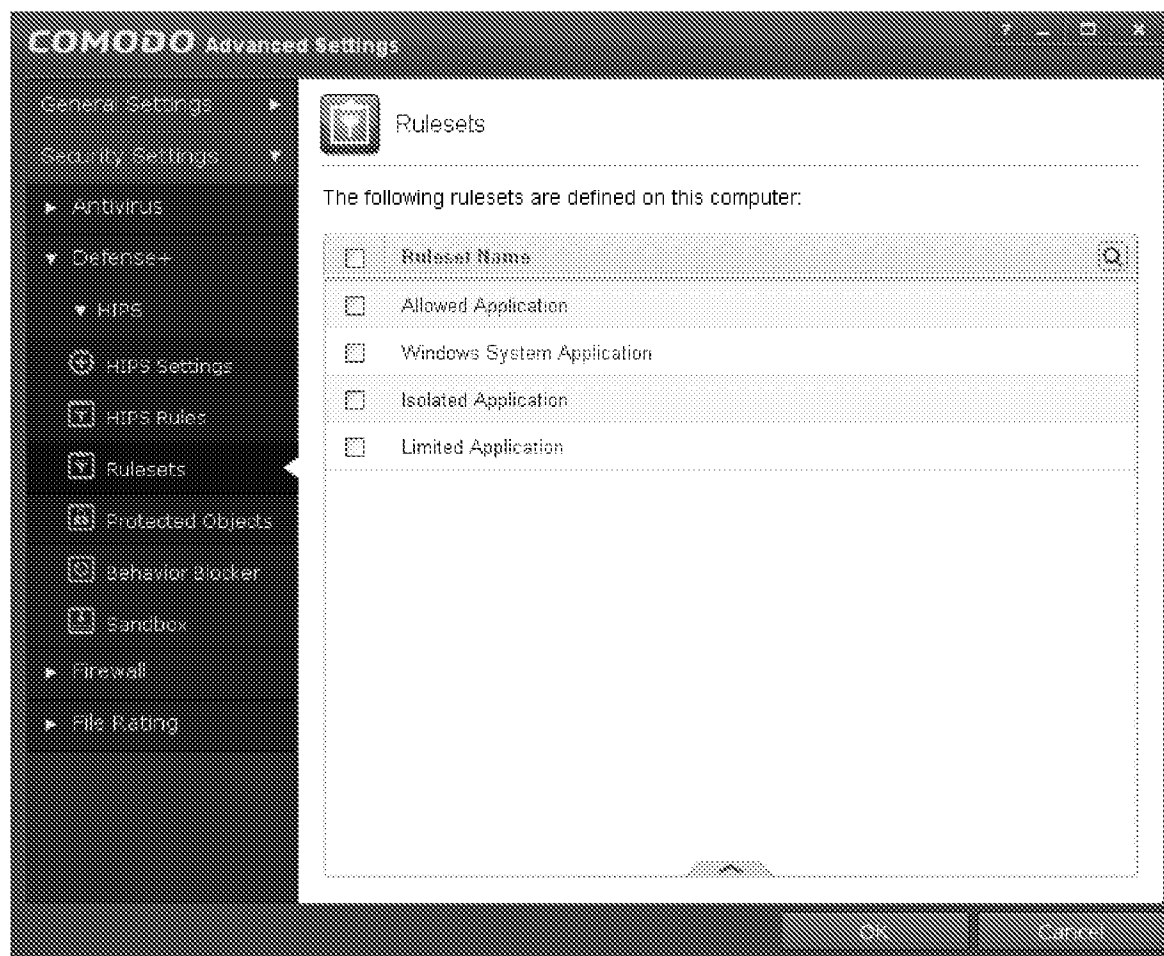
A Pre-defined ruleset is a set of access rights and protection settings that has been saved and can be re-used and deployed on multiple applications or groups. Each ruleset is comprised of a number of 'Rules' and each of these 'Rules' is defined by a set of conditions/settings/parameters. 'Predefined rulesets' is a set of rulesets that concern an application's access rights to memory, other programs, the registry etc.

Note: This section is for advanced and experienced users. If you are a novice user to Comodo Internet Security, we advise you first read the Active HIPS Rules section in this help guide if you have not already done so.

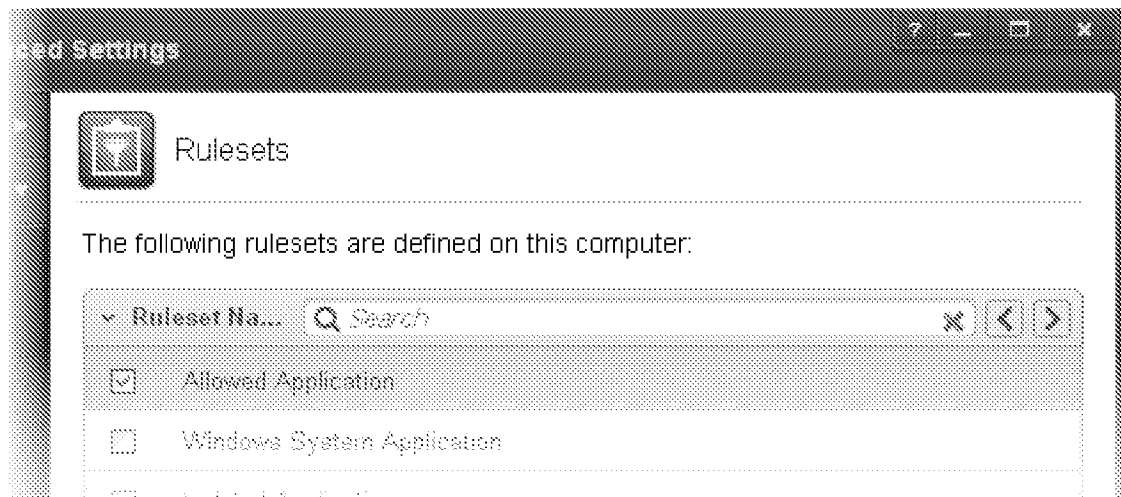
Although each application's ruleset could be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Internet Security contains a selection of rulesets according to broad application categories. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application. Users can, of course, modify these predefined rulesets to suit their environment and requirements.

To configure this category

- Navigate to: Advanced Tasks > Security Settings > Defense+ > HIPS > Rulesets. There are four default Rulesets listed under the 'Rules' column.



You can use the search option to find a ruleset in the list by clicking the search icon  at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the ruleset in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the  icon in the search field to close the search option.

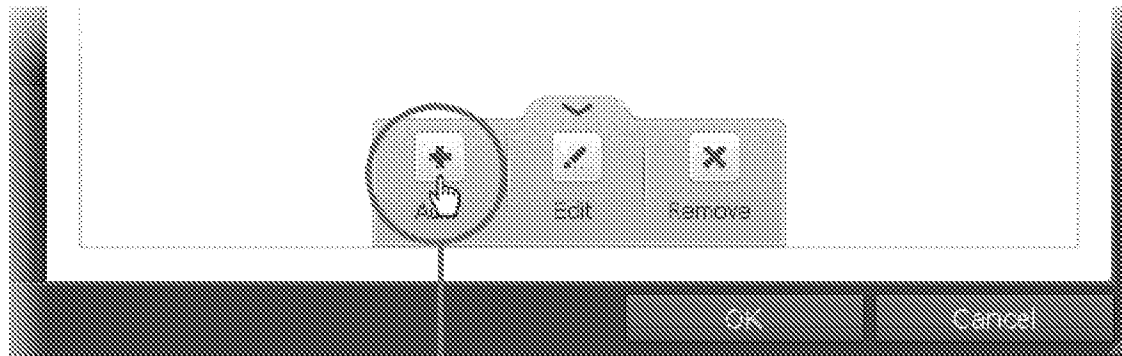
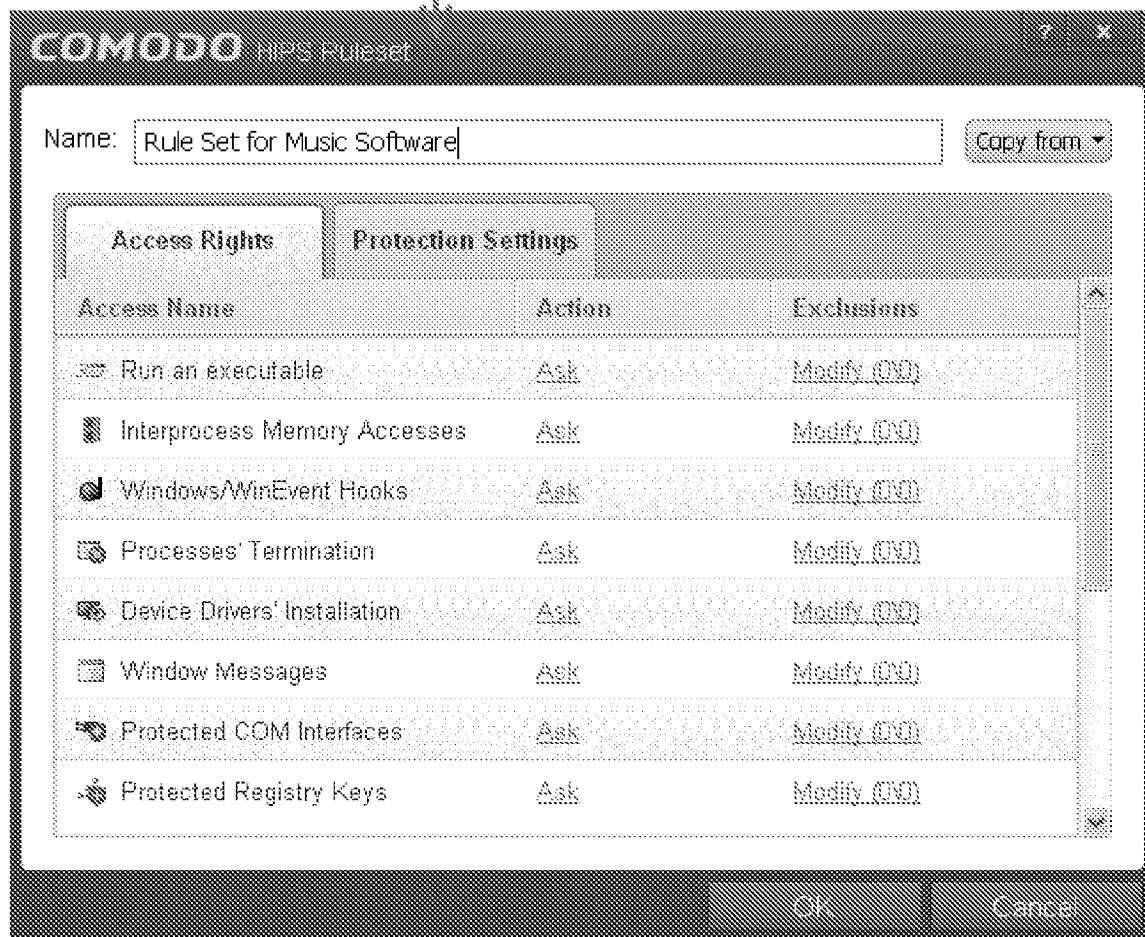
To view or edit an existing predefined ruleset

- Double click on the Ruleset in the list
or
- Select the Ruleset, click the handle at the bottom of the interface and choose 'Edit' from the options.

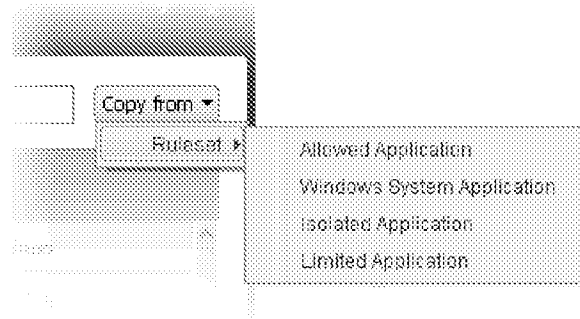
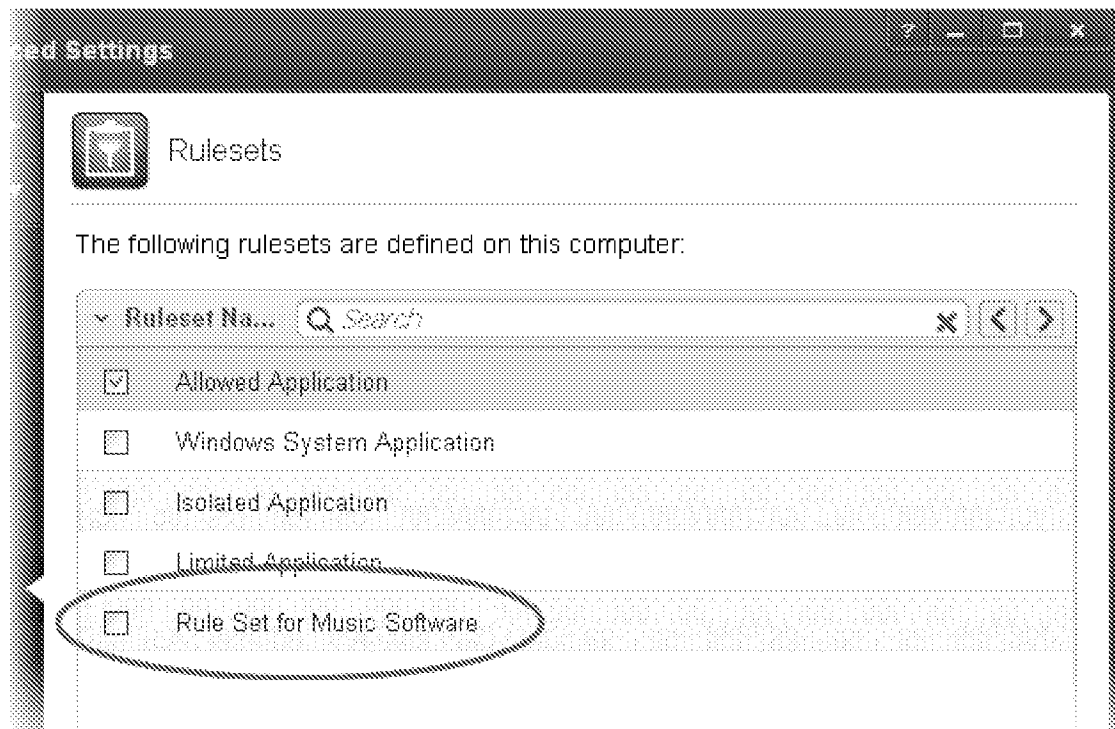
From here, you can modify a ruleset and, if desired, make changes to its 'Access Rights' and 'Protection Settings'. Any changes you make here are automatically rolled out to all applications that are currently applied with the ruleset.

To create a new predefined ruleset

- Click the handle at the bottom of the interface and choose 'Add' from the options.



- Enter a name for the new ruleset.
- To copy the Access Rights and Protection Settings from another pre-existing ruleset, click 'Copy From' and select the ruleset from the drop-down
- To customize the Access Rights and Protection Settings as per the requirements of this new rule set, follow the procedure explained in the section Use a Custom Ruleset.
- Click OK to save the new ruleset.

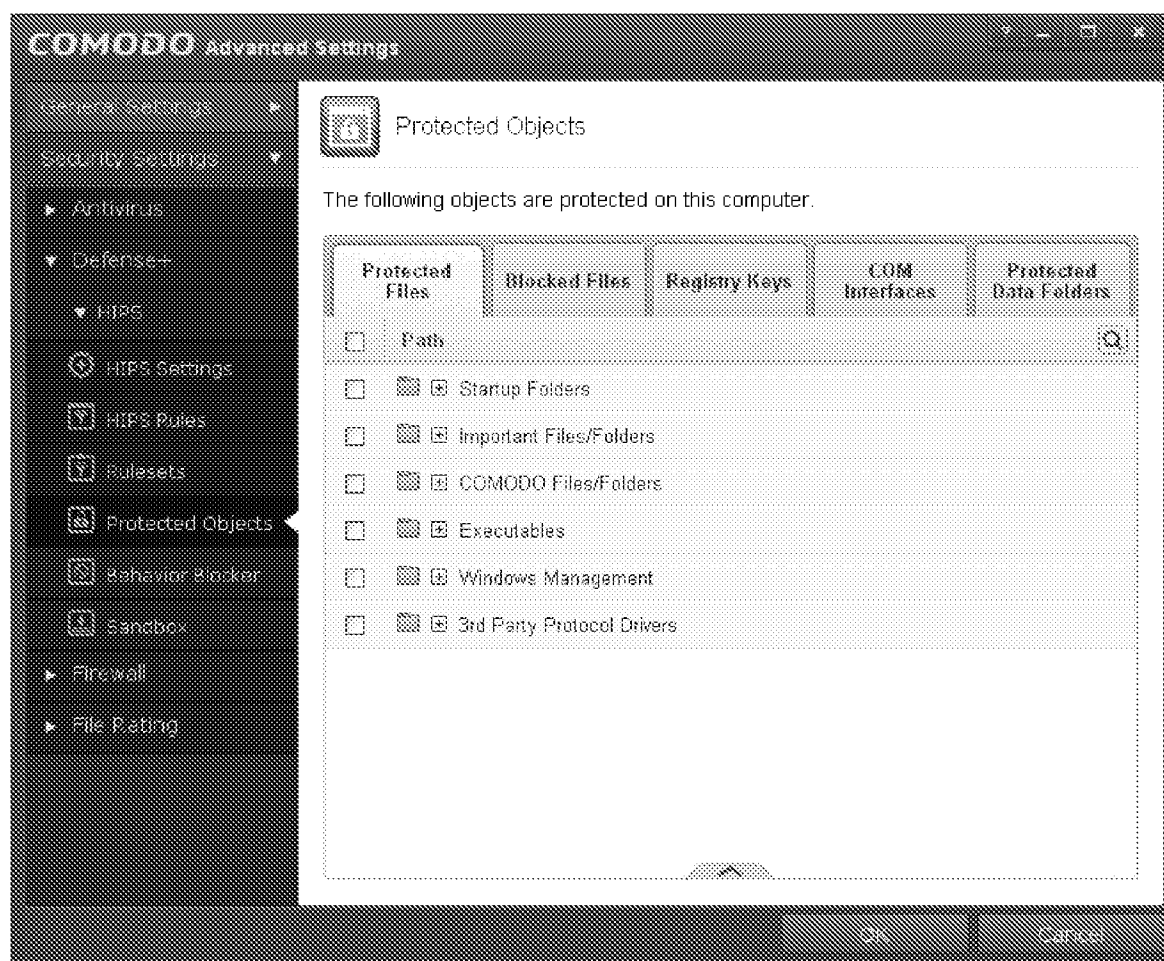


Once created, your ruleset is available for deployment onto specific application or file groups via the Active HIPS Rules interface.

6.2.2.4. Protected Objects

The Protected Objects panel allows you to protect specific files and folders, system critical registry keys and COM interfaces against access or modification by unauthorized processes and services.

The Protected Objects panel can be accessed by clicking Security Settings > Defense+ > HIPS > Protected Objects from the Advanced Settings interface.

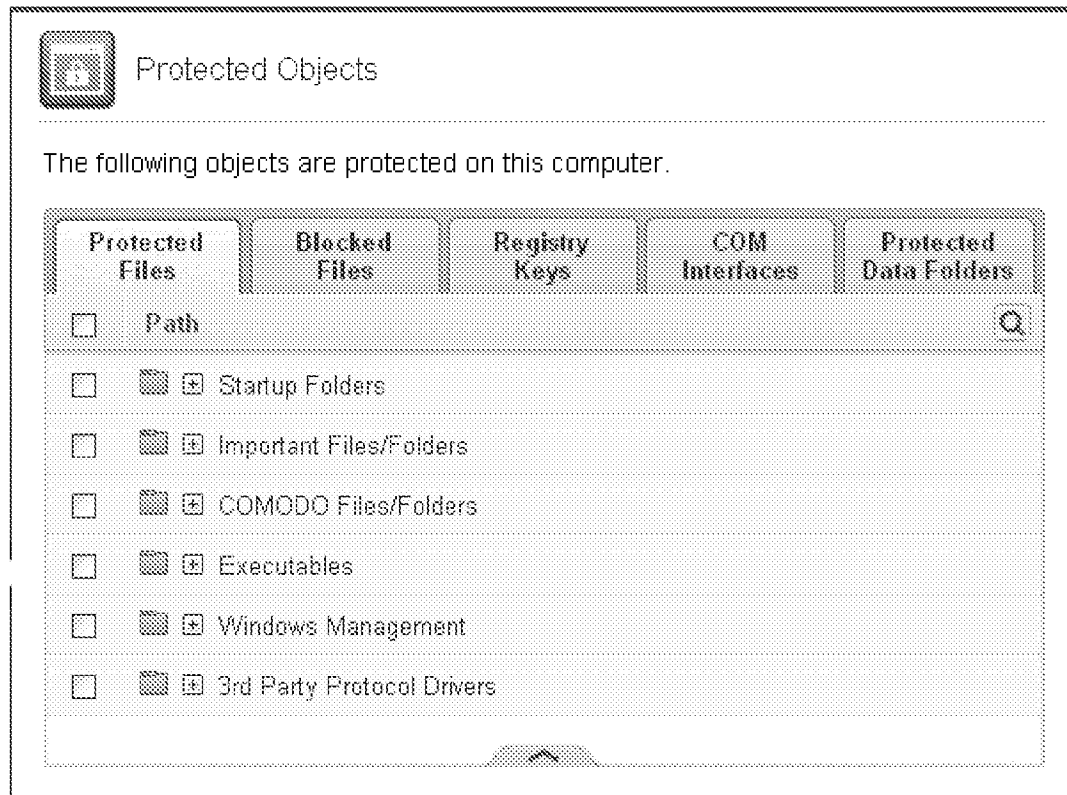


The panel has five tabs:

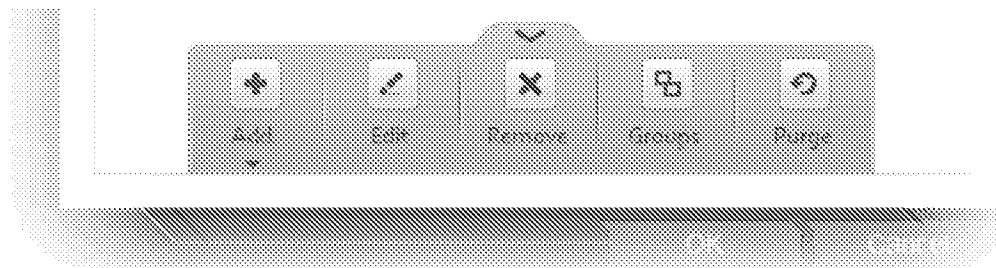
- **Protected Files** - Allows you to specify programs, applications and files that are to be protected from changes
- **Blocked Files** - Allows you to specify programs, applications and files that are to be blocked from execution and opening
- **Registry Keys** - Allows you to specify registry keys that are to be protected from changes
- **COM Interfaces** - Allows you to specify COM interfaces that are to be protected from changes
- **Protected Data Folders** - Allows you to specify folders containing data files that are to be protected from changes

6.2.2.4.1. Protected Files

The Protected Files tab displays a list of files and file groups that are protected from access by other programs, especially malicious programs such as virus, Trojans and spyware. It is also useful for safeguarding very valuable files (spreadsheets, databases, documents) by denying anyone and any program the ability to modify the file - avoiding the possibility of accidental or deliberate sabotage. If a file is 'Protected' it can still be accessed and read by users, but not altered. A good example of a file that ought to be protected is your 'hosts' file (c:\windows\system32\drivers\etc\hosts). Placing this in the 'Protected Files and Folders' area would allow web browsers to access and read from the file as per normal. However, should any process attempt to modify it then Comodo Internet Security blocks this attempt and produce a 'Protected File Access' pop-up alert.

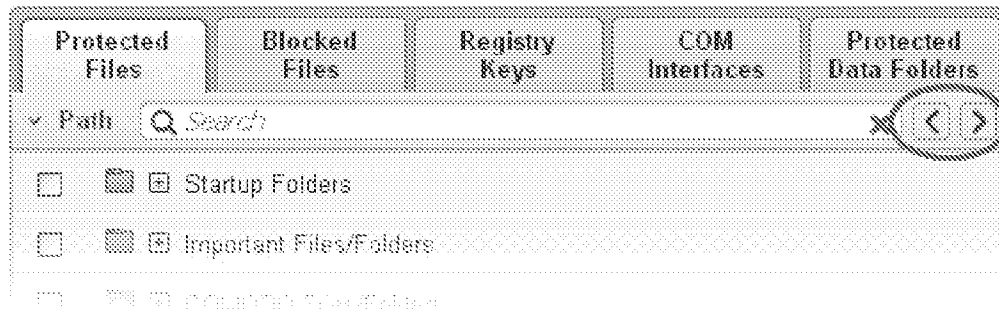


Clicking the handle at the bottom of the interface opens an options panel with the following options:

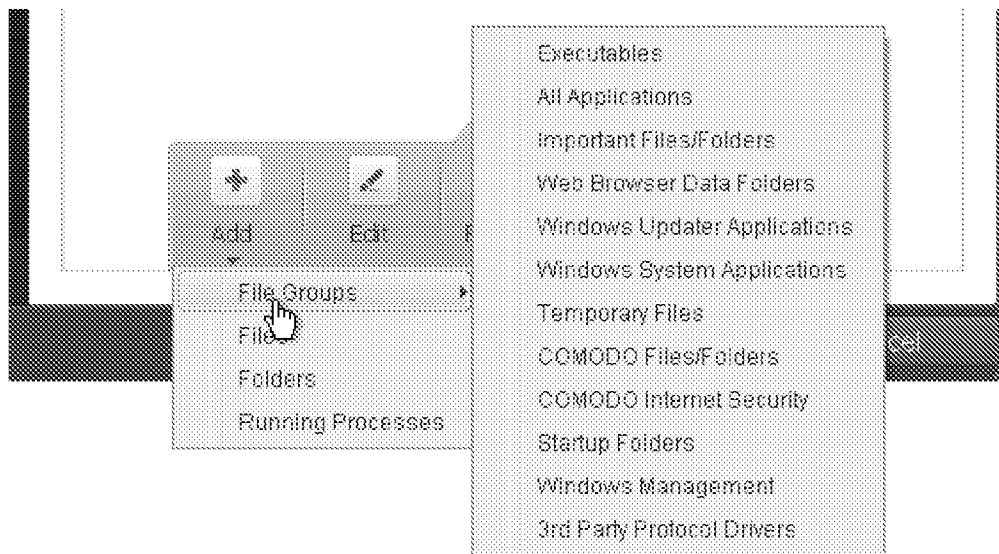


- **Add** - Allows you to add individual files, programs, applications to Protected Files.
- **Edit** - Allows you to edit the path of the file or group of a selected item in the Protected Files interface.
- **Remove** - Deletes the currently highlighted file or file group.
- **Groups** - Opens the Manage Groups interface that allows you to edit pre-defined file groups and define new file groups for inclusion in Protected Files list
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

You can use the search option to find a specific file or file group in the list by clicking the search icon  at the far right in the column header and entering the file/group name in full or part. You can navigate through the successive results by clicking the left and right arrows.



To manually add an individual file, folder, file group or process



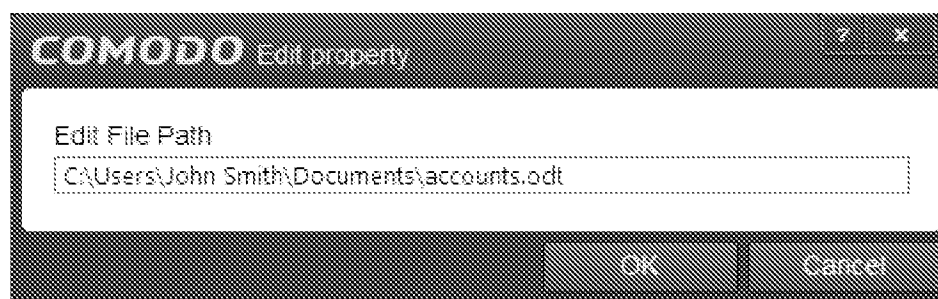
- Click the handle from the bottom center and select 'Add'.

You can add the files by following methods:

- Selecting from File Groups
- Selecting from currently running Processes
- Browsing to the File
- Browsing to the Folder

To edit an item in the Protected Files list

- Select the item from the list, click the handle from the bottom and select Edit. The 'Edit Property' dialog will appear.



- Edit the file path, if you have relocated the file and click OK

To delete an item from Protected Files list

- Select the item from the list, click the handle from the bottom and select 'Remove'.

The selected item will be deleted from the protected files list. CIS will not generate alerts, if the file or program is subjected to unauthorized access.

File Groups

File groups are handy, predefined groupings of one or more file types. Creating a file group allows you to quickly deploy a ruleset across multiple file types and applications.

To open the Manage File Groups interface

1. Click the handle from the bottom center of Protected Files interface and select 'Groups'.

The Manage File Groups interface will open.



This interface allows you to

- Create a new File Group
- Edit the names of an Existing File Group
- Add a file to an existing file group
- Remove existing file group(s) or individual file(s) from existing group

Note: This area is for the creation and modification of file groups only. You are not able to modify the security ruleset of any applications or files from here. To do that, you should use the NIPS Rules interface or the Predefined Rules Interface.

- To add a new group or add files to an existing group, click the handle from the bottom and click 'Add'.



- Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click OK

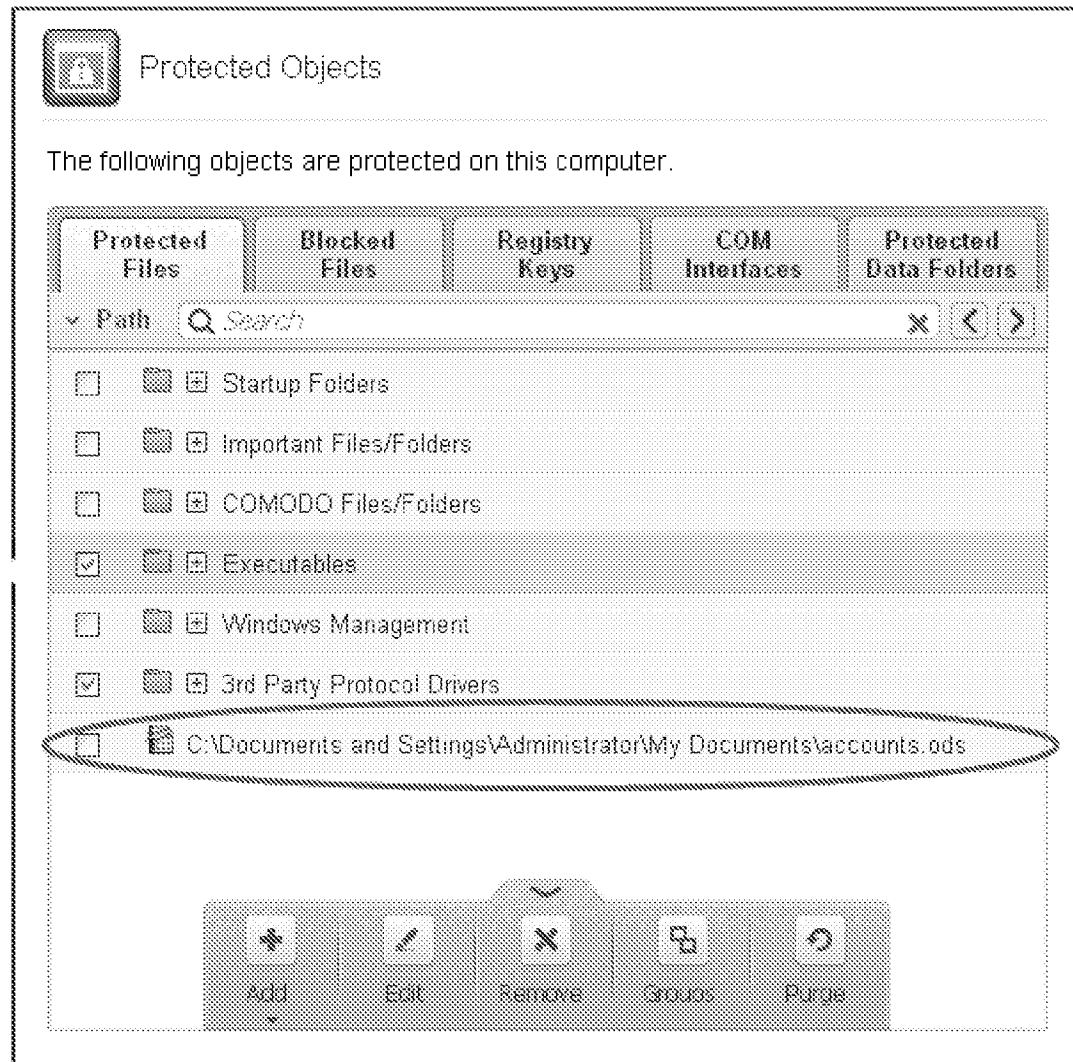


- Add files to a group** - Select the Group, click the handle and select Add. Choose from 'Files', 'Folders' or 'Running Processes' to add files by browsing to the file or folder or from currently running processes
- To edit an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the Edit Property dialog
- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual file from a group, click + at the left of the group to expand the group, select the file to be removed, click the handle and choose 'Remove'.

Exceptions

Users can choose to selectively allow another application (or file group) to modify a protected file by affording the appropriate Access Right in 'Active HIPS Rules' interface. A simplistic example would be the imaginary file 'Accounts.ods'. You would want the Open Office Calc program to be able to modify this file as you are working on it, but you would not want it to be accessed by a potential malicious program. You would first add the spreadsheet to the 'Protected Files' area. Once added to 'Protected Files', you would go into 'Active HIPS Rules' and create an exception for 'scalx' so that it alone could modify 'Accounts.ods'.

- First add Accounts.odt to Protected Files area.



- Then go to HIPS Rules interface and add it to the list of applications. Click the handle at the bottom and choose 'Edit' after selecting the checkbox beside it.



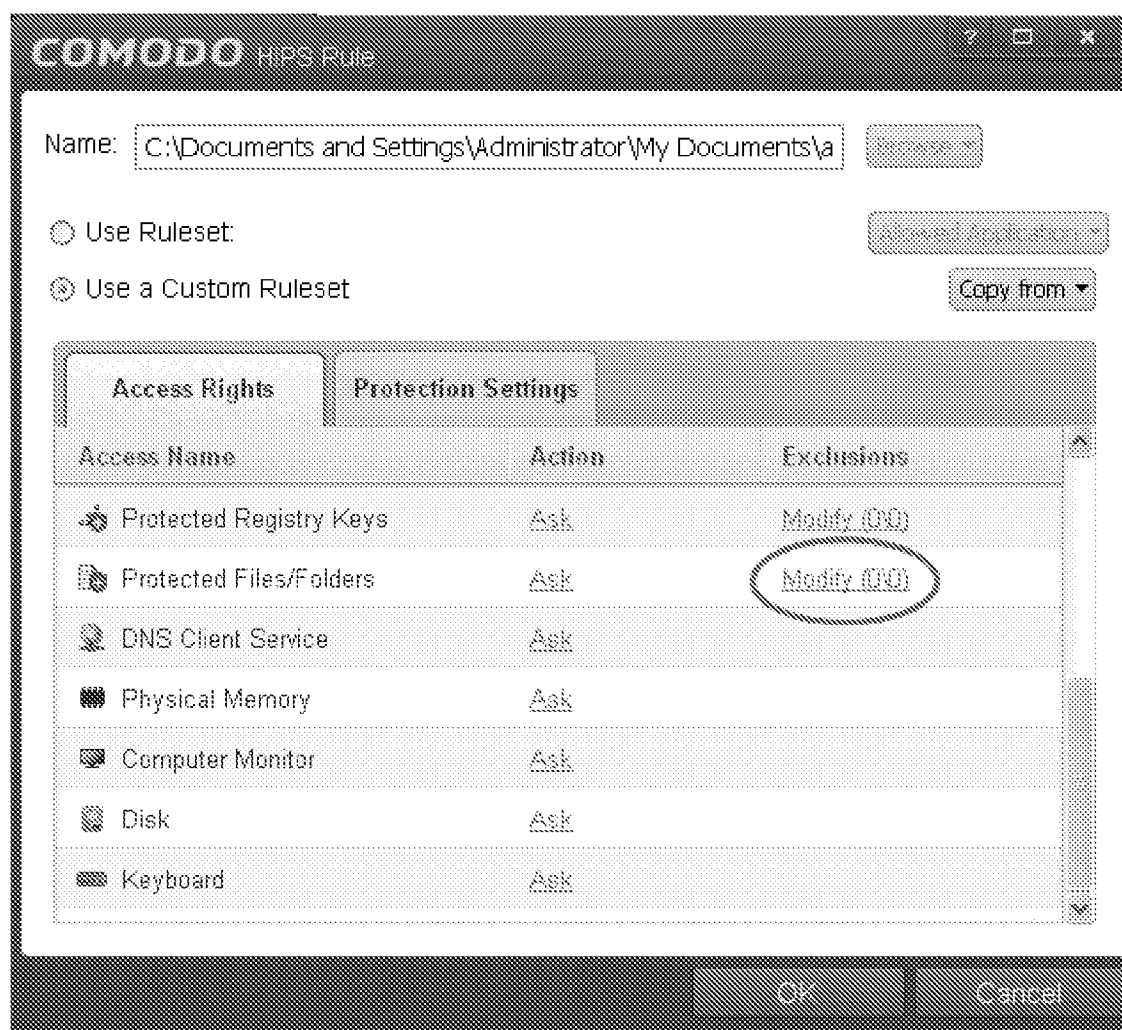
HIPS Rules

The following HIPS rules are active on this computer:

☐	Application	Treat As	Q
☐	Windows System Applications	Windows System Applic.	
☐	%windir%\explorer.exe	Windows System Applic.	
☐	Windows Updater Applications	Installer or Updater	
☐	COMODO Internet Security	Custom ruleset	
☐	All Applications	Custom ruleset	
☒	C:\Documents and Settings\Administrator\My D...	Allowed Application	

Add Edit Remove Move Up Move Down Purge

- In the HIPS Rule interface, select 'Use a custom rule set'.



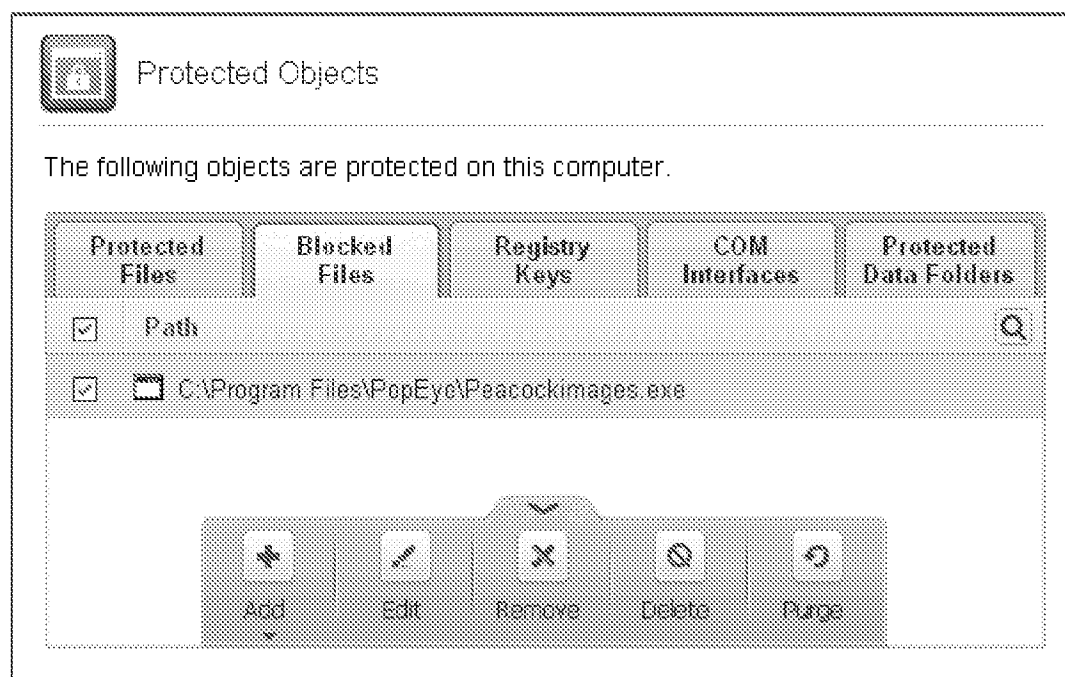
- Under the 'Access Rights' tab, click the link 'Modify' beside the entry Protected Files/Folders. The Protected Files and Folders interface will appear.
- Under the 'Allowed Files/Folders' tab, click the handle, choose 'Add' > 'Files' and add scale.exe as exceptions to the 'Ask' or 'Block' rule in the 'Access Rights'.



Another example of where protected files should be given selective access is the Windows system directory at 'c:\windows\system32'. Files in this folder should be off-limits to modification by anything except certain, Trusted, applications like Windows Updater Applications. In this case, you would add the directory c:\windows\system32* to the 'Protected Files' area (* = all files in this directory). Next go to 'HIPS Rules', locate the file group 'Windows Updater Applications' in the list and follow the same process outlined above to create an exception for that group of executables.

6.2.2.4.2. Blocked Files

Defense+ allows you to lock-down files and folders by completely denying all access rights to them from other processes or users - effectively cutting it off from the rest of your system. If the file you block is an executable, then neither you nor anything else is able to run that program. Unlike files that are placed in 'Protected Files', users cannot selectively allow any process access to a blocked file.



Clicking the handle at the bottom of the interface opens an options panel with the following options:

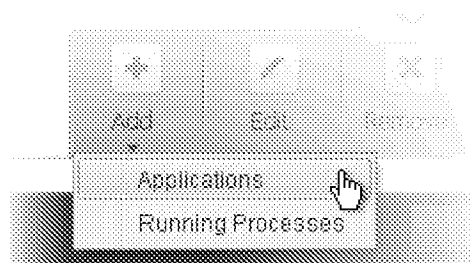
- **Add** - Allows you to add individual files, programs, applications to Blocked Files.
- **Edit** - Allows you to edit the path of the file.
- **Remove** - Releases the currently highlighted file from the blocked files list.
- **Delete** - Deletes the highlighted file from your computer
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

You can use the search option to find a specific file or file group in the list by clicking the search icon  at the far right in the column header and entering the file/group name in full or part. You can navigate through the successive results by clicking the left and right arrows.



To manually add an individual file or application

- Click the handle from the bottom center and select 'Add'.

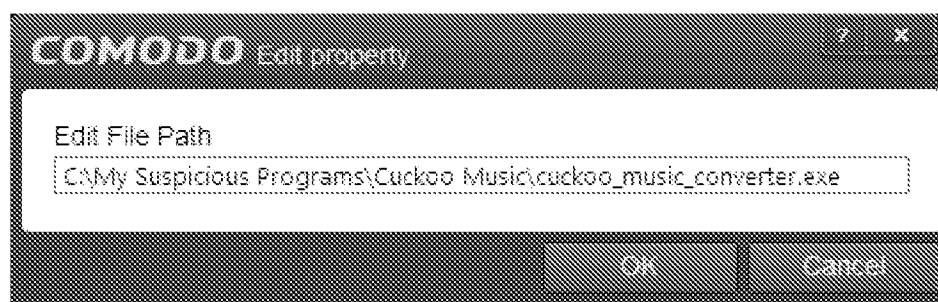


You can add the files by following methods:

- Selecting from currently running Processes
- Browsing to File

To edit an item in the Blocked Files list

- Select the item from the list, click the handle from the bottom and select Edit. The 'Edit Property' dialog will appear.



- Edit the file path, if you have relocated the file and click OK

To release an item from Blocked Files list

- Select the item from the list, click the handle from the bottom and select 'Remove'.

The selected item will be removed from the Blocked Files list. CIS will not block the application or file from execution or opening then onwards.

To permanently delete a blocked file from your system

- Select the item from the list, click the up arrow from the bottom and select 'Delete'.

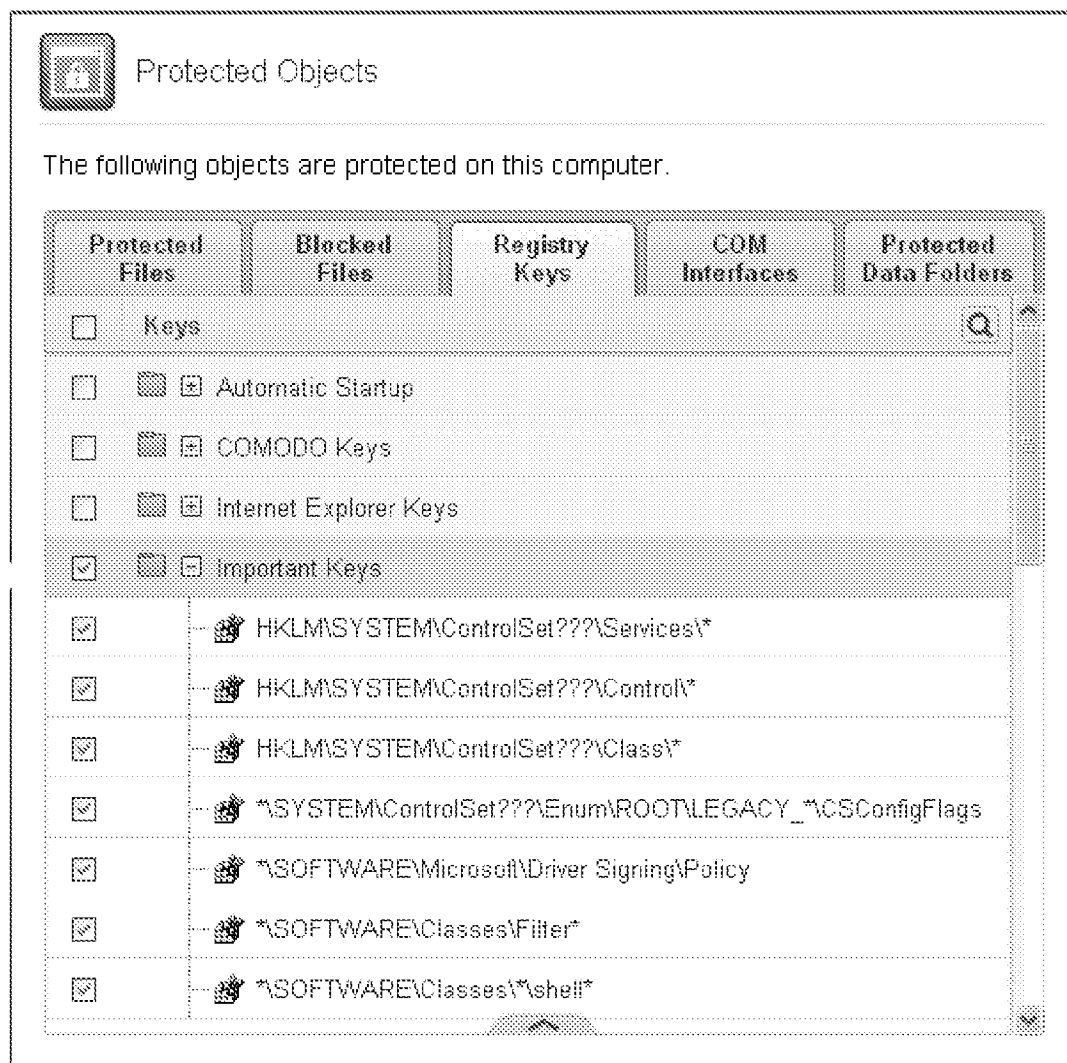
The selected item will be deleted from your computer immediately.

Warning: Deleting a file from from the Blocked Files interface permanently deletes the file from your system, rendering it inaccessible in future and it cannot be undone. Ensure that you have selected the correct file to be deleted before clicking 'Delete'.

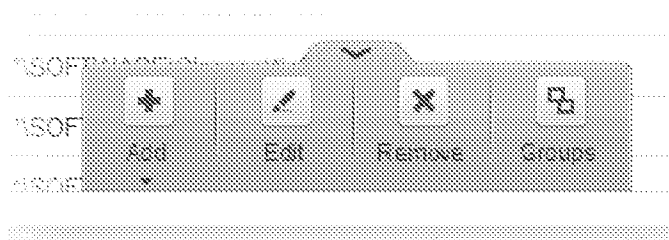
6.2.2.4.3. Protected Registry Keys

The 'Registry Keys' panel allows you to protect system critical registry keys against modification. Irreversible damage can be caused to your system if important registry keys are corrupted or modified in any way. It is essential that your registry keys are protected against any type of attack.

Click the 'Registry Keys' tab in the Protected Objects interface.



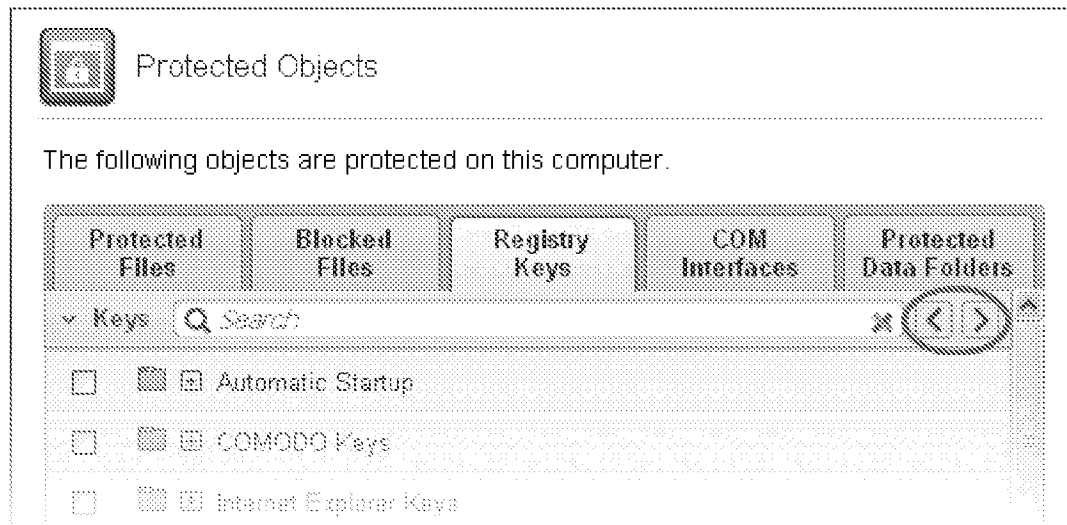
Clicking the handle at the bottom of the interface opens an options panel with the following options:



- **Add** - Allows you to add Registry groups or individual registry keys/entries to Registry Protection list.
- **Edit** - Allows you to edit the path of the Registry group or individual registry keys/entries of the selected item in the Registry Protection interface.
- **Remove** - Deletes the currently highlighted Registry group or individual registry key from the Registry Protection list.
- **Groups** - Opens the Manage Registry Groups interface that allows you to edit pre-defined Registry groups and define new Registry groups for inclusion in Registry Protection list.

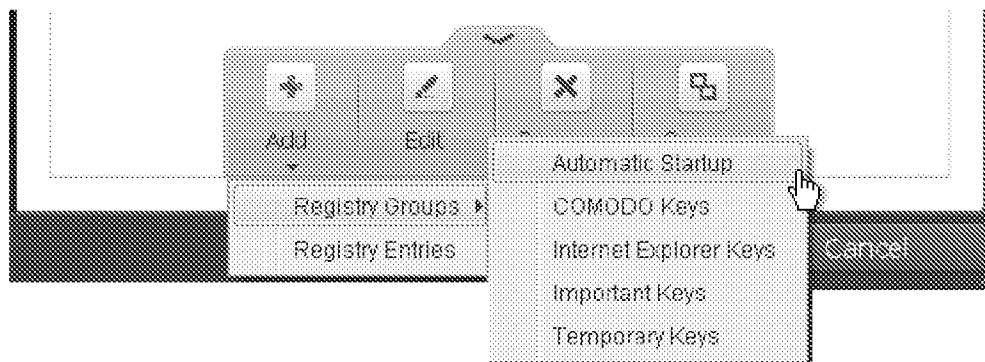
You can use the search option to find a specific registry key or group in the list by clicking the search icon  at the far right in

the column header and entering the key/group name in full or part. You can navigate through the successive results by clicking the left and right arrows.



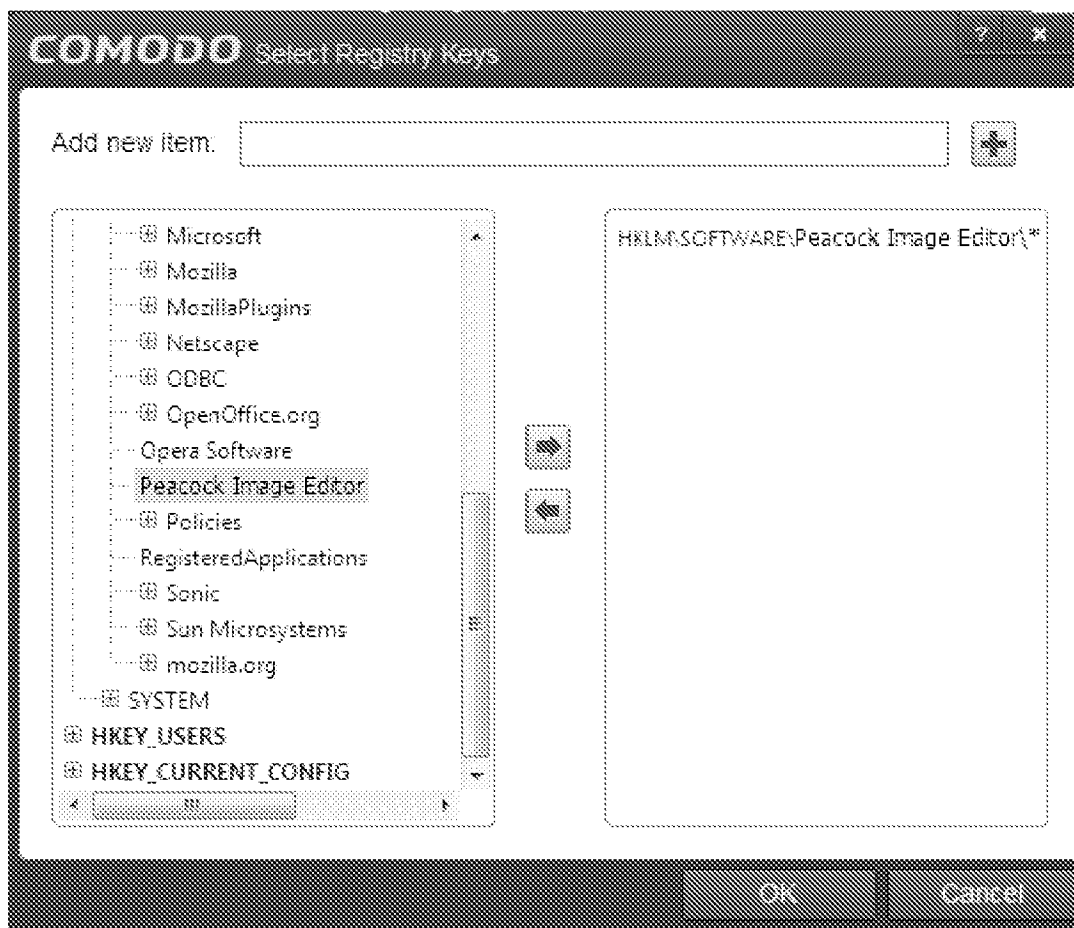
To manually add an individual Registry key or Registry Group

- Click the handle from the bottom center and select 'Add'.



You can add the items by following methods:

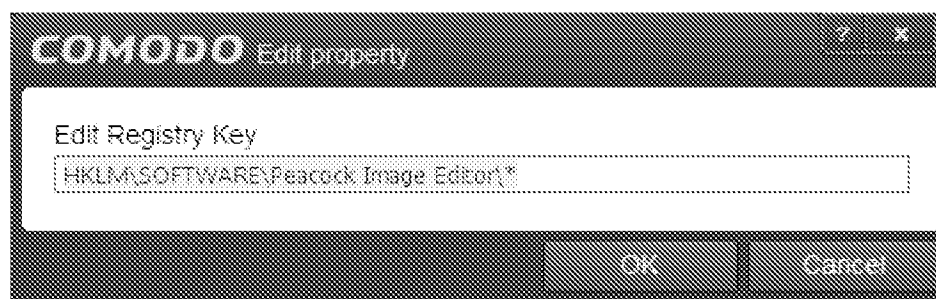
- **Adding Registry Groups** - Selecting Registry Groups allows you to batch select and import predefined groups of important registry keys. Comodo Internet Security provides a default selection of 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys' and 'Important Keys'. For explanations on editing existing registry groups and creating new groups refer to the section *Registry Groups*.
- **Adding Individual Registry Keys** - Selecting 'Registry Entries' opens the 'Select Registry Keys'.



You can add items by browsing the registry tree in the right hand pane, selecting the key and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

To edit an item in the Registry Protection list

- Select the key from the list, click the handle from the bottom and select Edit. The 'Edit Property' dialog will appear.



- Edit the key path, if you have relocated the file and click OK.

Note: The Registry Groups cannot be edited from this interface. You can edit Registry Groups from the Manage Registry Groups interface. Refer to the section [Registry Groups](#) for more details.

To delete an item from Registry Protection list

- Select the item from the list, click the up arrow from the bottom and select 'Remove'.

The selected item will be deleted from the Registry Protection list. CIS will not generate alerts, if the key or the group is modified by other programs.

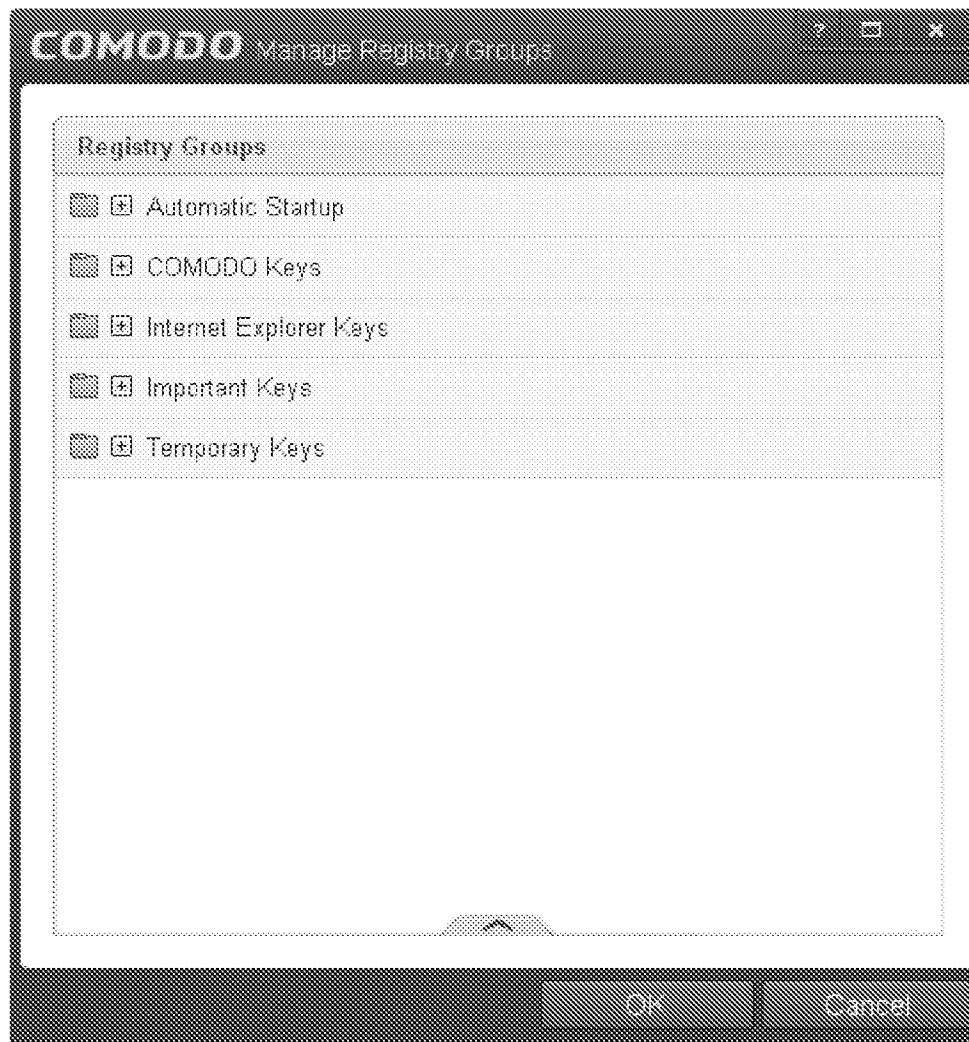
Registry Groups

Registry groups are predefined batches of one or more registry keys. Creating a registry group allows you to quickly add it to Registry Protection list.

To open the Manage Registry Groups interface

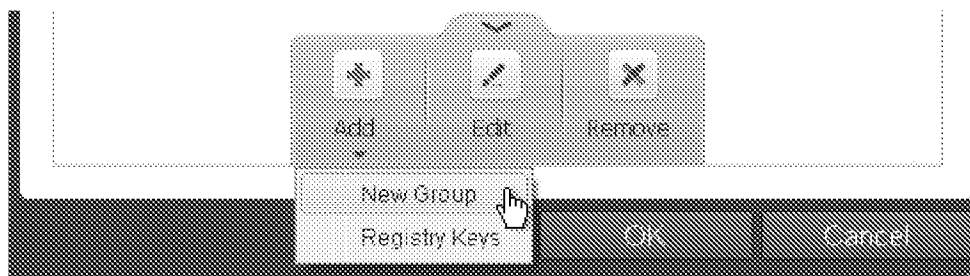
1. Click the handle from the bottom center of Registry Protection interface and select 'Groups'.

The 'Manage Registry Groups' interface will open.

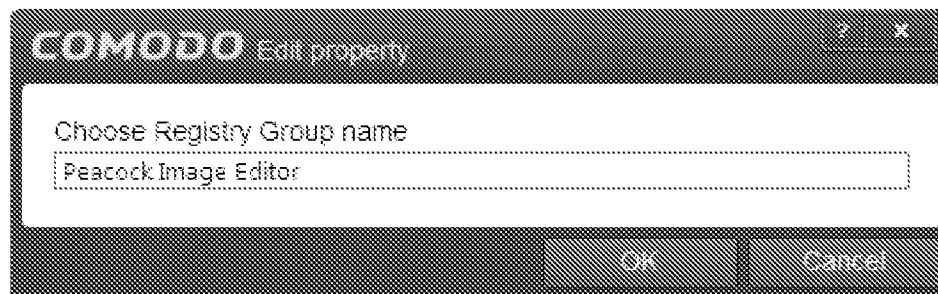


This interface allows you to

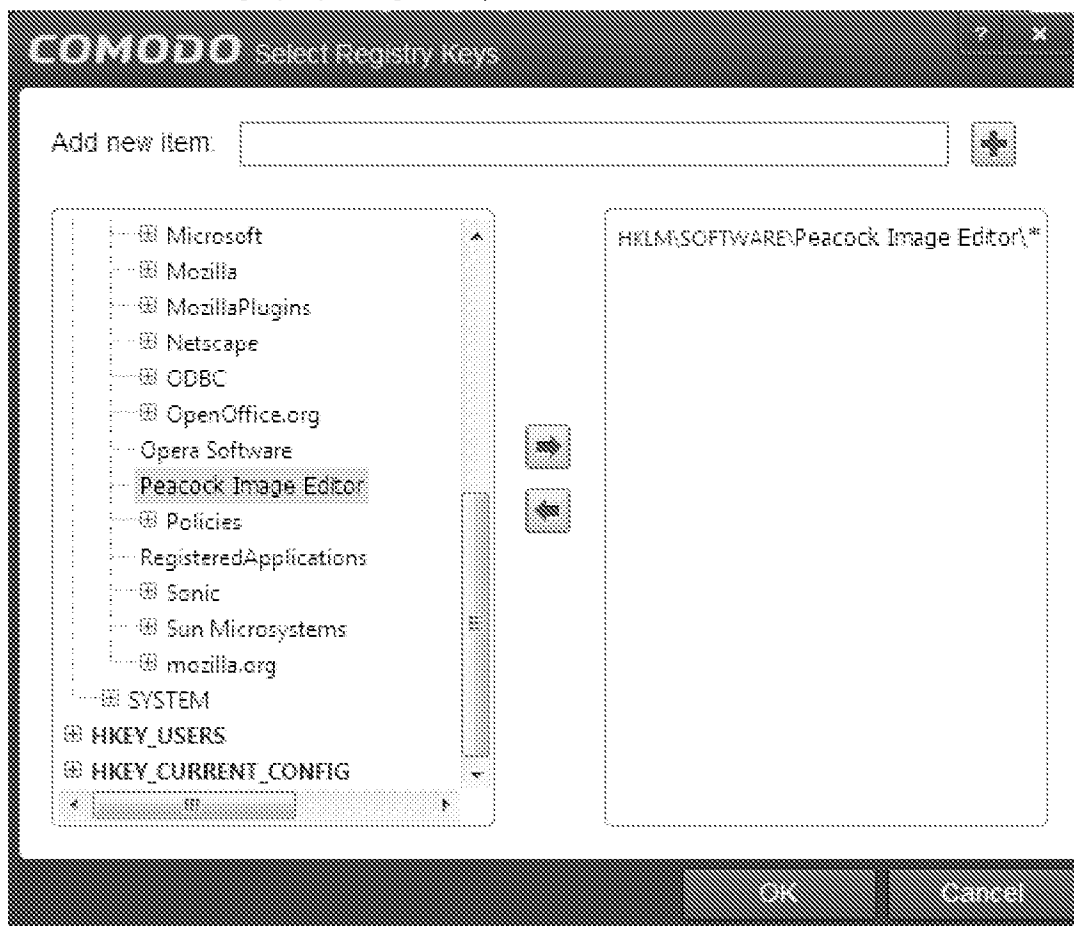
- Create a new Registry Group
- Add Registry key(s) to an existing group
- Edit the names of an Existing Registry Group
- Remove existing group(s) or individual key(s) from existing group
- To add a new group or add key(s) to an existing group, click the handle from the bottom and click 'Add'.



- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click OK



- **Add keys to a group** - Select the Group, click the handle and click Add and choose 'Registry Keys'. The 'Select Registry Keys' dialog will be opened.



You can add items by browsing the registry tree in the right hand pane, selecting the key and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new

item' field and press the '+' button.

- To edit an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the Edit Property dialog



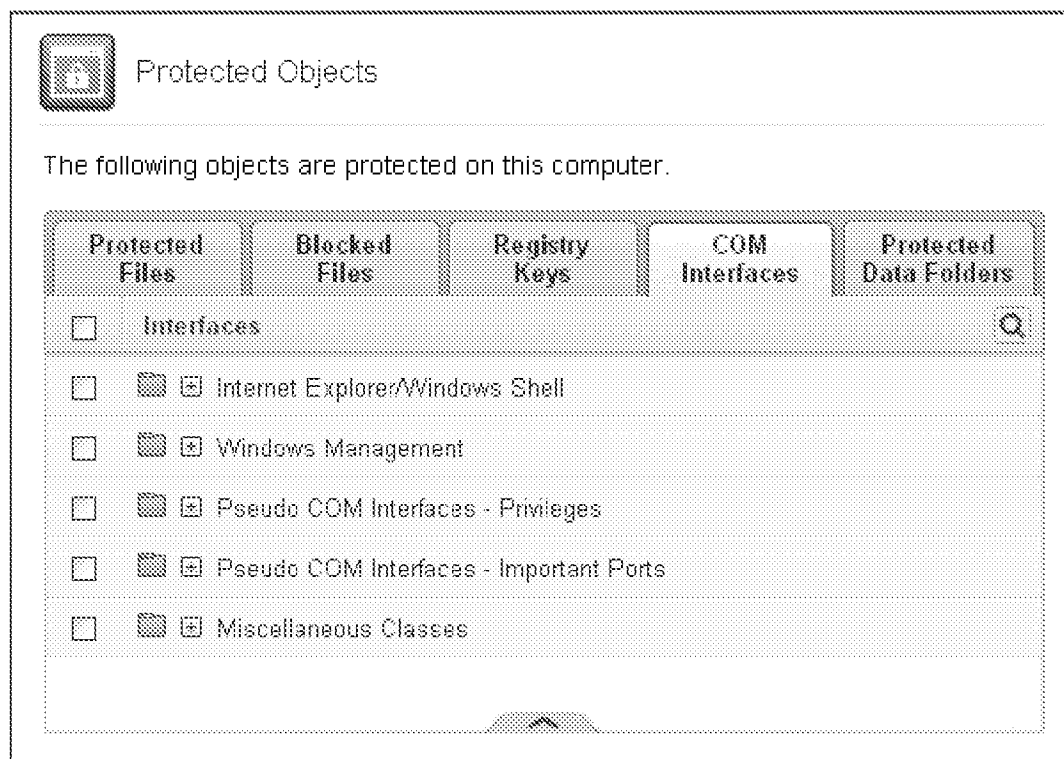
- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual file from a group, click + at the left of the group to expand the group, select the key or entry to be removed, click the handle and choose 'Remove'.

6.2.2.4.4. Protected COM interfaces

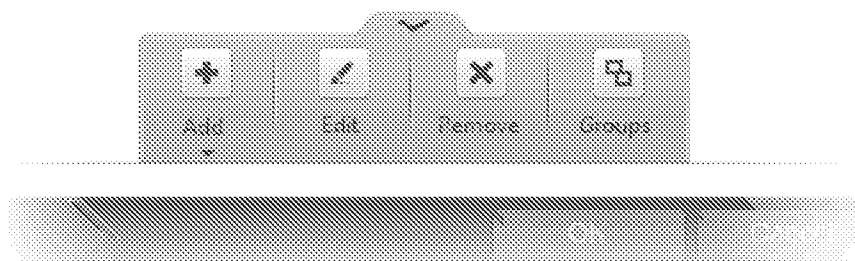
Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers and malicious programs to launch attacks on your computer. It is a critical part of any security system to restrict processes from accessing the Component Object Model - in other words, to protect the COM interfaces.

Comodo Internet Security automatically protects COM interfaces against modification, corruption and manipulation by malicious processes. The predefined COM Interface groups can be accessed by clicking the 'Groups...' button.

The 'COM Interface' allows you to view the list of predefined COM interface groups protected by CIS, edit them and to add new COM interface components to the list. This interface can be accessed by clicking the 'COM Interfaces' tab in the Protected Objects interface.



Clicking the handle at the bottom of the interface opens an options panel with the following options:



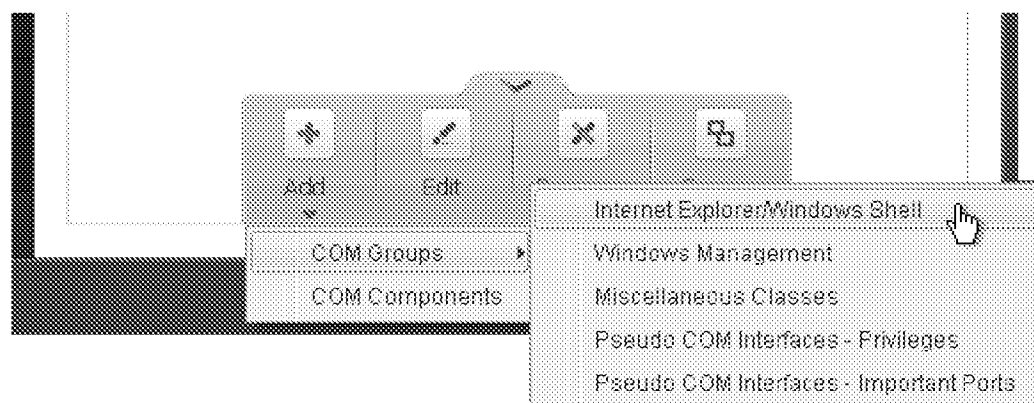
- **Add** - Allows you to add COM groups or individual COM components to COM Protection list.
- **Edit** - Allows you to edit the COM Class.
- **Remove** - Deletes the currently highlighted COM group or individual COM component from the COM Protection list.
- **Groups** - Opens the Manage COM Groups interface that allows you to edit pre-defined COM groups and define new groups for inclusion in COM Protection list.

You can search for a specific COM interface from the list by clicking the search icon  at the far right in the column header and entering the name of the COM interface in full or part. You can navigate through the successive results by clicking the left and right arrows.



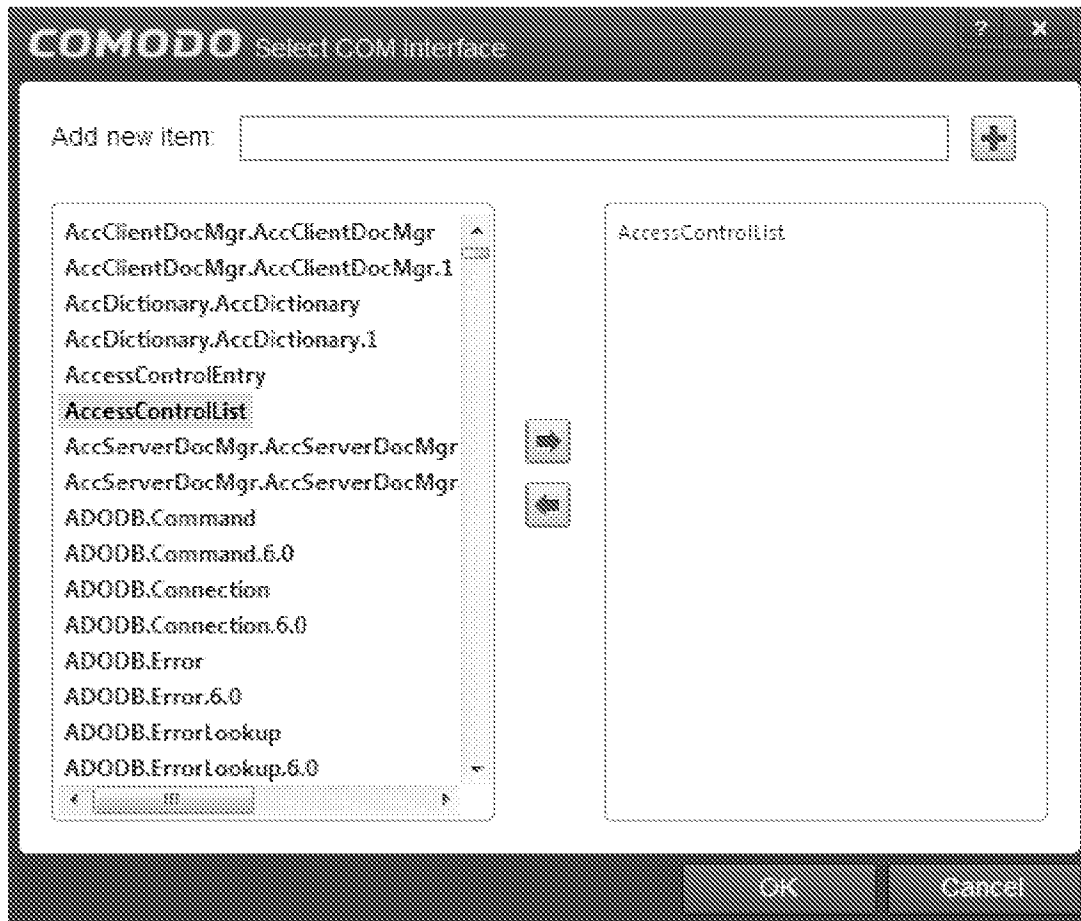
To manually add a COM Group or individual COM component

- Click the handle from the bottom center and select 'Add'.



You can add the items by following methods:

- **Adding COM Groups** - Selecting COM Groups allows you to batch select and import predefined groups of important COM interface components. For explanations on editing existing COM groups and creating new groups refer to the section COM Groups.
- **Adding COM Components** - Selecting 'COM components' opens the 'Select COM Interfaces' dialog.



You can add items by selecting from the left hand side pane and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

To edit an item in the COM Protection

- Select the COM component from the list, click the handle from the bottom and select Edit. The 'Edit Property' dialog will appear.



- Edit the COM Class and click OK

Note: The COM Groups cannot be edited from this interface. You can edit COM Groups from the Manage COM Groups interface. Refer to the section COM Groups for more details.

To delete an item from COM Protection list

- Select the item from the list, click the handle from the bottom and select 'Remove'.

The selected item will be deleted from the COM Protection list. CIS will not generate alerts, if the COM component or the group is modified by other programs or processes.

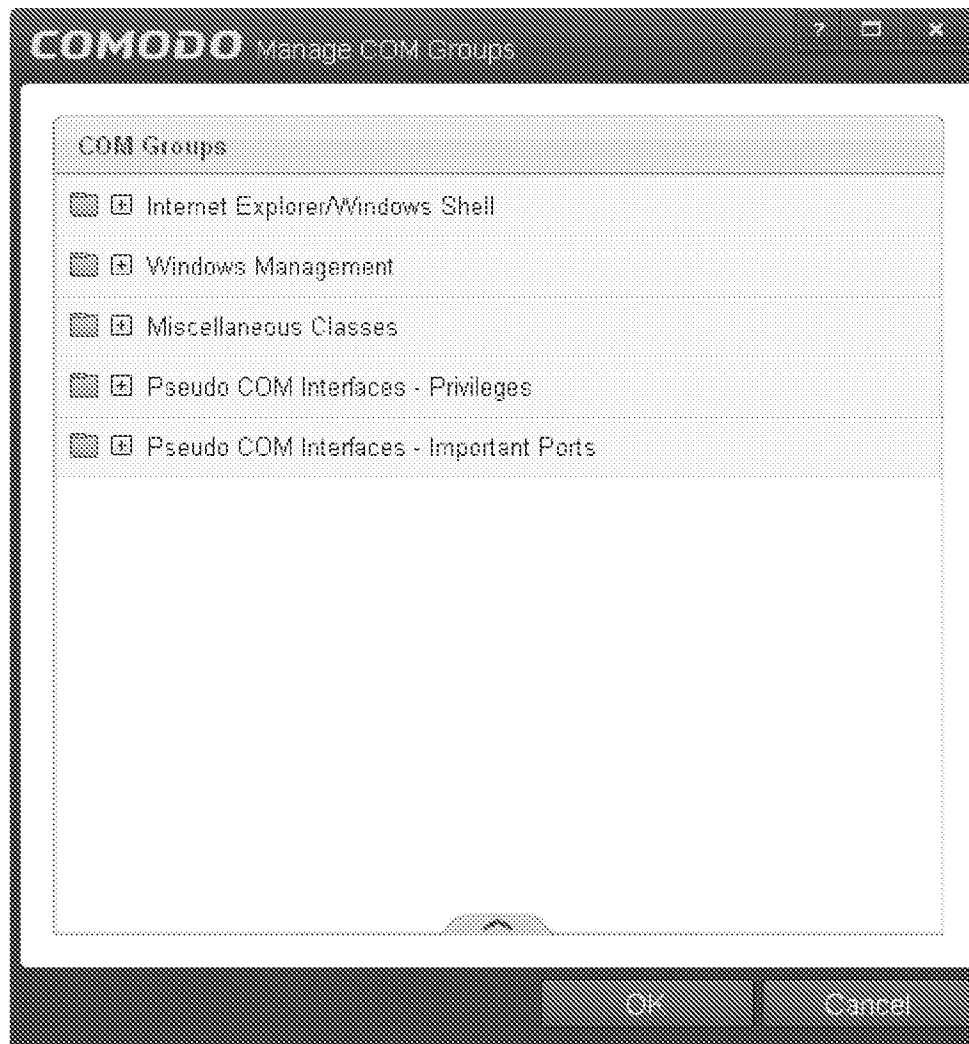
COM Groups

COM groups are handy, predefined groupings of COM interfaces. Creating a COM group allows you to quickly add it to COM Protection list.

To open the Manage COM Groups interface

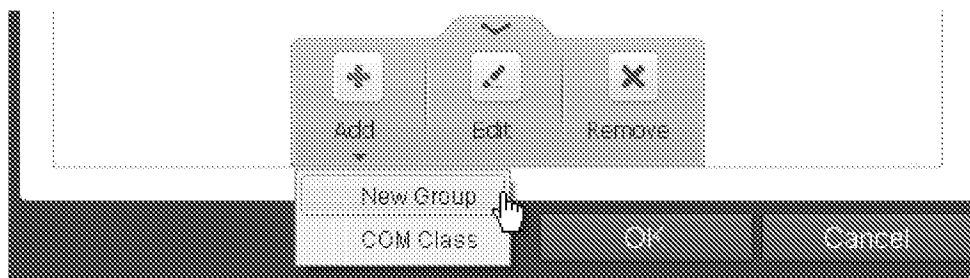
1. Click the handle from the bottom center of COM Protection interface and select 'Groups'.

The 'Manage COM Groups' interface will open.



This interface allows you to:

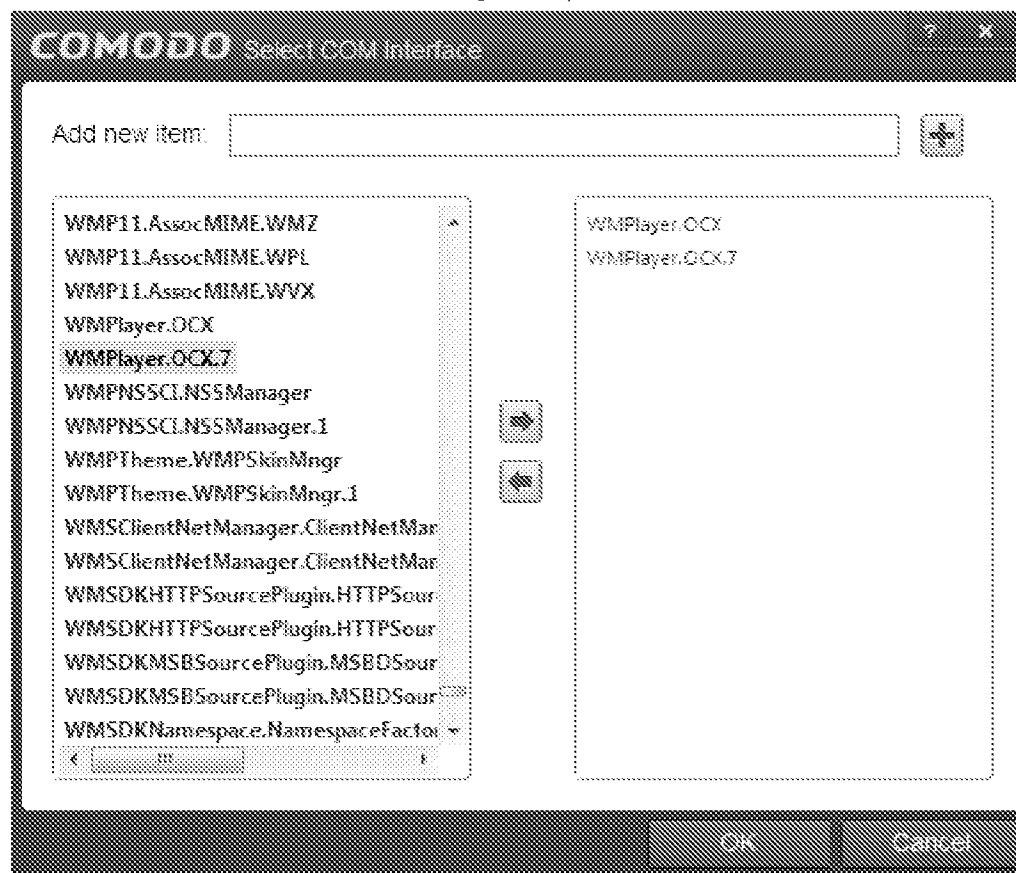
- Create a new COM Group
- Add COM Component(s) to an existing group
- Edit the names of an Existing COM Group
- Remove existing group(s) or individual COM Component(s) from existing group
- To add a new group or add new COM Component(s) to an existing group, click the handle from the bottom and click 'Add'.



- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click OK.



- **Add COM Components to a group** - Select the Group, click the handle and click Add and choose 'COM Class'. The 'Select COM Interface' dialog will be opened.



You can add items by selecting from the left hand side pane and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

- To edit an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the Edit

Property dialog



- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual COM Component from a group, click + at the left of the group to expand the group, select the item to be removed, click the handle and choose 'Remove'.

6.2.2.4.5. Protected Data Folders

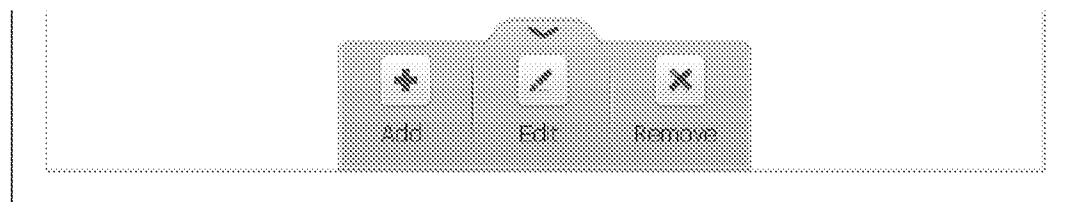
The data files in the folders listed under the Protected Data Folders area cannot be seen, accessed or modified by any known or unknown application that is running inside the sandbox.

Tip: Files and folders that are added to 'Protected Files' interface are allowed read access by other programs but cannot be modified, whereas the files/folders in 'Protected Data folders' are totally hidden to sandboxed programs. If you want a file to be read by other programs but protected from modifications, then add it to 'Protected Files' list. If you want to totally conceal a data file from all the sandboxed programs but allow read/write access by other known/trusted programs, then add it to Protected Data Folders.

To open the Protected Data Folders interface, Click the 'Protected Data Folders' tab in the Protected Objects interface:

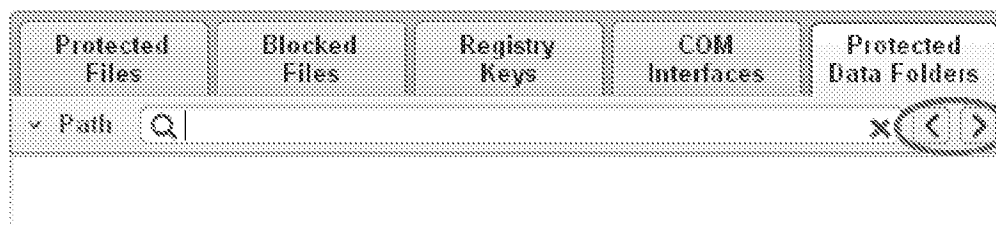


Clicking the handle at the bottom of the interface opens an options panel with the following options:



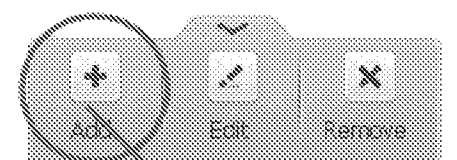
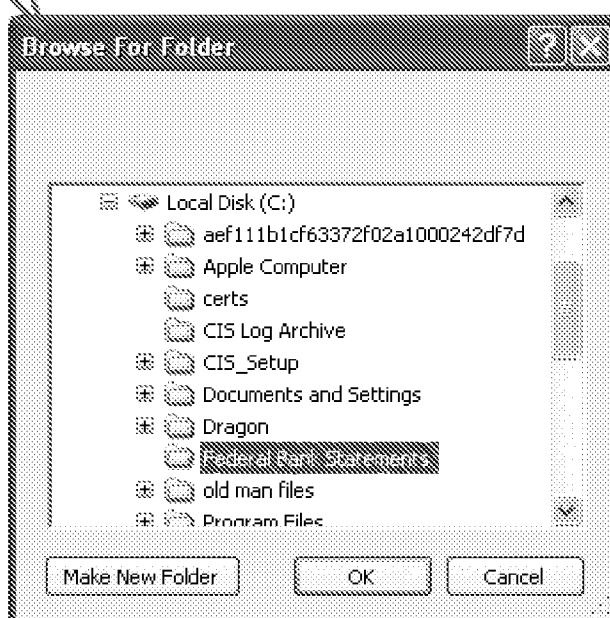
- **Add** - Allows you to add folders to Protected Data Folders list.
- **Edit** - Allows you to edit the path of the added folders.
- **Remove** - Deletes the currently selected folder.

You can use the search option to find a specific folder by clicking the search icon  at the far right of the column header. You can search by entering the folder name in full or part. You can navigate through the successive results by clicking the left and right arrows.

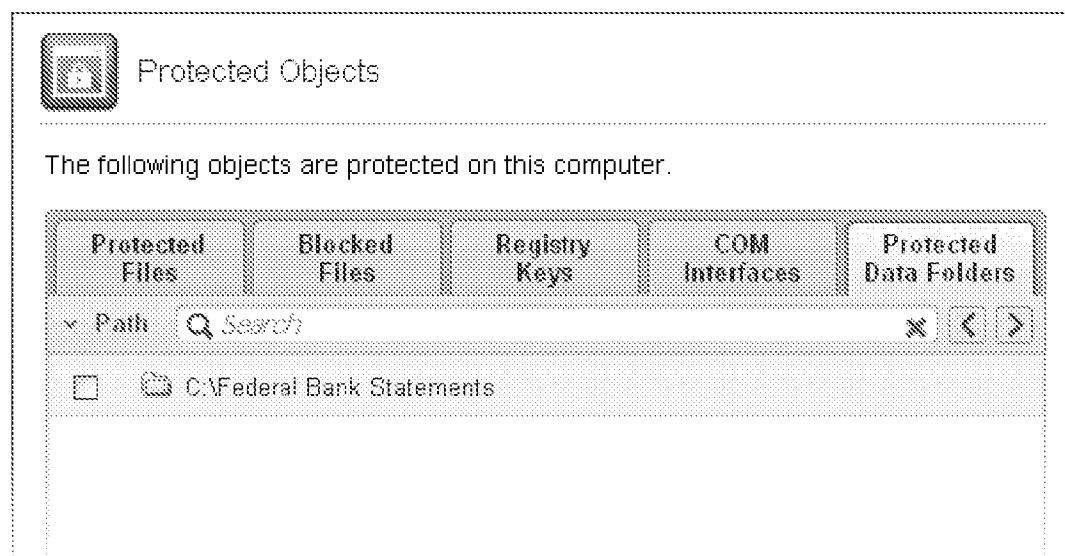


To add a folder to be protected

- Click the handle from the bottom center and select 'Add'.



- Navigate to the folder to be added and click OK.

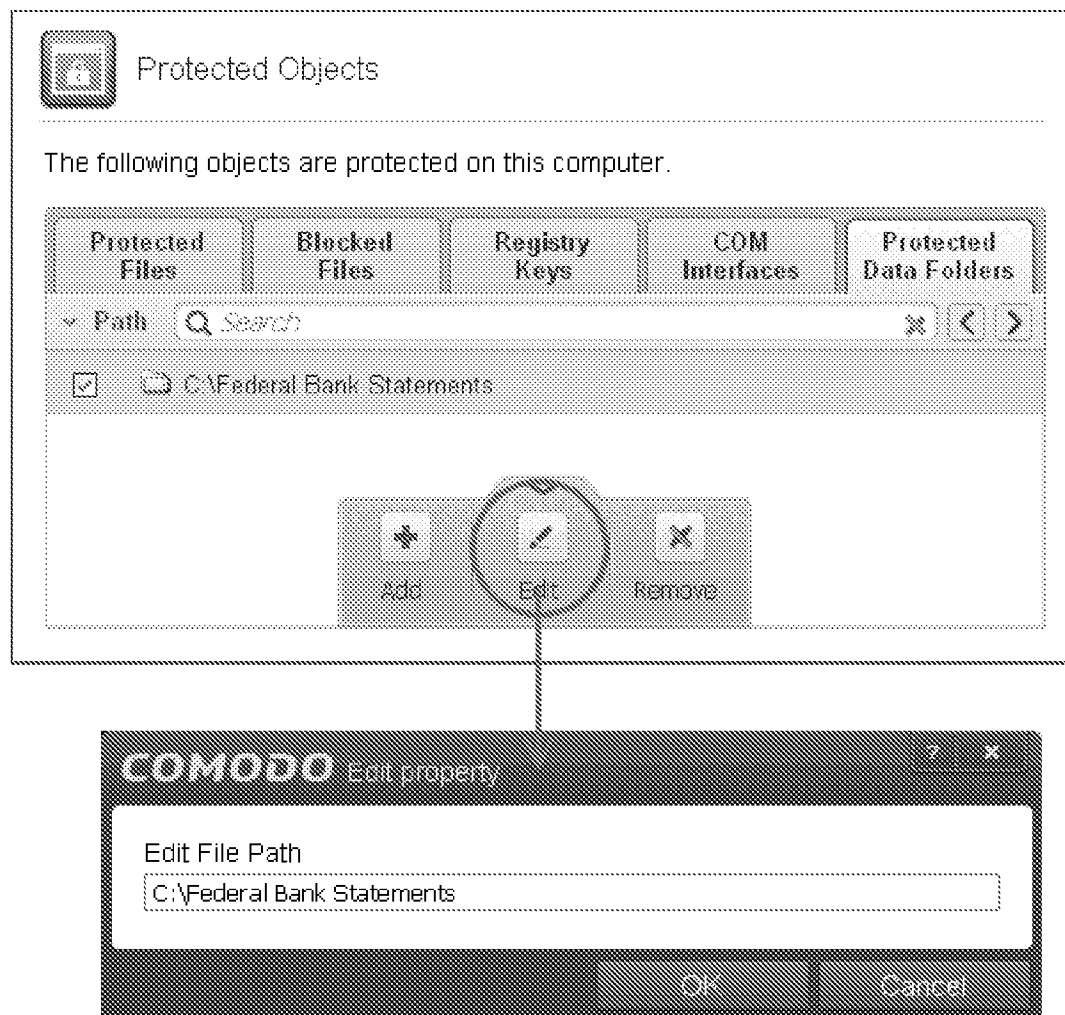


- Click OK to confirm your choice.

To edit the path of a protected folder

- Select the folder to be edited
- Click the handle from the bottom center and choose 'Edit'.

The Edit Property dialog will appear.



- Edit the file path, if you have relocated the folder and click OK

To remove an item from Protected Data Folders list

- Select the folder from the list, click the handle from the bottom and choose 'Remove'.
- The selected folder will be removed from the protected folders list. CIS will not generate alerts, if the folder is subjected to unauthorized access.

6.2.2.5. Behavior Blocker

The Behavior Blocker is an integral part of the Defense+ engine and is responsible for authenticating every executable image that is loaded into the memory. The Behavior Blocker intercepts all files before they are loaded and intercepts any prefetching/caching attempts. It calculates the hash of the executable at the point it attempts to load then compares this hash with the list of known / recognized applications that are on the Comodo safe list. If the hash matches the one on record for the executable, then the application is safe and the Behavior Blocker allows it to run. If no matching hash is found, then the executable is 'unrecognized' and is run inside the auto-sandbox. You will be notified via an alert when this happens.