

# Manuale utente per il software di sicurezza Zone Labs

Versione 6.1



A Check Point  
COMPANY

Smarter Security™

© 2005 Zone Labs, LLC. Tutti i diritti riservati.

© 2005 Check Point Software Technologies Ltd. Tutti i diritti riservati.

Check Point, Application Intelligence, Check Point Express, il logo Check Point, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecurRemote, SecurServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, TrueVector, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecurRemote, VPN-1 SecureServer, VPN-1 VSX, Web Intelligence, ZoneAlarm, Zone Alarm Pro, Zone Labs e il logo Zone Labs sono marchi commerciali o marchi registrati di Check Point Software Technologies Ltd. o delle sue affiliate. Tutti gli altri nomi di prodotti citati nel presente documento sono marchi commerciali o marchi registrati dei rispettivi proprietari. I prodotti descritti nel presente documento sono protetti da brevetto USA N. 5,606,668, 5,835,726 e 6,496,935 e possono essere protetti da altri brevetti USA, brevetti esteri o richieste di brevetto in sospenso.

**Zone Labs, LLC.**

***Una società Check Point***

475 Brannan, Suite 300

San Francisco, CA 94107

ZLD -0422-0610-2005-1107

# Sommario

---

<b>Tabelle</b> .....	ix
<b>Figure</b> .....	xi
<b>Introduzione</b> .....	xiii
Informazioni sul software di sicurezza Zone Labs .....	xiv
Novità della release 6.1 .....	xv
Informazioni su questa guida .....	xvi
Convenzioni .....	xvi
Forum degli utenti di Zone Labs .....	xvi
<b>Capitolo 1</b>	
<b>    Installazione e configurazione</b> .....	1
Requisiti di sistema e software supportato .....	2
Protocolli di protezione della posta elettronica supportati .....	2
Software browser supportati .....	2
Client IM (messaggistica immediata) supportati .....	3
Installazione del software di sicurezza Zone Labs .....	4
Installazione di ZoneAlarm .....	4
Installazione del software di sicurezza Zone Labs .....	5
Aggiornamento di una versione precedente .....	6
Aggiornamento e firewall connessione Internet (ICF) di Windows XP SP2 .....	6
Aggiornamento e impostazioni di IMsecure myVault .....	6
Aggiornamento e impostazioni di MailFrontier .....	6
Configurazione delle opzioni di base .....	7
Configurazione delle autorizzazioni di accesso ai programmi .....	7
Iscriversi alla comunità DefenseNet .....	7
Disinstallazione del software di sicurezza Zone Labs .....	9
<b>Capitolo 2</b>	
<b>    software di sicurezza Zone Labs - Nozioni di base</b> .....	11
Tour del Centro di controllo del software di sicurezza Zone Labs .....	12
Esplorazione del Centro di controllo .....	12
Utilizzo del dashboard .....	13
Icone nell'area di notifica del sistema .....	15
Menu di scelta rapida .....	15
Utilizzo della scheda Stato .....	16
Comprendere le zone .....	18
Le zone gestiscono la sicurezza del firewall .....	18
Le zone permettono di controllare i programmi .....	19

Come rispondere agli avvisi . . . . .	20
Nuovi avvisi Programma . . . . .	20
Nuovi avvisi di rete e VPN. . . . .	21
Impostazione delle preferenze del prodotto . . . . .	22
Impostazione delle opzioni di aggiornamento . . . . .	22
Impostazione della password. . . . .	22
Eseguire il backup e il ripristino delle impostazioni di sicurezza . . . . .	23
Impostazione delle preferenze generali del prodotto . . . . .	24
Impostazione delle preferenze di contatto . . . . .	25
Impostazione delle opzioni di visualizzazione del prodotto e del server proxy . . . . .	25
Creazione di un profilo di protezione dalle frodi online. . . . .	26
Licenza, registrazione e supporto . . . . .	28
Aggiornamento della licenza del prodotto . . . . .	28
Registrazione del software di sicurezza Zone Labs. . . . .	28
Accesso al supporto tecnico . . . . .	29

<b>Capitolo 3 Connessioni di rete con il software di sicurezza</b>	
<b>Zone Labs . . . . .</b>	<b>31</b>
Configurazione di una nuova connessione di rete. . . . .	32
Utilizzo della configurazione guidata Rete . . . . .	32
Disattivazione della configurazione guidata Rete. . . . .	33
Utilizzo della configurazione guidata Rete wireless . . . . .	33
Disattivazione della configurazione guidata Rete wireless . . . . .	34
Integrazione con i servizi di rete . . . . .	35
Attivazione della condivisione dei file e delle stampanti . . . . .	35
Collegamento ai server di posta della rete . . . . .	35
Protezione di una connessione a Internet condivisa. . . . .	36
Configurazione della connessione VPN . . . . .	37
Protocolli VPN supportati . . . . .	37
Configurazione automatica della connessione VPN . . . . .	37
Configurazione manuale della connessione VPN . . . . .	38
Aggiunta di un gateway VPN e altre risorse alla zona attendibile . . . . .	39
Rimozione di un gateway VPN da un intervallo o da una subnet bloccati . . . . .	39
Consentire l'utilizzo dei protocolli VPN . . . . .	39
Concedere le autorizzazioni di accesso al software VPN . . . . .	40
<b>Capitolo 4 Protezione assicurata dal firewall . . . . .</b>	<b>41</b>
Comprensione della protezione assicurata dal firewall. . . . .	42
Scelta dei livelli di sicurezza . . . . .	43
Impostazione del livello di sicurezza per una zona. . . . .	43
Impostazione delle opzioni di sicurezza avanzate . . . . .	45
Impostazione delle opzioni di sicurezza del gateway . . . . .	45
Impostazione delle opzioni di Condivisione connessione Internet (ICS) . . . . .	45
Impostazione delle opzioni di sicurezza generali . . . . .	46
Impostazione delle opzioni di sicurezza della rete . . . . .	47
Impostazione delle opzioni di sicurezza della rete wireless . . . . .	48

Gestione delle origini di traffico . . . . .	49
Visualizzazione dell'elenco delle origini di traffico . . . . .	49
Modifica delle origini di traffico . . . . .	49
Aggiunta alla zona attendibile . . . . .	50
Aggiunta alla zona bloccata . . . . .	51
Visualizzazione degli eventi relativi al firewall . . . . .	51
Blocco e sblocco delle porte . . . . .	53
Impostazioni delle autorizzazioni di porta predefinite . . . . .	53
Aggiunta di porte personalizzate . . . . .	54
Comprensione delle regole firewall della scheda Esperto . . . . .	56
Come sono applicate le regole del firewall della scheda Esperto . . . . .	56
Ordine di applicazione delle regole della scheda Esperto . . . . .	57
Creazione di regole firewall nella scheda Esperto . . . . .	58
Creazione di gruppi . . . . .	61
Creazione di un gruppo di posizioni . . . . .	61
Creazione di un gruppo di protocolli . . . . .	61
Creazione di un gruppo di giorni/ore . . . . .	64
Gestione delle regole del firewall della scheda Esperto . . . . .	66
Visualizzazione dell'elenco delle regole della scheda Esperto . . . . .	66
Modifica e riclassificazione delle regole . . . . .	67
<b>Capitolo 5 Controllo dei programmi . . . . .</b>	<b>69</b>
Comprendere il Controllo dei programmi . . . . .	70
Impostazione automatica delle autorizzazioni per i programmi . . . . .	70
Impostazione manuale delle autorizzazioni per i programmi . . . . .	71
Impostazione di opzioni generiche per Controllo dei programmi . . . . .	73
Impostazione del livello di Controllo dei programmi . . . . .	73
Impostazione dei livelli di SmartDefense Advisor . . . . .	75
Attivazione del Blocco automatico . . . . .	75
Visualizzazione del log degli eventi relativi ai programmi . . . . .	76
Visualizzare gli eventi di OSFirewall registrati . . . . .	78
Configurazione di impostazioni avanzate per i programmi . . . . .	79
Impostazione delle proprietà dei programmi globali . . . . .	79
Impostazione delle autorizzazioni d'accesso per i nuovi programmi . . . . .	79
Impostazione di autorizzazioni per programmi specifici . . . . .	81
Utilizzo dell'elenco dei programmi . . . . .	81
Aggiunta di un programma all'elenco dei programmi . . . . .	84
Concessione dell'autorizzazione di accesso a Internet per un programma . . . . .	85
Concessione a un programma dell'autorizzazione ad agire come server . . . . .	85
Concessione dell'autorizzazione di invio della posta a un programma . . . . .	86
Impostazione di opzioni per un programma specifico . . . . .	87
Impostazione di opzioni avanzate per Controllo dei programmi . . . . .	87
Disattivazione della protezione della posta in uscita per un programma . . . . .	87
Impostazione delle opzioni di filtro per un programma . . . . .	88
Impostazione delle opzioni di autenticazione . . . . .	88
Impostazione dell'autorizzazione Ignora blocco a un programma . . . . .	89
Gestione dei componenti dei programmi . . . . .	90
Creazione di regole della scheda Esperto per i programmi . . . . .	91
Creazione di una regola della scheda Esperto per un programma . . . . .	91
Condivisione di regole Esperto . . . . .	92

<b>Capitolo 6</b>	<b>Protezione da spyware e virus</b>	93
	Protezione contro spyware e virus	94
	Attivazione della protezione contro virus e spyware	94
	Pianificazione di una scansione	94
	Aggiornamento delle definizioni di virus e spyware	95
	Personalizzazione delle opzioni di protezione contro i virus	97
	Specificare le destinazioni di scansione	97
	Scansione all'accesso	98
	Scansione della posta elettronica	99
	Attivazione della cura automatica dei virus	99
	Specificare i metodi di rilevamento dei virus	100
	Personalizzazione delle opzioni di protezione contro lo spyware	101
	Attivazione della cura automatica dello spyware	101
	Definizione dei metodi di rilevamento dello spyware	101
	Esclusione dello spyware dalle scansioni	102
	Come prevenire gli attacchi dello spyware	102
	Esecuzione di una scansione dei virus	103
	Comprendere i risultati delle scansioni dei virus	104
	Cura manuale dei file dei virus	105
	Riparazione dei file in un archivio	105
	Invio di virus e spyware a Zone Labs per l'analisi	106
	Visualizzazione degli eventi di virus registrati	106
	Esecuzione di una scansione di spyware	108
	Comprendere i risultati delle scansioni di spyware	109
	Errori nei risultati di scansione di spyware	110
	Visualizzazione degli elementi in quarantena	110
	Visualizzare gli eventi di spyware registrati	111
	Visualizzazione dello stato di protezione da virus e spyware	113
	Monitoraggio della protezione contro i virus	114
	Copertura del monitoraggio	114
	Monitoraggio in ZoneAlarm, ZoneAlarm Pro e ZoneAlarm Wireless	115
	Monitoraggio in ZoneAlarm Anti-virus e ZoneAlarm Security Suite	115
	Attivazione e disattivazione della funzione Monitoraggio antivirus	115
	Visualizzazione dei messaggi di stato nel pannello Monitoraggio antivirus	116
	Visualizzazione degli avvisi di Monitoraggio antivirus	116
<b>Capitolo 7</b>	<b>Protezione della posta elettronica</b>	119
	Comprensione della protezione della posta elettronica	120
	Protezione di MailSafe in entrata	120
	Protezione di MailSafe in uscita	121
	Attivazione della protezione di MailSafe in entrata	121
	Attivazione della protezione di MailSafe in uscita	121
	Personalizzazione della protezione di MailSafe in entrata	122
	Visualizzazione dell'elenco di allegati	122
	Modifica dell'impostazione di quarantena per un tipo di allegato	122
	Aggiunta e rimozione di tipi di allegato	123
	Apertura di un allegato posto in quarantena	124
	Personalizzazione della protezione di MailSafe in uscita	125
	Attivazione della protezione di MailSafe in uscita per programma	125
	Impostazione delle opzioni di protezione di MailSafe in uscita	125

Filtro della posta indesiderata . . . . .	127
Consentire o bloccare la posta elettronica proveniente da mittenti specifici . . . . .	127
Consentire o bloccare la posta elettronica proveniente da società specifiche . . . . .	128
Aggiunta di contatti all'elenco Consentiti. . . . .	128
Scansione della Posta in arrivo . . . . .	128
Consentire la posta elettronica proveniente da liste di distribuzione . . . . .	129
Segnalazione di posta indesiderata. . . . .	129
Segnalazione di posta elettronica fraudolenta. . . . .	130
Definizione delle opzioni dei messaggi di posta indesiderata. . . . .	131
Contestazione di posta elettronica proveniente da mittenti sconosciuti . . . . .	132
Definizione del server della posta in uscita . . . . .	134
Personalizzazione delle impostazioni del filtro della posta indesiderata . . . . .	135
Ripristinare la posta elettronica erroneamente identificata come indesiderata . . . . .	136
Visualizzare i report del filtro della posta indesiderata . . . . .	137
Protezione antivirus per la posta elettronica. . . . .	138
Attivazione della scansione della posta elettronica . . . . .	138
Come viene gestita la posta elettronica infetta . . . . .	138
<b>Capitolo 8 Protezione della privacy . . . . .</b>	<b>141</b>
Comprendere la protezione della privacy. . . . .	142
Impostazione delle opzioni di privacy generali . . . . .	143
Impostazione dei livelli di protezione della privacy . . . . .	143
Applicazione della protezione della privacy a programmi diversi dai browser . . . . .	143
Come usare Privacy Advisor . . . . .	145
Impostazione delle opzioni di privacy per siti Web specifici . . . . .	146
Visualizzazione dell'elenco della privacy . . . . .	146
Aggiunta di siti all'elenco della privacy . . . . .	147
Modifica dei siti nell'elenco della privacy . . . . .	147
Personalizzazione del controllo dei cookie . . . . .	149
Blocco dei cookie di sessione . . . . .	149
Blocco dei cookie permanenti . . . . .	149
Blocco di cookie di terze parti . . . . .	150
Impostazione di una data di scadenza per i cookie . . . . .	150
Personalizzazione del blocco degli annunci . . . . .	152
Impostazione degli annunci da bloccare . . . . .	152
Impostazione delle opzioni di controllo degli annunci bloccati. . . . .	152
Personalizzazione del controllo del codice mobile . . . . .	154
Impostazione dei tipi di codice mobile da bloccare . . . . .	154
Comprensione di Cache Cleaner . . . . .	156
Utilizzo di Cache Cleaner . . . . .	156
Personalizzazione delle opzioni di ripulitura del disco rigido . . . . .	157
Personalizzazione delle opzioni di ripulitura del browser. . . . .	157
<b>Capitolo 9 Avvisi e log . . . . .</b>	<b>161</b>
Comprensione di avvisi e log . . . . .	162
Informazioni sugli avvisi del software di sicurezza Zone Labs . . . . .	162
Informazioni sulla registrazione degli eventi . . . . .	169

Impostazione delle opzioni di base per avvisi e log . . . . .	170
Impostazione del livello di visualizzazione degli avvisi . . . . .	170
Impostazione delle opzioni di registrazione dei log per eventi e programmi . . . . .	170
Mostrare o nascondere avvisi specifici . . . . .	171
Mostrare o nascondere gli avvisi del firewall . . . . .	171
Attivazione degli avvisi nell'area di notifica del sistema . . . . .	171
Impostazione delle opzioni di log per eventi e programmi . . . . .	172
Formattazione dei log . . . . .	172
Personalizzazione della registrazione degli eventi . . . . .	172
Personalizzazione della registrazione di programma . . . . .	173
Visualizzazione delle voci di log . . . . .	173
Visualizzazione del file di log . . . . .	175
Archiviazione delle voci di log . . . . .	176
Utilizzo di SmartDefense Advisor e Hacker ID . . . . .	178
<b>Capitolo 10 Protezione dei dati . . . . .</b>	<b>179</b>
Comprensione della funzione Blocco ID . . . . .	180
Come vengono protette le informazioni personali . . . . .	180
Impostazione del livello di protezione di Blocco ID . . . . .	182
Monitoraggio dello stato di Blocco ID . . . . .	182
Informazioni su myVAULT . . . . .	183
Aggiungere dati a myVAULT . . . . .	183
Modifica e rimozione dei contenuti di myVAULT . . . . .	185
Utilizzo dell'elenco dei siti attendibili . . . . .	186
Visualizzazione elenco dei siti attendibili . . . . .	186
Aggiunta all'elenco dei siti attendibili . . . . .	187
Modifica e rimozione dei siti attendibili . . . . .	187
<b>Capitolo 11 Controllo genitori . . . . .</b>	<b>189</b>
Comprendere il Controllo genitori . . . . .	190
Attivazione del Controllo genitori e del filtro intelligente . . . . .	191
Attivazione o disattivazione del Controllo genitori . . . . .	191
Attivazione o disattivazione del filtro intelligente . . . . .	191
Impostazione delle opzioni di timeout . . . . .	192
Scegliere quali categorie bloccare . . . . .	193
<b>Capitolo 12 IM Security (Instant Messaging Security) . . . . .</b>	<b>199</b>
Panoramica di IM Security . . . . .	200
Accesso . . . . .	200
Bloccare lo spam . . . . .	200
Controllo caratteristica . . . . .	202
Protezione in entrata . . . . .	203
Crittografia del traffico di messaggistica immediata . . . . .	204



Impostazione delle opzioni di IM Security . . . . .	206
Impostazione del livello di protezione . . . . .	206
Visualizzazione dello stato di protezione di IM Security . . . . .	206
Personalizzazione delle impostazioni di protezione . . . . .	207
Impostazione delle opzioni avanzate di IM Security . . . . .	207
Visualizzazione del log degli eventi relativi a IM Security . . . . .	208
<b>Appendice A</b>	
<b>Guida di riferimento agli avvisi . . . . .</b>	<b>211</b>
Avvisi informativi . . . . .	212
Avvisi del firewall o di protezione . . . . .	212
Avvisi di MailSafe . . . . .	213
Avvisi Programma bloccato . . . . .	214
Avvisi Blocco Internet . . . . .	215
Avvisi remoti . . . . .	216
Avvisi relativi ai programmi . . . . .	217
Avvisi Nuovo programma . . . . .	218
Avvisi Programma ripetuto . . . . .	219
Avvisi Programma modificato . . . . .	219
Avvisi Componente di programma . . . . .	220
Avvisi Programma server . . . . .	221
Avvisi Programma avanzato . . . . .	223
Avvisi Configurazione VPN automatica . . . . .	223
Avvisi Azione manuale obbligatoria . . . . .	224
Avvisi di OSFirewall . . . . .	226
Avvisi Comportamento sospetto . . . . .	226
Avvisi Comportamento pericoloso . . . . .	226
Avvisi Comportamento dannoso . . . . .	227
Avvisi blocco ID . . . . .	228
Avvisi Nuova rete . . . . .	229
Avvisi Messaggistica immediata . . . . .	230
<b>Appendice B</b>	
<b>Tasti di scelta rapida . . . . .</b>	<b>233</b>
Tasti di scelta rapida per lo spostamento nel programma . . . . .	234
Tasti di scelta rapida per funzioni globali . . . . .	236
Comandi per le finestre di dialogo . . . . .	238
Tasti di scelta rapida per pulsanti . . . . .	239
<b>Appendice C</b>	
<b>Risoluzione dei problemi . . . . .</b>	<b>243</b>
VPN . . . . .	244
Configurazione del software di sicurezza Zone Labs per il traffico VPN . . . . .	244
Configurazione automatica della VPN e regole della scheda Esperto . . . . .	244
Ritardo del rilevamento automatico della VPN . . . . .	245
Rete . . . . .	246
Rendere visibile il computer sulla rete locale . . . . .	246
Condivisione di file e stampanti in una rete locale . . . . .	246
Risoluzione del problema dell'avvio lento . . . . .	247

Connessione a Internet . . . . .	248
La connessione a Internet non riesce dopo l'installazione . . . . .	248
Consentire messaggi heartbeat dell'ISP . . . . .	249
Connessione tramite un client ICS . . . . .	250
Connessione tramite un server proxy . . . . .	250
Impossibile connettersi a un server per consigli sui programmi . . . . .	250
IM Security . . . . .	251
I programmi IM non appaiono nella tabella Stato della protezione . . . . .	251
Antivirus . . . . .	252
Problema di installazione della funzione antivirus . . . . .	252
Avviso Monitoraggio Antivirus . . . . .	252
Risoluzione di conflitti tra prodotti antivirus . . . . .	253
Scansione della posta elettronica o IM Security non disponibile . . . . .	253
Problemi legati a software di terzi . . . . .	254
Antivirus . . . . .	254
Browser . . . . .	255
Programmi di chat e messaggistica immediata . . . . .	255
Programmi di posta elettronica . . . . .	256
Programmi di segreteria telefonica Internet . . . . .	256
Programmi di condivisione file . . . . .	257
Programmi FTP . . . . .	257
Giochi . . . . .	257
Programmi di controllo remoto . . . . .	258
Programmi VNC . . . . .	259
Programmi per flussi multimediali . . . . .	260
Programmi Voice over IP . . . . .	260
Programmi per conferenze sul Web . . . . .	260
<b>Appendice D    Comportamento dei programmi . . . . .</b>	<b>261</b>
Comportamento sospetto . . . . .	262
Comportamento pericoloso . . . . .	263
<b>Glossario . . . . .</b>	<b>267</b>
<b>Indice . . . . .</b>	<b>1</b>

# Tabelle

---

Tabella 2-1: Icone nell'area di notifica del sistema	15
Tabella 2-2: Messaggi relativi all'aggiornamento	17
Tabella 3-1: Protocolli VPN supportati	37
Tabella 3-2: Risorse di rete relative a VPN necessarie	39
Tabella 4-1: Campi dell'elenco delle origini di traffico	49
Tabella 4-2: Campi del log per gli eventi relativi al firewall	51
Tabella 4-3: Autorizzazioni di accesso predefinite per tipi diversi di traffico in entrata e in uscita	53
Tabella 5-1: Campi del log per gli eventi relativi ai programmi	76
Tabella 5-2: Campi del log per gli eventi relativi a OSFirewall	78
Tabella 5-3: Simboli degli elenchi dei programmi	83
Tabella 6-1: Icone che indicano le destinazioni di scansione	98
Tabella 6-3: Campi del log per gli eventi relativi ai virus	106
Tabella 6-4: Campi del log per gli eventi relativi a spyware	111
Tabella 9-1: Campi del Visualizzatore log	174
Tabella 11-1: Categorie Controllo genitori	193
Tabella 12-1: Spiegazioni dei campi del Visualizzatore log	209
Tabella A-1: Messaggi di avviso IM	230
Tabella B-1: Tasti di scelta rapida per lo spostamento	234
Tabella B-2: Tasti di scelta rapida per funzioni globali	236
Tabella B-3: Tasti di scelta rapida per le finestre di dialogo	238
Tabella B-4: Sequenze di tasti per attivare pulsanti	239
Tabella C-1: Risoluzione di problemi con il software VPN	244
Tabella C-2: Risoluzione di problemi di rete	246
Tabella C-3: Risoluzione di problemi relativi al software antivirus	248
Tabella C-4: Risoluzione di problemi di IM Security	251
Tabella C-5: Risoluzione dei problemi di Zone Labs Anti-virus	252

---

Tabella D-1: Guida sul comportamento sospetto . . . . .	262
Tabella D-2: Guida sul comportamento pericoloso . . . . .	263

# Figure

---

Figura 2-1: Centro di controllo del software di sicurezza Zone Labs . . . . .	12
Figura 2-2: Dashboard del software di sicurezza Zone Labs . . . . .	13
Figura 4-1: Ordine di classificazione delle regole della scheda Esperto . . . . .	57
Figura 4-2: Elenco delle regole della scheda Esperto . . . . .	66
Figura 5-1: Elenco dei programmi . . . . .	82
Figura 5-2: Elenco dei componenti . . . . .	90
Figura 6-1: Stato Antivirus e Antispyware . . . . .	96
Figura 6-2: Finestra di dialogo Destinazioni della scansione . . . . .	97
Figura 6-3: Finestra di dialogo Risultati scansione . . . . .	104
Figura 6-4: Finestra di dialogo Risultati scansione . . . . .	109
Figura 6-5: Area di stato del monitoraggio antivirus in ZoneAlarm . . . . .	116
Figura 7-1: Elenco di allegati . . . . .	122
Figura 7-2: Barra degli strumenti del filtro della posta indesiderata . . . . .	127
Figura 7-3: Scheda con le opzioni di contestazione . . . . .	133
Figura 7-4: Esempio di report di infezione . . . . .	138
Figura 8-1: Privacy Advisor . . . . .	145
Figura 8-2: Elenco della privacy . . . . .	146
Figura 9-1: Avvisi del firewall . . . . .	163
Figura 9-2: Avvisi Nuovo programma . . . . .	164
Figura 9-3: Avviso Nuova rete . . . . .	165
Figura 9-4: Avvisi Blocco ID . . . . .	166
Figura 9-5: Avviso Comportamento sospetto . . . . .	167
Figura 9-6: Avviso Comportamento pericoloso . . . . .	168
Figura 10-1: Trasmissione di contenuti di myVAULT . . . . .	181
Figura 10-2: Ricezione di contenuti di myVAULT da parte del destinatario . . . . .	181
Figura 10-3: Sezione Stato di Blocco ID . . . . .	182

---

Figura 10-4: Elenco dei siti attendibili . . . . .	186
Figura 12-1: Invio di una trasmissione vocale bloccata . . . . .	202
Figura 12-2: Blocco di una trasmissione vocale in arrivo . . . . .	202
Figura 12-3: Invio di un URL eseguibile a un contatto . . . . .	203
Figura 12-4: Collegamento potenzialmente dannoso rimosso . . . . .	203
Figura 12-5: Esempio di conversazione crittografata . . . . .	204
Figura 12-6: Esempio di conversazione non crittografata . . . . .	205

# Introduzione

---

- "Informazioni sul software di sicurezza Zone Labs", a pagina xiv
- "Novità della release 6.1", a pagina xv
- "Informazioni su questa guida", a pagina xvi

ZLD 1-0422-0610-2005-1107

# Informazioni sul software di sicurezza Zone Labs

Il software di sicurezza Zone Labs è una famiglia di prodotti di sicurezza che offre un'ampia gamma di funzioni e vantaggi. Questa release supporta le versioni seguenti del software di sicurezza Zone Labs:

- **ZoneAlarm**

Offre la protezione del firewall e la protezione limitata della posta elettronica.

- **ZoneAlarm Anti-virus**

Include le stesse funzioni disponibili nella versione gratuita di ZoneAlarm più la protezione dai virus.

- **ZoneAlarm Wireless Security**

Offre la protezione del firewall e la protezione limitata della posta elettronica con supporto per reti wireless.

- **ZoneAlarm Pro**

Include la protezione avanzata del firewall, la protezione della posta in entrata e in uscita, il controllo della privacy, la protezione contro lo spyware e permette agli utenti avanzati di personalizzare le regole del firewall.

- **ZoneAlarm Security Suite**

Include le funzioni disponibili in ZoneAlarm Pro, più IM Security, Controllo genitori, protezione da spyware e virus, filtro della posta indesiderata e offre protezione agli utenti di laptop e alle reti domestiche wireless.



# Novità della release 6.1

La release 6.1 del software di sicurezza Zone Labs include le nuove funzioni seguenti:




- Protezione contro lo spyware – Previene, rileva e rimuove lo spyware prima che possa danneggiare il computer. Le opzioni di cura automatica e Anti-spyware Advisor rendono semplice la gestione dello spyware. "Protezione contro spyware e virus", a pagina 94.
- Protezione OSFirewall™ – Tiene sotto controllo il sistema operativo per eventuali attività sospette dei programmi, quali installazioni e modifiche al registro di sistema e impedisce al malware di danneggiare i programmi. Protegge le impostazioni dei browser contro gli attacchi degli hacker.
- Enhanced SmartDefense™ Advisor – Include ora una funzione automatica di blocco dei programmi, che disabilita automaticamente qualsiasi programma tenti attività pericolose o dannose.
- SmartDefense™ Rapid Response Network – Un team dedicato di esperti di Zone Labs che controlla costantemente le nuove minacce e regola automaticamente la sicurezza per assicurare la protezione ottimale. Aggiorna automaticamente il database delle firme con le informazioni sui più recenti attacchi spyware. Distribuisce automaticamente e su base regolare le firme dei virus e dello spyware.
- Supporto alle reti wi-fi – Rileva automaticamente le nuove reti wireless e visualizza il codice SSID (Service Set Identifier) nella finestra di dialogo di rilevamento delle reti. Identifica le reti wireless non protette e imposta automaticamente la sicurezza appropriata per proteggere il computer.
- Nuova esercitazione Flash – Fornisce un'introduzione al software di sicurezza Zone Labs completa di commento e immagini animate.

# Informazioni su questa guida

Il presente manuale è destinato agli utenti di ZoneAlarm, ZoneAlarm Anti-virus, ZoneAlarm Pro, ZoneAlarm Wireless Security e ZoneAlarm Security Suite. Nel manuale, per indicare l'insieme di questi prodotti si fa riferimento al software di sicurezza Zone Labs. Nei casi in cui sia necessario fare riferimento a un prodotto specifico, è usato il nome del prodotto.

## Convenzioni

In questo manuale si fa uso delle seguenti convenzioni per la formattazione e la grafica.

Convenzione	Descrizione
<b>Grassetto</b>	Usato per gli elementi dell'interfaccia utente come pannelli, schede, campi, pulsanti e opzioni di menu.
<i>Corsivo</i>	Usato per nomi di file e percorsi.
	Usato per separare il nome del pannello e il nome della scheda selezionati nelle procedure. Esempio: Selezionare <b>Panoramica</b>   <b>Stato</b> , quindi fare clic su <b>Aggiungi</b> .
	Icona Suggestivo. Suggestisce metodi alternativi per svolgere operazioni o procedure.
	Icona Nota. Rimarca informazioni importanti, correlate o di supporto.
	Icona Attenzione. Indica azioni o processi che possono potenzialmente danneggiare dati o programmi.

## Forum degli utenti di Zone Labs

Connettersi ad altri utenti del software di sicurezza Zone Labs. Porre domande, ottenere risposte e vedere in che modo gli altri utenti riescono a ottenere il meglio dal software di sicurezza Zone Labs. Visitare: [http://www.zonelabs.com/store/content/support/userForum/userForum\\_agreement.jsp](http://www.zonelabs.com/store/content/support/userForum/userForum_agreement.jsp)

# Capitolo

---

## Installazione e configurazione

# 1

Questo capitolo fornisce requisiti del sistema e istruzioni per l'installazione, l'aggiornamento, la configurazione e la disinstallazione del software di sicurezza Zone Labs.

Argomenti:

- "Requisiti di sistema e software supportato", a pagina 2
- "Installazione del software di sicurezza Zone Labs", a pagina 4
- "Aggiornamento di una versione precedente", a pagina 6
- "Configurazione delle opzioni di base", a pagina 7
- "Disinstallazione del software di sicurezza Zone Labs", a pagina 9

# Requisiti di sistema e software supportato

In questa sezione sono elencati i requisiti hardware e software necessari per eseguire il software di sicurezza Zone Labs.



La risoluzione ideale per il software di sicurezza Zone Labs è 1024 x 768 o superiore. Alcune schermate del software potrebbero non essere visualizzate correttamente con una risoluzione di 800 x 600 o inferiore.

Il computer su cui si installa il software di sicurezza Zone Labs deve disporre di:

- Uno dei seguenti sistemi operativi e della RAM minima necessaria:
  - Microsoft® Windows® XP, Home o Professional Edition, 128MB di RAM
  - Microsoft Windows 2000 Professional, 64 MB di RAM
- 50 MB di spazio libero sul disco rigido
- Pentium® III 450 Mhz o superiore

## Protocolli di protezione della posta elettronica supportati

- HTTP (filtro per la posta indesiderata in abbinamento a Outlook o Outlook Express)
- IMAP4 (solo in entrata) - IMAP4 non è supportato per la scansione antivirus della posta elettronica.
- POP3 (solo in entrata)
- SMTP (solo in uscita)

## Software browser supportati

- Internet Explorer 5.5, 6.0 SP1, 6.0 SP2
- Netscape Navigator 7.2, 8.0 Beta
- FireFox 1.00 e versione più recente (1.02)
- Mozilla 1.4 e versioni successive
- MSN Explorer 6.0 e la versione più recente (7.02)
- AOL 9.0
- Client IM (messaggistica immediata) supportati:
  - MSN 6.2.0205

- Windows Messenger 4.7.3001
- Yahoo! IM6.0.0.1922
- Yahoo! Japan IM\*6.0.0.1703

## Client IM (messaggistica immediata) supportati

- MSN 6.2.2005
- Windows Messenger4.7.3001
- Yahoo! IM 6.0.0.1922
- Yahoo! Japan IM 6.0.0.1703



Japan Yahoo IM non supporta ID Yahoo non giapponesi. Inoltre, Japan IM utilizza un processo diverso: *YPagerJ.exe*

- AOL Instant Messenger 5.9.3702
- ICQ Pro 2003b (build 3916)
- ICQ Lite 5.03 (build 2315)
- Trillian (/MSN/YIM/AIM/ICQ) 0.74i
- Trillian Pro (/MSN/YIM/AIM/ICQ) 3.1
- GAIM (/MSN/YIM/AIM/ICQ) 1.2.1
- Miranda (MSN/YIM/ICQ) 0.3.3.1

# Installazione del software di sicurezza Zone Labs

Il processo di installazione e di configurazione del software di sicurezza Zone Labs prevede l'installazione dei file del software, l'esecuzione della configurazione guidata per l'impostazione delle opzioni di protezione di base e la visualizzazione dell'esercitazione.



Se sul computer è installata una versione del software di sicurezza Zone Labs precedente, si potrebbe ricevere un avviso di sicurezza durante l'installazione. Fare clic su **OK** per chiudere questi avvisi prima di procedere all'installazione.

## Installazione di ZoneAlarm

Prima di iniziare il processo di installazione, è necessario scaricare ZoneAlarm dal sito Web di Zone Labs, quindi selezionare il percorso sul computer in cui è stato salvato il file di installazione.

1. Fare doppio clic sul file di installazione scaricato.

Viene avviato il programma di installazione.

2. Specificare una posizione per i file di installazione, oppure fare clic su **Avanti** per continuare.

Il percorso predefinito è *C:\Program Files\Zone Labs\ZoneAlarm*.

3. Digitare il proprio nome, quello della società (facoltativo) e l'indirizzo di posta elettronica, quindi fare clic su **Avanti**.

4. Leggere e accettare il contratto di licenza, quindi fare clic su **Installa**.

Viene avviato il programma di installazione.

5. Fare clic su **Fine** per chiudere il programma di installazione.

6. Fare clic su **Sì** per avviare ZoneAlarm.

Viene visualizzata la Configurazione guidata licenza.

7. Selezionare la versione di prova ZoneAlarm Pro o quella gratuita ZoneAlarm, quindi fare clic su **Avanti**.

Quando si installa ZoneAlarm, si ha l'opzione di installare la versione di prova ZoneAlarm Pro, gratuita per 15 giorni. Durante il periodo di prova è possibile usufruire delle opzioni di sicurezza avanzate disponibili in ZoneAlarm Pro. Al termine del periodo di prova, è possibile continuare a utilizzare queste funzioni avanzate acquistando ZoneAlarm Pro oppure tornare a ZoneAlarm. Se si decide di tornare a ZoneAlarm dopo il periodo di prova di ZoneAlarm Pro, qualsiasi impostazione personalizzata creata in ZoneAlarm Pro verrà eliminata.

## Installazione del software di sicurezza Zone Labs

Prima di poter avviare il processo di installazione, è necessario inserire il CD del software di sicurezza Zone Labs nell'unità CD-ROM del computer oppure, se il software è stato scaricato dal sito Web di Zone Labs, individuare la posizione in cui è stato salvato il file di installazione.

### Installare il software di sicurezza Zone Labs

1. Fare doppio clic sul file di installazione.

Viene avviato il programma di installazione.

2. Specificare una posizione per i file di installazione, oppure fare clic su **Avanti** per continuare.

Il percorso predefinito è *C:\Program Files\Zone Labs\ZoneAlarm*.

3. Digitare il proprio nome, quello della società (facoltativo) e l'indirizzo di posta elettronica, quindi fare clic su **Avanti**.
4. Leggere e accettare il contratto di licenza, quindi fare clic su **Installa**.
5. Fare clic su **Fine** per chiudere il programma di installazione.

Se si sta eseguendo l'aggiornamento di una versione precedente, sarà necessario riavviare il computer per completare il processo di installazione.

6. Fare clic su **OK** per riavviare il computer, o fare clic su **Annulla**.



Se si sceglie di fare clic su Annulla, è necessario ricordarsi di riavviare il computer successivamente per completare l'installazione.

# Aggiornamento di una versione precedente

Il software di sicurezza Zone Labs è ideato per consentire in modo semplice l'aggiornamento di una versione alla successiva. Nella maggior parte dei casi, non è necessario disinstallare la versione esistente prima di aggiornarla con la versione 6.1. Tuttavia, se si utilizza qualsiasi versione del client Integrity (solo per uso aziendale), occorre innanzi tutto disinstallare tale prodotto prima procedere con l'aggiornamento.

## Aggiornamento e firewall connessione Internet (ICF) di Windows XP SP2

Se si esegue Windows XP SP2 e si sta effettuando l'aggiornamento alla versione 6.1, dopo l'aggiornamento potrebbe essere necessario riattivare manualmente Windows Firewall incluso in Windows XP SP2. Per sapere come attivare Windows Firewall incluso in Windows XP, cercare *firewall* nella Guida in linea di Windows XP.

## Aggiornamento e impostazioni di IMsecure myVault

Se si esegue la versione standalone di IMsecure o IMsecure Pro e si sta effettuando l'aggiornamento a ZoneAlarm Security Suite, per ragioni di sicurezza il programma di aggiornamento è stato progettato in modo da non trasferire numeri e codici personali (previdenza sociale, carta di credito e PIN di accesso).

## Aggiornamento e impostazioni di MailFrontier

Se si esegue la versione standalone di MailFrontier e si sta effettuando l'aggiornamento a ZoneAlarm Security Suite, il processo di aggiornamento trasferisce la rubrica, mentre le altre impostazioni di MailFrontier andranno perse.

### Aggiornare una versione precedente

1. Fare doppio clic sul file di installazione.

Viene avviato il programma di installazione.

2. Selezionare una delle opzioni di aggiornamento, quindi fare clic su **Avanti** per continuare.

Aggiorna	Questa opzione mantiene le impostazioni di sicurezza esistenti e le applica alla nuova versione. Alle nuove caratteristiche che vengono aggiunte durante l'aggiornamento vengono applicate le impostazioni predefinite.
Nuova installazione	Quest'opzione annulla le impostazioni di sicurezza esistenti e ripristina quelle predefinite.



# Configurazione delle opzioni di base

Dopo aver completato l'installazione, verrà avviata la configurazione guidata. La configurazione guidata si apre solamente una volta terminata l'installazione e assiste l'utente durante l'impostazione delle opzioni di base del software di sicurezza Zone Labs. È possibile utilizzare la configurazione guidata per attivare la protezione della privacy, impostare il tipo di rilevamento della rete, specificare le impostazioni di avviso, attivare la protezione antivirus e configurare le autorizzazioni per i programmi.

## Configurazione delle autorizzazioni di accesso ai programmi

Il software di sicurezza Zone Labs può configurare molti dei programmi più comuni appartenenti alle seguenti categorie di software:

- Programmi di messaggistica immediata
- Browser Web
- Microsoft Office
- Posta elettronica
- Antivirus
- Processi di Microsoft Windows
- Utilità per i documenti
- Applicazioni software Zone Labs

Per ulteriori informazioni su come assegnare le autorizzazioni per i programmi, vedere "Impostazione di autorizzazioni per programmi specifici", a pagina 81.

## Iscriversi alla comunità DefenseNet

Gli utenti del software di sicurezza Zone Labs possono contribuire al futuro dei prodotti di sicurezza di Zone Labs iscrivendosi alla comunità DefenseNet dedicata alla protezione e inviando periodicamente, e in forma anonima, dati di configurazione per sottoporli all'analisi da parte di Zone Labs. Iscrivendosi a DefenseNet, gli utenti possono aiutarci a focalizzare l'attenzione su funzioni e servizi di maggior utilizzo al fine di introdurre nuove funzionalità che offrano un livello di sicurezza più avanzato.

I dati di configurazione non vengono raccolti da utenti di ZoneAlarm o ZoneAlarm Anti-virus.



Anche se nella scheda **PanoramicalPreferenze** è selezionata l'opzione "Avvisa con una finestra pop-up prima di stabilire il contatto", prima dell'invio dei dati di configurazione a Zone Labs non verrà visualizzato alcun avviso.

I dati raccolti sono completamente anonimi e destinati esclusivamente all'uso interno da parte di Zone Labs e non verranno distribuiti a terzi. Saranno raccolte le informazioni di

una piccola percentuale dei milioni di utenti del software di sicurezza Zone Labs. La frequenza della trasmissione dei dati dipende dalla configurazione del computer. Per la maggior parte degli utenti, i dati verranno inviati una volta al giorno.

Per l'invio dei dati di configurazione a Zone Labs, selezionare **Sì, condividi le mie impostazioni in modo anonimo e automatico** nella configurazione guidata.



Se in seguito si decide di non inviare i dati in modo anonimo, selezionare **PanoramicaPreferenze** nell'area Contatta Zone Labs, quindi deselezionare la casella di controllo **Condividi le mie impostazioni in modo anonimo....**

# Disinstallazione del software di sicurezza Zone Labs

Se è necessario disinstallare il software di sicurezza Zone Labs, eseguire il programma di disinstallazione incluso nei file di installazione invece dell'utilità *Aggiungi/Rimuovi* programmi di Windows. Questa procedura garantisce che tutte le tracce del software di sicurezza Zone Labs vengano rimosse dal computer.

Per disinstallare il software di sicurezza Zone Labs, è necessario avere i privilegi di amministratore.



Se si sta eseguendo l'aggiornamento, non c'è alcun bisogno di disinstallare la versione esistente. Per ulteriori informazioni, vedere il "Installazione del software di sicurezza Zone Labs", a pagina 4.

## Disinstallare il software di sicurezza Zone Labs:

1. Selezionare **Start** | **Programmi**.
2. Selezionare **Zone Labs** | **Disinstalla**.

Viene avviato il programma di disinstallazione.



# Capitolo

---

## software di sicurezza Zone Labs - Nozioni di base

# 2

Questo capitolo fornisce un'introduzione agli strumenti e ai concetti principali del software di sicurezza Zone Labs.

Argomenti:

- "Tour del Centro di controllo del software di sicurezza Zone Labs", a pagina 12
- "Comprendere le zone", a pagina 18
- "Come rispondere agli avvisi", a pagina 20
- "Impostazione delle preferenze del prodotto", a pagina 22
- "Licenza, registrazione e supporto", a pagina 28

# Tour del Centro di controllo del software di sicurezza Zone Labs

Il Centro di controllo del software di sicurezza Zone Labs offre un punto di accesso alle funzioni di sicurezza che proteggono il computer. Le principali funzioni del software di sicurezza Zone Labs sono incluse in un menu sul lato sinistro del Centro di controllo.

## Esplorazione del Centro di controllo

Per passare da una funzione all'altra, selezionare innanzi tutto la funzione desiderata dal menu, quindi scegliere la scheda da visualizzare.

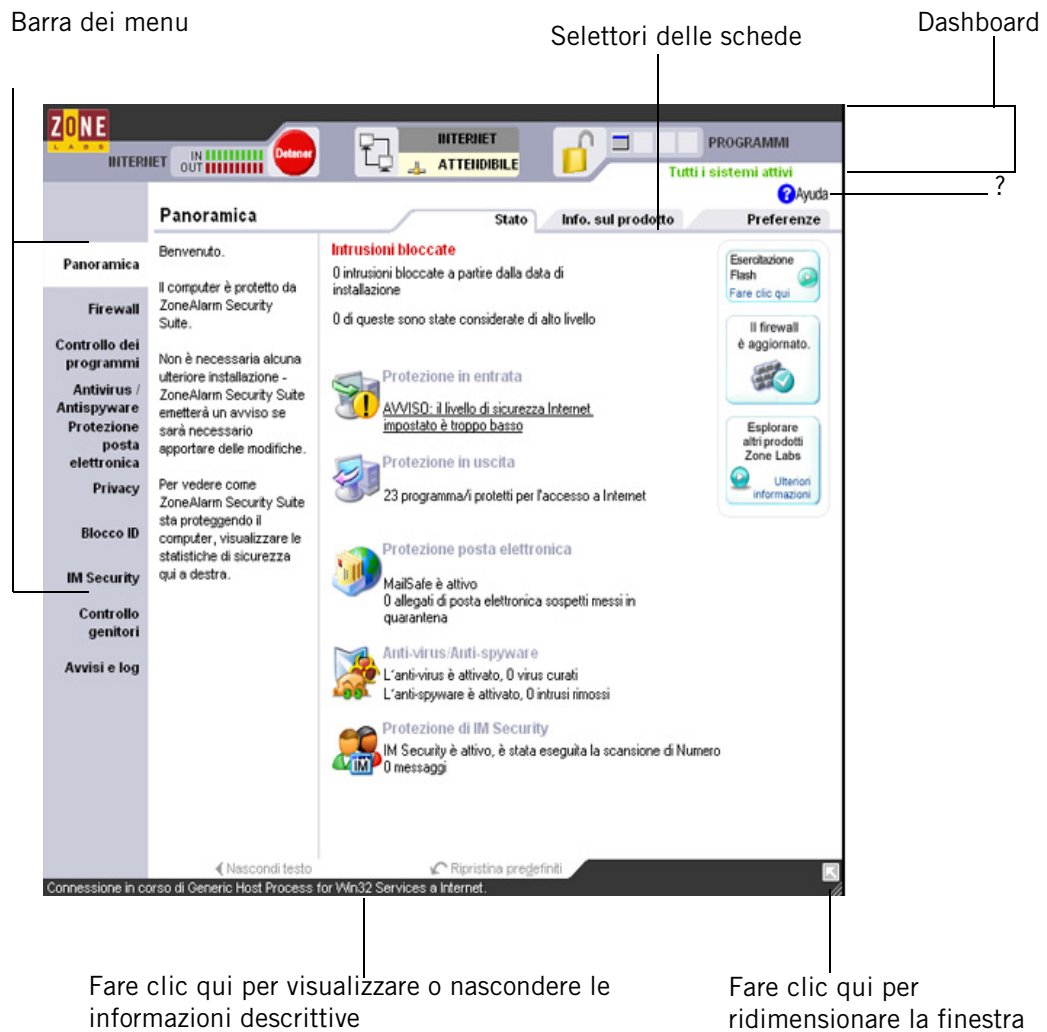


Figura 2-1: Centro di controllo del software di sicurezza Zone Labs

### Barra dei menu

La barra dei menu consente di accedere ai pannelli disponibili. Gli strumenti all'interno di ogni pannello sono suddivisi in due o più schede.

### ***Selettori delle schede***

Fare clic su un selettore di scheda per visualizzare i contenuti della scheda.

Tutti i pannelli del Centro di controllo, a eccezione di Panoramica, hanno una scheda Principale e una o due schede aggiuntive. La scheda Principale contiene le impostazioni globali del pannello.

### ***Mostra/Nascondi testo***

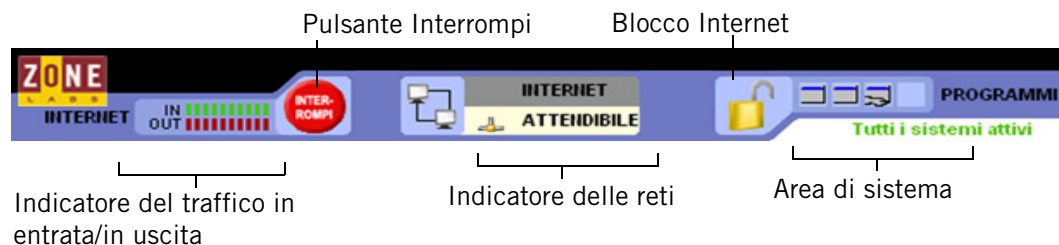
Fare clic su questo collegamento per visualizzare o nascondere il testo descrittivo per la scheda selezionata. Il testo fornisce una breve descrizione della scheda e delle sue impostazioni.

### ***Pulsante Guida (?)***

Per ottenere aiuto relativo alle impostazioni dei pannelli, fare clic sul pulsante Guida (?) nell'angolo in alto a destra. Il sistema di Guida in linea del software di sicurezza Zone Labs visualizza le informazioni della scheda selezionata.

## **Utilizzo del dashboard**

Il dashboard offre accesso costante agli indicatori e alle funzioni di sicurezza di base. Il dashboard appare sopra ogni pannello.



**Figura 2-2: Dashboard del software di sicurezza Zone Labs**

### ***Indicatore del traffico in entrata/in uscita***

L'indicatore del traffico mostra i dati in uscita (colore rosso) o in entrata (colore verde) dal computer. Questo non significa che il traffico sia illegale o che si sia verificato un problema di sicurezza.



Alcune applicazioni accedono alle risorse di rete in background, quindi l'indicatore del traffico è attivo anche quando non si sta accedendo direttamente a Internet.

### ***Pulsante Interrompi***

Fare clic sul pulsante Interrompi per bloccare immediatamente tutte le attività di rete, incluso l'accesso a Internet. Quando si fa clic sul pulsante Interrompi, il dashboard interrompe immediatamente il traffico in entrata e in uscita da/verso Internet. Quindi, fare clic sul pulsante Interrompi solo se si ritiene che il computer stia subendo un attacco, altrimenti il software di sicurezza Zone Labs potrebbe bloccare programmi validi che richiedono l'accesso, nonché messaggi DHCP (*Dynamic Host Configuration*

*Protocol*) o *messaggi heartbeat* dell'ISP utilizzati per mantenere la connessione a Internet. Per riattivare l'accesso, fare di nuovo clic sul pulsante **Interrompi**.

### ***Blocco Internet***

La funzione Blocco Internet interrompe tutto il traffico a eccezione di quello generato da programmi con autorizzazione *Ignora blocco*. Quando si fa clic su Blocco Internet, i messaggi DHCP o i messaggi heartbeat dell'ISP utilizzati per mantenere la connessione a Internet vengono immediatamente bloccati. Questo potrebbe provocare l'interruzione della connessione a Internet. Per poterla riattivare, fare clic di nuovo sul pulsante **Blocco Internet**.



Le funzioni Interrompi e Blocco Internet possono anche essere selezionate facendo clic col pulsante destro del mouse sull'icona dell'area di notifica del sistema e selezionando **Interrompi tutte le attività su Internet** o **Attiva blocco Internet** dal menu di scelta rapida.

### ***Indicatore delle reti***

L'indicatore delle reti mostra quando sono presenti reti cablate o wireless in una zona attendibile o in una zona Internet.

Fare clic sul simbolo di rete per visualizzare la scheda *Zone*, che contiene le impostazioni per la rete.

### ***Area dei programmi attivi***

L'area dei programmi attivi visualizza le icone dei programmi aperti e che hanno effettuato l'accesso a Internet durante la sessione corrente. Per visualizzare le informazioni su un programma, posizionare il puntatore del mouse sulla relativa icona.

Quando il programma invia o riceve dati, l'icona lampeggia.

Il simbolo di una mano sotto l'icona indica che il programma è attivo come server ed è in ascolto delle richieste di connessione.

### ***Area di sistema***

Quest'area visualizza due messaggi.

#### ■ Tutti i sistemi attivi

Indica che il software di sicurezza Zone Labs funziona correttamente.

#### ■ Errore di sistema: riavviare

Indica che il software di sicurezza Zone Labs non sta proteggendo il computer, perché il processo di sicurezza sottostante non è in esecuzione. Riavviare il computer per ripristinare il software di sicurezza Zone Labs.



## Icone nell'area di notifica del sistema

Le icone visualizzate nell'area di notifica del sistema consentono di monitorare lo stato di sicurezza e l'attività Internet ogni volta che si desidera e dà accesso alle impostazioni di sicurezza con pochi clic.






Icona	Descrizione
	Il software di sicurezza Zone Labs è installato e funziona correttamente.
	Il computer invia (colonna rossa) o riceve (colonna verde) traffico di rete. Questo non implica che ci sia un problema di sicurezza o che il traffico di rete sia pericoloso.
	Il software di sicurezza Zone Labs ha bloccato una comunicazione, ma le impostazioni impediscono la visualizzazione di un avviso completo.
	(lucchetto giallo) È stato attivato il Blocco Internet.
	(lucchetto rosso) È stato attivato il pulsante Interrompi. Potrebbero iniziare a essere visualizzati diversi avvisi.

Tabella 2-1: Icone nell'area di notifica del sistema

## Menu di scelta rapida

Fare clic col pulsante destro del mouse sulle icone dell'area di notifica del sistema per accedere al menu di scelta rapida.

### *Attiva blocco Internet*

Questa opzione di menu attiva il blocco Internet e visualizza l'icona del lucchetto giallo nell'area di notifica del sistema. Tutto il traffico Internet generato dai programmi senza autorizzazione Ignora blocco è bloccato. Fornisce la stessa funzione di quando si fa clic su Blocco Internet nel dashboard.

### *Interrompi tutte le attività su Internet*

Questa opzione di menu attiva il pulsante Interrompi e visualizza l'icona del lucchetto rosso nell'area di notifica del sistema. Tutte le attività su Internet sono bloccate. Fornisce la stessa funzione di quando si fa clic sul pulsante Interrompi nel dashboard.

### *Informazioni sul*

Visualizza le informazioni sulla versione per il software di sicurezza Zone Labs installato, tra cui quelle relative al driver e al motore. Se si verificano problemi con il software è possibile copiare queste informazioni negli Appunti e incollarle in un messaggio di posta elettronica da inviare all'assistenza clienti.

### *Ripristina ...Centro di controllo*

Ripristina il Centro di controllo del software di sicurezza Zone Labs alla dimensione completa. La dicitura di questa opzione di menu riflette la versione del software di sicurezza Zone Labs installata (per esempio Zone Labs Anti-virus o ZoneAlarm Security Suite).

***Chiudi...***

Chiude l'applicazione del software di sicurezza Zone Labs. La dicitura di questa opzione di menu riflette la versione del software di sicurezza Zone Labs installata (per esempio Zone Labs Anti-virus o ZoneAlarm Security Suite).

**Utilizzo della scheda Stato**

L'area di protezione della scheda Stato indica se le impostazioni di sicurezza sono attive e fornisce un riepilogo delle attività di sicurezza. Nella scheda Stato è possibile:

- Vedere a colpo d'occhio se il computer è protetto
- Vedere un riepilogo dell'attività del software di sicurezza di Zone Labs
- Vedere se la versione del software di sicurezza Zone Labs è aggiornata
- Accedere all'esercitazione del prodotto

Per ripristinare il conteggio degli avvisi in quest'area, fare clic su **Ripristina predefiniti** nella parte inferiore del pannello.

***Intrusioni bloccate***

Indica quante volte sono intervenuti il firewall del software di sicurezza Zone Labs e MailSafe per proteggere il computer e il numero di *avvisi di alto livello*.

***Protezione in entrata***

Indica se il firewall è attivo e visualizza il numero di avvisi del firewall, di MailSafe e di Blocco Internet generati dall'ultimo ripristino. Se viene visualizzato un avviso, fare clic sul testo sottolineato all'interno dell'avviso per accedere direttamente al pannello che consente di regolare le impostazioni.

***Protezione in uscita***

Indica se il Controllo dei programmi è configurato correttamente e visualizza il numero di avvisi Programma generati dall'ultimo ripristino. Il software di sicurezza Zone Labs avvisa se il Controllo dei programmi è disattivato.

***Monitoraggio prodotti antivirus***

Indica se il computer è protetto contro i virus e visualizza il numero di virus curati fino a quel momento. Lo stato Protezione antivirus appare solo in ZoneAlarm Anti-virus e ZoneAlarm Security Suite. Se si utilizza ZoneAlarm o ZoneAlarm Pro, sarà invece visualizzato lo stato Monitoraggio antivirus.

***Area Protezione posta elettronica***

Indica se MailSafe è attivo e visualizza il numero di allegati messi in quarantena dall'ultimo ripristino. Se viene visualizzato un avviso, fare clic sul testo sottolineato all'interno dell'avviso per accedere direttamente al pannello che consente di regolare le impostazioni.

***Antivirus/Antispyware***

Indica se è attivata la protezione contro virus e spyware e visualizza il numero di virus e spie che sono stati curati.

***Protezione di IM Security***

Indica se è attiva la protezione della messaggistica immediata e visualizza il numero di messaggi che sono stati esaminati.

***Informazioni sugli aggiornamenti e sull'esercitazione***

Quando si acquista il software di sicurezza Zone Labs, si riceve una sottoscrizione per un aggiornamento automatico valida per un anno.

La finestra di aggiornamento garantisce che si sta eseguendo la versione più aggiornata del software di sicurezza Zone Labs, e offre accesso rapido agli aggiornamenti del prodotto quando sono disponibili.

<b>Messaggio</b>	<b>Significato</b>
"Ricerca aggiornamenti"	Fare clic sul collegamento per verificare se sono disponibili per il download aggiornamenti significativi del software di sicurezza Zone Labs.
"È disponibile un aggiornamento."	La sottoscrizione automatica per l'aggiornamento indica che è disponibile un aggiornamento del software di sicurezza Zone Labs. Fare clic sul collegamento per accedere al sito Web Zone Labs e scaricare l'aggiornamento.
"Il firewall è aggiornato"	Sul computer è installata la versione più recente di software di sicurezza Zone Labs.
"La sottoscrizione agli aggiornamenti è scaduta. Fare clic per rinnovare."	La sottoscrizione automatica agli aggiornamenti è scaduta. Fare clic sul collegamento per accedere al sito Web Zone Labs e rinnovare la sottoscrizione.

**Tabella 2-2: Messaggi relativi all'aggiornamento**

Fare clic su **Esercitazione** per apprendere le nozioni di base relative al software di sicurezza Zone Labs.

# Comprendere le zone

Il software di sicurezza Zone Labs tiene traccia di quanto c'è di buono, di cattivo e di sconosciuto su Internet tramite contenitori virtuali, denominati zone, per classificare i computer e le reti che accedono al proprio computer.

La *zona Internet* è lo "sconosciuto". Tutti i computer e le reti del mondo appartengono a questa zona, a meno che vengano spostati in un'altra zona.

La *zona attendibile* è il "buono". Include tutti i computer e le reti attendibili con cui si desidera condividere le risorse, per esempio gli altri computer della rete locale o domestica.

La *zona bloccata* è il "cattivo". Include tutti i computer e le reti non considerati attendibili.

Quando un altro computer vuole comunicare col computer dell'utente, il software di sicurezza Zone Labs esamina la zona in cui si trova tale computer per decidere cosa fare.

Per sapere come includere un computer, una rete o un programma nella zona attendibile, vedere "Gestione delle origini di traffico", a pagina 49.

## Le zone gestiscono la sicurezza del firewall

Il software di sicurezza Zone Labs utilizza i livelli di sicurezza per determinare se consentire o bloccare il traffico in entrata da ogni zona. Utilizzare la scheda Principale del pannello Firewall per visualizzare e regolare i livelli di sicurezza.

### ***Impostazione di sicurezza Alta***

L'impostazione Alta attiva la *modalità invisibile*, rendendo il computer invisibile agli hacker. Questa è l'impostazione predefinita della zona Internet.

Con l'impostazione Alta, la condivisione di file e stampanti è disattivata, mentre sono consentiti il traffico DNS e DHCP in uscita e il traffico broadcast/multicast, in modo che sia possibile navigare su Internet. Tutte le altre porte del computer sono chiuse, tranne quando vengono usate da un programma con autorizzazione di accesso o autorizzazione server.

### ***Impostazione di sicurezza Media***

L'impostazione Media attiva la *modalità di apprendimento dei componenti*, dove il software di sicurezza Zone Labs individua rapidamente le firme MD5 dei componenti di programma utilizzati con maggiore frequenza senza interrompere il lavoro dell'utente con più avvisi. Questa è l'impostazione predefinita per la zona attendibile.

Con l'impostazione Media, la condivisione di file e stampanti è attivata e sono consentiti tutte le porte e tutti i protocolli (se si applica l'impostazione Media alla zona Internet, tuttavia, il traffico NetBIOS in arrivo è bloccato. Questo protegge il computer da potenziali attacchi ai servizi di rete di Windows). Con l'impostazione Media, la modalità invisibile viene disattivata.

Si consiglia di utilizzare l'impostazione di sicurezza Media per i primi giorni di normale utilizzo di Internet dopo l'installazione del software di sicurezza Zone Labs. Trascorso questo periodo, il software di sicurezza Zone Labs saprà riconoscere le firme della maggior parte dei componenti necessari ai programmi che accedono a Internet e ricorderà all'utente di incrementare il livello Autenticazione programma ad Alta.

Per la zona bloccata non servono livelli di sicurezza, perché non è consentito alcun tipo di traffico in entrata né in uscita.



Gli utenti avanzati possono personalizzare i livelli di sicurezza Alta e Media per ogni zona bloccando o aprendo determinate porte. Per ulteriori informazioni, vedere "Blocco e sblocco delle porte", a pagina 53.

## Le zone permettono di controllare i programmi

Quando un programma richiede un'*autorizzazione di accesso* o un'*autorizzazione server*, cerca di comunicare con un computer o una rete in una zona specifica. Per ogni programma è possibile concedere o negare le autorizzazioni seguenti:

- Autorizzazione di accesso per la zona attendibile.
- Autorizzazione di accesso per la zona Internet.
- Autorizzazione server per la zona attendibile.
- Autorizzazione server per la zona Internet.

Con l'autorizzazione di accesso o l'autorizzazione server per la zona attendibile, si consente a un programma di comunicare soltanto con i computer e le reti inclusi in tale zona. Si tratta di una strategia molto sicura. Anche se un programma è contraffatto o gli viene assegnata l'autorizzazione per errore, può comunicare solo con un numero limitato di reti o computer.

Con l'autorizzazione di accesso o l'autorizzazione server per la zona Internet, invece, si consente a un programma di comunicare con qualsiasi computer o rete.



Gli utenti avanzati possono specificare le porte e i protocolli che possono essere utilizzati da un programma, gli host a cui può accedere e altri dettagli. Per ulteriori informazioni, vedere "Creazione di una regola della scheda Esperto per un programma", a pagina 91.

# Come rispondere agli avvisi

Quando si inizia a usare il software di sicurezza Zone Labs, è normale vedere una serie di avvisi. Niente di preoccupante; questo non significa che il computer sta subendo un attacco. Significa che il software di sicurezza Zone Labs sta rilevando e memorizzando le configurazioni dei programmi e delle reti esistenti e dà l'opportunità di configurare la sicurezza nel modo desiderato.

La risposta a un avviso dipende dal tipo di avviso visualizzato. Per informazioni su come rispondere a un determinato tipo di avviso, vedere l'Appendix A, "Guida di riferimento agli avvisi" a partire da pagina 211.

## Nuovi avvisi Programma

La maggior parte degli avvisi iniziali visualizzati sono di tipo Nuovo programma. Questi avvisi vengono visualizzati quando un programma del computer richiede un'autorizzazione di accesso o un'autorizzazione server per Internet o per la rete locale. Utilizzare questo tipo di avviso per concedere l'autorizzazione di accesso ai programmi che ne hanno bisogno, come il browser e il programma di posta elettronica.



Selezionare la casella di controllo **Memorizza impostazione** per concedere l'autorizzazione permanente ai programmi attendibili.

Pochi programmi o processi richiedono l'autorizzazione server per lavorare correttamente. Alcuni processi, tuttavia, sono utilizzati da Microsoft Windows per svolgere funzioni "legittime". Di seguito sono elencati i file eseguibili delle operazioni più comuni che si potrebbero vedere negli avvisi:

- lsass.exe
- spoolsv.exe
- svchost.exe
- services.exe
- winlogon.exe

Se non si riconosce il programma o il processo che richiede l'autorizzazione server, cercare sul sito Web del supporto Microsoft (<http://support.microsoft.com/>) le informazioni relative al processo per sapere qual è la sua funzione. Tuttavia, molti processi Windows legittimi, inclusi quelli appena elencati, potrebbero essere utilizzati dagli hacker per mascherare virus e worm o per fornire loro l'accesso al sistema tramite virus di tipo Trojan. Se una funzione (per esempio esplorazione di file, accesso a una rete o download di file) non è in esecuzione quando appare l'avviso, la soluzione migliore è non concedere l'autorizzazione server. Le autorizzazioni possono essere concesse in qualsiasi momento a programmi e servizi specifici utilizzando l'elenco dei programmi disponibili sotto **Controllo dei programmi | Programmi**.

Per ulteriori informazioni sugli avvisi Programma e come rispondere, vedere "Avvisi Nuovo programma", a pagina 218.

## **Nuovi avvisi di rete e VPN**

Gli altri avvisi iniziali che potrebbero apparire riguardano la rete e la configurazione VPN. Questi vengono generati quando il software di sicurezza Zone Labs rileva una connessione di rete o VPN. Gli avvisi aiutano a configurare la zona attendibile, le autorizzazioni di porta/protocollo e le autorizzazioni programma correttamente per lavorare in modo sicuro sulla rete. Per informazioni su questi avvisi e come rispondere, vedere l'Appendix A, "Guida di riferimento agli avvisi " a partire da pagina 211.

# Impostazione delle preferenze del prodotto

Utilizzare la scheda Preferenze per impostare o cambiare la password del software di sicurezza Zone Labs, effettuare l'accesso o la disconnessione, gestire gli aggiornamenti, impostare le opzioni generali per la visualizzazione del Centro di controllo del software di sicurezza Zone Labs e configurare le impostazioni relative alla privacy per le comunicazioni tramite Zone Labs.

## Impostazione delle opzioni di aggiornamento

Quando si acquista il software di sicurezza Zone Labs si riceve una sottoscrizione di un anno per ricevere aggiornamenti gratuiti. È possibile verificare manualmente se sono presenti aggiornamenti oppure impostare il software di sicurezza Zone Labs per effettuare il controllo automaticamente.

### Impostare le opzioni per la ricerca degli aggiornamenti

1. Selezionare **Panoramica | Preferenze**.
2. Nell'area Ricerca aggiornamenti, selezionare un'opzione di aggiornamento.

Automatica	Il software di sicurezza Zone Labs avvisa automaticamente l'utente quando è disponibile un aggiornamento.
Manuale	L'utente controlla la scheda Stato per verificare la presenza di aggiornamenti. Per effettuare immediatamente la ricerca, fare clic su <b>Ricerca aggiornamenti</b> .

## Impostazione della password

Impostando una password si impedisce ad altre persone di arrestare o disinstallare il software di sicurezza Zone Labs oppure di apportare modifiche alle impostazioni di sicurezza. L'impostazione della password non impedisce, però, ad altre persone di accedere a Internet dal computer dell'utente.

La funzionalità di creazione della password non è disponibile in ZoneAlarm.

Se la versione del software di sicurezza Zone Labs è stata installata da un amministratore con password di installazione, quest'ultimo può accedere a tutte le funzioni.

Quando si imposta una password per la prima volta, è opportuno disconnettersi prima di allontanarsi dal computer, perché altrimenti un altro utente potrebbe cambiare le impostazioni.

### Impostare o modificare la password del software di sicurezza Zone Labs

1. Selezionare **Panoramica | Preferenze**.
2. Fare clic su **Imposta password**.



3. Digitare la password e confermarla nelle apposite caselle.
4. Selezionare **Consenti ad altri utenti di utilizzare i programmi senza una password (a meno che l'autorizzazione per i programmi non sia impostata su "Blocca")** per consentire ad altri utenti di utilizzare programmi che non sono stati esplicitamente bloccati, anche se non sono a conoscenza della password.
5. Fare clic su **OK**.



Le password valide possono contenere un minimo di 6 e un massimo di 31 caratteri. I caratteri validi includono A-Z, a-z, 0-9 e i simboli!, @, #, \$, %, ^, &, \*.

Dopo aver impostato la password, è necessario effettuare l'accesso prima di poter modificare le impostazioni, arrestare il motore di sicurezza di TrueVector o disinstallare il software di sicurezza Zone Labs.

## Eseguire il backup e il ripristino delle impostazioni di sicurezza

È possibile creare una copia di backup delle impostazioni di sicurezza in un file XML e ripristinarle in caso di necessità.



La funzione di backup e ripristino non deve essere usata per condividere impostazioni fra più computer o per distribuire criteri di sicurezza. Questo, infatti, potrebbe provocare la visualizzazione di molti avvisi a causa delle differenze fra i computer, le applicazioni e i processi di Windows.

La funzionalità di backup e ripristino delle impostazioni è disponibile solo in ZoneAlarm Pro e ZoneAlarm Security Suite.

### Eseguire il backup delle impostazioni di protezione

1. Selezionare **Panoramica | Preferenze**.
2. Nell'area Backup e ripristino delle impostazioni di sicurezza, fare clic su **Backup**.
3. Digitare un nome di file o selezionare un file esistente da sovrascrivere.
4. Fare clic su **Salva**.

### Eseguire il backup o ripristinare le impostazioni di protezione

1. Selezionare **Panoramica | Preferenze**.
2. Nell'area Backup e ripristino delle impostazioni di sicurezza, fare clic su **Ripristina**.
3. Selezionare il file XML che contiene le impostazioni da utilizzare.

4. Fare clic su **Apri**.

## Impostazione delle preferenze generali del prodotto

Per impostazione predefinita, il software di sicurezza Zone Labs si avvia automaticamente all'accensione del computer. Per cambiare questa impostazione e altre opzioni, utilizzare le impostazioni dell'area Impostazioni generali.

### Impostare le preferenze generali

1. Selezionare **Panoramica | Preferenze**.
2. Nell'area Impostazioni generali, specificare le preferenze desiderate..

Carica il software di sicurezza Zone Labs all'avvio	Il software di sicurezza Zone Labs si avvia automaticamente all'accensione del computer.
Proteggi il client del software di sicurezza Zone Labs	Impedisce a virus Trojan di inviare richieste eseguite tramite tastiera o mouse al software di sicurezza Zone Labs. <b>Nota:</b> per garantire la massima sicurezza, <b>disattivare questa funzione solo se</b> si hanno problemi con la tastiera o il mouse mentre si utilizzano programmi di accesso remoto.

3. Nell'area Generale, fare clic su **Opzioni**.  
Viene visualizzata la finestra di dialogo Opzioni.
4. Nell'area Impostazioni di visualizzazione, specificare le preferenze desiderate.

Memorizza l'ultima scheda consultata	All'apertura del software di sicurezza Zone Labs visualizza la scheda che è stata aperta l'ultima volta che è stato chiuso il Centro di controllo.
Combinazione di colori	Consente di cambiare la combinazione di colori predefinita del Centro di controllo. In ZoneAlarm non sono disponibili scelte di colore supplementari.

5. Nell'area Configurazione proxy, immettere l'indirizzo IP del server proxy solo se si è certi che occorra farlo.



Il software di sicurezza Zone Labs rileva automaticamente la maggior parte delle configurazioni proxy, quali quelle configurate tramite Internet Explorer, rendendo superfluo immettere qui tali informazioni. Occorre immettere le informazioni proxy solo se si dispone di una configurazione non comune, quale un proxy con script e se alcune funzioni come gli aggiornamenti antivirus o la messaggistica immediata non funzionano.

## Impostazione delle preferenze di contatto

L'impostazione delle preferenze di contatto garantisce la protezione della privacy quando il software di sicurezza Zone Labs comunica con Zone Labs (per esempio, per controllare automaticamente se sono disponibili degli aggiornamenti).

### Impostare le preferenze di contatto

1. Selezionare **Panoramica | Preferenze**.
2. Nell'area Contatta Zone Labs, specificare le preferenze desiderate.

Avvisa con una finestra pop-up prima di stabilire il contatto	Visualizza un avviso prima di contattare Zone Labs per inviare le informazioni sulla registrazione, scaricare gli aggiornamenti dei prodotti, cercare un avviso o accedere al sistema DNS per risolvere gli indirizzi IP.  <b>Nota:</b> esistono alcune situazioni in cui l'utente non viene avvisato prima di stabilire il contatto. Queste comprendono l'invio a Zone Labs di dati relativi a DefenseNet, quando si contatta Zone Labs per consigli su un programma, quando si esegue l'aggiornamento antivirus o si controlla lo stato dell'antivirus. L'opzione "Condividi impostazione in modo anonimo..." di seguito, disattiva il trasferimento di dati relativi al DefenseNet. Tutte le altre impostazioni possono essere disabilitate dalla scheda principale dei rispettivi pannelli.
Quando possibile, nascondi il mio indirizzo IP	Impedisce l'identificazione del computer quando si contatta Zone Labs, LLC.
Quando possibile, nascondi l'ultimo numero del mio indirizzo IP	Omette l'ultima parte dell'indirizzo IP (per esempio 123.456.789.XXX) quando si contatta Zone Labs, LLC.
Condividi le mie impostazioni di sicurezza con Zone Labs in modo anonimo	Invia periodicamente i dati di configurazione a Zone Labs. Per ulteriori informazioni, vedere "Iscriversi alla comunità DefenseNet", a pagina 7.  <b>Nota:</b> I dati di configurazione non vengono raccolti da utenti di ZoneAlarm o ZoneAlarm Anti-virus.

## Impostazione delle opzioni di visualizzazione del prodotto e del server proxy

È possibile utilizzare la finestra di dialogo Opzioni per specificare le opzioni di visualizzazione e le informazioni del server proxy.

### Impostare le opzioni di visualizzazione del prodotto e le informazioni sul proxy:

1. Selezionare **Panoramica | Preferenze**.
2. Nell'area **Impostazioni generali**, fare clic su **Opzioni**.

Viene visualizzata la finestra di dialogo Opzioni.

3. Nell'area Impostazioni di visualizzazione, specificare le preferenze desiderate.

Memorizza l'ultima scheda consultata	Alla successiva apertura del Centro di controllo di Zone Labs, vengono visualizzati il pannello e la scheda aperti per ultimi.
Combinazione di colori	Consente di cambiare la combinazione di colori predefinita del Centro di controllo. In ZoneAlarm non sono disponibili scelte di colore supplementari.

4. Se necessario, inserire le informazioni relative al server proxy.

Il software di sicurezza Zone Labs rileva automaticamente la maggior parte delle configurazioni proxy, quali quelle configurate tramite Internet Explorer, rendendo superfluo immettere qui tali informazioni. Le informazioni sul proxy devono essere inserite solo se si utilizza una configurazione insolita, per esempio uno script di configurazione del proxy e se alcune funzioni del prodotto, come gli aggiornamenti dell'antivirus, non funzionano.

## Creazione di un profilo di protezione dalle frodi online

Gli utenti di eBay possono proteggersi da frodi online memorizzando le proprie credenziali online nel software di sicurezza Zone Labs. Il software di sicurezza Zone Labs protegge il profilo dell'utente assicurandosi che sia inviato soltanto a destinazioni eBay autorizzate.

### Creare un profilo di protezione online in ZoneAlarm e ZoneAlarm Anti-virus:

1. Selezionare **Panoramica | Preferenze**.
2. Nell'area Profilo di protezione eBay, fare clic su **Password**.  
Viene visualizzata la finestra di dialogo Password di partner Alliance.
3. Nella casella di riepilogo Partner Alliance selezionare eBay.
4. Digitare la password eBay nelle caselle appropriate, quindi fare clic su **OK**.

### Immettere la password eBay in ZoneAlarm Pro o ZoneAlarm Security Suite:

1. Selezionare **Blocco ID | myVAULT**, quindi fare clic su **Aggiungi**.  
Viene visualizzata la finestra di dialogo Aggiunta di informazioni a myVAULT.
2. Digitare una descrizione dell'elemento, quindi selezionare **Password eBay** dall'elenco a discesa delle categorie.
3. Digitare la password eBay nelle caselle appropriate, quindi fare clic su **OK**.  
Al posto dei caratteri digitati vengono visualizzati gli asterischi e in myVAULT la password di eBay sarà memorizzata in forma crittografata. Le informazioni originali non vengono salvate sul computer.
4. Specificare se le informazioni devono essere protette quando si utilizza il Web e la posta elettronica.

5. Fare clic su **OK** per salvare le modifiche.

Per ulteriori informazioni su come il software di sicurezza Zone Labs protegge le password e altri dati personali, vedere il Capitolo 10, " Protezione dei dati " a partire da pagina 179.

# Licenza, registrazione e supporto

Per ricevere supporto e aggiornamenti per il software di sicurezza Zone Labs è necessario avere una licenza valida.

## Aggiornamento della licenza del prodotto

Se è stato utilizzato un codice di licenza per una versione di prova o demo e non è stata acquistata una licenza completa o se la versione di prova o beta sta per scadere, è possibile acquistare la licenza da Zone Labs.

### Acquistare una licenza:

1. Selezionare **Panoramica | Informazioni sul prodotto**.
2. Nell'area Informazioni sulla licenza, fare clic su **Compra adesso**

Si verrà indirizzati al sito Web di Zone Labs, dove è possibile completare l'acquisto del prodotto.

### Cambiare il codice di licenza

1. Selezionare **Panoramica | Informazioni sul prodotto**.
2. Nell'area Informazioni sulla licenza, fare clic su **Modifica lic.**

Viene visualizzata la finestra di dialogo Informazioni sulla licenza.

3. Nell'area fornita, digitare o incollare il codice di licenza.
4. Fare clic su **Applica**, quindi fare clic su **OK**.

## Registrazione del software di sicurezza Zone Labs

Registrare il software di sicurezza Zone Labs per ricevere novità sulla sicurezza di Zone Labs.

### Registrare il software di sicurezza Zone Labs:

1. Selezionare **Panoramica | Informazioni sul prodotto**.
2. Nell'area di Registrazione, fare clic su **Modifica reg.**

Viene visualizzata la finestra di dialogo Informazioni di registrazione.

3. Digitare il nome, la società e l'indirizzo di posta elettronica negli appositi campi.



L'indirizzo di posta elettronica immesso qui viene utilizzato per la configurazione della protezione MailSafe della posta in uscita. Accertarsi di immettere correttamente l'indirizzo di posta elettronica. Per ulteriori informazioni, vedere "Impostazione delle opzioni di protezione di MailSafe in uscita", a pagina 125.

4. Per essere avvisati sulle novità relative ai prodotti e sugli aggiornamenti, selezionare la casella di controllo **Desidero essere informato su aggiornamenti e news importanti**.
5. Fare clic su **OK**.

### **Modificare le informazioni di registrazione**

-  Selezionare **Panoramical | Informazioni sul prodotto**, quindi fare clic su **Modifica reg.**

## **Accesso al supporto tecnico**

Se si è abilitati a ricevere supporto tecnico, è possibile accedere alle risorse disponibili, come le FAQ e i problemi noti, direttamente dal software di sicurezza Zone Labs.

### **Accedere alle risorse di supporto**

1. Selezionare **Panoramica | Informazioni sul prodotto**.
2. Nell'area Informazioni sul supporto e sugli aggiornamenti, fare clic sul collegamento **fare clic qui**.

Viene visualizzato il sito Web del centro di supporto di Zone Labs.

3. Fare clic sul collegamento **Support & Services**, quindi selezionare il prodotto per il quale si richiede assistenza.





# Capitolo

## Connessioni di rete con il software di sicurezza Zone Labs

# 3

Se si lavora in una rete domestica, una rete LAN aziendale, una rete VPN (rete privata virtuale) o una rete wireless è opportuno garantire una comunicazione fluente con la rete pur mantenendo elevati livelli di sicurezza. La configurazione guidata Rete, la configurazione automatica della VPN e altre caratteristiche del software di sicurezza Zone Labs aiutano a impostare il proprio ambiente di rete in modo semplice e veloce.

### Argomenti:

- "Configurazione di una nuova connessione di rete", a pagina 32
- "Integrazione con i servizi di rete", a pagina 35
- "Configurazione della connessione VPN", a pagina 37

# Configurazione di una nuova connessione di rete

Se il computer è collegato alla rete, è necessario stabilire se aggiungere tale rete alla zona attendibile oppure alla zona Internet.

L'aggiunta di una rete alla zona attendibile consente di condividere file, stampanti e altre risorse con altri computer presenti sulla rete. Alla zona attendibile vanno aggiunte le reti note e considerate attendibili, come la LAN domestica o quella aziendale oppure le reti wireless protette.

Aggiungendo una rete alla zona Internet si impedisce la condivisione delle risorse con altri computer sulla rete e si è protetti dai rischi di sicurezza associati alla condivisione delle risorse. A tale zona è opportuno assegnare le reti non note e la maggior parte di quelle wireless, comprese le reti wireless sicure.

La configurazione guidata Rete aiuta a stabilire questa suddivisione determinando la natura pubblica o privata della rete LAN rilevata. La configurazione guidata Rete aiuta a stabilire questa suddivisione determinando se la rete wireless rilevata è sicura o non sicura.

☞ Disattivazione della configurazione guidata Rete wireless

## Utilizzo della configurazione guidata Rete

Quando il computer viene connesso a una nuova rete, il software di sicurezza Zone Labs avvia la configurazione guidata Rete, visualizzando l'indirizzo IP della rete rilevata.

L'indirizzo IP della rete viene utilizzato per determinare se si tratta di una *rete privata* o di una *rete pubblica*.

Solitamente le reti private sono reti domestiche oppure LAN aziendali. Le reti private vengono aggiunte alla *zona attendibile* per impostazione predefinita.

Solitamente le reti pubbliche sono molto più estese, come quelle associate a un ISP. Le reti pubbliche vengono aggiunte alla *zona Internet* per impostazione predefinita.

### Configurare la connessione di rete utilizzando la creazione guidata rete

1. Selezionare la zona alla quale si desidera aggiungere la rete, quindi fare clic su **Avanti**.
2. Assegnare un nome alla rete. Il nome inserito qui verrà visualizzato nella scheda Zone del pannello Firewall.




Se si preferisce non utilizzarla, fare clic su Annulla nella schermata della configurazione guidata. Sarà visualizzato un avviso Nuova rete. La rete rilevata verrà aggiunta alla zona Internet, anche se si tratta di una rete privata. Per informazioni sull'utilizzo dell'avviso Nuova rete, vedere "Avvisi Nuova rete", a pagina 229.

## Disattivazione della configurazione guidata Rete

La configurazione guidata rete è abilitata per impostazione predefinita. Se si preferisce utilizzare l'avviso Nuova rete per la configurazione di nuove reti, è possibile disabilitare la configurazione guidata rete.

### Disattivare la configurazione guidata Rete

 Nella schermata quattro della configurazione guidata, selezionare la casella di controllo **Non mostrare più la configurazione guidata al prossimo rilevamento di rete**, quindi fare clic su **Fine**.

## Utilizzo della configurazione guidata Rete wireless

Quando il computer viene connesso a una nuova rete wireless, il software di sicurezza Zone Labs avvia la configurazione guidata Rete wireless, visualizzando l'indirizzo IP della rete rilevata.

L'impostazione WEP (Wireless Encryption Protocol) sul punto di accesso wireless viene utilizzata per determinare se si tratta di una *rete wireless* sicura o una *rete wireless* non sicura.

Una rete wireless sicura è compatibile con il protocollo WEP. Il protocollo WEP fornisce una barriera iniziale che può essere penetrata facilmente dagli hacker. Per proteggere efficacemente la rete, è necessario implementare altre funzioni per il punto di accesso wireless, come un elenco di accesso limitato o broadcast SSID (Service Set Identifier) disabilitato. Collocare nella *zona attendibile* solo le reti wireless con un livello di sicurezza più elevato e dove occorre condividere risorse o stampanti.

Una rete wireless non sicura può essere completamente priva di protezione e accessibile a chiunque. Le reti non sicure vengono aggiunte alla *zona Internet* per impostazione predefinita.

### Configurare una connessione wireless

1. Selezionare la zona alla quale si desidera aggiungere la rete, quindi fare clic su **Avanti**.
2. Assegnare un nome alla rete.

Il nome inserito nella configurazione guidata verrà visualizzato nella scheda Zone del pannello Firewall.



Se si preferisce non utilizzare la configurazione guidata, fare clic su Annulla in una delle schermate. Sarà visualizzato un avviso Nuova rete. La rete rilevata verrà aggiunta alla zona Internet, anche se si tratta di una rete wireless sicura. Per informazioni sull'utilizzo dell'avviso Nuova rete, vedere "Avvisi Nuova rete", a pagina 229.

## Disattivazione della configurazione guidata Rete wireless

La configurazione guidata rete è abilitata per impostazione predefinita. Se si preferisce utilizzare l'avviso Nuova rete per la configurazione di nuove reti, è possibile disabilitare la configurazione guidata rete.

### Disattivare la configurazione guidata Rete wireless



Nella schermata quattro della configurazione guidata, selezionare la casella di controllo **Non mostrare più la configurazione guidata al prossimo rilevamento di rete**, quindi fare clic su **Fine**.

# Integrazione con i servizi di rete

Quando si lavora all'interno di una rete domestica o aziendale, si desidera condividere file, stampanti di rete o altre risorse con altre persone sulla rete, o inviare e ricevere messaggi di posta elettronica mediante i server di posta della rete. Usare le istruzioni contenute in questa sezione per attivare la condivisione sicura delle risorse.

## Attivazione della condivisione dei file e delle stampanti

Per condividere stampanti e file con altri computer sulla rete, è necessario configurare il software di sicurezza Zone Labs in modo da consentire l'accesso ai computer con i quali si pensa di condividere le risorse.

### Configurare il software di sicurezza Zone Labs per la condivisione di file e stampanti

1. Aggiungere la subnet della rete (o, in una rete di piccole dimensioni, l'indirizzo IP di ogni computer della rete) alla zona attendibile.

Vedere "Aggiunta alla zona attendibile", a pagina 50.

2. Impostare la sicurezza della zona attendibile su Media. Questa impostazione consente a computer attendibile di accedere ai file condivisi.

Vedere "Impostazione del livello di sicurezza per una zona", a pagina 43.

3. Impostare la sicurezza della zona Internet su Alta. Questa impostazione rende invisibile il computer a computer non attendibili.

Vedere "Impostazione del livello di sicurezza per una zona", a pagina 43.

## Collegamento ai server di posta della rete

Il software di sicurezza Zone Labs è configurato in modo da operare automaticamente con i server di posta basati su Internet utilizzando i protocolli POP3 e IMAP4; è sufficiente concedere al client di posta l'autorizzazione per l'accesso a Internet.

Alcuni server di posta, come Microsoft Exchange, includono funzioni di collaborazione e di sincronizzazione che, per poter funzionare, potrebbero richiedere che l'utente consideri il server attendibile.

### Configurare il software di sicurezza Zone Labs per i server di posta con funzioni di collaborazione e sincronizzazione

1. Aggiungere la subnet di rete o l'indirizzo IP per il server di posta alla zona attendibile.
2. Impostare la sicurezza della zona attendibile su Media. Questo consente alle funzioni di collaborazione del server di funzionare.
3. Impostare la sicurezza della zona Internet su Alta. Questa impostazione rende invisibile il computer a computer non attendibili.

## Protezione di una connessione a Internet condivisa

Se si utilizza l'opzione Condivisione connessione Internet (ICS) di Windows, o un programma di condivisione della connessione di terzi, è possibile proteggere tutti i computer che condividono la connessione da minacce in entrata installando il software di sicurezza Zone Labs solamente sul computer che funge da gateway. Tuttavia, per avere la protezione in uscita o per visualizzare gli avvisi sui computer client, è necessario che il software di sicurezza Zone Labs sia installato anche sui computer client.



Prima di configurare il software di sicurezza Zone Labs, utilizzare il software di condivisione della connessione per impostare le relazioni tra il gateway e i client. Se si utilizzano sistemi hardware come i router per condividere la connessione Internet, invece della funzione ICS di Microsoft, assicurarsi che la subnet locale sia presente nella zona attendibile.

# Configurazione della connessione VPN

Il software di sicurezza Zone Labs è compatibile con molti tipi di software per client VPN e può configurare la connessione per alcuni client VPN in modo automatico.

## Protocolli VPN supportati

Il software di sicurezza Zone Labs monitora i protocolli VPN elencati nella tabella sottostante.

Protocollo di rete	Spiegazione e commenti
AH	Protocollo di autenticazione per l'intestazione
ESP	Protocollo ESP (Encapsulating Security Payload)
GRE	Protocollo GRE (Generic Routing Encapsulation)
IKE	Protocollo IKE (Internet Key Exchange)
IPSec	Protocollo IP Security
L2TP	Protocollo L2TP (Layer 2 Tunneling); Il protocollo L2TP è una variante più sicura di PPTP.
LDAP	Protocollo LDAP (Lightweight Directory Access)
PPTP	Protocollo PPTP (Point-to-Point Tunneling)
SKIP	Protocollo SKIP (Simple Key Management for Internet)

**Tabella 3-1: Protocolli VPN supportati**

## Configurazione automatica della connessione VPN

Quando viene rilevato traffico VPN, viene visualizzato automaticamente un avviso Configurazione VPN automatica. In base al tipo di attività VPN rilevata e se il software di sicurezza Zone Labs ha potuto configurare la connessione VPN automaticamente, si può ricevere uno dei tre avvisi di Configurazione VPN automatica.

Per informazioni dettagliate sui tipi di avvisi Configurazione VPN automatica che potrebbero essere visualizzati e sul modo in cui rispondere, vedere "Avvisi Configurazione VPN automatica", a pagina 223.

Potrebbe essere necessaria, per esempio, una configurazione manuale se la scheda di loopback o l'indirizzo IP del gateway VPN rientrasse in un intervallo di indirizzi o in una subnet che sono stati bloccati. Per ulteriori informazioni, vedere "Configurazione manuale della connessione VPN", a pagina 38.



Se è stata creata una regola della scheda Esperto che blocca il traffico VPN, sarà necessario modificare tale regola per consentire il traffico VPN. Vedere "Creazione di regole firewall nella scheda Esperto", a pagina 58.

## Configurazione manuale della connessione VPN

Se la connessione VPN non può essere configurata automaticamente, il software di sicurezza Zone Labs visualizza un avviso Azione manuale obbligatoria che informa l'utente sulle modifiche manuali necessarie per configurare la connessione.

Consultare le sezioni seguenti per istruzioni sulla configurazione manuale:

- Aggiunta di un gateway VPN e altre risorse alla zona attendibile
- Rimozione di un gateway VPN da un intervallo o da una subnet bloccati
- Consentire l'utilizzo dei protocolli VPN
- Concedere le autorizzazioni di accesso al software VPN



Se è stata creata una regola della scheda Esperto che ha bloccato il traffico PPTP e il software utilizza il protocollo PPTP, sarà necessario modificare la regola. Vedere "Creazione di regole firewall nella scheda Esperto", a pagina 58.



## Aggiunta di un gateway VPN e altre risorse alla zona attendibile

Oltre al gateway VPN, potrebbero essere presenti altre risorse che devono necessariamente trovarsi nella zona attendibile per consentire al VPN di funzionare correttamente.

Risorse necessarie	Altre risorse
Le risorse presenti in questa colonna sono indispensabili per tutti i computer dei client VPN e devono essere aggiunte alla zona attendibile.	Le risorse presenti in questa colonna possono essere necessarie oppure no, a seconda della specifica implementazione della VPN.
Concentratore VPN	Server DNS
Computer host remoti collegati al client VPN (se non sono inclusi nelle definizioni della subnet per la rete aziendale)	Indirizzo di loopback del computer locale (a seconda della versione di Windows). Se si specifica l'indirizzo 127.0.0.1, non eseguire un software proxy sull'host locale.
Subnet della rete WAN (Wide Area Network) a cui si accederà dal computer del client VPN.	Gateway Internet
Reti LAN aziendali a cui si accederà dal computer VPN	Subnet locali
	Server di autenticazione (per esempio, RADIUS, ACE o TACACS)

**Tabella 3-2: Risorse di rete relative a VPN necessarie**

Per sapere come aggiungere risorse alla zona attendibile del computer, vedere "Aggiunta alla zona attendibile", a pagina 50.

## Rimozione di un gateway VPN da un intervallo o da una subnet bloccati

Se il gateway VPN rientra in un intervallo o in una subnet che sono stati bloccati, è necessario sbloccare l'intervallo manualmente.

### Sbloccare un intervallo IP o una subnet

1. Selezionare **Firewall | Zona**.
2. Nella colonna **Zona**, selezionare l'intervallo IP o la subnet bloccati.
3. Selezionare **Attendibile** dal menu di scelta rapida, quindi fare clic su **Applica**.

## Consentire l'utilizzo dei protocolli VPN

Per assicurarsi che la configurazione del software VPN all'interno del software di sicurezza Zone Labs funzioni correttamente, sarà necessario modificare le impostazioni di sicurezza generali per consentire l'utilizzo dei protocolli VPN.

### Consentire l'utilizzo dei protocolli VPN

1. Selezionare **Firewall | Principale**, quindi fare clic su **Avanzate**.
2. Nella sezione Impostazioni generali, selezionare la casella di controllo **Consenti protocolli VPN**.
3. Fare clic su **OK**.



Se il programma VPN utilizza protocolli diversi da GRE, ESP e AH, selezionare anche la casella di controllo **Consenti protocolli non comuni con sicurezza elevata**.

### Concedere le autorizzazioni di accesso al software VPN

Autorizzare l'accesso al client VPN e a qualsiasi altro programma relativo alla VPN.

#### Concedere le autorizzazioni al programma VPN

1. Selezionare **Controllo dei programmi | Programmi**.
2. Nella colonna Programmi, selezionare il programma VPN.
3. Nella colonna Accesso, fare clic sotto Attendibile, quindi selezionare **Consenti** dal menu di scelta rapida.



Se il programma VPN non è elencato, fare clic su **Aggiungi** per aggiungerlo all'elenco.

#### Concedere l'accesso ai componenti relativi alla VPN

1. Selezionare **Controllo dei programmi | Componenti**.
2. Nella colonna Componenti, selezionare il componente VPN al quale si desidera concedere l'accesso.
3. Nella colonna Accesso, selezionare **Consenti** dal menu di scelta rapida.

Se si hanno problemi con la connessione VPN, consultare i suggerimenti per la risoluzione dei problemi in Appendice C, " Risoluzione dei problemi ", a pagina 243.

# Capitolo

## Protezione assicurata dal firewall

# 4

La protezione assicurata dal firewall è la prima linea di difesa contro le minacce provenienti da Internet. Le zone e i livelli di sicurezza predefiniti del software di sicurezza Zone Labs offrono una protezione immediata contro gran parte di queste minacce. Le autorizzazioni di porta e le regole Esperto personalizzate offrono agli utenti avanzati un controllo dettagliato del traffico basato su origine, destinazione, porta, protocollo e altri fattori.

### Argomenti:

- "Comprensione della protezione assicurata dal firewall", a pagina 42
- "Scelta dei livelli di sicurezza", a pagina 43
- "Impostazione delle opzioni di sicurezza avanzate", a pagina 45
- "Gestione delle origini di traffico", a pagina 49
- "Blocco e sblocco delle porte", a pagina 53
- "Comprensione delle regole firewall della scheda Esperto", a pagina 56

# Comprensione della protezione assicurata dal firewall

Nel settore edile, il termine inglese "firewall" indica una parete tagliafuoco che impedisce alle fiamme di propagarsi. In informatica, il concetto è simile. Internet è devastata da "fuochi" quali attività di hacker, virus, worm e così via. Un firewall è un sistema che blocca i tentativi di danneggiare un computer.

Il firewall del software di sicurezza Zone Labs sorveglia gli "ingressi" del computer, ossia le porte attraverso le quali passa il traffico di Internet in entrata e in uscita. Il software di sicurezza Zone Labs esamina tutto il traffico di rete che perviene al computer e pone queste domande:

- Da quale zona proviene il traffico e a quale porta è indirizzato?
- Le regole relative a tale zona autorizzano il traffico attraverso quella porta?
- Il traffico viola qualche regola globale?
- Il traffico è autorizzato per un programma sul computer (impostazioni di Controllo dei programmi)?

Le risposte a queste domande determinano se il traffico sarà consentito o bloccato.

# Scelta dei livelli di sicurezza

I *livelli di sicurezza* predefiniti del firewall (Alta per la zona Internet, Media per la zona attendibile) proteggono dall'attività degli hacker (come una *scansione delle porte*), consentendo nello stesso tempo di condividere stampanti, file e altre risorse con computer attendibili sulla rete locale. Nella maggior parte dei casi, non è necessario apportare alcuna modifica a queste impostazioni predefinite. Il computer inizia a essere protetto non appena il software di sicurezza Zone Labs è installato.

## Impostazione del livello di sicurezza per una zona

I livelli di sicurezza semplificano la configurazione delle impostazioni del firewall. È possibile applicare un'impostazione di sicurezza preconfigurata (Alta, Media o Bassa) a ogni zona, oppure specificare le restrizioni di porta e di protocollo per ciascun livello. Vedere "Blocco e sblocco delle porte", a pagina 53.

### Impostare il livello di sicurezza per una zona

1. Selezionare **Firewall | Principale**.
2. Nella sezione Sicurezza zona Internet, trascinare il dispositivo di scorrimento sull'impostazione desiderata.

Alta	Il computer è in una modalità che lo rende invisibile agli altri computer. L'accesso ai servizi <i>NetBIOS (Network Basic Input/Output System)</i> di Windows, a stampanti e file condivisi <b>è bloccato</b> . Le porte sono bloccate, a meno che sia stata fornita l'autorizzazione di utilizzo a un programma.
Media	Il computer è visibile agli altri computer. L'accesso ai servizi di Windows, a stampanti e file condivisi <b>è consentito</b> . Le autorizzazioni per i programmi sono ancora in vigore.
Basso	Il computer è visibile agli altri computer. L'accesso ai servizi di Windows, a stampanti e file condivisi <b>è consentito</b> . Le autorizzazioni per i programmi sono ancora in vigore.

3. Nella sezione Sicurezza zona attendibile, trascinare il dispositivo di scorrimento sull'impostazione desiderata.

Alta	Il computer è in una modalità che lo rende invisibile agli altri computer. L'accesso ai servizi di Windows (NetBIOS), a stampanti e file condivisi <b>è bloccato</b> . Le porte sono bloccate, a meno che sia stata fornita l'autorizzazione di utilizzo a un programma.
Media	Il computer è visibile agli altri computer. L'accesso ai servizi di Windows, a stampanti e file condivisi <b>è consentito</b> . Le autorizzazioni per i programmi sono ancora in vigore.

Bassa	Il computer è visibile agli altri computer. L'accesso ai servizi di Windows, a stampanti e file condivisi <b>è consentito</b> . Le autorizzazioni per i programmi sono ancora in vigore.
-------	--

# Impostazione delle opzioni di sicurezza avanzate

Le opzioni di sicurezza avanzate consentono di configurare il firewall per una serie di situazioni speciali, come l'enforcement del gateway e la Condivisione connessione Internet (ICS).

## Impostazione delle opzioni di sicurezza del gateway

Alcune società richiedono ai dipendenti di utilizzare il software di sicurezza Zone Labs quando si connettono a Internet tramite il *gateway* aziendale. Quando la casella **Controlla automaticamente il gateway...** è selezionata, il software di sicurezza Zone Labs verifica l'eventuale presenza di gateway compatibili e segnala la sua installazione, in modo che i gateway che richiedono il software di sicurezza Zone Labs concedano l'accesso.

Si può lasciare questa casella selezionata anche se non ci si connette tramite un gateway. Le funzioni legate a Internet non saranno influenzate.

## Impostazione delle opzioni di Condivisione connessione Internet (ICS)

Se si utilizza *ICS (Condivisione connessione Internet)*, di seguito viene descritto come configurare il software di sicurezza Zone Labs per il riconoscimento del gateway ICS e dei client.

### Impostare le preferenze di Condivisione connessione Internet

1. Selezionare **Firewall | Principale**.
2. Fare clic su **Avanzate**.
3. Nella sezione Condivisione connessione Internet, scegliere le impostazioni di sicurezza.

Questo computer non è su una rete ICS/NAT	La condivisione della connessione a Internet è disattivata.
Questo computer è un client di un gateway ICS/NAT che esegue il software di sicurezza Zone Labs	Il software di sicurezza Zone Labs rileva automaticamente l'indirizzo IP del gateway ICS e lo visualizza nel campo Indirizzo gateway. È anche possibile digitare l'indirizzo IP nel campo Indirizzo locale.  Selezionando <b>Inoltra gli avvisi dal gateway a questo computer</b> gli avvisi del gateway saranno registrati e visualizzati sul computer client.

Questo computer è un gateway ICS/NAT	<p>Il software di sicurezza Zone Labs rileva automaticamente l'indirizzo IP del gateway ICS e lo visualizza nel campo Indirizzo locale. È anche possibile digitare l'indirizzo IP nel campo Indirizzo locale.</p> <p>Selezionando <b>Disattiva gli avvisi localmente se vengono inoltrati ai client, si eviterà che gli avvisi inoltrati dal gateway ai client siano visualizzati anche sul gateway.</b></p>
--------------------------------------	--

4. Fare clic su **OK**.

## Impostazione delle opzioni di sicurezza generali

Questi controlli applicano regole globali riguardanti determinati protocolli, tipi di pacchetto e altre forme di traffico (come il traffico di tipo server) sia verso la zona attendibile sia verso la zona Internet.

### Modificare le impostazioni di sicurezza generali

1. Selezionare **Firewall | Principale**.
2. Fare clic su **Avanzate**.
3. Nella sezione Impostazioni generali, scegliere le impostazioni di sicurezza.

Blocca tutti i frammenti	<p>Blocca tutti i pacchetti di dati IP incompleti (frammentati). Gli hacker a volte creano pacchetti frammentati per superare oppure ostacolare i dispositivi di rete che leggono le intestazioni dei pacchetti.</p> <p><b>Attenzione:</b> se si seleziona questa opzione, il software di sicurezza Zone Labs bloccherà tutti i pacchetti frammentati senza avvertire l'utente o creare una voce di log. Non selezionare questa opzione a meno che si conosca la modalità di gestione dei pacchetti frammentati utilizzata dalla connessione online.</p>
Blocca server attendibili	<p>Impedisce a tutti i programmi sul computer di agire come server rispetto alla zona attendibile. Notare che questa impostazione ignora le autorizzazioni concesse nel pannello Programmi.</p>
Blocca server Internet	<p>Impedisce a tutti i programmi sul computer di agire come server rispetto alla zona Internet. Notare che questa impostazione ignora le autorizzazioni concesse nel pannello Programmi.</p>
Abilita protezione ARP	<p>Blocca tutte le richieste ARP (Address Resolution Protocol) in ingresso eccetto le richieste di broadcast per l'indirizzo del computer di destinazione. Blocca anche tutte le risposte ARP in ingresso eccetto quelle in risposta a richieste ARP in uscita.</p>



Consenti protocolli VPN	Consente l'utilizzo di protocolli VPN (ESP, AH, GRE, SKIP) anche quando è applicata l'impostazione di sicurezza Alta. Con questa opzione disattivata, tali protocolli sono consentiti solo con sicurezza Media.
Consenti protocolli non comuni con sicurezza elevata	Consente l'utilizzo di protocolli diversi da ESP, AH, GRE e SKIP quando l'impostazione di sicurezza è Alta.
Blocca file hosts	Impedisce che gli hacker apportino modifiche al file hosts del computer tramite virus di tipo Trojan. Siccome alcuni programmi legittimi devono poter modificare il file hosts per funzionare, questa opzione è deselezionata per impostazione predefinita.
Disabilita Windows Firewall	Rileva e disabilita Windows Firewall. Questa opzione apparirà soltanto se si utilizza Windows XP con Service Pack 2.
Filtro IP su traffico 1394	Filtra il traffico FireWire.

4. Fare clic su **OK**.

## Impostazione delle opzioni di sicurezza della rete

Il rilevamento automatico della rete facilita la configurazione della zona attendibile, in modo che le tradizionali attività della rete locale, come la condivisione di file e stampanti, non siano interrotte. Il software di sicurezza Zone Labs rileva solo le reti a cui si è fisicamente connessi. Le connessioni di rete instradate o virtuali non sono rilevate.

È possibile fare in modo che il software di sicurezza Zone Labs includa automaticamente nella zona attendibile ogni rete rilevata oppure che chieda ogni volta se aggiungere la rete appena rilevata.

### Specificare le impostazioni di rete

1. Selezionare **Firewall | Principale**.
2. Fare clic su **Avanzate**.
3. Nella sezione Impostazioni rete, scegliere le impostazioni di sicurezza.

Includi reti nella zona attendibile dopo il rilevamento	Sposta automaticamente le nuove reti nella zona attendibile. Questa impostazione offre la sicurezza minore.
Escludi reti dalla zona attendibile dopo il rilevamento	Blocca automaticamente l'aggiunta di nuove reti alla zona attendibile e le colloca nella zona Internet. Questa impostazione offre la sicurezza maggiore.
Chiedi in quale zona aggiungere nuove reti durante il rilevamento	Il software di sicurezza Zone Labs visualizza un avviso di nuova rete o la configurazione guidata Rete, che permette di specificare la zona.

Aggiungi automaticamente nuove reti wireless non protette (WEP o WPA) nella zona Internet	Pone automaticamente le reti wireless non sicure nella zona Internet, impedendo l'accesso non autorizzato ai dati da parte di terzi che accedono alla rete.
---	---

4. Fare clic su **OK**.

Per ulteriori informazioni sulle connessioni di rete, vedere il Capitolo 3, "Connessioni di rete con il software di sicurezza Zone Labs", a pagina 31.

## Impostazione delle opzioni di sicurezza della rete wireless

Il rilevamento automatico delle reti wireless aiuta a configurare la zona Internet per assicurare che il computer rimanga protetto senza essere interrotti ogni volta che viene rilevata una nuova rete wireless. Il software di sicurezza Zone Labs rileva soltanto le reti wireless alle quali è connesso il computer (le reti alle quali non si è effettivamente connessi potrebbero apparire come disponibili in Risorse di rete, ma la configurazione guidata Rete wireless appare soltanto quando si stabilisce una connessione a tale rete).

È possibile far sì che il software di sicurezza Zone Labs includa automaticamente ogni rete wireless rilevata nella zona Internet.

### Specificare le impostazioni di rete

1. Selezionare **Firewall | Principale**.
2. Fare clic su **Avanzate**.
3. Nella sezione Impostazioni rete wireless, scegliere le impostazioni di sicurezza.

Aggiungi automaticamente nuove reti wireless non protette (WEP o WPA) nella zona Internet	Il software di sicurezza Zone Labs pone le nuove reti wireless nella zona Internet quando vengono rilevate.
---	---

4. Fare clic su **OK**.

Per ulteriori informazioni sulle connessioni di rete, vedere il Capitolo 3, "Connessioni di rete con il software di sicurezza Zone Labs", a pagina 31.

# Gestione delle origini di traffico

La scheda *Zone* contiene le origini di traffico (computer, reti o siti) che sono state aggiunte alla zona attendibile o alla zona bloccata. Contiene inoltre qualsiasi rete rilevata dal software di sicurezza *Zone Labs*. Se si utilizza un singolo PC non collegato in rete, l'elenco delle origini di traffico visualizzerà soltanto la rete dell'ISP (provider di servizi Internet), che dovrebbe essere nella zona Internet.

## Visualizzazione dell'elenco delle origini di traffico

L'elenco delle origini di traffico visualizza le origini di traffico e la zona a cui appartengono. È possibile ordinare l'elenco per qualsiasi campo, facendo clic sull'intestazione di colonna. La freccia (^) accanto al nome dell'intestazione indica l'ordine di disposizione. Fare di nuovo clic sulla stessa intestazione per invertire l'ordine.

Campo	Descrizione
Nome	Il nome che è stato assegnato a questo computer, sito o rete
Indirizzo IP / Sito	L'indirizzo IP o il nome host dell'origine di traffico
Tipo voce	Il tipo di origine di traffico: Rete, Host, IP, Sito o Subnet
Zona	La zona a cui è assegnata l'origine di traffico: Internet, attendibile o bloccata

Tabella 4-1: Campi dell'elenco delle origini di traffico

## Modifica delle origini di traffico

Utilizzando l'elenco delle origini di traffico, è possibile spostare un'origine di traffico da una zona all'altra, nonché aggiungere, modificare o rimuovere un'origine di traffico.

### Modificare la zona di un'origine di traffico

1. Selezionare **Firewall | Zona**.
2. Individuare l'origine di traffico, quindi fare clic nella colonna **Zona**.
3. Selezionare una zona dal menu di scelta rapida, quindi fare clic su **Applica**.

### Aggiungere, rimuovere o modificare un'origine di traffico

1. Selezionare **Firewall | Zona**.
2. Nella colonna **Nome**, fare clic sull'origine di traffico, quindi fare clic su **Aggiungi**, **Modifica** o **Rimuovi**.
3. Fare clic su **Applica**.

## Aggiunta alla zona attendibile

La zona attendibile contiene i computer considerati attendibili con cui si desidera condividere delle risorse. Per esempio, se si possiedono tre PC domestici collegati insieme in una rete Ethernet, è possibile aggiungere ciascuno di essi o l'intera subnet della scheda di rete alla zona attendibile. L'impostazione predefinita di sicurezza Media della zona attendibile consente di condividere in tutta sicurezza file, stampanti e altre risorse sulla rete domestica. Gli hacker sono relegati nella zona Internet, dove l'impostazione di sicurezza Alta garantisce la protezione.

### Aggiungere un singolo indirizzo IP

1. Selezionare **Firewall | Zone**.
2. Fare clic su **Aggiungi**, quindi selezionare **Indirizzo IP** dal menu di scelta rapida.  
Viene visualizzata la finestra di dialogo Aggiungi indirizzo IP.
3. Selezionare **Attendibile** dall'elenco a discesa Zona.
4. Digitare l'indirizzo IP e una descrizione nelle relative caselle, quindi fare clic su **OK**.

### Aggiungere un intervallo di indirizzi IP

1. Selezionare **Firewall | Zone**.
2. Fare clic su **Aggiungi**, quindi selezionare **Indirizzo IP** dal menu di scelta rapida.  
Viene visualizzata la finestra di dialogo Aggiungi intervallo IP.
3. Selezionare **Attendibile** dall'elenco a discesa Zona.
4. Digitare l'indirizzo IP iniziale nel primo campo e l'indirizzo IP finale nel secondo campo.
5. Digitare una descrizione nel relativo campo, quindi fare clic su **OK**.

### Aggiungere una subnet

1. Selezionare **Firewall | Zone**.
2. Fare clic su **Aggiungi**, quindi selezionare **Subnet** dal menu di scelta rapida.  
Viene visualizzata la finestra di dialogo Aggiungi subnet.
3. Selezionare **Attendibile** dall'elenco a discesa Zona.
4. Digitare l'indirizzo IP nel primo campo e la subnet mask nel secondo campo.
5. Digitare una descrizione nel relativo campo, quindi fare clic su **OK**.

### Aggiungere un host o un sito alla zona attendibile

1. Selezionare **Firewall | Zone**.
2. Fare clic su **Aggiungi**, quindi selezionare **Host/sito**.  
Viene visualizzata la finestra di dialogo Aggiungi host/sito.

3. Selezionare **Attendibile** dall'elenco a discesa Zona.
4. Digitare il nome host completo nel campo **Nome host**.
5. Digitare una descrizione per l'host o il sito, quindi fare clic su **OK**.

#### Aggiungere una rete alla zona attendibile

1. Selezionare **Firewall | Zone**.
2. Nella colonna Zona, fare clic sulla riga contenente la rete, quindi selezionare **Attendibile** dal menu di scelta rapida.
3. Fare clic su **Applica**.



Il software di sicurezza Zone Labs rileva automaticamente le nuove connessioni di rete e aiuta ad aggiungerle alla zona appropriata. Per ulteriori informazioni, vedere il Capitolo 3, "Connessioni di rete con il software di sicurezza Zone Labs", a pagina 31.

## Aggiunta alla zona bloccata

Per effettuare aggiunte alla zona bloccata, seguire le istruzioni per l'aggiunta alla zona attendibile, ma selezionare **Bloccata** dall'elenco a discesa nel passaggio 2.

## Visualizzazione degli eventi relativi al firewall

Per impostazione predefinita, tutti gli eventi relativi a OSFirewall sono presenti nel Visualizzatore log.

### Visualizzare gli eventi del firewall presenti nel log

1. Selezionare **Avvisi e log | Visualizzatore log**.
2. Selezionare **Firewall** dall'elenco a discesa Tipo di avviso.

La tabella 4-2 fornisce una spiegazione dei campi del Visualizzatore log per gli eventi relativi al firewall.

Campo	Informazioni
Livello	Ogni avviso è di livello alto o medio. Gli avvisi di alto livello sono quelli che probabilmente sono causati da attività di hacker. Gli avvisi di medio livello probabilmente sono causati da traffico di rete indesiderato ma inoffensivo.
Data/Ora	La data e l'ora in cui si è verificato l'avviso.

**Tabella 4-2: Campi del log per gli eventi relativi al firewall**

<b>Campo</b>	<b>Informazioni</b>
Tipo	Il tipo di avviso: Firewall, Programma, Blocco ID o Blocco attivato.
Protocollo	Il protocollo di comunicazione utilizzato dal traffico che ha causato l'avviso.
Programma	Il nome del programma che sta tentando di inviare o ricevere dati (si applica solo ad avvisi Programma e Blocco ID).
IP di origine	L'indirizzo IP del computer che ha inviato il traffico bloccato dal software di sicurezza Zone Labs.
IP di destinazione	L'indirizzo del computer a cui era destinato il traffico bloccato.
Direzione	La direzione del traffico bloccato. "In ingresso" significa che il traffico è stato inviato al proprio computer. "In uscita" significa che il traffico è stato inviato dal proprio computer.
Azione eseguita	Il modo in cui il traffico è stato gestito dal software di sicurezza Zone Labs.
Conteggio	Il numero di volte per cui un avviso dello stesso tipo, con la stessa origine, destinazione e protocollo si è verificato durante una singola sessione.
DNS di origine	Il nome di dominio del mittente del traffico che ha causato l'avviso.
DNS di destinazione	Il nome di dominio del destinatario a cui era diretto il traffico che ha causato l'avviso.

**Tabella 4-2: Campi del log per gli eventi relativi al firewall**

# Blocco e sblocco delle porte

I livelli di sicurezza predefiniti del software di sicurezza Zone Labs determinano quali porte e protocolli sono consentiti e quali sono bloccati. Gli utenti avanzati possono modificare la definizione dei livelli di sicurezza modificando le autorizzazioni di porta e aggiungendo porte personalizzate.

## Impostazioni delle autorizzazioni di porta predefinite

La configurazione predefinita per la sicurezza Alta blocca tutto il traffico in entrata e in uscita che passa attraverso le porte non utilizzate dai programmi a cui non si è concessa l'autorizzazione di accesso o server, eccetto:

- broadcast/multicast DHCP
- DHCP in uscita (porta 67) - su sistemi Windows 9x
- DNS in uscita (porta 53) - se il computer è configurato come gateway ICS

Tipo di traffico	Livelli di sicurezza		
	ALTA	MEDIA	BASSA
DNS in uscita	blocca	n/d	consenti
DHCP in uscita	blocca	n/d	consenti
broadcast/multicast	consenti	consenti	consenti
<b>ICMP</b>			
in arrivo (ping echo)	blocca	consenti	consenti
in arrivo (altro)	blocca	consenti	consenti
in uscita (ping echo)	blocca	consenti	consenti
in uscita (altro)	blocca	consenti	consenti
<b>IGMP</b>			
in arrivo	blocca	consenti	consenti
in uscita	blocca	consenti	consenti
<b>NetBIOS</b>			
in arrivo	n/d	blocca	consenti
in uscita	n/d	consenti	consenti
<b>UDP (porte non in uso da un programma autorizzato)</b>			
in arrivo	blocca	consenti	consenti
in uscita	blocca	consenti	consenti
<b>TCP (porte non in uso da un programma autorizzato)</b>			

Tabella 4-3: Autorizzazioni di accesso predefinite per tipi diversi di traffico in entrata e in uscita

Tipo di traffico	Livelli di sicurezza		
	ALTA	MEDIA	BASSA
in arrivo	blocca	consenti	consenti
in uscita	blocca	consenti	consenti

**Tabella 4-3: Autorizzazioni di accesso predefinite per tipi diversi di traffico in entrata e in uscita**

### Modificare l'autorizzazione di accesso di una porta

1. Selezionare **Firewall | Principale**.
2. Nella sezione Sicurezza zona Internet o Sicurezza zona attendibile, fare clic su **Personalizza**.  
Viene visualizzata la finestra di dialogo Impostazioni firewall personalizzate.
3. Scorrere per individuare le impostazioni di sicurezza alta e media.
4. Per bloccare o consentire una porta o un protocollo specifico, selezionare la casella di controllo accanto.



Ricordarsi che, quando si seleziona un tipo di traffico nell'elenco delle impostazioni di sicurezza alta, si sta scegliendo di **CONSENTIRE** a quel tipo di traffico di introdursi nel computer quando l'impostazione è Alta, diminuendo la protezione Alta. Al contrario, quando si seleziona un tipo di traffico nell'elenco delle impostazioni di sicurezza media, si sta scegliendo di **BLOCCARE** quel tipo di traffico quando l'impostazione è Media, aumentando quindi la protezione Media.

5. Fare clic su **Applica**, quindi fare clic su **OK**.

### Aggiunta di porte personalizzate

È possibile consentire la comunicazione tramite porte aggiuntive con l'impostazione di sicurezza Alta, oppure bloccare porte aggiuntive con l'impostazione di sicurezza Media specificando singoli numeri di porta o intervalli di porta.

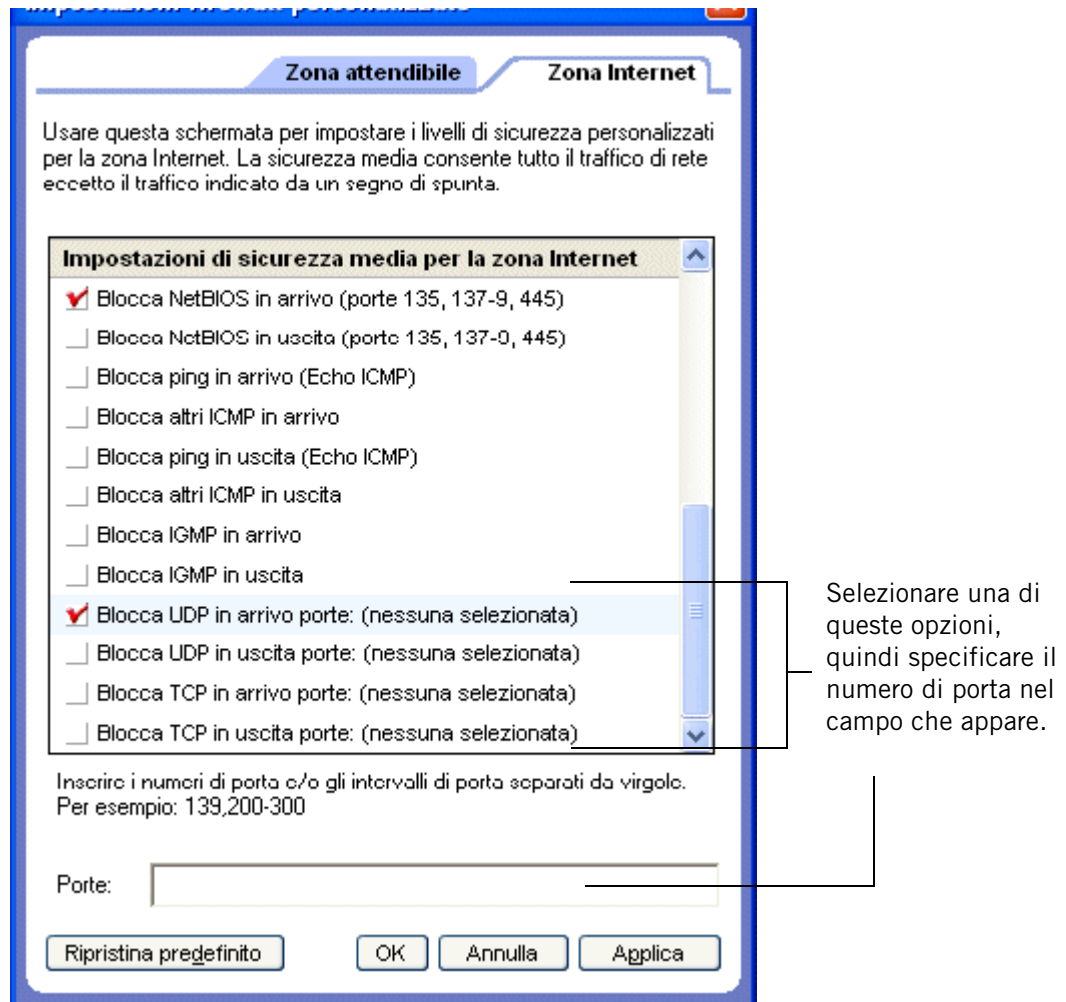
#### Specificare porte aggiuntive

1. Selezionare **Firewall | Principale**.



2. Nella sezione Sicurezza zona attendibile o Sicurezza zona Internet, fare clic su **Personalizza**.

Viene visualizzata la finestra di dialogo Impostazioni firewall personalizzate.



3. Scorrere fino al livello di sicurezza (Alta o Media) a cui aggiungere porte.
4. Selezionare il tipo di porta desiderato: UDP in arrivo, UDP in uscita, TCP in arrivo o TCP in uscita.
5. Digitare la porta o gli intervalli di porta da autorizzare o bloccare nel campo Porte, separandoli con delle virgole. Per esempio, è possibile digitare 139, 200-300.
6. Fare clic su **Applica**, quindi fare clic su **OK**.

# Comprensione delle regole firewall della scheda Esperto

Le regole firewall della scheda Esperto sono destinate a utenti che hanno esperienza con i firewall e i protocolli di rete.

Le regole della scheda Esperto non sostituiscono altre regole. Sono parte integrante dell'approccio di sicurezza a più livelli e funzionano in aggiunta alle altre regole del firewall.

Le regole della scheda Esperto sfruttano quattro attributi per filtrare i pacchetti:

- Indirizzo IP di origine e/o destinazione
- Numero di porta di origine e/o destinazione
- Protocollo di rete/tipo di messaggio
- Giorno e ora

Gli indirizzi di origine e destinazione possono essere specificati in una serie di formati, fra cui un singolo indirizzo IP di rete, un intervallo di indirizzi IP, la descrizione di una subnet, un indirizzo gateway o un nome di dominio.

Le porte di origine e destinazione servono soltanto per protocolli di rete che utilizzano le porte, come UDP e TCP/IP. I messaggi ICMP e IGMP, per esempio, non utilizzano le informazioni di porta.

I protocolli di rete possono essere selezionati da un elenco di protocolli IP o VPN comuni o specificati con un numero di protocollo IP. Per ICMP, si può anche specificare il tipo di messaggio.

Gli intervalli di giorno e di ora possono essere applicati a una regola per limitare l'accesso in base al giorno della settimana e all'ora del giorno.

## Come sono applicate le regole del firewall della scheda Esperto

È importante comprendere come sono applicate le regole della scheda Esperto in combinazione con le regole della zona, le autorizzazioni per i programmi e altre regole della scheda Esperto.

### *Regole della scheda Esperto e regole della zona*

Le regole della scheda Esperto sono applicate al firewall prima delle regole della zona. Questo significa che se un pacchetto corrisponde a una regola della scheda Esperto, quest'ultima viene applicata e il software di sicurezza Zone Labs evita di valutare le regole della zona.

Esempio: si supponga di avere impostato la sicurezza della zona attendibile a Media. Ciò consente il traffico NetBIOS in uscita. Tuttavia, è stata anche creata una regola nella scheda Esperto che blocca tutto il traffico NetBIOS tra le ore 17:00 e le ore 7:00.

Qualsiasi traffico NetBIOS in uscita durante quelle ore sarà bloccato, nonostante l'impostazione della zona attendibile.

### ***Regole della scheda Esperto e autorizzazioni dei programmi***

Le regole della scheda Esperto e le regole della zona vengono applicate insieme alle autorizzazioni per i programmi. Ciò significa che se le autorizzazioni per i programmi o le regole del firewall (della scheda Esperto e della zona) determinano che il traffico deve essere bloccato, questo verrà bloccato. Notare che questo significa che è possibile utilizzare le regole del firewall per ridefinire le autorizzazioni per i programmi.









I pacchetti provenienti dalla zona bloccata non saranno bloccati se sono consentiti da una regola Esperto del firewall.

## **Ordine di applicazione delle regole della scheda Esperto**

Nell'ambito delle regole del firewall, l'ordine di valutazione è un fattore importante. Il software di sicurezza Zone Labs controlla inizialmente le regole della scheda Esperto. Se si ha una corrispondenza e una regola viene applicata, la comunicazione è contrassegnata come bloccata o consentita e il software di sicurezza Zone Labs evita di valutare le regole della zona. Se non si ha corrispondenza con le regole della scheda Esperto, il software di sicurezza Zone Labs controlla le regole della zona per verificare se la comunicazione deve essere bloccata.

Anche l'ordine di applicazione delle regole della scheda Esperto è importante. Ogni regola ha un numero di classificazione univoco e le regole sono valutate in ordine in base al parametro Classifica. Solo la prima regola che corrisponde viene eseguita. Considerare queste due regole:

			Nome	Origine	Destinazione	Protocollo	Ora	Commenti
1			FTP Consenti	Risorse del computer	Zona Internet	FTP	Qualunque	
2			FTP Nega	Risorse del computer	Qualunque	FTP	Qualunque	

**Figura 4-1: Ordine di classificazione delle regole della scheda Esperto**

La regola 1 consente ai client FTP nella zona attendibile di connettersi a un server FTP sulla porta 21. La regola 2 blocca tutti i client FTP dalla connessione sulla porta 21, indipendentemente dalla zona. Queste due regole insieme consentono ai client nella zona attendibile di utilizzare un server FTP sul computer client, ma bloccano tutti gli altri accessi FTP.

Se l'ordine delle regole fosse invertito, la regola 2 verrebbe applicata per prima e tutti gli accessi FTP sarebbero bloccati. La regola 1 non avrebbe possibilità di essere eseguita, quindi i client FTP nella zona attendibile sarebbero comunque bloccati.

# Creazione di regole firewall nella scheda Esperto

La creazione di regole firewall nella scheda Esperto prevede la specifica dell'origine o della destinazione del traffico di rete a cui è applicata la regola, l'impostazione delle opzioni di traccia e la specifica dell'azione della regola, cioè se bloccare o consentire il traffico che corrisponde alle specifiche della regola. È possibile creare nuove regole da zero oppure copiare una regola esistente e modificarne le proprietà.

## Creare una nuova regola nella scheda Esperto

1. Selezionare **Firewall | Esperto**, quindi fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo **Aggiungi regola**.

2. Nella sezione **Impostazioni generali**, specificare le impostazioni della regola.

Classifica	L'ordine in cui le regole saranno applicate. Una regola con valore 1 è applicata per prima.
Nome	Fornire un nome descrittivo per la regola.
Stato	Specificare se la regola è attivata o disattivata.
Azione	Indica se bloccare o consentire il traffico che corrisponde a questa regola.
Traccia	Indica se registrare, avvisare e registrare o non eseguire azioni quando la regola è applicata.
Commenti	Campo facoltativo per immettere note sulla regola.

3. Nella sezione **Origine**, selezionare una posizione dall'elenco o fare clic su **Modifica**, quindi selezionare **Aggiungi posizione** dal menu di scelta rapida. È possibile aggiungere qualsiasi numero di origini a una regola.

Risorse del computer	Applica la regola al traffico originato dal computer.
Zona attendibile	Applica la regola al traffico di rete proveniente dalle origini nella zona attendibile.
Zona Internet	Applica la regola al traffico di rete proveniente dalle origini nella zona Internet.
Tutti	Applica la regola al traffico di rete proveniente da qualsiasi origine.
Host/sito	Applica la regola al traffico di rete proveniente da un nome di dominio specificato.
Indirizzo IP	Applica la regola al traffico di rete proveniente da un indirizzo IP specificato.
Intervallo IP	Applica la regola al traffico di rete proveniente da un computer nell'intervallo IP specificato.

Subnet	Applica la regola al traffico di rete proveniente da un computer della subnet specificata.
Gateway	Applica la regola al traffico di rete proveniente da un computer sul gateway specificato.
Nuovo gruppo	Selezionare questa opzione, quindi fare clic su <b>Aggiungi</b> per creare un nuovo gruppo di posizioni da applicare alla regola.
Gruppo esistente	Scegliere questa opzione per selezionare uno o più gruppi di posizioni da applicare alla regola, quindi fare clic su <b>OK</b> .

4. Nella sezione Destinazione, selezionare una posizione dall'elenco o fare clic su **Modifica**, quindi selezionare **Aggiungi posizione** dal menu di scelta rapida.

I tipi di posizione disponibili per le posizioni Origine e Destinazione sono gli stessi.

5. Nella sezione Protocollo, selezionare un protocollo dall'elenco o fare clic su **Modifica**, quindi selezionare **Aggiungi protocollo**.

Aggiungi protocollo	Selezionare questa opzione per aggiungere un protocollo alla regola. Specificare: TCP, UDP, TCP e UDP, ICMP, IGMP o Personalizzato.
Nuovo gruppo	Selezionare questa opzione, quindi fare clic su <b>Aggiungi</b> per creare un nuovo gruppo di protocolli da applicare alla regola.
Gruppo esistente	Scegliere questa opzione per selezionare uno o più gruppi di protocolli da applicare alla regola, quindi fare clic su <b>OK</b> .

6. Nella sezione Ora, selezionare un'ora dall'elenco o fare clic su **Modifica**, quindi selezionare **Aggiungi ora**.

Intervallo giorni/ore	Selezionare questa opzione per aggiungere un intervallo di giorni/ore alla regola. Specificare una descrizione, un intervallo di ore e uno o più giorni. L'intervallo di ore è specificato utilizzando il formato di 24 ore.
Nuovo gruppo	Selezionare questa opzione, quindi fare clic su <b>Aggiungi</b> per creare un nuovo gruppo di giorni/ore da applicare alla regola.
Gruppo esistente	Scegliere questa opzione per selezionare uno o più gruppi di giorni/ore da applicare alla regola, quindi fare clic su <b>OK</b> .

7. Fare clic su **OK**.

### Creare una nuova regola da una regola esistente

1. Selezionare **Firewall | Esperto**.
2. Selezionare la regola della scheda Esperto da duplicare, quindi premere **Ctrl+C** o fare clic con il pulsante destro del mouse sulla regola e selezionare **Copia**.

3. Incollare la regola copiata premendo **Ctrl+V** o facendo clic con il pulsante destro del mouse e selezionando **Incolla**.



Se una regola è correntemente selezionata nell'elenco, la regola incollata sarà inserita sopra essa. Se non ci sono regole selezionate, la regola incollata sarà inserita in cima all'elenco delle regole.

Al nome della regola copiata viene aggiunto un "1". Se si incolla una regola una seconda volta, verrà aggiunto il numero 2 alla seconda regola copiata.

4. Fare clic su **Applica** per salvare le modifiche.
5. Fare clic con il pulsante destro del mouse sulla nuova regola e selezionare **Modifica** per modificare le proprietà della regola come opportuno.

# Creazione di gruppi

Utilizzare i gruppi per semplificare la gestione di posizioni, protocolli e giorni/ore impiegati nelle regole contenute nella scheda Esperto.

## Creazione di un gruppo di posizioni

Utilizzare i gruppi di posizioni per combinare indirizzi e intervalli IP non contigui o tipi diversi di posizioni (per esempio, subnet e host) in un set facilmente gestibile. È possibile aggiungere facilmente tale set di posizioni a qualsiasi regola della scheda Esperto.

### Creare un gruppo di posizioni

1. Selezionare **Firewall | Esperto**, quindi fare clic su **Gruppi**.

Viene visualizzata la finestra di dialogo Gestore gruppi.

2. Fare clic sulla scheda **Posizioni**, quindi fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo Aggiungi gruppo di posizioni.

3. Specificare il nome e la descrizione del gruppo di posizioni, quindi fare clic su **Aggiungi** e selezionare un tipo di posizione dal menu.

Host/sito	Aggiungere una descrizione e un nome host per la posizione Host/sito, quindi fare clic su <b>OK</b> . Non includere http:// nel nome host. Fare clic su <b>Ricerca</b> per visualizzare in anteprima l'indirizzo IP del sito.
Indirizzo IP	Aggiungere una descrizione e un indirizzo IP per la posizione Indirizzo IP, quindi fare clic su <b>OK</b> .
Intervallo IP	Aggiungere una descrizione, un indirizzo IP iniziale e uno finale per la posizione Intervallo IP, quindi fare clic su <b>OK</b> .
Subnet	Specificare una descrizione, un indirizzo IP e una subnet mask per la posizione Subnet, quindi fare clic su <b>OK</b> .
Gateway	Specificare un indirizzo IP, un indirizzo MAC e una descrizione per la posizione Gateway, quindi fare clic su <b>OK</b> .

4. Fare clic su **OK** per chiudere la finestra di dialogo Gestore gruppi.



Una volta creati, i nomi dei gruppi non possono essere modificati. Per esempio, se si crea un gruppo di posizioni denominato "Casa" e successivamente si decide di chiamarlo "Lavoro", sarà necessario rimuovere il gruppo chiamato "Casa" e crearne uno nuovo con il nome "Lavoro".

## Creazione di un gruppo di protocolli

Si crea un gruppo di protocolli per combinare porte TCP/UDP note, protocolli e tipi di messaggio specifici del protocollo (per esempio, tipi di messaggio ICMP) in set

facilmente aggiungibili alle regole della scheda Esperto. Per esempio, si potrebbe creare un gruppo che includa i protocolli POP3 e IMAP4 allo scopo di semplificare l'amministrazione delle regole riguardanti il traffico di posta elettronica.

### Creare un gruppo di protocolli

1. Selezionare **Firewall | Esperto**, quindi fare clic su **Gruppi**.

Viene visualizzata la finestra di dialogo Gestore gruppi.

2. Fare clic sulla scheda **Protocolli**, quindi fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo Aggiungi gruppo di protocolli.

3. Specificare il nome e la descrizione per il gruppo di protocolli, quindi fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo Aggiungi protocollo.

4. Selezionare un tipo di protocollo dall'elenco a discesa Protocollo.

- TCP
- UDP
- TCP e UDP
- ICMP
- IGMP
- Personalizzato

5. Se si sceglie TCP, UDP o TCP e UDP nel passaggio 4, specificare una destinazione, un'origine e un numero di porta.

Nome	Numero di porta
FTP	21
Telnet	23
POP3	110
NNTP	119
Nome NetBIOS	137
Datagramma NetBIOS	138
Sessione NetBIOS	139
IMAP4	143
HTTPS	443
RTSP	554
Windows Media	1755



AOL	5190
Real Networks	7070
Altro	Specificare il numero della porta
Dati FTP	20
TFTP	69
HTTP	80
DHCP	67
Client DHCP	68
SMTP	25
DNS	53

6. Se si seleziona ICMP nel passaggio 4, specificare una descrizione, un nome di messaggio e un numero tipo.

Nome messaggio	Numero tipo
Source Quench	4
Redirect	5
Alt	6
Echo Request	8
Router Advertisement	9
Router Solicitation	10
Time Exceeded	11
Parameter Problem	12
Timestamp	13
Timestamp reply	14
Information request	15
Information reply	16
Address Mask Request	17
Address Mask Reply	18
Traceroute	30
Altro	Specificare il numero corrispondente al tipo

7. Se si seleziona IGMP nel passaggio 4, specificare una descrizione, un nome di messaggio e il numero corrispondente al tipo.

Membership Query	17
Membership Report (ver 1)	18
Cisco Trace	21
Membership Report (ver 2)	22
Leave Group (ver 2)	23
Multicast Traceroute Response	30
Multicast Traceroute	31
Membership Report (ver 3)	34
Altro	Specificare il numero corrispondente al tipo.

8. Se si seleziona Personalizzato nel passaggio 4, specificare una descrizione, un tipo di protocollo e un numero di protocollo.

RDP	27
GRE	47
ESP	50
AH	51
SKIP	57
Altro	Specificare il numero del protocollo.

9. Fare clic su **OK** per chiudere la finestra di dialogo Aggiungi protocollo.

## Creazione di un gruppo di giorni/ore

Per consentire o bloccare il traffico di rete da o verso il proprio computer durante intervalli di tempo specificati, è possibile creare un gruppo di giorni/ore e aggiungerlo a una regola della scheda Esperto. Per esempio, per bloccare il traffico proveniente dai server che visualizzano finestre pop-up pubblicitarie durante le ore di lavoro, si può creare un gruppo che blocchi il traffico HTTP proveniente da un dominio specificato durante le ore dalle 9 del mattino alle 17, da lunedì a venerdì.

### Creare un gruppo di giorni/ore

1. Selezionare **Firewall | Esperto**, quindi fare clic su **Gruppi**.

Viene visualizzata la finestra di dialogo Gestore gruppi.

2. Fare clic sulla scheda **Ore**, quindi fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo Aggiungi gruppo di orari.

3. Specificare il nome e la descrizione per il gruppo di orari, quindi fare clic su **Aggiungi**.  
Viene visualizzata la finestra di dialogo *Aggiungi ora*.
4. Specificare una descrizione dell'ora, quindi selezionare un intervallo di orari e di giorni.
5. Fare clic su **OK**, quindi di nuovo su **OK** per chiudere la finestra di dialogo *Gestore gruppo*.

# Gestione delle regole del firewall della scheda Esperto

Dalla scheda Esperto del pannello Firewall, è possibile visualizzare lo stato delle regole esistenti, attivare o disattivare regole, modificarle o rimuoverle, aggiungerne di nuove, modificarne l'ordine e creare dei gruppi.

## Visualizzazione dell'elenco delle regole della scheda Esperto

La scheda Esperto presenta un elenco di tutte le regole create dall'utente per il firewall. Le regole sono elencate in ordine di priorità di applicazione (classifica). I pulsanti con le frecce sul lato destro spostano le regole selezionate verso l'alto e verso il basso nell'elenco, modificandone l'ordine di applicazione.

Si può anche modificare l'ordine di classificazione delle regole trascinandole e rilasciandole da una posizione a un'altra.

Per esempio, trascinare e rilasciare la regola 2 nella parte superiore dell'elenco per portare il valore di quella regola a 1.

Classifica    Traccia

Utilizzare i controlli per modificare l'ordine di applicazione delle regole

			Nome	Origine	Destinazione	Protocollo	Ora	Commenti
Disattivato	✓	⚠	FTP Consenti	Risorse del computer	Zona Internet	FTP	Qualunque	
2	✓	⚠	HTTP Nega	Risorse del computer	popup ads	HTTP	Qualunque	
3	✓	⚠	FTP Nega	Risorse del computer	Qualunque	FTP	Qualunque	

Dettagli voce

Classifica	Disattivato
Nome	FTP Allow
Origine	Risorse del computer
Destinazione	Zona Internet
Protocollo	FTP
Azione	Consenti

Fare clic per aggiungere gruppi di posizioni, protocolli oppure orari.

Figura 4-2: Elenco delle regole della scheda Esperto

### Classifica


La priorità di applicazione della regola. Le regole sono valutate in ordine di classifica, iniziando dal numero 1, e la prima regola che corrisponde sarà applicata. Le regole disattivate visualizzeranno "Disattivato" al posto del numero di classifica, ma conserveranno l'ordine di classifica nell'elenco.


**Azione**

Un simbolo **X** rosso significa che la regola bloccherà il traffico di rete; un segno di spunta verde **✓** significa che la regola consentirà il traffico di rete.

**Traccia**

L'assenza di icone indica che non vi saranno notifiche quando la regola sarà applicata.

L'icona del log () indica che sarà creata una voce di log quando la regola verrà applicata.

L'icona di avvisi e log () indica che sarà visualizzato un avviso e sarà creata una voce di log quando la regola verrà applicata.

**Nome**

Un nome descrittivo per la regola.

**Origine**

Gli indirizzi di origine e le porte per la regola.

**Destinazione**

Gli indirizzi di destinazione e le porte per la regola.

**Protocollo**

Il protocollo di rete a cui si applica la regola.

**Ora**

Il periodo di tempo durante il quale la regola è attiva.

## Modifica e riclassificazione delle regole

È possibile modificare o riordinare le regole esistenti nell'elenco selezionandole e trascinandole nella posizione desiderata. Notare che se una regola della scheda Esperto è stata copiata nelle regole per un programma, la sua modifica non avrà automaticamente effetto sulla regola per il programma. Per ulteriori informazioni, vedere "Creazione di regole della scheda Esperto per i programmi", a pagina 91.

**Modificare una regola**

1. Selezionare **Firewall | Esperto**.
2. Selezionare la regola che si desidera modificare, quindi fare clic su **Modifica**.

Viene visualizzata la finestra di dialogo Modifica regola.

3. Modificare gli attributi della regola come opportuno, quindi fare clic su **OK**.

**Modificare la classifica di una regola**

1. Selezionare **Firewall | Esperto**.

2. Fare clic con il pulsante destro del mouse sulla regola da spostare, quindi selezionare **Sposta regola**.

Sposta in alto	Sposta la regola selezionata in cima all'elenco di regole.
Sposta in basso	Sposta la regola selezionata in fondo all'elenco di regole.
Sposta su	Sposta la regola selezionata in su di una riga nell'elenco di regole.
Sposta giù	Sposta la regola selezionata in giù di una riga nell'elenco di regole.

# Capitolo

## Controllo dei programmi

# 5

Il Controllo dei programmi protegge l'utente garantendo l'accesso a Internet o l'esecuzione di determinate azioni sul computer solo da parte di programmi attendibili. È possibile assegnare le autorizzazioni ai programmi manualmente o consentire al software di sicurezza Zone Labs di concederle quando sono disponibili suggerimenti sui programmi. Gli utenti avanzati possono anche controllare le porte che ogni programma può utilizzare.

ZoneAlarm Security Suite comprende la protezione supplementare di Triple Defense Firewall, che impedisce anche ai programmi attendibili di assumere comportamenti potenzialmente pericolosi.

### Argomenti:

- "Comprendere il Controllo dei programmi", a pagina 70
- "Impostazione di opzioni generiche per Controllo dei programmi", a pagina 73
- "Configurazione di impostazioni avanzate per i programmi", a pagina 79
- "Impostazione di autorizzazioni per programmi specifici", a pagina 81
- "Gestione dei componenti dei programmi", a pagina 90
- "Creazione di regole della scheda Esperto per i programmi", a pagina 91

# Comprendere il Controllo dei programmi

Tutte le operazioni svolte su Internet – dall'apertura di pagine Web al download di file MP3 – sono gestite da programmi specifici sul computer.

Gli hacker sfruttano questo fatto inserendo "malware" – ovvero, software dannoso – sul computer. Il malware può camuffarsi da innocuo allegato di posta elettronica o da aggiornamento di un programma legittimo. Tuttavia, una volta sul computer, è in grado di dirottare programmi attendibili ed espletare attività pericolose in apparente legittimità.

Il software di sicurezza Zone Labs protegge il computer dagli hacker e dagli attacchi maligni assegnando criteri ai programmi che ne indicano il livello di attendibilità e ne specificano le azioni che sono autorizzati a eseguire.

Gli utenti di ZoneAlarm Security Suite dispongono della funzione supplementare della protezione di OSFirewall, che rileva quando i programmi eseguono azioni sospette o potenzialmente pericolose, come la modifica delle impostazioni del registro del computer.

## Impostazione automatica delle autorizzazioni per i programmi

Le impostazioni di SmartDefense Advisor e Controllo dei programmi operano assieme per garantire che ai programmi "buoni" venga consentito l'accesso e che ai programmi "cattivi" venga negato l'accesso. In base alle impostazioni predefinite, il Controllo dei programmi è impostato a Medio e SmartDefense Advisor è impostato ad Automatico. Con queste impostazioni predefinite, il software di sicurezza Zone Labs assegna automaticamente l'autorizzazione ai programmi. Per informazioni sulla personalizzazione di Controllo dei programmi e Smart Defense Advisor, vedere "Impostazione di opzioni generiche per Controllo dei programmi", a pagina 73.

Quando un programma richiede accesso per la prima volta, può verificarsi una delle seguenti situazioni:

- Viene consentito l'accesso - Viene consentito l'accesso se il programma è sicuro e ha bisogno delle autorizzazioni richieste per poter funzionare correttamente. Ciò si verifica quando il Controllo dei programmi è impostato a Medio e SmartDefense Advisor è impostato ad Automatico.
- L'accesso viene negato - L'accesso viene negato se il programma non è sicuro oppure se non ha bisogno delle autorizzazioni richieste per poter funzionare. Ciò si verifica quando il Controllo dei programmi è impostato a Medio e SmartDefense Advisor è impostato ad Automatico.



- Viene visualizzato un avviso Nuovo programma - Gli avvisi relativi ai programmi appaiono quando si deve decidere se consentire o negare l'accesso a un programma. Questi avvisi offrono suggerimenti che aiutano a decidere come rispondere.



In alcuni casi, SmartDefense Advisor potrebbe non disporre di informazioni su un determinato programma e, quindi, non essere in grado di concedere automaticamente le autorizzazioni. In questi casi, si riceverà un avviso relativo ai programmi. Fare clic su **Ulteriori informazioni** nella finestra di avviso per leggere dettagli sul programma che aiuteranno l'utente a rispondere. Per ulteriori informazioni, vedere "Avvisi relativi ai programmi", a pagina 217.

### ***Programmi sicuri***

Il software di sicurezza Zone Labs convalida i programmi in base a un database di programmi sicuri e assegna automaticamente le autorizzazioni richieste per i programmi che ne hanno bisogno per poter funzionare correttamente. Se sono state accettate le impostazioni predefinite per i programmi nella configurazione guidata, il software di sicurezza Zone Labs è impostato per configurare automaticamente i programmi più comuni nelle seguenti categorie generali:

- Browser (per esempio, Internet Explorer, Netscape)
- Client di posta elettronica (per esempio, Microsoft Outlook, Eudora)
- Programmi di messaggistica immediata (per esempio, MSN Messenger, Yahoo!)
- Antivirus (per esempio, Symantec, Zone Labs)
- Utilità per i documenti (per esempio, WinZip<sup>®</sup> e Adobe<sup>®</sup> Acrobat<sup>®</sup>)
- Applicazioni software Zone Labs

Persino i programmi considerati sicuri possono essere utilizzati dagli hacker per l'esecuzione di azioni che non lo sono. La protezione di OSFirewall, disponibile in ZoneAlarm Security Suite, visualizza avvisi quando rileva il comportamento sospetto o pericoloso di un programma. Per ulteriori informazioni su questi avvisi, vedere l'Appendice A, "Avvisi relativi ai programmi", Avvisi relativi ai programmi pagina 217.

## **Impostazione manuale delle autorizzazioni per i programmi**

Se si preferisce assegnare le autorizzazioni manualmente, oppure se il software di sicurezza Zone Labs non è riuscito ad assegnarle automaticamente, è possibile assegnarle usando gli avvisi relativi ai programmi oppure impostando autorizzazioni per programmi specifici nella scheda Programmi del pannello Controllo dei programmi.

### ***Avvisi relativi ai programmi***

Quando un programma richiede accesso per la prima volta, un avviso Nuovo programma chiede se si desidera consentire l'autorizzazione di accesso. Quando si rileva un programma in ascolto sulle porte del computer, viene visualizzato un avviso Programma server.

Gli avvisi di tipo Comportamento sospetto e Comportamento pericoloso informano l'utente che un programma attendibile sul computer sta tentando di eseguire un'azione che potrebbe essere considerata sospetta o pericolosa. Per un elenco delle azioni considerate sospette o pericolose, vedere "Comportamento dei programmi", a pagina 261.

Per evitare di ricevere numerosi avvisi per lo stesso programma, selezionare la casella di controllo **Memorizza impostazione** prima di fare clic su **Consenti** o **Nega**.

Dopodiché, il software di sicurezza Zone Labs bloccherà o autorizzerà automaticamente il programma. Se lo stesso programma chiederà di nuovo l'autorizzazione di accesso, un avviso Programma ripetuto domanderà all'utente se concedere (o negare) l'autorizzazione a un programma che l'ha già richiesta prima d'ora.

Poiché i Trojan horse e altri tipi di malware necessitano spesso di diritti server per poter agire, è necessario fare molta attenzione e concedere l'autorizzazione server solo ai programmi conosciuti e attendibili e che necessitano dell'autorizzazione per funzionare correttamente. Molti tipi di applicazioni comuni, come i programmi di chat, i client di posta elettronica e i programmi di chiamate in attesa su Internet, potrebbero richiedere l'autorizzazione server per funzionare correttamente. È bene concedere l'autorizzazione server solo ai programmi attendibili che ne hanno assolutamente bisogno per funzionare.

Se possibile, evitare di concedere a un programma un'autorizzazione server per la zona Internet. Se è necessario accettare le connessioni in entrata solo da un ristretto numero di computer, aggiungere questi ultimi alla zona attendibile, quindi concedere al programma l'autorizzazione server solo per la zona attendibile.

Per ulteriori informazioni sugli avvisi relativi ai programmi, vedere "Avvisi relativi ai programmi", a pagina 217.



È anche possibile impostare il software di sicurezza Zone Labs per concedere o negare automaticamente l'autorizzazione ai nuovi programmi senza visualizzare avvisi. Per esempio, se si è certi di aver concesso l'autorizzazione di accesso a tutti i programmi desiderati, è possibile negare automaticamente l'accesso a tutti gli altri programmi che lo richiedono. Per ulteriori informazioni, vedere "Impostazione delle autorizzazioni d'accesso per i nuovi programmi", a pagina 79.

### ***Elenco dei programmi***

L'elenco dei programmi consente di impostare o personalizzare le autorizzazioni per programmi specifici in base alle singole necessità. Per ulteriori informazioni sull'elenco dei programmi e la personalizzazione delle autorizzazioni, vedere "Utilizzo dell'elenco dei programmi", a pagina 81.

# Impostazione di opzioni generiche per Controllo dei programmi

Quando si usa il software di sicurezza Zone Labs, nessun programma sul computer può accedere a Internet o alla rete locale, oppure agire come server, se non è espressamente autorizzato dall'utente.

## Impostazione del livello di Controllo dei programmi

Utilizzare il livello di Controllo dei programmi per definire il numero di avvisi relativi ai programmi visualizzati quando si inizia a usare il software di sicurezza Zone Labs.



Zone Labs, LLC. consiglia l'impostazione Medio per i primi giorni con un uso normale. Questa *modalità di apprendimento dei componenti* consente al software di sicurezza Zone Labs di apprendere velocemente le firme MD5 per i componenti più usati senza interrompere il lavoro dell'utente con troppi avvisi. Utilizzare questa impostazione fino a quando i programmi di accesso a Internet (per esempio, il browser, il client di posta e il programma chat) sono stati usati almeno una volta con il software di sicurezza Zone Labs in esecuzione. Dopo aver usato tutti i programmi che necessitano di una connessione a Internet, è possibile impostare il Controllo dei programmi ad Alto.

### Impostare il livello di Controllo dei programmi

1. Selezionare **Controllo dei programmi | Principale**.
2. Nella sezione Controllo dei programmi, trascinare il dispositivo di scorrimento sull'impostazione desiderata.

Alto	<p>È attivato il controllo avanzato dei programmi e dei componenti. Con questa impostazione, saranno visualizzati numerosi avvisi.</p> <ul style="list-style-type: none"><li>◆ I programmi e i componenti sono autenticati.</li><li>◆ Le autorizzazioni per i programmi sono in vigore.</li><li>◆ I programmi vengono monitorati alla ricerca di comportamenti sospetti e pericolosi.</li></ul>
------	---

Medio	<p>Questa è l'impostazione predefinita.</p> <ul style="list-style-type: none"> <li>◆ Il Controllo dei programmi avanzato è disattivato.</li> <li>◆ La modalità di apprendimento dei componenti è attiva.</li> <li>◆ I programmi vengono autenticati; i componenti vengono appresi.</li> <li>◆ Le autorizzazioni per i programmi sono in vigore.</li> <li>◆ I programmi vengono monitorati alla ricerca di comportamenti pericolosi.</li> </ul> <p><b>Nota:</b> dopo aver usato tutti i programmi che necessitano di una connessione a Internet, impostare il Controllo dei programmi ad Alto.</p>
Basso	<ul style="list-style-type: none"> <li>◆ Il Controllo dei programmi avanzato è disattivato.</li> <li>◆ La modalità di apprendimento dei programmi e dei componenti è attiva.</li> <li>◆ Non vengono visualizzati avvisi relativi ai programmi.</li> </ul>
Disattivato	<p>Il Controllo dei programmi è disattivato.</p> <ul style="list-style-type: none"> <li>◆ I programmi e i componenti non vengono autenticati e non ne viene eseguito l'apprendimento.</li> <li>◆ Le autorizzazioni per i programmi non sono in vigore.</li> <li>◆ A tutti i programmi sono concessi diritti di accesso/server.</li> <li>◆ Viene consentito a tutti i programmi di assumere un comportamento sospetto e pericoloso.</li> <li>◆ Non vengono visualizzati avvisi relativi ai programmi.</li> </ul>

### Impostare opzioni di controllo dei programmi personalizzate

1. Selezionare **Controllo dei programmi | Principale**.
2. Nell'area Controllo dei programmi, fare clic su **Personalizza**.

Viene visualizzata la finestra di dialogo Impostazioni personalizzate Controllo dei programmi.

3. Specificare le impostazioni da applicare.

Attiva il Controllo dei programmi avanzato	Impedisce a programmi attendibili, che cercano di eludere la protezione in uscita, di utilizzare programmi attendibili.
Attiva il controllo di interazione delle applicazioni	Avvia quando un processo cerca di usare un altro processo oppure ogni volta che un programma avvia un altro programma.
Attiva controllo dei componenti	Consente il monitoraggio dei componenti di un programma alla ricerca di comportamenti non autorizzati.

4. Fare clic su **OK**.

## Impostazione dei livelli di SmartDefense Advisor

Quando si utilizza un programma che richiede l'autorizzazione all'accesso, SmartDefense Advisor interroga il server di Zone Labs per determinare quale criterio applicare per quel programma. SmartDefense Advisor può impostare le autorizzazioni per il programma automaticamente, oppure si può scegliere di configurare manualmente i diritti di accesso. Per impostazione predefinita, il livello di SmartDefense Advisor è impostato ad Automatico.

### Impostare i livelli di SmartDefense Advisor

1. Selezionare **Controllo dei programmi | Principale**.
2. Nella sezione SmartDefense Advisor, scegliere l'impostazione desiderata.

Automatico	In modalità Automatico, SmartDefense Advisor implementa automaticamente l'impostazione consigliata dal server. Per impostare SmartDefense Advisor, il Controllo dei programmi deve essere impostato a Medio o Alto.
Manuale	In modalità Manuale, si riceveranno avvisi relativi ai programmi quando i programmi richiedono l'accesso e l'utente può impostare l'autorizzazione manualmente.
Disattivato	SmartDefense Advisor non contatterà il server per consigli sui programmi.

Se non esistono consigli disponibili per un programma, oppure se SmartDefense Advisor è impostato su Disattivato, sarà possibile impostare le autorizzazioni manualmente. Vedere "Impostazione di autorizzazioni per programmi specifici", a pagina 81.

## Attivazione del Blocco automatico

Il Blocco automatico Internet protegge il computer se rimane connesso a Internet per lunghi periodi anche quando non si utilizzano le risorse su Internet o sulla rete in modo attivo.

Quando il blocco è attivo, è consentito solo il traffico proveniente da programmi ai quali sono state concesse le autorizzazioni Ignora blocco. Tutto il traffico da e verso il computer viene fermato, compresi i messaggi DHCP o gli heartbeat dell'ISP, che servono a mantenere la connessione a Internet. Questo potrebbe provocare l'interruzione della connessione a Internet.

È possibile impostare il Blocco Internet per essere attivato:

- All'attivazione dello screensaver, oppure
- Dopo un numero specificato di minuti di inattività della rete.

**Attivare o disattivare il Blocco automatico**

1. Selezionare **Controllo dei programmi** | **Principale**.
2. Nella sezione Blocco automatico, selezionare **Attivato** o **Disattivato**.

**Impostare le opzioni di Blocco automatico**

1. Selezionare **Controllo dei programmi** | **Principale**.
2. Nell'area Blocco automatico, fare clic su **Personalizza**.

Viene visualizzata la finestra di dialogo Impostazioni personalizzate blocco.

3. Specificare la modalità di blocco da utilizzare.

Blocca dopo n minuti di inattività.	Attiva il blocco automatico dopo che sono trascorsi i minuti indicati. Specificare un valore compreso tra 1 e 999.
Blocca quando si attiva lo screensaver	Attiva il blocco automatico all'attivazione dello screen saver.

**Visualizzazione del log degli eventi relativi ai programmi**

Per impostazione predefinita, tutti gli eventi relativi ai programmi sono presenti nel Visualizzatore log.

**Visualizzare gli eventi dei programmi presenti nel log**

1. Selezionare **Avvisi e log** | **Visualizzatore log**.
2. Selezionare **Programma** dall'elenco a discesa Tipo di avviso.

La tabella 5-1 fornisce una spiegazione dei campi del Visualizzatore log per gli eventi relativi ai programmi.

Campo	Spiegazione
Livello	Livello dell'evento in base al <b>Livello della protezione</b> dell'opzione di sicurezza.
Data/Ora	Data e ora in cui si è verificato l'evento.
Tipo	Tipo di avviso relativo ai programmi che si è verificato. I valori possibili per questa colonna includono: <ul style="list-style-type: none"> <li>• Accesso al programma</li> <li>• Programma ripetuto</li> <li>• Nuovo programma</li> </ul>

**Tabella 5-1: Campi del log per gli eventi relativi ai programmi**

<b>Campo</b>	<b>Spiegazione</b>
Programma	Il programma (visualizzato come file dell'applicazione) che ha richiesto l'accesso. Se il nome di un programma non è disponibile, fare riferimento al campo Descrizione nella finestra Dettagli voce.
IP di origine	L'indirizzo IP del computer che ha inviato la richiesta. Se non è possibile determinare l'indirizzo IP di origine, questo campo sarà vuoto.
IP di destinazione	L'indirizzo IP del computer che ha ricevuto la richiesta. Se non è possibile determinare l'indirizzo IP di destinazione, questo campo sarà vuoto.
Direzione	Specifica se la richiesta che ha causato l'evento era in ingresso, in uscita o si è verificata come risultato di traffico interno sul computer (dati).
Azione eseguita	Specifica se la richiesta è stata consentita o bloccata. L'azione è seguita da /
Conteggio	Quante volte l'azione è stata eseguita.
DNS di origine	Il nome di dominio del computer che invia la richiesta.
DNS di destinazione	Il nome di dominio del computer che riceve la richiesta.

**Tabella 5-1: Campi del log per gli eventi relativi ai programmi (continua)**

## Visualizzare gli eventi di OSFirewall registrati

Per impostazione predefinita, tutti gli eventi relativi a OSFirewall sono presenti nel Visualizzatore log.

### Visualizzare gli eventi dei programmi presenti nel log

1. Selezionare **Avvisi e log** | **Visualizzatore log**.
2. Selezionare **OSFirewall** dall'elenco a discesa Tipo di avviso.

La tabella 5-2 fornisce una spiegazione dei campi del Visualizzatore log per gli eventi di OSFirewall.

Campo	Spiegazione
Livello	Livello dell'evento in base al <b>Livello della protezione</b> dell'opzione di sicurezza.
Data/Ora	Data e ora in cui si è verificato l'evento.
Tipo	Tipo di avviso OSFirewall visualizzato. I valori possibili per questa colonna includono: <ul style="list-style-type: none"> <li>• Processo</li> <li>• Messaggio</li> <li>• Modulo</li> <li>• Registro</li> <li>• File</li> <li>• Esecuzione</li> <li>• Driver</li> <li>• Memoria fisica</li> </ul>
Sottotipo	L'evento specifico che ha avviato il tipo di accesso richiesto (per esempio, OpenThread sarebbe un sottotipo di Processo).
Dati	Il percorso del file che tentava di essere modificato.
Programma	Visualizza il percorso del programma che ha assunto il comportamento.
Azione eseguita	Specifica se la richiesta è stata consentita o bloccata. L'azione è seguita da /manuale o /auto per indicare se l'azione è stata eseguita dall'utente o da SmartDefense Advisor.
Conteggio	Quante volte l'azione è stata eseguita.

**Tabella 5-2: Campi del log per gli eventi relativi a OSFirewall**



# Configurazione di impostazioni avanzate per i programmi

Per impostazione predefinita, il software di sicurezza Zone Labs chiede sempre se bloccare o consentire i tentativi di connessione e di accesso al server per le zone Internet e attendibile. Inoltre, se il servizio TrueVector è in esecuzione, ma il software di sicurezza Zone Labs non lo è, l'accesso ai programmi è negato per impostazione predefinita.

## Impostazione delle proprietà dei programmi globali

Il Controllo dei programmi può essere personalizzato specificando se consentire o negare sempre l'accesso, oppure se chiedere all'utente ogni volta in cui un programma nella zona Internet o attendibile richiede l'accesso.

### Impostare proprietà dei programmi globali

1. Selezionare **Controllo dei programmi** | **Principale**.
2. Fare clic su **Avanzate**, quindi fare clic sulla scheda **Avvisi e funzionalità**.
3. Specificare le opzioni dei programmi globali.

Mostra avvisi quando l'accesso a Internet viene negato	Visualizza un avviso Programma bloccato quando il software di sicurezza Zone Labs nega l'accesso a un programma. Per negare automaticamente l'accesso, deselezionare questa opzione.
Nega l'accesso se le autorizzazioni sono impostate su "chiedi" e il servizio TrueVector è in esecuzione ma il software di sicurezza Zone Labs non è attivo.	In rare occasioni, un processo indipendente come un Trojan horse potrebbe chiudere l'interfaccia di software di sicurezza Zone Labs ma lasciare il servizio TrueVector in esecuzione.  L'impostazione impedisce all'applicazione di accedere in queste situazioni.
Richiedi password per consentire a un programma l'accesso temporaneo a Internet	Richiede di digitare una password per consentire l'autorizzazione di accesso. È necessario essere registrati per poter rispondere Sì a un avviso relativo ai programmi.  Per consentire l'accesso senza l'immissione di una password, deselezionare l'opzione.

4. Fare clic su **OK**.

## Impostazione delle autorizzazioni d'accesso per i nuovi programmi

Il software di sicurezza Zone Labs visualizza un avviso Nuovo programma quando un programma sul computer cerca di accedere alle risorse su Internet o sulla rete locale per la prima volta. Visualizza un avviso Programma server quando un programma cerca di agire come server per la prima volta. È, comunque, possibile impostare il software di

sicurezza Zone Labs per consentire o bloccare automaticamente i nuovi programmi senza visualizzare avvisi. Per esempio, se si è certi di aver concesso l'autorizzazione di accesso a tutti i programmi desiderati, è possibile negare automaticamente l'accesso a tutti gli altri programmi che lo richiedono.

### Impostare autorizzazioni per i tentativi di connessione per i nuovi programmi

1. Selezionare **Controllo dei programmi** | **Principale**.
2. Fare clic su **Avanzate**.
3. Nella sezione Tentativi di connessione, specificare le preferenze per ogni zona.

Consenti sempre l'accesso	Consente a tutti i nuovi programmi di accedere alla zona specificata.
Nega sempre l'accesso	Non consente ai programmi di accedere alla zona specificata.
Chiedi sempre l'autorizzazione	Visualizza un messaggio che chiede se autorizzare l'accesso alla zona specificata per il programma.



Le impostazioni per i singoli programmi possono essere definite nella scheda Programmi. Le impostazioni in questo pannello valgono SOLO per i programmi non ancora elencati nella suddetta scheda.

### Impostare autorizzazioni per i tentativi di agire come server per i nuovi programmi

1. Selezionare **Controllo dei programmi** | **Principale**.
2. Fare clic su **Avanzate**.

Nella sezione Tentativi di agire come server, specificare le preferenze per ogni zona.

Accetta sempre la connessione	Consente a tutti i programmi di agire come server.
Nega sempre la connessione	Nega tutti i tentativi dei programmi di agire come server.
Chiedi sempre prima della connessione	Visualizza un messaggio che chiede se autorizzare il programma ad agire come server.

# Impostazione di autorizzazioni per programmi specifici

Impostando il livello di Controllo dei programmi ad **Alto**, **Medio** o **Basso**, si specifica a livello globale se i programmi e i relativi componenti devono richiedere l'autorizzazione prima di accedere a Internet o prima di agire come server. In alcuni casi, si potrebbe voler specificare per un singolo programma delle impostazioni diverse da queste impostazioni globali. Per esempio, se si desidera consentire l'accesso a un determinato programma lasciando impostata ad Alto la sicurezza per tutti gli altri programmi, impostare l'autorizzazione per quel programma a **Consenti**.



Dopo aver impostato manualmente le autorizzazioni per un programma, queste non cambieranno nemmeno se, in seguito, si imposta il livello di SmartDefense Advisor ad Automatico. Per ricevere i suggerimenti automatici sui programmi, rimuovere il programma dall'elenco dei programmi, quindi impostare il livello di SmartDefense Advisor ad Automatico.

## Utilizzo dell'elenco dei programmi

L'elenco dei programmi fornisce una panoramica dei programmi sul computer che hanno tentato di accedere a Internet o alla rete locale. Per ciascuna applicazione, l'elenco dei programmi fornisce informazioni dettagliate sul suo stato corrente, l'attendibilità e le funzioni che è autorizzata a eseguire. L'elenco è organizzato in ordine alfabetico. I programmi in elenco possono essere ordinati per qualsiasi colonna facendo clic sulla sua intestazione. Mentre si lavora al computer, il software di sicurezza Zone Labs rileva ogni programma che richiede accesso alla rete e lo aggiunge all'elenco dei programmi. Per accedere all'elenco dei programmi, selezionare **Controllo dei programmi | Programmi**.

Selezionando il nome di un programma nell'elenco, vengono visualizzate le relative informazioni nella sezione Dettagli voce in giallo, sotto l'elenco. Questa sezione fornisce i dettagli relativi al programma, compreso il nome completo, i criteri di OSFirewall e la data dell'ultimo aggiornamento dei criteri.

Le colonne SmartDefense Advisor e Livello di attendibilità indicano la protezione di OSFirewall per il computer e specificano se un programma è autorizzato a eseguire

azioni a livello di sistema, come la modifica dei parametri TCP/IP, il caricamento o l'installazione di driver o la modifica delle impostazioni predefinite del browser.

indicatore dello stato

Attivo	Programmi ▲	Accesso		Server		Invia posta	
		Attend...	Internet	Attend...	Internet		
	CA eTrust Security ...	?	?	?	?	X	
	Generic Host Proce...	✓	✓	?	?	?	
	Internet Explorer	✓	✓	?	?	?	
	LSA Shell (Export V...	✓	✓	?	?	?	
	Spooler SubSystem...	✓	?	?	?	?	
	Windows Movie Ma...	✓	✓	✓	✓	✓	
	ZoneAlarm Stub Pr...	✓	✓	✓	✓	✓	

Dettagli voce			
Nome prodotto	Microsoft® Windows® Operating System	▲	Aggiungi
Nome file	C:\WINDOWS\system32\spoolsv.exe	■	
Criterio	Configurazione manuale	▼	Opzioni
Ultimo aggiorna	Non applicabile		

Figura 5-1: Elenco dei programmi

### *Attivo*

Indica lo stato corrente di un programma. Un cerchio verde indica che il programma è attualmente in esecuzione.

### *Programmi*

Nome del programma.

### *SmartDefense Advisor*

Auto significa che i criteri del programma sono stati determinati dagli esperti di sicurezza di Zone Labs. Personalizzato significa che i criteri sono stati definiti manualmente dall'utente. Se si apporta una modifica a qualsiasi autorizzazione di programma (per esempio cambiando un valore in qualsiasi colonna della riga relativa a un programma), la colonna SmartDefense Advisor riporterà "Personalizzato" per tale programma. I criteri dei programmi contrassegnati come "Sistema" vengono anch'esse stabilite automaticamente da Zone Labs. Questi programmi sono contrassegnati come "Sistema" invece di "Auto" per indicare che sono utilizzati dal sistema operativo del computer.



La modifica manuale dei criteri dei programmi di sistema potrebbe interferire con le funzioni normali del computer.

***Livello di attendibilità***

Livello di attendibilità determina l'azione che un programma è autorizzato a eseguire. Sono presenti cinque livelli di affidabilità: Super, Attendibile, Limitato, Chiedi e Blocca. La designazione del livello di attendibilità di un programma è determinata dai suoi criteri. Il software di sicurezza Zone Labs assegna automaticamente i criteri ai programmi noti. Il team di sicurezza di SmartDefense Advisor controlla costantemente i programmi per le eventuali modifiche nel comportamento o nell'attendibilità e aggiorna di conseguenza le autorizzazioni per il programma. Un programma con impostazione di livello di attendibilità Super, potrebbe avere in futuro un livello Limitato, nel caso gli esperti di sicurezza determinassero che il programma espone a rischi il computer. Tuttavia, se l'impostazione dei criteri di un programma viene modificata da Auto a Personalizzato, il monitoraggio di cambiamenti nella colonna Livello attendibilità non sarà eseguito. Per questo motivo, si consiglia di mantenere le impostazioni di OSFirewall predefinite per i programmi. Fare riferimento alla tabella seguente per una descrizione dei simboli utilizzati nell'elenco.

***Accesso***

La colonna Accesso si riferisce al diritto di un programma a recuperare informazioni da Internet o dalle reti nella zona attendibile.



***Server***

Consente a un programma di rimanere in ascolto in modo passivo di traffico proveniente da Internet o dalla rete. Un numero limitato di programmi necessita di agire da server.







***Invia posta***

consente a un programma di inviare e ricevere messaggi di posta elettronica.

Fare riferimento alla tabella seguente per una descrizione dei simboli utilizzati nell'elenco.

<b>Simbolo</b>	<b>Significato</b>
	Al programma sono concessi diritti di accesso/ server.
	Quando nelle colonne Accesso o Server appare questo simbolo, significa che il software di sicurezza Zone Labs visualizzerà un avviso Programma se il programma richiede di agire sul server.  Quando nella colonna Livello di attendibilità appare questo simbolo, significa che il software di sicurezza Zone Labs visualizzerà un avviso di tipo Comportamento sospetto o Comportamento pericoloso se un programma esegue azioni considerate sospette o pericolose.

**Tabella 5-3: Simboli degli elenchi dei programmi**

Simbolo	Significato
	Al programma sono negati diritti di accesso/server.
	Il programma è attualmente attivo.
	Il programma può eseguire azioni sospette e pericolose senza chiedere alcuna autorizzazione. Non viene visualizzato alcun avviso.
	Accesso Attendibile. Un programma può eseguire azioni sospette senza chiedere autorizzazione, ma deve chiederla per eseguire azioni pericolose.
	Accesso Limitato. Un programma può eseguire azioni di livello attendibile ma non può eseguire azioni sospette o pericolose.
	Nessun accesso. I programmi contrassegnati con il simbolo Nessun accesso (Blocca) non possono essere eseguiti.

#### Tabella 5-3: Simboli degli elenchi dei programmi

Per ulteriori informazioni su quali azioni di programma sono considerate sospette o pericolose, vedere l'Appendice D, "Comportamento dei programmi", Comportamento dei programmi pagina 261.

## Aggiunta di un programma all'elenco dei programmi

Se si desidera concedere l'autorizzazione di accesso o server a un programma che non appare nell'elenco dei programmi, è possibile aggiungerlo all'elenco e concedere poi le autorizzazioni appropriate.

### Aggiungere un programma all'elenco dei programmi

1. Selezionare **Controllo dei programmi | Programmi**, quindi fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo Aggiungi programma.

2. Selezionare il programma che si desidera aggiungere, quindi fare clic su **Apri**.

Controllare di selezionare il file eseguibile del programma (per esempio, programma.exe).

### Modificare un programma nell'elenco dei programmi

1. Selezionare **Controllo dei programmi | Programmi**.

2. Fare clic col pulsante destro del mouse nella colonna Programmi e selezionare una delle opzioni disponibili.

Cambia di frequente	Se questa opzione è selezionata, il software di sicurezza Zone Labs utilizzerà solo le informazioni sul percorso al file per autenticare il programma. La firma MD5 non verrà controllata. <b>Attenzione:</b> questa è un'impostazione di sicurezza di livello basso.
Opzioni	Apre la finestra di dialogo Opzioni programma, in cui è possibile personalizzare le opzioni di sicurezza e creare regole della scheda Esperto per i programmi.
Proprietà	Apre la finestra delle proprietà di sistema per il programma.
Rimuovi	Elimina il programma dall'elenco.

## Concessione dell'autorizzazione di accesso a Internet per un programma

Molti dei programmi più comuni possono essere configurati automaticamente per accedere a Internet in modo sicuro. Per determinare se un programma è stato configurato manualmente o automaticamente, selezionarlo nell'elenco dei programmi ed esaminare il campo Criterio nella sezione Dettagli voce.

### Concedere l'autorizzazione di accesso a Internet per un programma

1. Selezionare **Controllo dei programmi** | **Programmi**.
2. Nella colonna Programmi, fare clic sul programma a cui si desidera concedere l'accesso, quindi selezionare **Consenti** dal menu che appare.

Per informazioni su come concedere l'autorizzazione ai programmi rispondendo a un avviso, vedere "Avvisi Nuovo programma", a pagina 218.



Le regole incorporate garantiscono criteri di sicurezza coerenti per ogni programma. I programmi che possono accedere alla zona Internet accedono anche alla zona attendibile e i programmi con l'autorizzazione server in una zona godono anche dell'autorizzazione di accesso per quella zona. Ecco perché, per esempio, selezionando Consenti sotto Zona attendibile/Server, vengono impostate a Consenti anche tutte le altre autorizzazioni del programma.

## Concessione a un programma dell'autorizzazione ad agire come server

Fare attenzione quando si concede ai programmi l'autorizzazione ad agire come server, perché i Trojan horse ed altri tipi di malware necessitano spesso di diritti server per poter funzionare. L'autorizzazione ad agire come server dovrebbe essere riservata ai programmi conosciuti, attendibili e che necessitano di diritti server per funzionare correttamente.

**Concedere a un programma l'autorizzazione ad agire come server**

1. Selezionare **Controllo dei programmi** | **Programmi**.
2. Nella colonna Programmi, fare clic col pulsante destro del mouse sul programma a cui si desidera concedere l'accesso server, quindi selezionare **Consenti** dal menu di scelta rapida.

**Concessione dell'autorizzazione di invio della posta a un programma**

Per abilitare il client di posta elettronica a inviare messaggi di posta e attivare la protezione contro le minacce inviate per posta, concedere l'autorizzazione di invio della posta al client di posta elettronica. Per ulteriori informazioni sulla protezione della posta elettronica, vedere il Capitolo 7, "Protezione della posta elettronica", a pagina 119.

**Concedere l'autorizzazione di invio della posta a un programma**

1. Selezionare **Controllo dei programmi** | **Programmi**.
2. Selezionare un programma dall'elenco e fare clic nella colonna **Invia posta**.
3. Selezionare **Consenti** dal menu di scelta rapida.



È inoltre possibile accedere alla finestra di dialogo Opzioni programma facendo clic con il pulsante destro del mouse sul nome di un programma e selezionando **Opzioni**.



# Impostazione di opzioni per un programma specifico

Se un programma viene autenticato, se utilizza la protezione di MailSafe in uscita, oppure se osserva gli standard di privacy viene determinato globalmente impostando il livello di Controllo dei programmi. È possibile modificare queste e altre impostazioni a livello di programma dall'elenco dei programmi.

## Impostazione di opzioni avanzate per Controllo dei programmi

Il Controllo dei programmi avanzato rafforza la sicurezza impedendo a programmi sconosciuti di utilizzare i programmi attendibili per accedere a Internet, oppure impedendo agli hacker di utilizzare le funzioni CreateProcess e OpenProcess di Windows per modificare i processi del computer.

### Attivare il Controllo dei programmi avanzato per un programma

1. Selezionare **Controllo dei programmi | Programmi**.
2. Nella colonna Programmi, selezionare il nome di un programma e fare clic su **Opzioni**.  
Viene visualizzata la finestra di dialogo Opzioni programma.
3. Visualizzare la scheda **Sicurezza**, quindi selezionare le opzioni desiderate per Controllo dei programmi avanzato.

Questo programma può utilizzare altri programmi per accedere a Internet	Consente al programma selezionato di utilizzare altri programmi per accedere a Internet.
Consenti interazione applicazioni	Consente al programma selezionato di utilizzare le funzioni OpenProcess e CreateProcess sul computer.

4. Fare clic su **OK**.

## Disattivazione della protezione della posta in uscita per un programma

Per impostazione predefinita, la protezione della posta in uscita è attivata per tutti i programmi. Poiché la possibilità di inviare posta non è una caratteristica di tutti i programmi, si può scegliere di disattivare la protezione della posta in uscita per i programmi che non la richiedono.

### Disattivare la protezione della posta in uscita per un programma

1. Selezionare **Controllo dei programmi | Principale**.
2. Selezionare un programma dall'elenco e fare clic su **Opzioni**.  
Viene visualizzata la finestra di dialogo Opzioni programma.

3. Fare clic sulla scheda **Sicurezza**.
4. Deselezionare la casella di controllo **Attiva protezione posta elettronica in uscita per questo programma**.
5. Fare clic su **Applica** per salvare le modifiche, quindi fare clic su **OK**.

Per ulteriori informazioni sulla protezione della posta elettronica in uscita, vedere "Protezione di MailSafe in uscita", a pagina 121

## Impostazione delle opzioni di filtro per un programma

Quando le funzioni Controllo genitori e Privacy sono attivate globalmente, i singoli programmi quali gli elaboratori di testo possono comunque accedere a contenuto limitato, a meno che non siano state impostate opzioni di filtro anche per tale programma. Per esempio, sebbene Controllo genitori blocchi l'accesso al sito "http://www.playboy.com" dal browser, è comunque possibile accedere al sito facendo clic su un URL in un documento di Microsoft Word, a meno che Controllo genitori non sia stato attivato anche per tale programma.

### Attivare le opzioni di filtro per un programma

1. Selezionare **Controllo dei programmi | Principale**.
2. Selezionare un programma dall'elenco e fare clic su **Opzioni**.

Viene visualizzata la finestra di dialogo Opzioni programma.

3. Fare clic sulla scheda **Sicurezza**.
4. Sotto Opzioni filtro, selezionare la casella di controllo accanto alla protezione desiderata, quindi fare clic su **OK**.

Per ulteriori informazioni sulla protezione della privacy, vedere il Capitolo 8, "Protezione della privacy", a pagina 141. Per ulteriori informazioni sul Controllo genitori, vedere il Capitolo 11, "Controllo genitori", a pagina 189.

## Impostazione delle opzioni di autenticazione

È possibile specificare se un programma è autenticato utilizzando il suo nome completo o mediante i suoi componenti. Per impostazione predefinita, tutti i programmi vengono autenticati in base ai loro componenti.

### Specificare un metodo di autenticazione

1. Selezionare **Controllo dei programmi | Principale**.
2. Selezionare un programma dall'elenco e fare clic su **Opzioni**.

Viene visualizzata la finestra di dialogo Opzioni programma.

3. Fare clic sulla scheda **Sicurezza**.
4. Sotto Autenticazione, selezionare la casella di controllo accanto all'opzione desiderata, quindi fare clic su **OK**.

## Impostazione dell'autorizzazione Ignora blocco a un programma

Quando il Blocco Internet è attivato, i programmi a cui viene concessa l'autorizzazione Ignora blocco possono continuare ad accedere a Internet. Se si concede l'autorizzazione Ignora blocco a un programma e quel programma utilizza altre applicazioni per svolgere le sue funzioni (per esempio, services.exe), concedere l'autorizzazione anche agli altri programmi.

### Concedere o revocare privilegi Ignora blocco

1. Selezionare **Controllo dei programmi** | **Principale**.
2. Selezionare un programma dall'elenco e fare clic su **Opzioni**.
3. Selezionare la casella di controllo **Attiva blocco**.
4. Fare clic su **Applica**, quindi fare clic su **OK**.

# Gestione dei componenti dei programmi

Per ogni programma sul computer, è possibile specificare se il software di sicurezza Zone Labs autenticherà solamente l'eseguibile, oppure l'eseguibile e tutti i componenti caricati. Inoltre, si può consentire o negare l'accesso ai singoli componenti del programma.

L'elenco dei componenti contiene una lista dei componenti dei programmi autorizzati che hanno cercato di accedere a Internet o alla rete locale. La colonna Accesso indica se il componente è sempre autorizzato all'accesso o se il software di sicurezza Zone Labs deve avvisare l'utente quando il componente richiede l'accesso.

L'elenco è organizzato in ordine alfabetico. I componenti in elenco possono essere ordinati per qualsiasi colonna facendo clic sulla sua intestazione. Mentre si lavora al computer, il software di sicurezza Zone Labs rileva i componenti utilizzati dai programmi e li aggiunge all'elenco.

## Accedere all'elenco dei componenti

🔗 Selezionare **Controllo dei programmi | Componenti**.

Componente	Descrizione	Acces...	
activeds.dll	ADs Router Layer DLL	✓	
actxprxy.dll	ActiveX Interface Marshaling Library	✓	
adslrpc.dll	ADs LDAP Provider C DLL	✓	
atl.dll	ATL Module for Windows NT (Unicode)	✓	
authz.dll	Authorization Framework	✓	
cabinet.dll	Microsoft® Cabinet File API	✓	
clbcatq.dll	COM Services	✓	
cnbjmon.dll	Language Monitor for Canon Bubble-Jet Printer	✓	
comctl32.dll	User Experience Controls Library	✓	
comctl32.dll	Common Controls Library	✓	

Dettagli voce	
Nome componente	ASN.1 Runtime APIs
Nome file	C:\WINDOWS\system32\msasn1.dll
Tipo file	Dynamic Link Library
Autenticazione	Manuale

Figura 5-4: Elenco dei componenti

## Concedere l'autorizzazione di accesso a un componente di programma

1. Selezionare **Controllo dei programmi | Componenti**.
2. Selezionare un componente dall'elenco e fare clic nella colonna Accesso.
3. Selezionare **Consenti** dal menu che appare.

# Creazione di regole della scheda Esperto per i programmi

Per impostazione predefinita, i programmi che ricevono l'autorizzazione di accesso o server possono utilizzare qualsiasi porta o protocollo e contattare qualsiasi indirizzo IP o host in qualunque momento. Al contrario, i programmi bloccati non hanno alcun diritto d'accesso. Creando regole della scheda Esperto per determinati programmi, è possibile aumentare la protezione contro programmi dannosi specificando porte e protocolli, indirizzi di origine e destinazione e intervalli di ore e giorni durante i quali l'attività viene consentita o negata. È anche possibile applicare opzioni di tracciamento a tipi specifici di traffico per vedere avvisi o generare voci di log quando si verifica traffico consentito, attivare o disattivare le regole secondo necessità e applicare più regole classificate a un programma.



Se sono state create regole delle porte per i programmi in una versione del software di sicurezza Zone Labs precedente alla 4.0, queste verranno automaticamente convertite in regole della scheda Esperto e saranno visibili nella scheda Esperto della finestra di dialogo Opzioni programma. Per visualizzare questa scheda, selezionare **Controllo dei programmi | Programmi**, quindi fare clic su **Opzioni**.

## Creazione di una regola della scheda Esperto per un programma

Le regole della scheda Esperto vengono applicate nell'ordine di classificazione. Di conseguenza, quando si creano regole per un programma, accertarsi che l'ultima creata per quel programma sia una regola "Blocca tutti".



Per suggerimenti su come impostare le regole della scheda Esperto per i programmi, visitare il forum degli utenti di Zone Labs (<http://www.zonelabs.com/forum>) e cercare "program rules".

### Creare una regola della scheda Esperto per un programma

1. Selezionare **Controllo dei programmi | Programmi**, quindi fare clic su **Opzioni**.
2. Selezionare **Regole Esperto**, quindi fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo Aggiungi regola.

### 3. Creare una regola per il programma.



La finestra di dialogo Aggiungi regola contiene gli stessi campi e opzioni disponibili per la creazione di regole Esperto per il firewall. Notare, comunque, che non è possibile utilizzare protocolli IGMP e personalizzati alle regole della scheda Esperto per i programmi. Vedere "Creazione di regole firewall nella scheda Esperto", a pagina 58.

### 4. Fare clic su **OK**.

## Condivisione di regole Esperto

Le regole per il firewall (create nella scheda Esperto del pannello Firewall) non possono essere applicate direttamente a un singolo programma. Se attivata, la regola viene applicata a livello globale. Allo stesso modo, una regola creata per un programma non può essere applicata direttamente a un altro programma.

È, tuttavia, possibile creare una copia della regola esistente e applicarla a qualsiasi programma. Notare che le modifiche apportate alla copia non si rifletteranno nell'originale.

### Applicare una regola esistente per il firewall a un programma

1. Selezionare **Firewall | Esperto**.
2. Selezionare la regola che si desidera applicare, quindi premere **CTRL+C**.
3. Selezionare **Controllo dei programmi | Programmi**.
4. Nella colonna Programmi, selezionare il programma a cui si desidera applicare la regola, quindi fare clic su **Opzioni**.
5. Selezionare Regole Esperto, quindi premere **CTRL+V**.

La regola viene applicata al programma.

6. Fare clic su **Applica**, quindi fare clic su **OK**.

### Disattivare una regola

1. Selezionare **Controllo dei programmi | Programmi**.
2. Selezionare il programma con la regola da disattivare, quindi fare clic col pulsante destro del mouse e selezionare **Disattiva** dal menu di scelta rapida.

La regola verrà visualizzata in grigio.

3. Fare clic su **Applica**, quindi fare clic su **OK**.

# Capitolo

## Protezione da spyware e virus

# 6

La funzione integrata Antivirus e Antispyware protegge il computer contro i virus e lo spyware in un'unica e potente operazione. Le varie opzioni di scansione rilevano automaticamente virus e spyware, rendendoli innocui prima che possano danneggiare il computer.

Spyware Community Watch aggiorna il database delle firme con informazioni sulle più recenti diffusioni di spyware raccolte da oltre 30 milioni di utenti di Zone Labs.

La funzione antivirus è disponibile solo in ZoneAlarm Antivirus e ZoneAlarm Security Suite.

La funzione antispyware è disponibile solo in ZoneAlarm Pro e ZoneAlarm Security Suite.

### Argomenti:

- "Protezione contro spyware e virus", a pagina 94
- "Personalizzazione delle opzioni di protezione contro i virus", a pagina 97
- "Personalizzazione delle opzioni di protezione contro lo spyware", a pagina 101
- "Esecuzione di una scansione dei virus", a pagina 103
- "Esecuzione di una scansione di spyware", a pagina 108
- "Visualizzazione dello stato di protezione da virus e spyware", a pagina 113
- "Monitoraggio della protezione contro i virus", a pagina 114

# Protezione contro spyware e virus

La funzione antispyware rileva componenti spyware presenti sul computer e li rimuove automaticamente o li pone in quarantena, in modo da poterli rimuovere manualmente dopo avergli assegnato il livello di rischio.

La funzione antivirus impedisce che virus noti e sconosciuti infettino il computer, eseguendo la scansione dei file e confrontandoli a un database di virus conosciuti rispetto a un insieme di caratteristiche che tende a riflettere il comportamento dei virus. I file possono essere sottoposti a scansione quando vengono aperti, chiusi, eseguiti o durante un'operazione di scansione parziale o completa del computer. Se viene rilevato un virus, il software di sicurezza Zone Labs lo rende innocuo, riparandolo o negando l'accesso al file infetto.

## Attivazione della protezione contro virus e spyware

Se si utilizza ZoneAlarm Security Suite e si sceglie di non attivare la funzione di protezione dai virus nella configurazione guidata a seguito dell'installazione, sarà possibile farlo manualmente.



La funzione antivirus di Zone Labs non è compatibile con altri software di protezione dai virus. Prima di attivare la funzione antivirus, è necessario disinstallare altri software antivirus presenti, compresi i pacchetti che includono una funzione di protezione dai virus. Il software di sicurezza Zone Labs è in grado di disinstallare automaticamente alcune applicazioni antivirus. Se si utilizza un programma che non può essere disinstallato in modo automatico, è possibile disinstallarlo mediante l'opzione Installazione applicazioni, accessibile dal Pannello di controllo di Windows.

### Attivare la protezione contro virus e spyware

1. Selezionare **Antivirus/Antispyware** | **Principale**
2. Nella sezione **Antivirus**, selezionare **Attivato**.
3. Nella sezione **Antispyware**, selezionare **Attivato**.

### Pianificazione di una scansione

La scansione del computer per la rilevazione di virus e spyware è una delle operazioni più importanti per proteggere l'integrità dei dati e l'ambiente operativo. Poiché la scansione è maggiormente efficace se eseguita a intervalli regolari, è spesso opportuno pianificarla come attività ad esecuzione automatica. Se il computer non è acceso nel momento in cui la scansione è stata impostata, questa verrà eseguita quindici minuti dopo il riavvio del sistema.

### Pianificare una scansione

1. Selezionare **Antivirus/Antispyware** | **Principale**.



2. Nell'area Antivirus, fare clic su **Opzioni avanzate**.

Viene visualizzata la finestra di dialogo Opzioni avanzate.

3. Sotto Impostazioni avanzate, selezionare **Pianificazione scansione**.

4. Selezionare la casella di controllo **Esegui scansione alla ricerca di virus**, quindi specificare giorno e ora della scansione.

5. Specificare la frequenza di scansione.

Per impostazione predefinita, viene eseguita una scansione dei virus una volta alla settimana.

6. Selezionare la casella di controllo **Esegui scansione alla ricerca di spyware**, quindi specificare giorno e ora della scansione.

7. Specificare la frequenza di scansione.

Per impostazione predefinita, viene eseguita una scansione alla ricerca di spyware una volta alla settimana.

8. Fare clic su **OK**.

## **Aggiornamento delle definizioni di virus e spyware**

Tutte le applicazioni virus o spyware contengono informazioni identificative univoche, note come file di definizione. Questi file di definizione sono le mappe utilizzate per individuare virus e spyware sul computer. Con la scoperta di nuove applicazioni virus o spyware, il software di sicurezza Zone Labs aggiorna il i propri database con tali file di definizione, necessari a rilevare le nuove minacce. Per tale ragione, il computer è vulnerabile a virus e spyware ogni volta che il database dei file di definizione diventa obsoleto. La sezione **Dettagli** situata sulla scheda Principale del pannello **Antivirus/ Antispyware** visualizza lo stato dei file di definizione.



Indica che i file di definizione sono obsoleti

Fare clic qui per aggiornare i file di definizione.

**Figura 6-1: Stato Antivirus e Antispyware**

Attivando la funzione di aggiornamento automatico, si riceveranno sempre i file di definizione più recenti quando questi sono disponibili.

#### **Attivare gli aggiornamenti automatici**

1. Selezionare **Antivirus/Antispyware | Principale**.
2. Nell'area Antivirus, fare clic su **Opzioni avanzate**.  
Viene visualizzata la finestra di dialogo Opzioni avanzate.
3. Selezionare **Aggiornamenti**, quindi attivare la casella di controllo **Attiva aggiornamenti antivirus automatici**.
4. Selezionare la casella di controllo **Attiva aggiornamenti antispyware automatici**.
5. Fare clic su **OK**.

# Personalizzazione delle opzioni di protezione contro i virus

Oltre alla scelta del tipo di scansione che si desidera eseguire, è possibile specificare il metodo utilizzato per il rilevamento dei virus e impostare i metodi di cura.

Il software di sicurezza Zone Labs offre diversi tipi di scansione dei virus per la protezione dei dati del computer: scansioni di sistema, scansioni all'accesso e scansioni di posta elettronica.

## Specificare le destinazioni di scansione

È possibile specificare quali unità, cartelle e file sottoporre a scansione durante una scansione di sistema. Escludere o includere un elemento nella scansione selezionando la relativa casella di controllo. Per impostazione predefinita, il software di sicurezza Zone Labs esegue la scansione dei soli dischi rigidi locali.

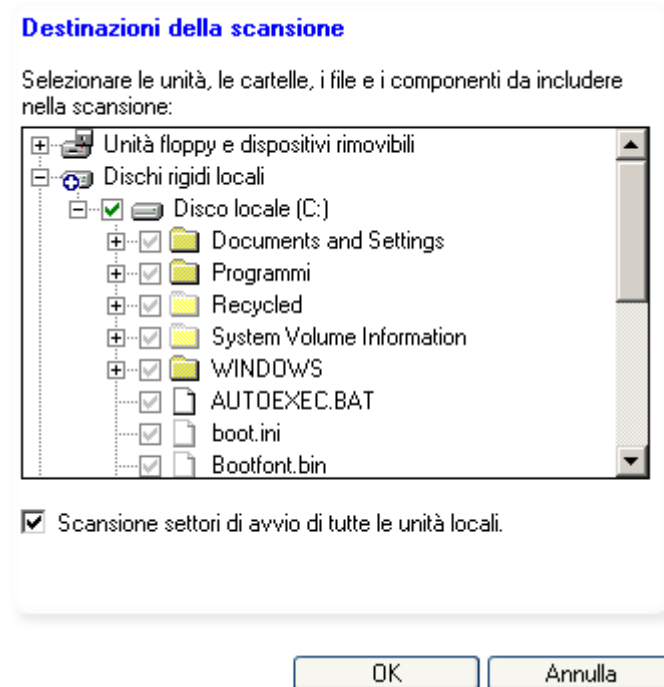








Figura 6-2: Finestra di dialogo Destinazioni della scansione

Nella Tabella 6-2 seguente è fornita una spiegazione delle icone riportate nella finestra di dialogo Destinazioni della scansione.

Icona	Spiegazione
	Il disco selezionato e tutte le sottocartelle e i file saranno inclusi nella scansione.
	Il disco selezionato e tutte le sottocartelle e i file saranno esclusi dalla scansione.
	Il disco selezionato sarà incluso nella scansione, ma una o più sottocartelle o file saranno esclusi.
	Il disco selezionato sarà escluso dalla scansione, ma una o più sottocartelle o file saranno inclusi.
 	La cartella selezionata sarà inclusa nella scansione. Un segno di spunta grigio indica che è attivata la scansione della cartella o del file perché questa è stata attivata per un disco o una cartella di livello superiore.
 	La cartella selezionata sarà esclusa dalla scansione. Un segno "x" grigio indica che è disattivata la scansione della cartella o del file perché questa è stata disattivata per un disco o una cartella di livello superiore.

**Tabella 6-1: Icone che indicano le destinazioni di scansione**

### Specificare le destinazioni di scansione

1. Selezionare **Antivirus/Antispyware | Principale**.
2. Fare clic su **Opzioni avanzate**.  
Viene visualizzata la finestra di dialogo Opzioni avanzate.
3. Sotto Gestione virus, selezionare **Destinazioni della scansione**.
4. Selezionare le unità, le cartelle e i file da sottoporre a scansione.
5. Selezionare o deselezionare la casella di controllo **Scansione settori di avvio di tutte le unità locali**, quindi fare clic su **OK**.

### Scansione all'accesso

La scansione all'accesso protegge il computer dai virus rilevando e trattando quelli che potrebbero trovarsi in stato di latenza sul computer. La scansione all'accesso è attivata per impostazione predefinita. La scansione all'accesso fornisce la forma più attiva di protezione contro i virus. I file vengono sottoposti a scansione contro i virus nel momento in cui vengono aperti, eseguiti o chiusi, consentendo perciò l'immediato rilevamento e la cura dei virus.

#### Attivare la scansione all'accesso

1. Selezionare **Antivirus/Antispyware | Principale**.

2. Nell'area Protezione, fare clic su **Opzioni avanzate**.

Viene visualizzata la finestra di dialogo Impostazioni avanzate antivirus.

3. Sotto Impostazioni avanzate, selezionare **Scansione all'accesso**.
4. Selezionare la casella di controllo **Attiva scansione all'accesso**, quindi fare clic su **OK**.

## Scansione della posta elettronica

La scansione della posta elettronica si basa sulla protezione offerta da MailSafe, eseguendo la scansione dei virus nel corpo e negli allegati dei messaggi e rimuovendoli prima che possano creare danni. Mentre MailSafe esegue la scansione di eventuali allegati dannosi in base all'estensione dei file, la funzione di scansione della posta elettronica la esegue confrontando gli allegati ai file delle firme dei virus noti. Gli allegati infetti rilevati vengono rimossi dal messaggio di posta elettronica e sostituiti da un file di testo (log) che fornisce i dettagli relativi ai file rimossi. Per i dettagli relativi all'esecuzione di una scansione della posta elettronica, vedere "Protezione antivirus per la posta elettronica", a pagina 138. La scansione della posta elettronica è attiva per impostazione predefinita.

### Attivare o disattivare la scansione della posta elettronica

1. Selezionare **Antivirus/Antispyware | Principale**, quindi fare clic su **Opzioni avanzate**.

Viene visualizzata la finestra di dialogo Opzioni avanzate.

2. Sotto Gestione virus, selezionare **Scansione posta elettronica**.
3. Selezionare o deselezionare la **casella di controllo Attiva scansione posta elettronica**, quindi fare clic su **OK**.

## Attivazione della cura automatica dei virus

Se viene rilevata un'infezione da virus, la finestra della scansione offre le opzioni di cura disponibili, come Quarantena, Ripara o Elimina. Per impostazione predefinita, il software di sicurezza Zone Labs tenta di curare automaticamente i file che contengono virus. L'utente verrà informato qualora non sia possibile riparare il file e potrà, quindi, intraprendere le azioni necessarie.

### Attivare la cura automatica dei virus

1. Selezionare **Antivirus/Antispyware | Principale**, quindi fare clic su **Opzioni avanzate**.
2. Sotto Gestione virus, selezionare **Cure automatiche**.
3. Selezionare l'opzione di cura desiderata:

▪	Avvisami – non curare automaticamente
▪	Prova a riparare e avvisami se il tentativo non riesce

▪	Prova a riparare e metti in quarantena se il tentativo non riesce (consigliato)
---	---

4. Fare clic su **OK**.

## Specificare i metodi di rilevamento dei virus

Vi sono due metodi principali utilizzati per eseguire la scansione dei virus: l'analisi euristica e la scansione a livello di byte. L'analisi euristica esegue la scansione dei file e identifica le infezioni basate sul comportamento caratteristico dei virus. L'analisi euristica è attivata per impostazione predefinita. Il filtro a livello di byte esegue la scansione di ogni byte del file per l'identificazione di un virus. L'esecuzione della scansione a livello di byte può richiedere un tempo considerevole. Di conseguenza, è consigliata solo a seguito di un massiccio attacco di virus per accertarsi che non vi siano infezioni residue.



L'attivazione o la disattivazione della scansione euristica non ha alcun effetto sulla scansione degli allegati di posta elettronica. Gli allegati vengono comunque sottoposti a scansione con questo metodo. La scansione a livello di byte non supporta le funzioni di scansione all'accesso e della posta elettronica.

### Specificare un metodo di rilevamento

1. Selezionare **Antivirus/Antispyware | Principale**, quindi fare clic su **Opzioni avanzate**.

Viene visualizzata la finestra di dialogo Opzioni avanzate.

2. Sotto **Gestione virus**, selezionare **Rilevamento**.
3. Selezionare i metodi di rilevamento preferiti, quindi fare clic su **OK**.

# Personalizzazione delle opzioni di protezione contro lo spyware

Oltre alla scelta del tipo di scansione che si desidera eseguire, è possibile specificare il metodo utilizzato per il rilevamento dello spyware e impostare i metodi di cura.

Il software di sicurezza Zone Labs offre diversi tipi di scansione dei virus per la protezione dei dati del computer: scansioni di sistema, scansioni all'accesso e scansioni di posta elettronica.

## Attivazione della cura automatica dello spyware

Se viene rilevata un'infezione da spyware, la finestra della scansione offre le opzioni di cura disponibili, quali Quarantena o Elimina. La finestra della scansione visualizza la cura suggerita per lo spyware in modo che l'utente possa intraprendere l'azione appropriata.

### Attivare la cura automatica dello spyware

1. Selezionare **Antivirus/Antispyware | Principale**, quindi fare clic su **Opzioni avanzate**.
2. Sotto Gestione spyware, selezionare **Cure automatiche**.
3. Selezionare la casella di controllo **Attiva cure spyware automatiche**, quindi fare clic su **OK**.

## Definizione dei metodi di rilevamento dello spyware

Oltre al rilevamento predefinito che esegue la ricerca di spyware attivo all'interno del registro del computer, vi sono altri metodi per il rilevamento dello spyware latente e di quello di difficile individuazione.

### Specificare un metodo di rilevamento dello spyware

1. Selezionare **Antivirus/Antispyware | Principale**, quindi fare clic su **Opzioni avanzate**.
2. Sotto Gestione spyware, selezionare **Rilevamento**.
3. Selezionare la casella di controllo **Scansione alla ricerca di cookie spia**.
4. Sotto Opzioni di rilevamento alla massima potenza, selezionare l'opzione desiderata:

scansione rapida intelligente	Questa opzione è selezionata per impostazione predefinita.
Scansione completa del sistema	Effettua la scansione del file system locale. Questa opzione può rallentare le prestazioni della scansione. Selezionare questa opzione solo se si sospetta la presenza di spyware non rilevato sul computer.

Scansione approfondita.	Effettua la scansione di ogni byte di dati sul computer. Questa opzione può rallentare le prestazioni della scansione. Selezionare questa opzione solo se si sospetta la presenza di spyware non rilevato sul computer.
-------------------------	---

5. Fare clic su **OK**.

## Esclusione dello spyware dalle scansioni

Sebbene alcuni spyware possono potenzialmente danneggiare il computer o danneggiare o rendere i dati vulnerabili agli hacker, sono presenti molte applicazioni valide che vengono comunque rilevate come spyware durante una scansione. Se si utilizza una di queste applicazioni, per esempio un software di riconoscimento vocale, è possibile escluderlo dalle scansioni di spyware aggiungendolo all'elenco delle eccezioni. È possibile aggiungere lo spyware all'elenco delle eccezioni facendo clic con il pulsante destro del mouse sull'elemento e scegliendo **Ignora sempre** nel menu.

Quando lo spyware si trova nell'elenco delle eccezioni, non verrà più rilevato durante le scansioni di spyware. Se lo spyware è stato aggiunto accidentalmente all'elenco delle eccezioni, è possibile rimuoverlo manualmente.

### Rimuovere lo spyware dall'elenco delle eccezioni

1. Selezionare **Antivirus/Antispyware | Principale**, quindi fare clic su **Opzioni avanzate**.
2. Sotto **Gestione spyware**, selezionare **Eccezioni**.
3. Nella sezione **Eccezioni cura spyware**, selezionare l'applicazione spyware che si desidera rimuovere, quindi fare clic su **Rimuovi dall'elenco**.
4. Fare clic su **OK**.

## Come prevenire gli attacchi dello spyware

Per farsi strada nel computer, spesso lo spyware viene camuffato da programma legittimo, ingannando l'utente e ottenendo l'autorizzazione per accedere ai file e proseguire nelle sue funzioni. In che modo si può essere sicuri che l'avviso pop-up relativo a un aggiornamento del sistema operativo sia realmente dannoso come sembra? Il software di sicurezza **Zone Labs** fornisce controlli speciali che impediscono allo spyware di installarsi sul computer. Le colonne **SmartDefense Advisor** e **Livello di attendibilità** nell'elenco dei programmi determinano l'autorizzazione concessa a un programma per eseguire determinate funzioni. Per ulteriori informazioni su questi controlli e il modo in cui proteggono il computer dallo spyware, vedere "Utilizzo dell'elenco dei programmi", a pagina 81.



# Esecuzione di una scansione dei virus

Vi sono svariati modi per avviare una scansione dei virus del computer.

- Fare clic su **Scansione di virus** nell'area Antivirus della scheda Principale nel pannello **Antivirus/Anti-spyware**.
- È possibile fare clic con il pulsante destro del mouse su un file del computer, quindi scegliere **Scansione con antivirus Zone Labs**.
- È possibile pianificare l'esecuzione di una scansione di sistema una volta o a intervalli regolari.
- È possibile aprire un file (se è attiva la funzione di scansione all'accesso).

È possibile eseguire fino a 5 scansioni simultanee. Le scansioni vengono eseguite nell'ordine in cui sono state avviate. Le scansioni di sistema forniscono un ulteriore livello di protezione consentendo di eseguire la scansione dell'intero contenuto del computer in una volta sola. Le scansioni di sistema rilevano i virus che potrebbero essere latenti sul disco rigido del computer e, se eseguite frequentemente, possono assicurare che i file delle firme antivirus siano aggiornati.

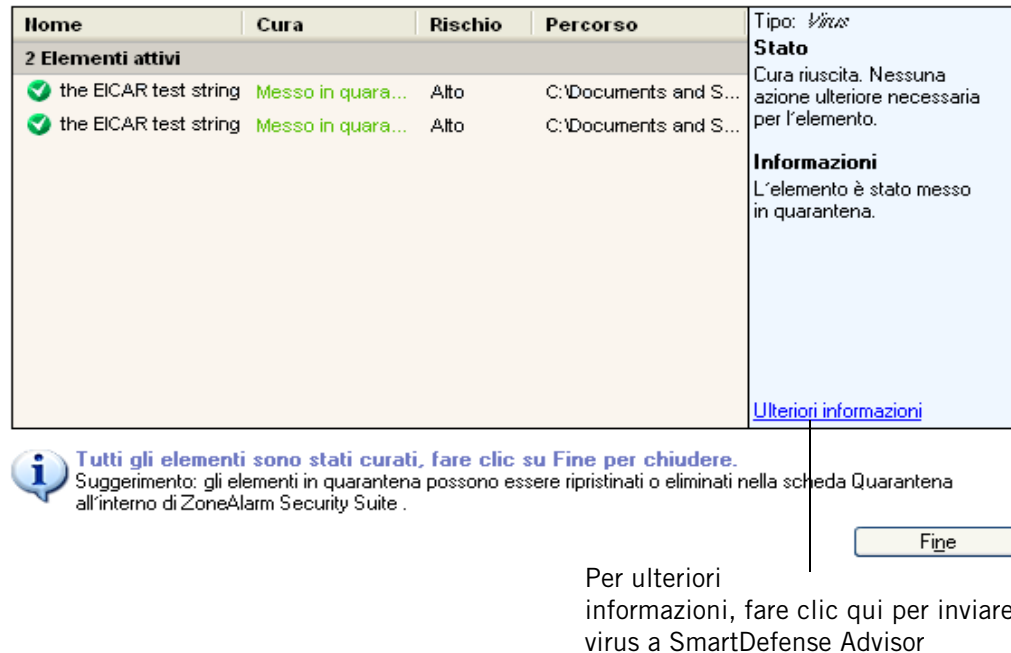
Data la natura approfondita delle scansioni dell'intero sistema, la loro esecuzione può richiedere del tempo. Di conseguenza, le prestazioni del sistema possono ridursi durante una scansione di questo tipo. Per evitare qualsiasi conseguenza sul flusso di lavoro, è possibile pianificare l'esecuzione delle scansioni in un orario in cui l'utilizzo del computer sia minimo o assente.



Facendo clic su **Pausa** nella finestra della scansione durante l'esecuzione di una scansione, questa viene sospesa e viene disattivata la scansione all'accesso. Fare nuovamente clic su **Pausa** per riprendere la scansione e riattivare la scansione all'accesso.

## Comprendere i risultati delle scansioni dei virus

A prescindere dal metodo utilizzato per avviare la scansione, i risultati vengono visualizzati nella finestra di dialogo Risultati scansione, come illustrato nella figura 6-4.



**Figura 6-3: Finestra di dialogo Risultati scansione**

La sezione Elementi attivi della finestra della scansione elenca le infezioni rilevate che non possono essere curate automaticamente. Per accettare le cure consigliate nella colonna Cura, fare clic su **Applica**. Gli elementi elencati sotto Cure automatiche sono già stati curati e non occorre intraprendere alcuna azione supplementare.

### **Nome**

Nome dello spyware che ha causato l'infezione.

### **Cura**

Specifica la cura applicata all'infezione. I valori possibili sono In quarantena o Eliminato.

### **Rischio di sicurezza**

Indica il livello di rischio dell'infezione. Tutti i virus sono considerati ad alto rischio.

### **Percorso**

Posizione del virus che ha causato l'infezione.

### **Tipo**

Specifica se l'infezione è stata causata da un virus, un worm o un Trojan.

**Stato**

Informa l'utente se il file è stato riparato, eliminato o se rimane infetto. Se il software di sicurezza Zone Labs non è stato in grado di curare l'elemento, appare **qui un collegamento** che indirizza l'utente verso ulteriori informazioni e istruzioni.

**Informazioni**

Fornisce ulteriori dettagli sull'infezione. Per ottenere ulteriori informazioni su un virus o uno spyware, fare clic sul collegamento **Ulteriori informazioni**.

**Cura manuale dei file dei virus**

Se la cura automatica non è attivata o se non è stato possibile riparare automaticamente il file, è possibile tentare di curarlo manualmente dalla finestra della scansione.

**Curare un file manualmente**

1. Nella finestra di dialogo Risultati scansione, selezionare l'elemento da curare.
2. Nella colonna Cura, scegliere l'opzione di cura desiderata:

Ripara	Tenta di riparare il file selezionato.
CANC	Elimina il file selezionato.
Quarantena	Aggiunge l'estensione .z16 al file infetto per renderlo innocuo. Il file viene posto in quarantena.

3. Fare clic su **Chiudi**, quando si è terminata la cura dei file.

**Riparazione dei file in un archivio**

Se il file infetto si trova in un file di archivio (come un file .zip), il software di sicurezza Zone Labs non sarà in grado di curarlo (riparandolo, eliminandolo o ponendolo in quarantena) mentre il file è ancora incluso nell'archivio.

**Riparare un file in un archivio**

1. Selezionare **Antivirus/Antispyware | Principale**, quindi fare clic su **Opzioni avanzate**.
2. Selezionare **Scansione all'accesso**, quindi selezionare la casella di controllo **Attiva scansione all'accesso**.
3. Fare clic su **Applica**, quindi fare clic su **OK**.
4. Aprire il file che è stato specificato nella finestra di dialogo Risultati scansione con un'utilità di archiviazione, per esempio WinZip.

La scansione all'accesso effettua la scansione dei file per rilevare eventuali infezioni. Viene visualizzata la finestra di dialogo Risultati scansione con i risultati della scansione. Se il file non può ancora essere riparato, vedere "Cura manuale dei file dei virus", a pagina 105.

## Invio di virus e spyware a Zone Labs per l'analisi

La segnalazione e l'invio di malware sospetto a Zone Labs, LLC aiuta a migliorare la sicurezza e la protezione di tutti gli utenti Internet. Il team di sicurezza di Zone Labs controlla tutti i messaggi all'arrivo per rilevare la presenza di nuovi file. Il team di sicurezza di Zone Labs agirà in modo appropriato in base alle segnalazioni e potrebbe contattare gli utenti per ulteriori informazioni o fornire ulteriori dettagli sui file inviati.

A causa del volume di malware rilasciato ogni giorno, i nostri ricercatori non possono rispondere a ogni invio di file degli utenti. Tuttavia, apprezziamo l'assistenza da parte dei nostri utenti e li ringraziamo per il loro contributo al fine di rendere Internet sicura.

Inviare qualsiasi domanda o dubbio a: [security@zonelabs.com](mailto:security@zonelabs.com)

### Inviare malware a Zone Labs per l'analisi

1. Collocare il file malware in un archivio .zip protetto con la password *infected*.

Per assistenza nella creazione di un archivio protetto da password, consultare la Guida di WinZip.

2. Inviare il file .zip a [malware@zonelabs.com](mailto:malware@zonelabs.com).

Utilizzare questo indirizzo di posta elettronica solo per l'invio di malware al team di sicurezza di Zone Labs.



Non inviare file di malware se si ha la sensazione di non riuscire a farlo in modo sicuro o se si aumenta il rischio di infezione o danni al sistema. Non inviare file malware sospetti ad altri utenti tramite posta elettronica, poiché potrebbero essere dannosi.

## Visualizzazione degli eventi di virus registrati

Per impostazione predefinita, tutti gli eventi relativi ai virus sono registrati nel Visualizzatore log.

### Visualizzare gli eventi dei virus registrati

1. Selezionare **Avvisi e log** | **Visualizzatore log**.
2. Selezionare **Virus** dall'elenco a discesa Tipo di avviso.

La tabella 6-3 fornisce una spiegazione dei campi del Visualizzatore log per gli eventi relativi ai virus.

Campo	Informazioni
Data	Data dell'infezione.

Tabella 6-3: Campi del log per gli eventi relativi ai virus

Campo	Informazioni
Tipo	<p>Tipo di evento verificatosi. I valori possibili per questo campo includono:</p> <ul style="list-style-type: none"> <li>• Aggiorna</li> <li>• Scansione</li> <li>• Cura</li> <li>• Posta elettronica</li> </ul>
Nome virus	Nome comune del virus. Per esempio, <i>iloveyou.exe</i> .
Nome file	Il nome del file infetto, il nome dei file che vengono sottoposti a scansione o il nome e il numero di versione dell'aggiornamento e/o del motore.
Azione eseguita	<p>Il modo in cui il traffico è stato gestito dal software di sicurezza Zone Labs. I valori possibili includono:</p> <ul style="list-style-type: none"> <li>• Aggiornato, Aggiornamento annullato, Aggiornamento non riuscito</li> <li>• Scansione eseguita, Scansione annullata, Scansione non riuscita</li> <li>• File Riparato, Riparazione del file non riuscita</li> <li>• In quarantena, Quarantena non riuscita</li> <li>• Eliminato, Eliminazione non riuscita</li> <li>• Ripristinato, Ripristino non riuscito</li> <li>• Rinominato, Ridenominazione non riuscita</li> </ul>
Attore	Se l'azione è stata manuale o automatica.
Posta elettronica	Se il virus è stato rilevato in un messaggio di posta elettronica, l'indirizzo del mittente del messaggio infetto.

**Tabella 6-3: Campi del log per gli eventi relativi ai virus**

# Esecuzione di una scansione di spyware

Vi sono svariati modi per avviare una scansione di spyware del computer.

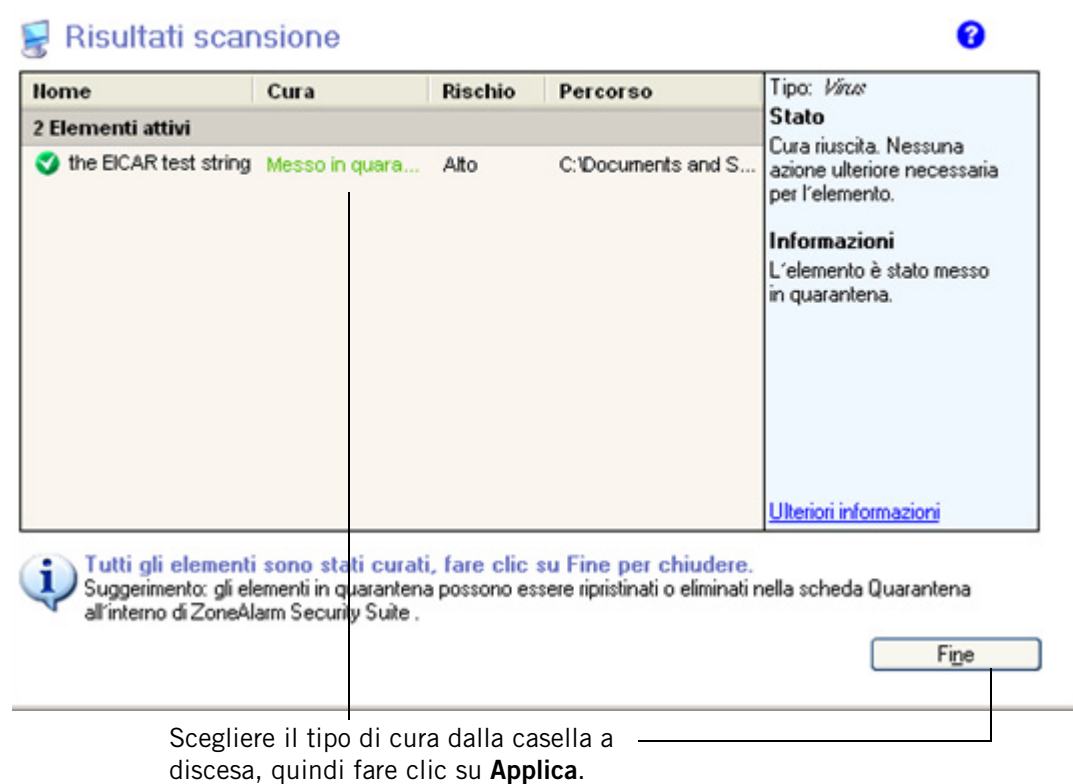
- È possibile fare clic su **Esegui scansione alla ricerca di spyware** nella sezione Antispyware sulla scheda Principale del pannello **Antivirus/Antispyware**.
- È possibile fare clic con il pulsante destro del mouse su un file del computer, quindi scegliere **Scansione con antivirus Zone Labs**.
- È possibile pianificare l'esecuzione di una scansione di sistema una volta o a intervalli regolari.
- È possibile aprire un file (se è attiva la funzione di scansione all'accesso).

È possibile eseguire fino a 5 scansioni simultanee. Le scansioni vengono eseguite nell'ordine in cui sono state avviate. Le scansioni di sistema forniscono un ulteriore livello di protezione consentendo di eseguire la scansione dell'intero contenuto del computer in una volta sola. Le scansioni di sistema rilevano i virus che potrebbero essere latenti sul disco rigido del computer e, se eseguite frequentemente, possono assicurare che i file delle firme antivirus siano aggiornati.

Data la natura approfondita delle scansioni dell'intero sistema, la loro esecuzione può richiedere del tempo. Di conseguenza, le prestazioni del sistema possono ridursi durante una scansione di questo tipo. Per evitare qualsiasi conseguenza sul flusso di lavoro, è possibile pianificare l'esecuzione delle scansioni in un orario in cui l'utilizzo del computer sia minimo o assente.

## Comprendere i risultati delle scansioni di spyware

I risultati della scansione di spyware vengono visualizzati nella finestra di dialogo Risultati scansione come illustrato nella figura 6-4.



**Figura 6-4: Finestra di dialogo Risultati scansione**

La sezione Elementi attivi della finestra della scansione elenca le infezioni rilevate che non possono essere curate automaticamente. Per accettare le cure consigliate nella colonna Cura, fare clic su **Applica**. Gli elementi elencati sotto Cure automatiche sono già stati curati e non occorre intraprendere alcuna azione supplementare.

### **Nome**

Nome dello spyware.

### **Cura**

Specifica la cura applicata all'infezione. I valori possibili sono In quarantena o Eliminato.

### **Rischio di sicurezza**

Indica il livello di rischio dell'infezione. I valori possibili per questa colonna includono:

- Basso - Adware o altro software valido ma fastidioso.
- Medio - Potenziale violazione della privacy.

- Alto - Pone una minaccia alla sicurezza.

### ***Percorso***

Posizione del virus o dello spyware che ha causato l'infezione.

### ***Tipo***

Categoria dello spyware rilevato. I valori possibili di questo campo includono il software di registrazione della pressione dei tasti e i cookie di tracciamento.

### ***Stato***

Informa l'utente se il file è stato riparato, eliminato o se rimane infetto. Se il software di sicurezza Zone Labs non è stato in grado di curare l'elemento, appare qui un **collegamento** che indirizza l'utente verso ulteriori informazioni e istruzioni.

### ***Informazioni***

Fornisce ulteriori dettagli sull'infezione. Per ottenere ulteriori informazioni su un virus o uno spyware, fare clic sul collegamento **Ulteriori informazioni**.

## **Errori nei risultati di scansione di spyware**

Se i risultati di una scansione di spyware contengono Errore, Nessuna cura disponibile o Cura non riuscita, significa che non esiste ancora un modo per rimuovere automaticamente lo spyware senza mettere a rischio l'integrità del computer o di altri file. Si tratta di una cosa non comune, poiché gli scrittori di spyware impiegano spesso tattiche molto pesanti per tenere lo spyware nel computer dell'utente senza preoccuparsi dei danni che possono causare.

Nella maggior parte dei casi, sono disponibili cure manuali. Per scoprirlo, immettere il nome dello spyware insieme alla parola "rimozione" nel motore di ricerca, quale Google o Yahoo e vedere se si trovano le istruzioni di rimozione. In ogni caso, eseguiamo costantemente ricerche sullo spyware di questo genere e sviluppiamo modi sicuri per rimuoverlo. È possibile che una cura sia disponibile in breve tempo.

## **Visualizzazione degli elementi in quarantena**

In alcuni casi, gli elementi rilevati durante una scansione di virus o spyware non possono essere curati o rimossi automaticamente. Questi elementi vengono solitamente collocati in quarantena in modo da renderli innocui ma conservarli per poter essere curati in futuro dopo un aggiornamento dei file delle firme dei virus e dello spyware.

### **Visualizzare i virus in quarantena**

1. Selezionare **Antivirus/Antispyware**.
2. Fare clic sulla scheda **Quarantena**.
3. Scegliere **Virus** dall'elenco a discesa Visualizzazione elementi in quarantena.

La visualizzazione dei virus in quarantena contiene le colonne informative seguenti:

### ***Infezione***

Nome dello spyware che ha causato l'infezione.



***Giorni in quarantena***

Numero dei giorni di presenza del virus in quarantena.

***Percorso***

Posizione del virus sul computer.

**Visualizzare lo spyware in quarantena**

1. Selezionare **Antivirus/Antispyware**.
2. Fare clic sulla scheda **Quarantena**.
3. Scegliere **Spyware** dall'elenco a discesa Visualizzazione elementi in quarantena.

La visualizzazione dello spyware in quarantena contiene le colonne informative seguenti:

***Tipo***

Nome dello spyware che ha causato l'infezione.

***Nome***

Nome dello spyware rilevato.

***Rischio***

Livello di rischio dell'infezione. Indica se lo spyware è di tipo benigno come adware o è una seria minaccia come un software di registrazione della pressione dei tasti.

***Giorni in quarantena***

Numero dei giorni di presenza del virus in quarantena.

**Visualizzare gli eventi di spyware registrati**

Per impostazione predefinita, tutti gli eventi relativi allo spyware sono presenti nel Visualizzatore log.

**Visualizzare gli eventi di spyware presenti nel log**

1. Selezionare **Avvisi e log** | Visualizzatore log.
2. Selezionare **Spyware** dall'elenco a discesa Tipo di avviso.

La tabella 6-3 fornisce una spiegazione dei campi del Visualizzatore log per gli eventi relativi allo spyware.

Campo	Informazioni
Data	Data dell'infezione.

**Tabella 6-4: Campi del log per gli eventi relativi a spyware**

Campo	Informazioni
Tipo	Tipo di spyware rilevato. I valori possibili per questo campo includono: <ul style="list-style-type: none"> <li>• Adware</li> <li>• Browser Helper Object</li> <li>• Dialer</li> <li>• Software di registrazione della pressione dei tasti</li> <li>• Screenlogger</li> <li>• Trojan</li> <li>• Worm</li> <li>• Spy Cookie</li> </ul>
Nome spyware	Nome comune dello spyware. Per esempio, <i>NavExcel</i> .
Nome file	Nome del file spyware file, per esempio <i>gmt.exe</i> .
Azione	Il modo in cui lo spyware è stato gestito dal software di sicurezza Zone Labs.
Attore	Se l'azione è stata eseguita dall'utente (manuale) o dal software di sicurezza Zone Labs (automatico)

**Tabella 6-4: Campi del log per gli eventi relativi a spyware**

# Visualizzazione dello stato di protezione da virus e spyware

Sono presenti due punti in cui è possibile visualizzare lo stato della protezione contro i virus e lo spyware. Uno è nella pagina **Panoramica | Stato** e l'altro è nella scheda **Antivirus/Antispyware | Principale**.

La scheda Principale del pannello Antivirus/Antispyware visualizza lo stato della protezione contro i virus e lo spyware. Da quest'area è possibile:

- Verificare che la protezione contro i virus e lo spyware sia attivata.
- Visualizzare data e ora delle ultime scansioni.
- Aggiornare i file di definizione.
- Richiamare una scansione.
- Visualizzare i risultati dell'ultima scansione.
- Accedere alle impostazioni avanzate.

Per ulteriori informazioni sui dettagli relativi allo stato presenti nel pannello Panoramica, vedere "Utilizzo della scheda Stato", a pagina 16. La sezione seguente descrive le informazioni sullo stato presenti nella scheda Principale del pannello Antivirus/Antispyware.

# Monitoraggio della protezione contro i virus

Una delle cose più importanti da fare per proteggere il computer dai virus è installare un prodotto software antivirus. Tuttavia, una volta installato, il software antivirus deve essere tenuto aggiornato al fine di assicurare la protezione contro i nuovi virus nel momento in cui questi vengono creati.

Indipendentemente dal prodotto software antivirus che si utilizza, se ci si trova in una delle situazioni seguenti, si pone il computer al rischio di un attacco da virus:

- Il periodo di prova o la sottoscrizione è scaduta.
- I file delle firme dei virus non sono aggiornati.

La funzione di monitoraggio antivirus è disponibile in ZoneAlarm, ZoneAlarm Antivirus, ZoneAlarm Pro e ZoneAlarm Security Suite.

La funzione Monitoraggio antivirus è un sistema di difesa secondario che tiene traccia del software antivirus installato sul computer e consente di sapere quando il software non è aggiornato o è disattivato. Questo sistema di avviso secondario funziona da backup per il sistema di avviso e aggiornamento integrato nell'antivirus. Notare che questa caratteristica non supporta tutti i programmi antivirus.

La maggior parte dei prodotti antivirus include l'aggiornamento automatico e avvisa l'utente quando i file di definizione sono diventati obsoleti.

## Copertura del monitoraggio

La funzione Monitoraggio antivirus rileva al momento il software antivirus dei principali produttori seguenti:

- Symantec
- McAfee
- Computer Associates
- Trend Micro

Se si utilizza un prodotto antivirus diverso, questo non viene al momento riconosciuto dalla funzione Monitoraggio antivirus. Ciò non significa che il prodotto ZoneAlarm non funzioni correttamente; la sicurezza che offre è assolutamente garantita. Nel tempo, verrà aggiunta al software di sicurezza Zone Labs la capacità di riconoscere ulteriori prodotti. Se il prodotto antivirus in uso non è attualmente supportato, è sufficiente disattivare la funzione Monitoraggio antivirus. Nessun problema, la funzione Monitoraggio antivirus è soltanto una funzione di controllo e non ha alcun effetto sul firewall e sulla sicurezza.

## Monitoraggio in ZoneAlarm, ZoneAlarm Pro e ZoneAlarm Wireless

In questi prodotti è possibile vedere il pannello di Monitoraggio antivirus. In questo pannello è possibile vedere lo stato del prodotto antivirus. È inoltre possibile attivare o disattivare il monitoraggio oppure attivare e disattivare gli avvisi di monitoraggio.

### Disattivare il monitoraggio e gli avvisi di monitoraggio

1. Selezionare **Monitoraggio antivirus | Principale**.
2. Nella sezione **Monitoraggio**, selezionare **Disattivato**.
3. Deselezionare la casella di controllo **Avvisa quando decade la sicurezza antivirus**.

## Monitoraggio in ZoneAlarm Anti-virus e ZoneAlarm Security Suite

In questi prodotti, non esiste alcun pannello Monitoraggio antivirus perché i prodotti sono dotati di Zone Labs Anti-virus. Sono invece presenti gli avvisi di monitoraggio. Quando Zone Labs Anti-virus viene disattivato, la funzione Monitoraggio antivirus viene attivata. Il monitoraggio può essere disattivato da qualsiasi avviso di monitoraggio o dalla finestra di dialogo Opzioni avanzate.

### Disattivare il monitoraggio

1. Selezionare **Avvisi e log**, quindi fare clic su **Avanzate**.
2. Selezionare la scheda **Eventi di avviso**.
3. Deselezionare le caselle di controllo seguenti:

<input type="checkbox"/>	Protezione antivirus non trovata
<input type="checkbox"/>	Eventi Monitoraggio antivirus

4. Fare clic su **OK**.

## Attivazione e disattivazione della funzione Monitoraggio antivirus

Se Zone Labs Anti-virus non è installato sul computer e si utilizza un altro prodotto software antivirus, la funzione Monitoraggio antivirus verrà attivata per impostazione predefinita. Inoltre, è possibile scegliere di attivare gli avvisi di monitoraggio, che appariranno ogni volta che decade la protezione.

### Attivare o disattivare Monitoraggio antivirus

1. Selezionare **Monitoraggio antivirus | Principale**.
2. Nella sezione Monitoraggio antivirus, selezionare **Attivato**.

## Visualizzazione dei messaggi di stato nel pannello Monitoraggio antivirus

L'area di stato del pannello Monitoraggio antivirus visualizza lo stato corrente dei prodotti antivirus installati, nonché quello della funzione Monitoraggio antivirus.



Figura 6-5: Area di stato del monitoraggio antivirus in ZoneAlarm

### *Monitoraggio prodotti antivirus*

Il software di sicurezza Zone Labs è in grado di rilevare la maggior parte dei prodotti software antivirus. Quest'area include un elenco a discesa che visualizza i prodotti software antivirus rilevati.

### *Protezione*

Visualizza se i prodotti antivirus sono attivi e proteggono il computer.

### *Aggiornamento antivirus*

Visualizza se i prodotti antivirus sono aggiornati o se la sottoscrizione è aggiornata.



Per provare Zone Labs Anti-virus, fare clic sul pulsante **Prova...** nell'area di stato.

## Visualizzazione degli avvisi di Monitoraggio antivirus

Se il fornitore del prodotto antivirus non ha inviato le definizioni dei virus più recenti, se la funzione di notifica del prodotto antivirus è stata disabilitata o se si esegue un prodotto antivirus che non è stato rilevato (vedere "Copertura del monitoraggio", a pagina 114) la funzione Monitoraggio antivirus fornisce un'avvertenza come seconda linea di difesa.

Se la protezione decade, viene visualizzato un avviso di monitoraggio. Questo avviso appare con un certo ritardo per consentire al prodotto antivirus di avvisare per primo

l'utente. L'avviso visualizzato fornisce informazioni e istruzioni per rendere il prodotto antivirus sicuro.



Se si esegue Windows 98, la caratteristica di scansione antivirus della posta elettronica rinomina MailSafe in *isafe.exe* invece del nome del programma di posta elettronica del computer.





# Capitolo

## Protezione della posta elettronica

# 7

Worm, virus e altre minacce spesso sfruttano la posta elettronica per diffondersi da un computer all'altro. MailSafe difende il computer dalle minacce trasmesse via posta elettronica, proteggendo nello stesso tempo gli indirizzi di amici, colleghi e altre persone contenuti nella propria rubrica.

Argomenti:

- "Comprensione della protezione della posta elettronica"
- "Attivazione della protezione di MailSafe in entrata"
- "Attivazione della protezione di MailSafe in uscita"
- "Personalizzazione della protezione di MailSafe in entrata"
- "Personalizzazione della protezione di MailSafe in uscita"
- "Filtro della posta indesiderata"
- "Protezione antivirus per la posta elettronica"

# Comprensione della protezione della posta elettronica

Allegare file ai messaggi di posta elettronica è utile per scambiarsi informazioni. Tuttavia, è anche rischioso perché offre agli hacker un facile modo per diffondere virus, worm, virus di tipo Trojan e malware di altro tipo.

Le funzioni di protezione di MailSafe in entrata e in uscita mettono gli allegati sospetti in quarantena, in modo che non possano infettare il computer, e impediscono ai worm di auto-inviarsi a tutti i contatti contenuti nella rubrica.

## Protezione di MailSafe in entrata

Gli allegati potenzialmente pericolosi possono essere identificati dall'estensione del nome del file, ossia dai caratteri che appaiono dopo il "punto" nel nome del file. L'estensione identifica il tipo di file, in modo che quest'ultimo possa essere aperto dal programma o dal componente di sistema appropriato.

Per esempio:

- .exe (file eseguibile)
- .js (file JavaScript)
- .bat (file di elaborazione batch)

Quando si riceve un messaggio di posta elettronica con un allegato nella posta in arrivo, MailSafe esamina l'estensione del nome del file allegato e la confronta con le estensioni presenti nel proprio elenco. Se il tipo di allegato compare nell'elenco e gli allegati di quel tipo sono impostati per essere messi in quarantena, il software di sicurezza Zone Labs trasforma l'estensione del nome del file in ".zl\*" (dove \* è un numero o una lettera).

La modifica dell'estensione del nome del file consente di mettere in quarantena l'allegato impedendone l'esecuzione automatica. Quando si apre il messaggio di posta elettronica contenente l'allegato, il software di sicurezza Zone Labs visualizza un avviso di MailSafe per informare che ha messo in quarantena l'allegato. Se si tenta di aprire l'allegato, un avviso avverte che questa azione è potenzialmente rischiosa. In ogni modo, è possibile aprire l'allegato se si è certi che sia sicuro.

Oltre a verificare i messaggi tramite l'estensione di file, il software di sicurezza Zone Labs analizza gli allegati in entrata alla ricerca di potenziali virus. Se trova un virus, questo viene rimosso dal messaggio prima che possa causare danni. Per ulteriori informazioni sulla protezione dell'antivirus e sui messaggi di posta elettronica, vedere "Scansione della posta elettronica".

La protezione di MailSafe in entrata funziona con qualsiasi applicazione di posta elettronica che utilizza il protocollo POP3 o IMAP.



La protezione di MailSafe in entrata è concepita solo per l'accesso locale. Se il client POP3 è stato configurato per l'accesso remoto, la protezione di MailSafe in entrata potrebbe non essere disponibile.

## Protezione di MailSafe in uscita

La protezione di MailSafe in uscita avverte quando il programma di posta elettronica tenta di inviare un numero di messaggi insolitamente elevato o di inviare un messaggio a un numero di destinatari insolitamente elevato. Ciò impedisce che il computer dell'utente venga utilizzato a sua insaputa per inviare allegati infetti ad altre persone. Inoltre, la protezione di MailSafe in uscita verifica che il programma che sta tentando di inviare messaggi di posta elettronica abbia l'autorizzazione per farlo.

La protezione di MailSafe in uscita funziona con qualsiasi applicazione di posta elettronica che utilizza il protocollo SMTP.

La funzione di protezione di Mailsafe in uscita è disponibile solo in ZoneAlarm Anti-virus, ZoneAlarm Pro e ZoneAlarm Security Suite.

## Attivazione della protezione di MailSafe in entrata

La protezione di MailSafe in entrata è attivata per impostazione predefinita. Quando è attivata, questa funzione mette in quarantena i tipi di allegato elencati nella scheda Allegati.

### Attivare o disattivare la protezione di MailSafe in entrata

1. Selezionare **Protezione posta elettronica | Principale**.
2. Selezionare **Attivata** o **Disattivata**.

Attivata	MailSafe mette in quarantena i tipi di allegato specificati nella scheda Allegati.
Disattivato	MailSafe consente tutti i tipi di allegato.

## Attivazione della protezione di MailSafe in uscita

Per sicurezza, la protezione della posta in uscita è attivata per impostazione predefinita. Quando la protezione in uscita è attivata, le impostazioni di protezione di MailSafe in uscita sono applicate a tutti i programmi autorizzati all'invio della posta.

### Attivare o disattivare la protezione della posta in uscita

1. Selezionare **Protezione posta elettronica | Principale**.
2. Nella sezione Protezione posta elettronica in uscita, selezionare **Attivata** o **Disattivata**.

# Personalizzazione della protezione di MailSafe in entrata

Tutti i tipi di allegato supportati dalla protezione di MailSafe in entrata sono impostati in modo predefinito per essere messi in quarantena. È possibile personalizzare la protezione di MailSafe in entrata modificando l'impostazione dei tipi di allegato in Consenti, oppure aggiungendo nuovi tipi di allegato.

La funzionalità di personalizzazione delle impostazioni della protezione di MailSafe in entrata non è disponibile in ZoneAlarm.

## Visualizzazione dell'elenco di allegati

I tipi di allegato sono elencati in ordine alfabetico. È possibile ordinare l'elenco facendo clic sull'intestazione di colonna. La freccia (^) accanto al nome dell'intestazione indica l'ordine di disposizione. Fare di nuovo clic sulla stessa intestazione per invertire l'ordine.

### Accedere all'elenco di allegati

☞ Selezionare **Protezione posta elettronica**, quindi fare clic sulla scheda **Allegati**.

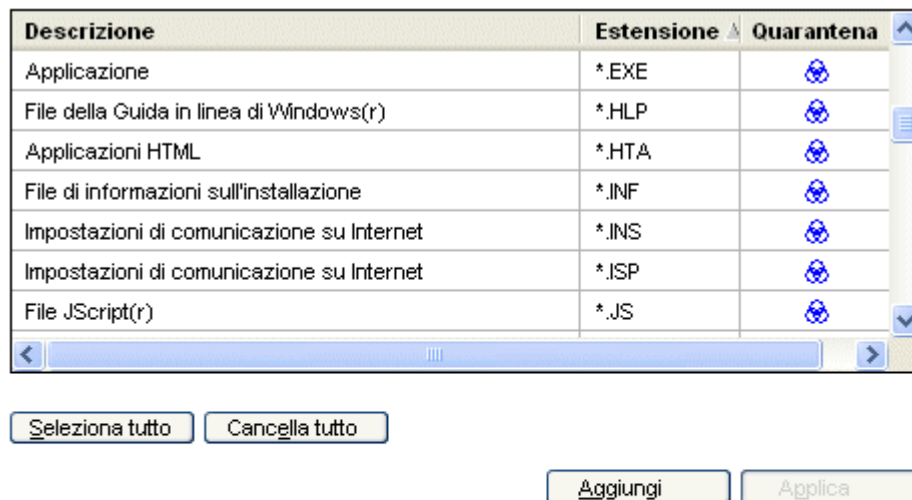


Figura 7-1: Elenco di allegati

## Modifica dell'impostazione di quarantena per un tipo di allegato

Il software di sicurezza Zone Labs è configurato con più di 45 tipi di allegato che sono in grado di contenere worm o altro codice dannoso. Per impostazione predefinita, il

software di sicurezza Zone Labs mette in quarantena tutti questi tipi di allegato. Questi tipi di allegato sono visualizzati nell'elenco della scheda Allegati.

### **Modificare l'impostazione di quarantena per un tipo di allegato specifico**

1. Selezionare **Protezione posta elettronica | Allegati**.
2. Nella colonna Quarantena, fare clic sulla riga di un tipo di estensione.
3. Selezionare **Quarantena** o **Consenti**, quindi fare clic su **Applica**.

## **Aggiunta e rimozione di tipi di allegato**

Se si vogliono mettere in quarantena gli allegati di un tipo che non appare nell'elenco, è possibile aggiungere a quest'ultimo tutti i tipi di allegato possibili.

Per garantire la protezione, il software di sicurezza Zone Labs impedisce la rimozione dei tipi di allegato predefiniti. Tuttavia, è possibile rimuovere qualsiasi tipo di allegato aggiunto all'elenco.

### **Aggiungere un tipo di allegato all'elenco**

1. Selezionare **Protezione posta elettronica | Allegati**.
2. Fare clic su **Aggiungi**.
3. Digitare una descrizione e un'estensione del nome file (con o senza il carattere "."), quindi fare clic su **OK**.
4. Fare clic su **Applica** per salvare le modifiche.

### **Rimuovere un tipo di allegato dall'elenco**

1. Selezionare **Protezione posta elettronica | Allegati**.
2. Nella colonna **Estensioni**, fare clic con il pulsante destro del mouse su un tipo di allegato.
3. Selezionare **Rimuovi**.

## Apertura di un allegato posto in quarantena

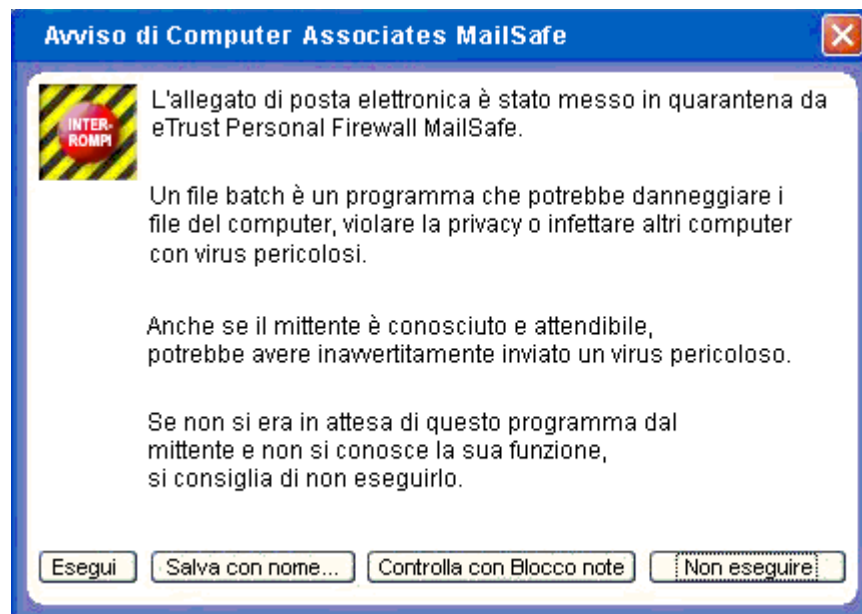
Per visualizzare il codice dell'allegato stesso, è possibile aprire l'allegato in Blocco note.



Per garantire la sicurezza, non bisognerebbe mai aprire un allegato di posta elettronica che è stato messo in quarantena dal software di sicurezza Zone Labs, tranne nei casi in cui il mittente sia una persona fidata che conferma di avere inviato il messaggio intenzionalmente e assicura che l'allegato è sicuro.

### Aprire un allegato posto in quarantena

1. In Esplora risorse, individuare il file da aprire.
2. Fare doppio clic sull'allegato per aprirlo.
3. Quando si tenta di aprire un allegato che è stato messo in quarantena, il software di sicurezza Zone Labs avverte del potenziale rischio di tale azione.



4. Fare clic su **Controlla con Blocco note**.

# Personalizzazione della protezione di MailSafe in uscita

Per impostazione predefinita, viene visualizzato un avviso di protezione di MailSafe in uscita quando l'applicazione di posta elettronica tenta di inviare più di cinque messaggi in due secondi, oppure se un messaggio ha più di cinquanta destinatari. È possibile personalizzare queste impostazioni per ampliare l'intervallo di tempo, aumentare il numero di messaggi e di destinatari consentito o specificare gli indirizzi di posta elettronica a cui è consentito inviare messaggi di posta dal computer.

## Attivazione della protezione di MailSafe in uscita per programma

Quando la protezione di MailSafe in uscita è impostata ad Attivata, la protezione è attivata per tutti i programmi a cui è stata concessa l'autorizzazione a inviare posta elettronica.

È possibile personalizzare la protezione di MailSafe in uscita attivandola o disattivandola per programmi specifici.

Per informazioni sull'impostazione delle autorizzazioni per un programma, vedere "Impostazione di autorizzazioni per programmi specifici".

### Attivare o disattivare la protezione di MailSafe in uscita per un programma

1. Selezionare **Controllo dei programmi | Programmi**.
2. Nella colonna Programmi, fare clic con il pulsante destro del mouse sul nome di un programma, quindi selezionare **Opzioni**.
3. Fare clic sulla scheda **Sicurezza**.
4. Nell'area Protezione posta elettronica in uscita, selezionare la casella di controllo **Attiva protezione posta elettronica in uscita per questo programma**.

Per disattivare la protezione della posta elettronica in uscita, deselezionare questa casella di controllo.

5. Fare clic su **OK**.

## Impostazione delle opzioni di protezione di MailSafe in uscita

Per impostazione predefinita, la protezione di MailSafe in uscita è attivata quando il computer tenta di inviare più di cinque messaggi di posta elettronica in due secondi o un messaggio con più di 50 destinatari.

Dato che anche i messaggi di posta elettronica sicuri potrebbero presentare una di queste caratteristiche o entrambe, potrebbe essere opportuno personalizzare le impostazioni di protezione di MailSafe in uscita per soddisfare meglio le proprie esigenze.

**Personalizzare le impostazioni di protezione di MailSafe in uscita**

1. Selezionare **Protezione posta elettronica | Principale**, quindi fare clic su **Avanzate**.

Viene visualizzata la finestra di dialogo Protezione avanzata della posta elettronica.

2. Nell'area **Mostra avvisi di protezione posta in uscita quando**, scegliere le proprie impostazioni.

Sono inviati troppi messaggi contemporaneamente	Viene visualizzato un avviso di protezione di MailSafe in uscita quando il computer tenta di inviare un numero di messaggi superiore a quello specificato nell'intervallo di tempo specificato.
Un messaggio ha troppi destinatari	Viene visualizzato un avviso di protezione di MailSafe in uscita quando il computer tenta di inviare un messaggio di posta elettronica con un numero di destinatari superiore a quello specificato.
L'indirizzo del mittente non è in questo elenco	Viene visualizzato un avviso di protezione di MailSafe in uscita quando il computer tenta di inviare un messaggio di posta elettronica il cui indirizzo di origine (ossia l'indirizzo nel campo <b>Da:</b> ) non appare nell'elenco. Per evitare che il software di sicurezza Zone Labs blocchi tutta la posta in uscita, assicurarsi che il proprio indirizzo di posta elettronica valido sia nell'elenco.

3. Fare clic su **OK**.



# Filtro della posta indesiderata

Il filtro della posta indesiderata è disponibile in ZoneAlarm Security Suite.

Utilizzare il filtro della posta elettronica per evitare che la posta indesiderata (comunemente denominata *spam*) intasi la posta in arrivo. Il filtro della posta indesiderata supporta Microsoft Outlook e Outlook Express (ai quali si fa riferimento nel presente documento semplicemente come "Outlook").

Durante l'installazione, il software di sicurezza Zone Labs aggiunge la barra degli strumenti del filtro della posta indesiderata a quella del programma di posta Outlook.



Figura 7-2: Barra degli strumenti del filtro della posta indesiderata



Se è stato installato il software di sicurezza Zone Labs ma la barra degli strumenti del filtro della posta indesiderata non appare in Outlook, fare clic con il pulsante destro del mouse sulla barra degli strumenti di Outlook e scegliere **ZoneAlarmOutlookAddin**.

Il filtro della posta indesiderata aggiunge inoltre tre cartelle speciali all'elenco delle cartelle di Outlook: Posta contestata ZoneAlarm, Posta indesiderata ZoneAlarm e Posta fraudolenta ZoneAlarm. Quando il software di sicurezza Zone Labs identifica un messaggio di posta elettronica come indesiderato, fraudolento o contestato, lo pone in una di queste cartelle. Se si utilizza Outlook per accedere a Hotmail, occorre utilizzare le funzioni di blocco dello spam del filtro della posta indesiderata e le cartelle speciali invece di quelle di Hotmail.

## Consentire o bloccare la posta elettronica proveniente da mittenti specifici

Ogni volta che si invia un messaggio di posta elettronica a una nuova persona, il filtro della posta indesiderata aggiunge automaticamente l'indirizzo presente nel campo A all'elenco Consentiti. I messaggi inviati all'utente da tali indirizzi verranno collocati nella posta in arrivo.

Quando si riceve un messaggio di posta elettronica da un mittente presente nell'elenco Bloccati, il filtro della posta indesiderata sposta automaticamente il messaggio sulla cartella di Outlook denominata *Posta indesiderata ZoneAlarm*.

Se arriva un messaggio di posta elettronica indesiderato nella Posta in arrivo di Outlook, è possibile aggiungere facilmente il mittente di tale messaggio all'elenco Bloccati.

### **Aggiungere indirizzi di posta elettronica all'elenco Consentiti o Bloccati**

1. Nel programma di posta Outlook o Outlook Express, selezionare un messaggio di posta elettronica.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm**, quindi scegliere **Consenti mittente** o **Blocca mittente**.

## **Consentire o bloccare la posta elettronica proveniente da società specifiche**

Il filtro della posta indesiderata consente di aggiungere tutti gli indirizzi di posta elettronica provenienti da una particolare società o dominio di rete all'elenco delle società consentite o delle società bloccate.

### **Aggiungere società all'elenco Consentiti o Bloccati**

1. Nel programma di posta Outlook o Outlook Express, selezionare un messaggio di posta elettronica.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm**, quindi scegliere **Consenti società mittente** o **Blocca società mittente**.

Il filtro della posta indesiderata aggiunge la parte del dominio dell'indirizzo del mittente (per esempio, *esempio.com*) all'elenco degli indirizzi consentiti o bloccati.

## **Aggiunta di contatti all'elenco Consentiti**

È possibile eseguire la scansione della cartella dei contatti predefinita nel programma di posta per aggiungere contatti all'elenco di mittenti dai quali si desidera ricevere la posta elettronica.

### **Aggiungere contatti all'elenco Consentiti**

1. Aprire il programma di posta Outlook o Outlook Express.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm**, quindi scegliere **Completa elenco dei consentiti**.

## **Scansione della Posta in arrivo**

È possibile eseguire la scansione del contenuto della Posta in arrivo alla ricerca di posta fraudolenta e spam.

### **Scansione della posta in arrivo**

1. Aprire il programma di posta Outlook o Outlook Express.
2. Selezionare la posta in arrivo da sottoporre a scansione.

3. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm**, quindi scegliere **Scansione posta in arrivo**.



L'opzione Scansione posta in arrivo può essere usata per la scansione di account IMAP, POP3 e Hotmail creati in Outlook Express e account POP3 creati in Outlook. Non è possibile, invece, eseguire la scansione di account IMAP creati in Outlook.

## Consentire la posta elettronica proveniente da liste di distribuzione

Se si riceve o si invia posta elettronica a più indirizzi contenuti in una lista di distribuzione, il filtro della posta indesiderata potrebbe bloccare il nome della lista a meno che non sia stato aggiunto alla scheda Elenchi.

### Consentire la posta elettronica proveniente da mailing list

1. Aprire il programma di posta Outlook o Outlook Express.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm | Configura preferenze | Elenchi**.
3. Fare clic su **Aggiungi**.
4. Digitare l'indirizzo di posta elettronica della lista di distribuzione nell'area di immissione del testo, quindi fare clic su **OK**.

Il filtro della posta indesiderata aggiunge l'indirizzo di posta elettronica della lista di distribuzione all'elenco degli indirizzi consentiti.

5. Fare clic su **Chiudi** per salvare le modifiche e chiudere la scheda Elenchi.

## Segnalazione di posta indesiderata

Il filtro della posta indesiderata consente all'utente di arricchire il database del Filtro collaborativo di Zone Labs.

Il filtro della posta indesiderata non invia mai posta elettronica di alcun tipo dal computer senza l'autorizzazione dell'utente. Quando si aggiungono istanze di posta indesiderata al database del filtro collaborativo, è possibile scegliere di inviare il messaggio di posta elettronica o un riepilogo elaborato digitalmente (a volte definito "hashed") della posta elettronica che rimuove dal messaggio tutto il contenuto, le intestazioni e le informazioni che identificano l'utente. L'invio dell'intero messaggio

consente l'analisi completa del contenuto; l'invio di un riepilogo elaborato digitalmente del messaggio garantisce la completa privacy.



MailFrontier, un partner di Zone Labs attendibile, gestisce il database del filtro collaborativo di Zone Labs. È possibile visualizzare il testo completo dell'informativa sulla privacy di MailFrontier all'indirizzo: <http://www.mailfrontier.com/privacy.html>

### Segnalare posta indesiderata

1. Nel programma di posta Outlook o Outlook Express, selezionare un messaggio di posta elettronica.
2. Nella barra degli strumenti del filtro della posta indesiderata:
  - Per inviare la posta indesiderata, fare clic su **Opzioni di ZoneAlarm**, quindi scegliere **Rapporto posta indesiderata**.
  - Per inviare un riepilogo elaborato digitalmente della posta elettronica indesiderata, fare clic su **Posta indesiderata**.
3. Nella finestra di dialogo **Contribuisci con posta elettronica**, fare clic su **OK**.

Il filtro della posta indesiderata segnala questa posta al database del filtro collaborativo e sposta il messaggio nella cartella speciale di Outlook **Posta indesiderata ZoneAlarm**.



Per ripristinare la posta elettronica identificata erroneamente come indesiderata, selezionarla nella cartella Posta indesiderata ZoneAlarm e fare clic su Posta accettata. La posta elettronica viene ripristinata nella Posta in arrivo di Outlook.

## Segnalazione di posta elettronica fraudolenta

Il filtro della posta indesiderata consente all'utente di segnalare istanze di posta fraudolenta (a volte definita come *phishing*) a Zone Labs.

Il filtro della posta indesiderata non invia mai posta elettronica di alcun tipo dal computer senza l'autorizzazione dell'utente. Quando si segnala posta elettronica fraudolenta, il filtro della posta indesiderata inoltra il messaggio originale completo a Zone Labs.

Zone Labs non divulga mai l'indirizzo di posta elettronica, il nome o altri dati personali dell'utente contenuti in un messaggio di posta elettronica fraudolento, tranne quando necessario per indagare e perseguire il responsabile dello stesso.

Zone Labs inoltra parti selezionate del messaggio segnalato a enti governativi e organi di legge competenti in materia di frode di posta elettronica. È previsto dalla legge che tali enti proteggano la riservatezza delle informazioni contenute nel messaggio. Zone Labs informa separatamente i privati o le istituzioni minacciate inoltrando loro solo le informazioni necessarie ad avvisarli.

### Segnalare posta elettronica fraudolenta

1. Nel programma di posta Outlook o Outlook Express, selezionare un messaggio di posta elettronica.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm**, quindi scegliere **Rapporto messaggi fraudolenti**.
3. Nella finestra di dialogo **Contribuisci con posta elettronica**, fare clic su **OK**.

Il filtro della posta indesiderata segnala la posta fraudolenta a Zone Labs e sposta il messaggio nella cartella speciale di Outlook *Posta fraudolenta ZoneAlarm*. Se si utilizza Outlook per accedere a Hotmail, occorre utilizzare le funzioni di blocco dello spam del filtro della posta indesiderata e le cartelle speciali invece di quelle di Hotmail.



MailFrontier, un partner di Zone Labs attendibile, gestisce l'elaborazione della posta elettronica fraudolenta per Zone Labs. È possibile visualizzare il testo completo dell'informativa sulla privacy di MailFrontier all'indirizzo:

<http://www.mailfrontier.com/privacy.html>

## Definizione delle opzioni dei messaggi di posta indesiderata

Il filtro della posta indesiderata utilizza tre tecniche di filtro dei messaggi: *filtro collaborativo*, *filtri dei messaggi* e *filtri lingue straniere*. Le impostazioni del filtro determinano il modo in cui i messaggi vengono trattati quando ricevuti da mittenti sconosciuti.

### *Filtro collaborativo*

Il filtro collaborativo utilizza le informazioni estratte dalla segnalazione della posta indesiderata dall'utente e da altri utenti del software di sicurezza Zone Labs per determinare la probabilità che nuovi messaggi provenienti da mittenti sconosciuti siano spam.

### *Filtri dei messaggi*

I filtri dei messaggi utilizzano regole euristiche per l'analisi delle caratteristiche della posta elettronica comuni a vari tipi di posta indesiderata.

### *Filtri lingue straniere*

I filtri delle lingue straniere bloccano la posta elettronica contenente lingue non europee (il filtro della posta indesiderata gestisce automaticamente la posta nelle comuni lingue europee, quali francese, tedesco o spagnolo).

### Personalizzare le opzioni di filtro dei messaggi

1. Aprire il programma di posta Outlook o Outlook Express.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm | Configura preferenze | Messaggi**.

<b>Filtro collaborativo</b>	Spostare il dispositivo di scorrimento per regolare la reattività alle caratteristiche della posta indesiderata segnalata da altri utenti del software di sicurezza Zone Labs.
-----------------------------	--

---

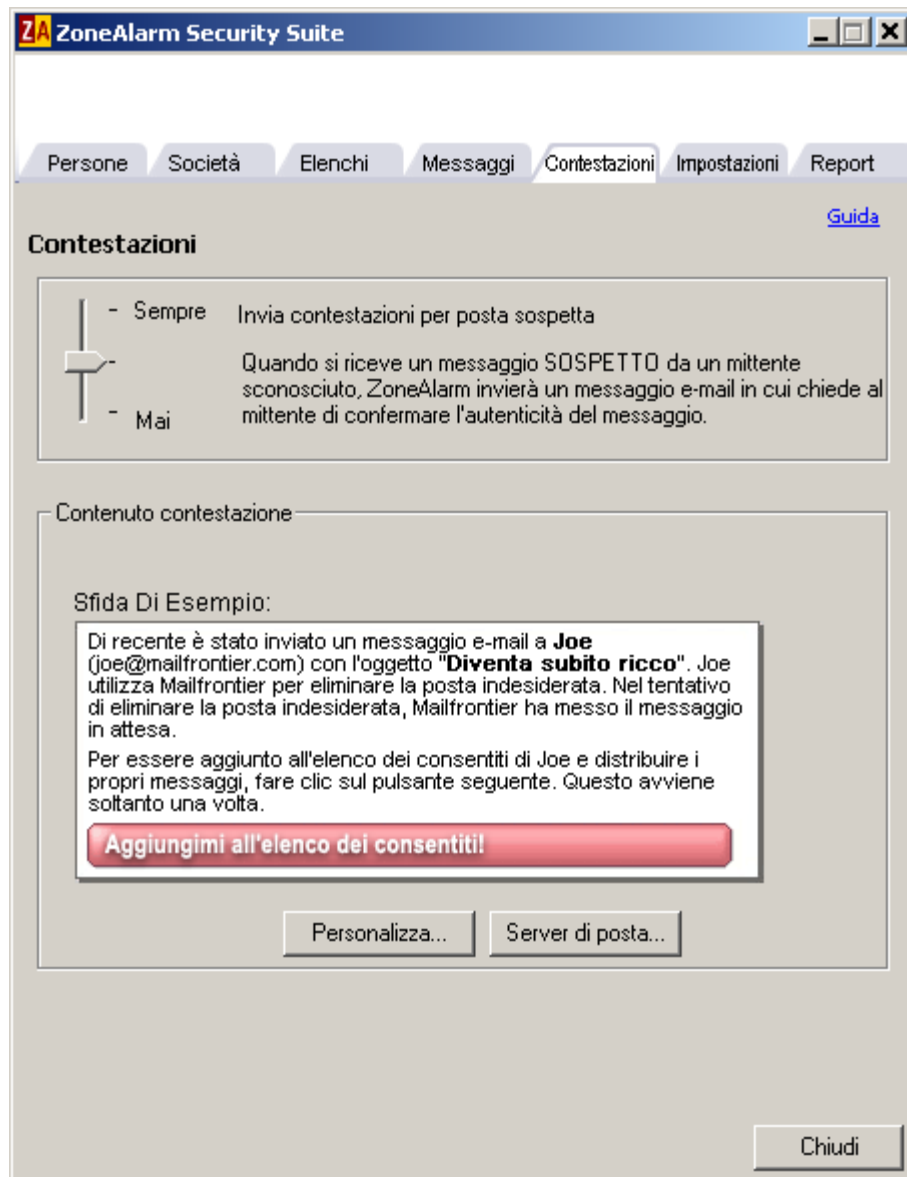
<b>Filtri dei messaggi</b>	Spostare il dispositivo di scorrimento disponibile in quest'area per regolare la reattività alla posta indesiderata comune. È inoltre possibile regolare la reattività a specifiche categorie di posta indesiderata.
<b>Filtri delle lingue</b>	In quest'area, fare clic su Configura, quindi scegliere le lingue da bloccare.

3. Fare clic su **Chiudi**.

## **Contestazione di posta elettronica proveniente da mittenti sconosciuti**

È possibile scegliere che il filtro della posta indesiderata risponda a un messaggio proveniente da un mittente sconosciuto con un messaggio di contestazione. Poiché la posta indesiderata contiene raramente un indirizzo valido, la non risposta a un messaggio di contestazione conferma che si tratta di posta indesiderata.

Il messaggio di contestazione richiede al mittente di fare clic su un pulsante nel messaggio per confermare che è lui l'autore. Se il mittente fa clic sul pulsante, il filtro della posta indesiderata sposta il messaggio dalla cartella speciale di Outlook **Posta contestata ZoneAlarm** alla Posta in arrivo di Outlook.



**Figura 7-3: Scheda con le opzioni di contestazione**

Per i messaggi provenienti da un mittente sconosciuto, è possibile scegliere se inviare sempre un messaggio di contestazione, se inviare una contestazione solo quando il messaggio in arrivo sembra essere posta indesiderata oppure non inviare mai una contestazione. Inoltre, è possibile personalizzare il messaggio di contestazione inviato agli utenti.

#### **Attivare i messaggi di contestazione**

1. Aprire il programma di posta Outlook o Outlook Express.

2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm | Configura preferenze | Contestazioni**.
3. Nella sezione **Contestazioni**, utilizzare il dispositivo di scorrimento per scegliere quando inviare un messaggio di contestazione.

Alta	<p>Il software di sicurezza Zone Labs invierà messaggi di contestazione a tutti i messaggi di posta elettronica ricevuti, a meno che non siano noti come validi all'utente (presenti sull'elenco Consentiti) o a MailFrontier (mittenti validi noti).</p> <p>Qualsiasi messaggio di posta elettronica ricevuto e immediatamente classificabile come indesiderato, viene inviato direttamente alla cartella Posta indesiderata ZoneAlarm per la successiva eliminazione e NON viene inviato alcun messaggio di contestazione.</p>
Bassa	<p>Il software di sicurezza Zone Labs invierà messaggi di contestazione ai messaggi incerti.</p> <p>Il software di sicurezza Zone Labs invierà messaggi di contestazione solo ai messaggi di posta elettronica che non vengono determinati con certezza come spam o messaggi validi. Si tratta solitamente di una piccola percentuale della posta ricevuta.</p>
Disattivato	<p>I messaggi di posta elettronica di contestazione non vengono inviati.</p> <p>Il software di sicurezza Zone Labs non invierà messaggi di posta elettronica di contestazione. Spostare il dispositivo di scorrimento verso l'alto per attivare i messaggi di contestazione per eliminare la posta indesiderata inviata da computer spammer.</p>

4. Per aggiungere un messaggio personale a quello predefinito di contestazione, fare clic su **Personalizza**, digitare il nome e il messaggio personale, quindi fare clic su **OK**.
5. Fare clic su **Chiudi**.

Il filtro della posta indesiderata sposta il messaggio nella cartella **Posta contestata ZoneAlarm**.



Nell'attesa di una risposta a un messaggio di contestazione, il filtro della posta indesiderata memorizza l'indirizzo dell'utente. Non appena la contestazione è stata elaborata, il filtro della posta indesiderata scarta l'indirizzo. Nel caso di difficoltà nell'invio dei messaggi di contestazione, vedere il paragrafo seguente "Definizione del server della posta in uscita".

## Definizione del server della posta in uscita

Per inviare messaggi di contestazione, il filtro della posta indesiderata necessita dell'autorizzazione a inviare posta elettronica. Nella maggior parte dei casi il filtro della posta indesiderata utilizza il server della posta in uscita predefinito di Outlook. Nel caso di difficoltà nell'invio di messaggi di contestazione, potrebbe essere necessario specificare il nome del server della posta in uscita.



### **Specificare il nome del server della posta in uscita**

1. Aprire il programma di posta Outlook o Outlook Express.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm | Configura preferenze | Contestazioni**.
3. Nella sezione Contenuto contestazione, fare clic su **Server di posta**.
4. Digitare il nome del server della posta in uscita, quindi fare clic su **OK**.
5. Fare clic su **Chiudi**.

## **Personalizzazione delle impostazioni del filtro della posta indesiderata**

Per impostazione predefinita, il filtro della posta indesiderata conserva i messaggi fraudolenti nella cartella **Posta fraudolenta ZoneAlarm** finché non vengono eliminati manualmente. È possibile specificare per quanto tempo i messaggi vengono memorizzati nelle cartelle **Posta indesiderata ZoneAlarm** e **Posta contestata ZoneAlarm**, nonché rendere automatica la segnalazione della posta elettronica fraudolenta e configurare l'inoltro a periferiche wireless.

### **Specificare la durata di memorizzazione della posta indesiderata**

1. Aprire il programma di posta Outlook o Outlook Express.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm | Configura preferenze | Impostazioni**.
3. Nell'area **Impostazioni cartella Posta indesiderata**, fare clic su **Configura**.
4. Digitare il numero di giorni di conservazione della posta indesiderata nelle cartelle **Posta indesiderata ZoneAlarm** e **Posta contestata ZoneAlarm**.

Il filtro della posta indesiderata sposta i messaggi rimasti nella cartella per il numero specificato di giorni nella cartella Posta eliminata di Outlook senza chiedere conferma all'utente.

5. Fare clic su **Chiudi**.

### **Attivare la segnalazione automatica della posta elettronica fraudolenta**

1. Aprire il programma di posta Outlook o Outlook Express.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm | Configura preferenze | Impostazioni**.
3. Nella sezione **E-mail rapporto automatico sulla frode**, selezionare **Attiva il rapporto automatico**.
4. Fare clic su **Chiudi**.

### **Configurare una connessione wireless**

1. Aprire il programma di posta Outlook o Outlook Express.

2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm | Configura preferenze | Impostazioni**.
3. Nell'area **Supporto dispositivo wireless**, fare clic su **Configura**.
4. Nella finestra di dialogo **Supporto wireless ZoneAlarm**, digitare l'indirizzo di posta elettronica della periferica wireless.  
  
È inoltre possibile scegliere di inoltrare soltanto le intestazioni della posta elettronica e di specificare il numero di messaggi convalidati inoltrati alla periferica in un periodo di 24 ore.
5. Se occorre specificare un server di posta non predefinito, fare clic su **Server di posta**, digitare il nome del server della posta in uscita, quindi fare clic su **OK**.
6. Fare clic su **Chiudi** per salvare le modifiche e chiudere la scheda Impostazioni.

#### Personalizzare i messaggi di conferma

1. Aprire il programma di posta Outlook o Outlook Express.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm | Configura preferenze | Impostazioni**.
3. Nella sezione **Mostra conferme**, specificare le impostazioni desiderate.

Contribuire con posta indesiderata	Visualizza un avviso prima di inviare posta indesiderata a Zone Labs.
Contribuire con posta elettronica fraudolenta	Visualizza un avviso prima di inviare posta elettronica fraudolenta a Zone Labs.

4. Fare clic su **OK**.

### Ripristinare la posta elettronica erroneamente identificata come indesiderata

Il filtro della posta indesiderata aggiunge tre cartelle speciali all'elenco delle cartelle di Outlook: **Posta contestata ZoneAlarm**, **Posta indesiderata ZoneAlarm** e **Posta fraudolenta ZoneAlarm**. Quando il software di sicurezza Zone Alarm identifica un messaggio di posta elettronica come indesiderato, fraudolento o di contestazione, lo pone in una di queste cartelle speciali.

Se si utilizza Outlook per accedere a Hotmail, occorre utilizzare le funzioni di blocco dello spam del filtro della posta indesiderata e le cartelle speciali invece di quelle di Hotmail.

È possibile ripristinare la posta che il filtro della posta indesiderata ha erroneamente collocato in una cartella speciale nella Posta in arrivo di Outlook.

### Ripristinare la posta elettronica erroneamente identificata come indesiderata

1. Nel programma di posta Outlook o Outlook Express, nelle cartelle **Posta contestata ZoneAlarm**, **Posta indesiderata ZoneAlarm** o **Posta fraudolenta ZoneAlarm**, selezionare un messaggio di posta elettronica.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Posta accettata.**:

Il filtro della posta indesiderata ripristina il messaggio selezionato nella Posta in arrivo di Outlook.

### Visualizzare i report del filtro della posta indesiderata

Utilizzare la scheda Report del filtro della posta indesiderata per visualizzare un riepilogo dell'attività di elaborazione della posta.

#### Visualizzare i report del filtro della posta indesiderata

1. Aprire il programma di posta Outlook o Outlook Express.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm | Configura preferenze | Report.**
3. Scegliere uno dei quattro tipi di report:

<b>Posta indesiderata al giorno</b>	Il numero totale di messaggi di posta elettronica legittimi e indesiderati ricevuti al giorno.
<b>Motivi</b>	I motivi per i quali il filtro della posta indesiderata ha bloccato i messaggi al giorno
<b>Cronologia totale Posta indesiderata al giorno</b>	Il numero totale di messaggi di posta elettronica legittimi e indesiderati ricevuti da quando il software di sicurezza Zone Labs è stato installato.
<b>Motivi totali</b>	Il numero totale di motivi per i quali il filtro della posta indesiderata ha bloccato la posta elettronica in arrivo da quando il software di sicurezza Zone Labs è stato installato.

4. Fare clic su **Chiudi** per chiudere la scheda Report.

# Protezione antivirus per la posta elettronica

Oltre alla protezione offerta da MailSafe per la posta elettronica in arrivo, ZoneAlarm Anti-virus e ZoneAlarm - Suite offrono la protezione aggiuntiva garantita dalla scansione antivirus dei messaggi di posta elettronica in arrivo. A differenza di MailSafe, questa scansione della posta elettronica è in grado di rilevare i virus nel corpo di un messaggio, oltre che negli allegati.

☞ Attivazione della scansione della posta elettronica

☞ Come viene gestita la posta elettronica infetta

## Attivazione della scansione della posta elettronica

Gli utenti di ZoneAlarm Anti-virus e ZoneAlarm Security Suite hanno la protezione antivirus per la posta elettronica attivata per impostazione predefinita.

### Attivare o disattivare la scansione della posta elettronica

1. Selezionare **Antivirus/Antispyware | Principale**.
2. Nell'area Protezione, fare clic su **Opzioni avanzate**.  
Viene visualizzata la finestra di dialogo Opzioni avanzate.
3. Sotto Gestione virus, selezionare **Scansione posta elettronica**.
4. Selezionare o deselezionare la casella di controllo **Attiva scansione posta elettronica**, quindi fare clic su **OK**.

## Come viene gestita la posta elettronica infetta

Quando il software di sicurezza Zone Labs rileva un'infezione in un allegato di posta elettronica, il file infetto viene rimosso e viene allegato un report di infezione al messaggio. Il report di infezione è un file di testo contenente informazioni sull'allegato rimosso dal messaggio di posta elettronica, fra cui il nome file dell'infezione.



Figura 7-4: Esempio di report di infezione

Gli allegati infetti sono rinominati con l'estensione di file `.z16` in modo che non possano più essere aperti direttamente.



Se si utilizza Eudora e si hanno più report di infezione nella posta in arrivo, il nome del report di infezione può contenere un numero prima dell'estensione `.txt`.

Quando si esegue Windows 98, la caratteristica di scansione antivirus della posta elettronica rinomina MailSafe in *isafe.exe* invece del nome del programma di posta elettronica del computer.

Per ulteriori informazioni sulla protezione del computer dai virus, vedere il Capitolo 6, "Protezione da spyware e virus", a pagina 93.



# Capitolo

## Protezione della privacy

# 8

Tanto tempo fa, il World Wide Web non conteneva che pagine di testo inoffensive. Oggi, le pagine Web spesso contengono elementi che divulgano informazioni private dell'utente, interrompono il lavoro con noiose finestre pop-up e possono persino creare danni sul computer. Inoltre, i file che restano nel computer quando si utilizza il Web possono rallentare le prestazioni del computer stesso. L'uso della protezione della privacy consente di difendersi dall'uso improprio di cookie, annunci pubblicitari e contenuto Web dinamico, nonché di liberare periodicamente il computer dai file di Internet non necessari.

La funzione Privacy è disponibile in ZoneAlarm Pro e ZoneAlarm Pro Security Suite.

### Argomenti:

- "Comprendere la protezione della privacy", a pagina 142
- "Impostazione delle opzioni di privacy generali", a pagina 143
- "Come usare Privacy Advisor", a pagina 145
- "Impostazione delle opzioni di privacy per siti Web specifici", a pagina 146
- "Personalizzazione del controllo dei cookie", a pagina 149
- "Personalizzazione del blocco degli annunci", a pagina 152
- "Personalizzazione del controllo del codice mobile", a pagina 154
- "Comprensione di Cache Cleaner", a pagina 156

# Comprendere la protezione della privacy

La protezione della privacy aiuta a gestire gli elementi dei siti Web comunemente utilizzati per visualizzare contenuto pubblicitario o per raccogliere dati sull'utente e sulle sue abitudini di esplorazione del Web. Inoltre, le impostazioni relative alla privacy proteggono dall'uso improprio di determinati tipi di contenuto Web dinamico o codice mobile.

*Controllo cookie* impedisce agli autori di annunci pubblicitari di spiare le abitudini di utilizzo di Internet dell'utente e impedisce che le informazioni confidenziali (le password, per esempio) vengano memorizzate nei cookie, dove potrebbero essere rubate se un hacker riuscisse ad accedere al computer.

*Blocco annunci* impedisce che annunci pubblicitari indesiderati disturbino il lavoro su Internet. Con il software di sicurezza Zone Labs è possibile bloccare tutti i tipi di annunci (*annuncio su banner*, *annuncio animato* e così via) o solo dei tipi specifici.

*Controllo codice mobile* impedisce agli hacker di utilizzare il contenuto attivo delle pagine Web come applet Java, *controlli ActiveX* e plug-in per compromettere la sicurezza o danneggiare il computer. È necessario ricordare che molti siti Web legittimi utilizzano il codice mobile e che l'attivazione del controllo del codice mobile potrebbe influire sulla funzionalità di tali siti Web.

*Cache Cleaner* mantiene il computer sempre ordinato eliminando i file in eccesso raccolti durante l'esplorazione del Web e l'utilizzo del computer. Inoltre tutela la privacy cancellando la cronologia degli URL, la cache del browser e altri file specificati dall'utente.

La funzione Privacy è disponibile in ZoneAlarm Pro e ZoneAlarm Security Suite.



# Impostazione delle opzioni di privacy generali

La protezione della privacy per il browser è attivata solo se viene selezionata durante l'installazione. Se non si attiva la privacy durante l'installazione, è possibile attivarla manualmente.

Il gruppo di funzioni per la privacy che include le opzioni di privacy generali è disponibile in Zone Alarm Pro e ZoneAlarm Security Suite.

## Impostazione dei livelli di protezione della privacy

Impostando il livello di protezione della privacy, si stabilisce se consentire o bloccare cookie, annunci pubblicitari e codice mobile.

### Impostare i livelli di privacy

1. Selezionare **Privacy | Principale**.
2. Nell'area Controllo cookie, trascinare il dispositivo di scorrimento sull'impostazione desiderata.

Alta	Blocca tutti i cookie eccetto i cookie di sessione. Questa impostazione potrebbe impedire il caricamento di alcuni siti Web.
Media	Impedisce ai cookie permanente e ai cookie di terze parti di eseguire il tracciamento dei siti Web. Consente i cookie per servizi personalizzati.
Disattivato	Consente tutti i cookie.

3. Nell'area Blocco annunci, trascinare il dispositivo di scorrimento sull'impostazione desiderata.

Alta	Blocca tutti gli annunci. Blocca tutti gli annunci pop-up/pop-under e gli annuncio animato.
Media	Blocca tutti gli annunci pop-up/pop-under e gli annunci animati. Consente gli annunci su banner.
Disattivato	Consente tutti gli annunci.

4. Nell'area Controllo codice mobile, selezionare **Attivato** o **Disattivato**.
5. Fare clic su **OK**.

## Applicazione della protezione della privacy a programmi diversi dai browser

Per impostazione predefinita, la protezione della privacy viene applicata solo a programmi browser standard come Internet Explorer. Si può anche attivare la protezione della privacy per qualsiasi programma sul computer.

**Applicare il controllo della protezione della privacy a un programma diverso da un browser**

1. Selezionare **Controllo dei programmi | Programmi**.
2. Nella colonna Programmi, selezionare il nome di un programma, quindi fare clic su **Opzioni**.  
Viene visualizzata la finestra di dialogo Opzioni programma.
3. Fare clic sulla scheda **Sicurezza**.
4. Nell'area Opzioni filtro, selezionare la casella di controllo **Attiva Privacy per questo programma**.

# Come usare Privacy Advisor

Privacy Advisor appare sotto forma di avviso quando il software di sicurezza Zone Labs blocca i cookie o il codice mobile; l'avviso permette di consentire tali elementi per una determinata pagina.



Figura 8-1: Privacy Advisor

Il gruppo di funzioni per la privacy che include Privacy Advisor è disponibile in Zone Alarm Pro e ZoneAlarm Security Suite. Onde evitare che Privacy Advisor appaia ogni volta che gli elementi di pagina Web vengono bloccati, selezionare la casella di controllo **Disattiva Privacy Advisor**.



Sebbene la verifica dei siti sia visualizzata nella stessa finestra di avviso di Privacy Advisor, queste due funzioni sono attivabili e disattivabili in modo indipendente. Se si disattiva Privacy Advisor, l'avviso di verifica dei siti sarà visualizzato da solo e viceversa. Per ulteriori informazioni sulla verifica dei siti, vedere "Licenza, registrazione e supporto", a pagina 28.

## Attivare o disattivare Privacy Advisor

1. Selezionare **Privacy | Principale**.
2. Nell'area Controllo cookie, fare clic su **Personalizza**.  
Viene visualizzata la finestra di dialogo Impostazioni personalizzate per la privacy.
3. Nell'area Privacy Advisor, deselezionare la casella di controllo **Mostra Privacy Advisor**.
4. Fare clic su **OK**.



Per visualizzare i dettagli o modificare le impostazioni della privacy immediatamente, fare clic sul collegamento **Fare clic qui per i dettagli**. Il software di sicurezza Zone Labs apre il pannello Privacy.

# Impostazione delle opzioni di privacy per siti Web specifici

Quando si esplora Internet, i siti visitati vengono aggiunti all'elenco della privacy, dove è possibile specificare le opzioni di privacy personalizzate per ogni sito. Si può anche aggiungere un sito all'elenco per personalizzare le impostazioni relative alla privacy. Il gruppo di funzioni per la privacy è disponibile in ZoneAlarm Pro e ZoneAlarm Security Suite.

## Visualizzazione dell'elenco della privacy

L'elenco visualizza i siti visitati nella sessione corrente del software di sicurezza Zone Labs, nonché i siti per cui esistono impostazioni personalizzate in precedenza. Se non si personalizzano le impostazioni per un sito visitato, questo viene eliminato dall'elenco quando si spegne il computer o si chiude il software di sicurezza Zone Labs.



La protezione della privacy è applicata a livello di dominio, anche se nell'elenco dei siti appare un sottodominio. Per esempio, se si aggiunge manualmente il sottodominio news.google.com all'elenco, la protezione della privacy sarà applicata all'intero dominio google.com.

## Accedere all'elenco della privacy

Selezionare **Privacy** | **Elenco siti**.

Sito ▲	Modificato	Codice mobile	Controllo cookie			Web beacon	Intestazione privata
			Sessione	Permanente	Terze parti		
ca.com		X	✓	✓	X	✓	✓
calcio.com		✓	✓	X	X	✓	✓
computerassociates.com		✓	✓	✓	X	✓	✓
ebay.com		✓	✓	X	X	✓	✓
italiano.com		X	✓	✓	X	✓	✓
msn.com		X	✓	✓	X	✓	✓
zonelabs.com		✓	✓	✓	X	✓	✓

Figura 8-2: Elenco della privacy

L'icona di una matita nella colonna Modificato indica che esistono delle impostazioni della privacy personalizzate per tale sito e che quest'ultimo resterà nell'elenco.



L'utilizzo di software di terze parti per il blocco di annunci insieme a software di sicurezza Zone Labs potrebbe compromettere il normale completamento dell'elenco della privacy.

## Aggiunta di siti all'elenco della privacy

Per personalizzare le impostazioni relative alla privacy di un sito che non appare nell'elenco, è possibile aggiungere tale sito manualmente, quindi modificare le relative opzioni di privacy.

### Aggiungere un sito all'elenco della privacy

1. Selezionare **Privacy** | **Elenco siti**.
2. Fare clic su **Aggiungi**.  
Viene visualizzata la finestra di dialogo Aggiungi sito.
3. Nel campo **URL**, immettere l'URL del sito da aggiungere, quindi fare clic su **OK**.  
L'URL deve essere un nome host completo, per esempio `www.yahoo.com`.



Se si utilizza AOL con ZoneAlarm Pro ed è stata attivata la protezione della privacy, viene aggiunto all'elenco della privacy il sito `ie3.proxy.aol.com` quando si visita un sito qualsiasi durante una sessione AOL. Per esempio, se durante una sessione AOL si visita il sito `www.cnn.com`, viene aggiunto all'elenco della privacy solo il sito proxy di AOL, `ie3.proxy.aol.com`. Le impostazioni della privacy per il sito `ie3.proxy.aol.com` avranno effetto su tutti i siti visitati in AOL. Se si aggiunge manualmente un sito all'elenco della privacy, le impostazioni della privacy per tale sito saranno ignorate e saranno effettive solo le impostazioni di sicurezza per il sito proxy di AOL, `ie3.proxy.aol.com`.

## Modifica dei siti nell'elenco della privacy

È possibile personalizzare il comportamento di Controllo cookie, Blocco annunci e Controllo codice mobile modificando le opzioni di privacy dei siti nell'elenco della privacy.

1. Selezionare **Privacy** | **Elenco siti**.
2. Nella colonna Sito, selezionare il sito da modificare, quindi fare clic su **Opzioni**.  
Viene visualizzata la finestra di dialogo Opzioni sito.

3. Fare clic sulla scheda Cookie, Blocco annunci o Codice mobile.

Per ricevere aiuto nella selezione delle opzioni personalizzate, vedere "Personalizzazione del controllo dei cookie", a pagina 149, "Personalizzazione del blocco degli annunci", a pagina 152 e "Personalizzazione del controllo del codice mobile", a pagina 154.

4. Specificare le opzioni, quindi fare clic su **OK**.

# Personalizzazione del controllo dei cookie

I cookie di Internet consentono ai siti di commercio elettronico (come Amazon, per esempio) di riconoscere gli utenti appena questi visitano il sito e di personalizzare le pagine. Tuttavia, i cookie possono anche essere utilizzati per registrare informazioni sulle abitudini di esplorazione del Web e fornirle a società che si occupano di marketing e di pubblicità.

Per impostazione predefinita, il Controllo cookie è disabilitato e sono consentiti tutti i tipi di cookie. All'occorrenza, è possibile bloccare tutti i cookie impostando il livello Alto, che offre una protezione completa contro tutti i tipi di abuso dei cookie, ma a scapito della comodità di utilizzo offerta da questi elementi.

All'occorrenza, è possibile bloccare tutti i cookie impostando il livello Alto, che offre una protezione completa contro tutti i tipi di abuso dei cookie, ma a scapito della comodità di utilizzo offerta da questi elementi.

È possibile personalizzare il controllo dei cookie specificando quali tipi di cookie sono bloccati e, se i cookie sono consentiti, quando devono scadere.

Il gruppo di funzioni per la privacy che comprende il Controllo cookie è disponibile in ZoneAlarm Pro e ZoneAlarm Security Suite.

## Blocco dei cookie di sessione

I cookie di sessione sono memorizzati nella cache del browser durante l'esplorazione di un sito Web e scompaiono quando si chiude la finestra del browser. I cookie di sessione sono il tipo di *cookie* più sicuro, data la loro durata.

### Bloccare cookie di sessione

1. Selezionare **Privacy | Principale**.
2. Nell'area Controllo cookie, fare clic su **Personalizza**.
3. Nell'area Cookie di sessione, selezionare la casella di controllo **Blocca cookie di sessione**.
4. Fare clic su **OK**.

## Blocco dei cookie permanenti

I cookie permanenti sono registrati sul disco rigido dai siti Web visitati, in modo che questi ultimi li possano recuperare alla successiva visita dell'utente. Benché utili, sono fonte di vulnerabilità perché memorizzano in un file di testo informazioni personali, sul computer o sull'utilizzo di Internet.

### Bloccare i cookie permanenti

1. Selezionare **Privacy | Principale**.

2. Nell'area Controllo cookie, fare clic su **Personalizza**.
3. Nell'area Cookie permanenti, selezionare la casella di controllo **Blocca cookie permanenti**.
4. Fare clic su **OK**.

## Blocco di cookie di terze parti

Un cookie di terze parti è un tipo di cookie permanente posizionato sul computer non dal sito Web che si sta visitando, ma da un autore di pubblicità o da altre terze parti. Questi cookie sono comunemente usati per trasmettere informazioni sull'attività Internet a quelle terze parti.

### Bloccare cookie di terze parti

1. Selezionare **Privacy | Principale**.
2. Nell'area Controllo cookie, fare clic su **Personalizza**.
3. Nell'area Cookie di terze parti, specificare il tipo o i tipi di cookie da bloccare.

Blocca cookie di terze parti	Blocca i cookie provenienti da siti Web di terze parti.
Disattiva Web beacon	Impedisce agli autori di pubblicità di scoprire quali pubblicità e quali pagine Web sono state visualizzate dagli utenti. I Web beacon bloccati appaiono come aree vuote.
Rimuovi informazioni di intestazione private	Impedisce il trasferimento di indirizzo IP, nome della workstation, nome di accesso e altre informazioni personali verso origini di terze parti.

## Impostazione di una data di scadenza per i cookie

I siti che utilizzano i cookie permanenti potrebbero impostare tali cookie affinché rimangano attivi per alcuni giorni, diversi mesi o a tempo indefinito. Mentre è attivo, un cookie può essere utilizzato dal sito (o dalla terza parte) che lo ha creato per recuperare informazioni. Quando scade, non è più possibile accedere al cookie.

Se si sceglie di consentire i cookie permanenti, è possibile ridefinire le loro date di scadenza specificando per quanto tempo resteranno attivi prima di scadere.

### Impostare una data di scadenza per i cookie

1. Selezionare **Privacy | Principale**.
2. Nell'area Controllo cookie, fare clic su **Personalizza**.
3. Nell'area Scadenza cookie, selezionare la casella di controllo **I cookie scadono**.



4. Specificare quando scadono i cookie.

Subito dopo la ricezione	Consente il funzionamento dei cookie permanenti solo durante la sessione in cui sono stati ricevuti.
Dopo [n] giorni	Consente ai cookie permanenti di restare attivi per il numero di giorni specificato. È possibile scegliere un numero qualsiasi da 1 a 999. L'impostazione predefinita è 1.

5. Fare clic su **Applica**, quindi fare clic su **OK**.

# Personalizzazione del blocco degli annunci

Blocco annunci è disattivato per impostazione predefinita. È possibile personalizzare il blocco degli annunci per bloccare tutti gli annunci o solo tipi specifici. Inoltre, è possibile specificare ciò che sarà visualizzato dal software di sicurezza Zone Labs al posto degli annunci bloccati.

Il gruppo di funzioni per la privacy che comprende il Blocco annunci è disponibile in ZoneAlarm Pro e ZoneAlarm Security Suite.

## Impostazione degli annunci da bloccare

La protezione della privacy consente di specificare quali tipi di annunci bloccare o consentire.

### Specificare gli annunci da bloccare

1. Selezionare **Privacy | Principale**.

2. Nell'area Blocco annunci, fare clic su **Personalizza**.

Viene visualizzata la finestra di dialogo Impostazioni personalizzate per la privacy.

3. Nell'area Annunci da bloccare, selezionare il tipo di annuncio che si desidera bloccare.

Banner/ annunci verticali	Blocca gli annunci che appaiono in un banner orizzontale o verticale.
Pop-up/pop- under	Blocca gli annunci che appaiono in una nuova finestra del browser davanti o dietro la finestra correntemente visualizzata.
Animazioni	Blocca gli annunci che contengono immagini in movimento.

4. Fare clic su **OK**.

## Impostazione delle opzioni di controllo degli annunci bloccati

Quando software di sicurezza Zone Labs blocca banner, annunci verticali o annunci animati, resta uno spazio vuoto sullo schermo, nel punto in cui era prevista la visualizzazione dell'annuncio. Il controllo degli annunci bloccati consente di specificare ciò che sarà visualizzato in tale spazio.

### Specificare ciò che appare al posto degli annunci bloccati

1. Selezionare **Privacy | Principale**.

2. Nell'area Blocco annunci, fare clic su **Personalizza**.

Viene visualizzata la finestra di dialogo Impostazioni personalizzate per la privacy.

3. Nell'area Controllo annunci bloccati, specificare il metodo per controllare gli annunci bloccati.

Nessun elemento	Blocca gli annunci senza alcuna indicazione riguardo a ciò che doveva essere visualizzato.
Un riquadro con la parola "[AD]"	Visualizza una finestra contenente la parola AD (per advertising). Questa è l'impostazione predefinita.
Una casella che visualizza l'annuncio al passaggio del mouse	Visualizza una finestra contenente l'annuncio che appare solo quando viene attivata utilizzando il mouse.

4. Fare clic su **OK**.

# Personalizzazione del controllo del codice mobile

Il codice mobile è il contenuto di una pagina Web che è attivo o di natura eseguibile. Esempi di contenuto attivo comprendono *applet Java*, *controlli ActiveX* e *JavaScript*, tutti utilizzabili per aumentare l'interattività e la dinamicità delle pagine Web.

Il codice mobile dannoso, tuttavia, può copiare file, cancellare il disco rigido, rubare password o impartire comandi ai server. Il controllo del codice mobile impedisce agli hacker di sfruttare il contenuto attivo per compromettere la sicurezza o danneggiare i computer.

L'impostazione predefinita per il controllo del codice mobile è Disattivato. Quando è Attivato, tutto il codice mobile tranne JavaScript viene bloccato. È possibile personalizzare le impostazioni di controllo del codice mobile specificando quali tipi di codice mobile vengono bloccati quando il controllo del codice mobile è impostato ad Attivato.

Il gruppo di funzioni per la privacy che comprende il controllo del codice mobile è disponibile in ZoneAlarm Pro e ZoneAlarm Security Suite.

## Impostazione dei tipi di codice mobile da bloccare

È possibile personalizzare il controllo del codice mobile impostando i tipi di contenuto attivo da bloccare e da consentire.

### Personalizzare il controllo del codice mobile

1. Selezionare **Privacy | Principale**.
2. Nell'area Controllo codice mobile, fare clic su **Personalizza**.

Viene visualizzata la finestra di dialogo Impostazioni personalizzate per la privacy.

3. Nell'area Controllo codice mobile, specificare i tipi di codice mobile da bloccare.

Blocca JavaScript	Blocca il contenuto JavaScript, compreso quello necessario per usi comuni come i collegamenti utilizzati in Indietro e Cronologia, le immagini rollover e l'apertura e la chiusura delle finestre del browser.
Blocca script (vbscript, e così via)	Blocca gli script con esecuzione automatica, compresi quelli necessari per visualizzare banner, annunci pop-up e menu dinamici.
Blocca oggetti incorporati (Java, ActiveX)	Blocca gli oggetti incorporati nelle pagine Web, compresi file audio e di immagine.

---

Blocca oggetti integrati di tipo MIME	Questa opzione blocca gli oggetti il cui tipo MIME indica che sono applicazioni. <b>Nota:</b> questa opzione blocca anche i file eseguibili sicuri inviati tramite il browser, compresi i download che si vorrebbero consentire. Quando accade, sarà visualizzato nel browser un errore che indica che l'oggetto è stato bloccato. Per i download richiesti dall'utente, è più sicuro deselezionare l'opzione Blocca oggetti integrati di tipo MIME.
---------------------------------------	---

# Comprensione di Cache Cleaner

Ogni volta che si apre un file, si visualizza una pagina Web o si completa un modulo online, le copie delle pagine Web visualizzate vengono memorizzate nella cache del browser, consentendo un successivo caricamento più rapido delle pagine stesse. Se si lavora su un computer condiviso, questi file possono essere visualizzati da chiunque lo utilizzi.

Analogamente, quando si apre, si elimina o si cerca un file sul computer, queste azioni lasciano una traccia elettronica concepita per tenere traccia dei passaggi e poterli eventualmente utilizzare in futuro. Benché utili, questi file in eccesso possono col tempo avere effetto sulle prestazioni e la capacità di elaborazione del computer. Ancora una volta, nel caso di un computer condiviso, chiunque lo utilizzi può scoprire quali siti Web sono stati visitati in precedenza.

L'utilizzo di Cache Cleaner del software di sicurezza Zone Labs serve per liberare periodicamente il computer da questi file in eccesso per recuperare spazio su disco e garantire la privacy.

Il gruppo di funzioni per la privacy che comprende Cache Cleaner è disponibile in ZoneAlarm Pro e ZoneAlarm Security Suite.

## Utilizzo di Cache Cleaner

Cache Cleaner può essere eseguito manualmente in qualsiasi momento. Se si preferisce pianificare le "ripuliture" della cache, è possibile configurare Cache Cleaner per l'esecuzione automatica a intervalli regolari: da una volta al giorno a una volta ogni 99 giorni. Il valore predefinito per la cancellazione automatica del contenuto della cache è ogni 14 giorni.

### Eeguire Cache Cleaner manualmente

1. Selezionare **Privacy | Cache Cleaner**.

2. Fare clic su **Cancella ora**.

Viene visualizzato un messaggio di verifica.

3. Fare clic su **OK**.

Durante l'esecuzione di Cache Cleaner sarà visualizzata una barra di avanzamento.

### Pianificare l'esecuzione automatica di Cache Cleaner

1. Selezionare **Privacy | Cache Cleaner**.

2. Selezionare la casella di controllo **Cancella cache automaticamente ogni**.

3. Nell'area Cancella cache automaticamente, specificare un intervallo di cancellazione da 1 a 99.

Le date dell'ultima cancellazione e della successiva cancellazione pianificata sono visualizzate sotto la casella di controllo.

## Personalizzazione delle opzioni di ripulitura del disco rigido

Per impostazione predefinita, Cache Cleaner cancella dal disco rigido i seguenti file:

- Contenuto del Cestino
- Contenuto della directory dei file temporanei
- Frammenti di file dall'utilità ScanDisk di Windows

È possibile personalizzare queste impostazioni specificando aree aggiuntive da cancellare, compresa la cronologia dei documenti, la cronologia delle ricerche o la cronologia di Windows Media Player.

### Personalizzare le opzioni di ripulitura per il disco rigido

1. Selezionare **Privacy | Cache Cleaner**, quindi fare clic su **Personalizza**.
2. Fare clic sulla scheda **Disco rigido**, quindi specificare le opzioni di ripulitura.

Cancella la cronologia dei documenti	Cancella l'elenco dei file che appaiono in <b>Start   Documenti recenti</b> . Questa impostazione si applica solo alla cronologia dei documenti per l'utente correntemente connesso.
Svuota il Cestino	Cancella il contenuto del Cestino di Windows. Opzione selezionata per impostazione predefinita.
Elimina i file temporanei	Elimina i file temporanei di Windows. Opzione selezionata per impostazione predefinita.
Cancella la cronologia delle ricerche di Windows	Cancella i termini utilizzati dall'utente per eseguire ricerche in Windows.
Cancella i frammenti di file creati da ScanDisk	Elimina i frammenti di dati persi o danneggiati recuperati dal programma ScanDisk di Windows. Opzione selezionata per impostazione predefinita.
Cancella la cronologia di Windows Media Player	Ripulisce l'elenco di clip multimediali riprodotti di recente in Windows Media Player.
Cancella la cronologia del comando Esegui	Elimina le voci che appaiono nell'elenco a discesa Apri della finestra Esegui, visualizzata selezionando <b>Start   Esegui</b> .

3. Fare clic su **Applica**, quindi fare clic su **OK**.

## Personalizzazione delle opzioni di ripulitura del browser

Se si utilizza Internet Explorer o Netscape, è possibile configurare Cache Cleaner per rimuovere file dei cookie memorizzati sul computer mentre si naviga sul Web. Cache Cleaner identifica i cookie da rimuovere dall'origine del cookie, anziché dal singolo file del cookie. Quando si specifica un'origine di cookie da rimuovere, Cache Cleaner rimuove tutti i cookie di quell'origine. Se ci sono cookie sul computer che non si desidera rimuovere, è possibile configurare Cache Cleaner per conservarli.

**Personalizzare le opzioni di ripulitura per IE/MSN**

1. Selezionare **Privacy | Cache Cleaner**, quindi fare clic su **Personalizza**.
2. Fare clic sulla scheda **IE/MSN**.
3. Nell'area Opzioni di Internet Explorer/MSN, specificare le aree da ripulire.

Cancella cache	Ripulisce la cache del browser Internet Explorer. Opzione selezionata per impostazione predefinita.
Cancella la cronologia degli URL	Cancella l'elenco degli URL del campo Indirizzo. Opzione selezionata per impostazione predefinita.
Cancella i dati di completamento automatico	Cancella le voci immesse in precedenza nei moduli Web, comprese le password. <b>Nota:</b> se non si desidera che le password vengano cancellate, deselezionare la casella di controllo Cancella i dati di completamento automatico.
Cancella le password di completamento automatico	Cancella le password per cui era stata selezionata l'opzione di memorizzazione.
Cancella i file Index.dat bloccati	Elimina i file <i>Index.dat</i> correntemente in uso sul computer. Opzione selezionata per impostazione predefinita.
Cancella la cronologia degli URL digitati	Cancella gli URL che sono stati digitati dall'utente nel campo Indirizzo. Opzione selezionata per impostazione predefinita.

4. Per rimuovere i cookie, selezionare la casella di controllo **Cancella i cookie di IE/MSN**, quindi fare clic su **Seleziona**.

Viene visualizzata la finestra di dialogo Selezionare i cookie di IE/MSN da conservare. L'elenco a sinistra mostra i siti per cui il browser conserva attualmente dei cookie. L'elenco a destra mostra i siti di cui non si vogliono cancellare i cookie.

5. Per conservare i cookie di un'origine, selezionarla, quindi fare clic su **Conserva**.
6. Per rimuovere i cookie rimanenti, fare clic su **Rimuovi**, quindi fare clic su **OK**.

**Personalizzare le opzioni di ripulitura per Netscape**

1. Selezionare **Privacy | Cache Cleaner**, quindi fare clic su **Personalizza**.
2. Fare clic sulla scheda **Netscape**.
3. Nell'area Opzioni di Netscape, specificare le aree da ripulire.

Cancella cache	Ripulisce la cache del browser Netscape. Opzione selezionata per impostazione predefinita.
Cancella la cronologia degli URL	Cancella l'elenco di URL del campo degli indirizzi. Opzione selezionata per impostazione predefinita.
Cancella la posta eliminata	Ripulisce la cartella della posta eliminata di Netscape.



---

Cancella i dati dei moduli	Cancella le voci immesse in precedenza nei moduli Web.
----------------------------	--

---

4. Per rimuovere i cookie, selezionare la casella di controllo **Cancella i cookie di Netscape**.

Viene visualizzata la finestra di dialogo Selezionare i cookie di Netscape da conservare. L'elenco a sinistra mostra i siti per cui il browser conserva attualmente dei cookie. L'elenco a destra mostra i siti di cui non si vogliono cancellare i cookie.

5. Per conservare i cookie di un'origine, selezionarla, quindi fare clic su **Conserva**.
6. Per rimuovere i cookie rimanenti, fare clic su **Rimuovi**, quindi fare clic su **OK**.



# Capitolo

## Avvisi e log

# 9

Che l'utente sia il tipo di persona che vuole essere a conoscenza di tutto ciò che succede all'interno del suo computer, oppure che voglia solo sapere che il suo computer è protetto, il software di sicurezza Zone Labs è in grado di soddisfare le sue esigenze. È possibile ricevere un avviso ogni volta che il software di sicurezza Zone Labs entra in azione per proteggere il computer, oppure solamente quando l'avviso è probabilmente il risultato dell'attività di hacker. È anche possibile registrare tutti gli avvisi, solamente quelli di alto livello, o quelli causati da tipi di traffico specifici.

### Argomenti:

- "Comprensione di avvisi e log", a pagina 162
- "Impostazione delle opzioni di base per avvisi e log", a pagina 170
- "Mostrare o nascondere avvisi specifici", a pagina 171
- "Impostazione delle opzioni di log per eventi e programmi", a pagina 172
- "Utilizzo di SmartDefense Advisor e Hacker ID", a pagina 178

# Comprensione di avvisi e log

Le caratteristiche di avviso e registrazione dei log del software di sicurezza Zone Labs permettono all'utente di essere al corrente di ciò che succede all'interno del suo computer senza essere eccessivamente invadenti, e gli consentono di tornare in ogni momento a esaminare gli avvisi passati. Le opzioni delle regole della scheda Esperto consentono di tenere traccia non solo del traffico bloccato, ma anche del traffico autorizzato, fornendo agli utenti avanzati le opzioni di informazione più complete durante la personalizzazione delle regole di sicurezza per il loro ambiente.

## Informazioni sugli avvisi del software di sicurezza Zone Labs

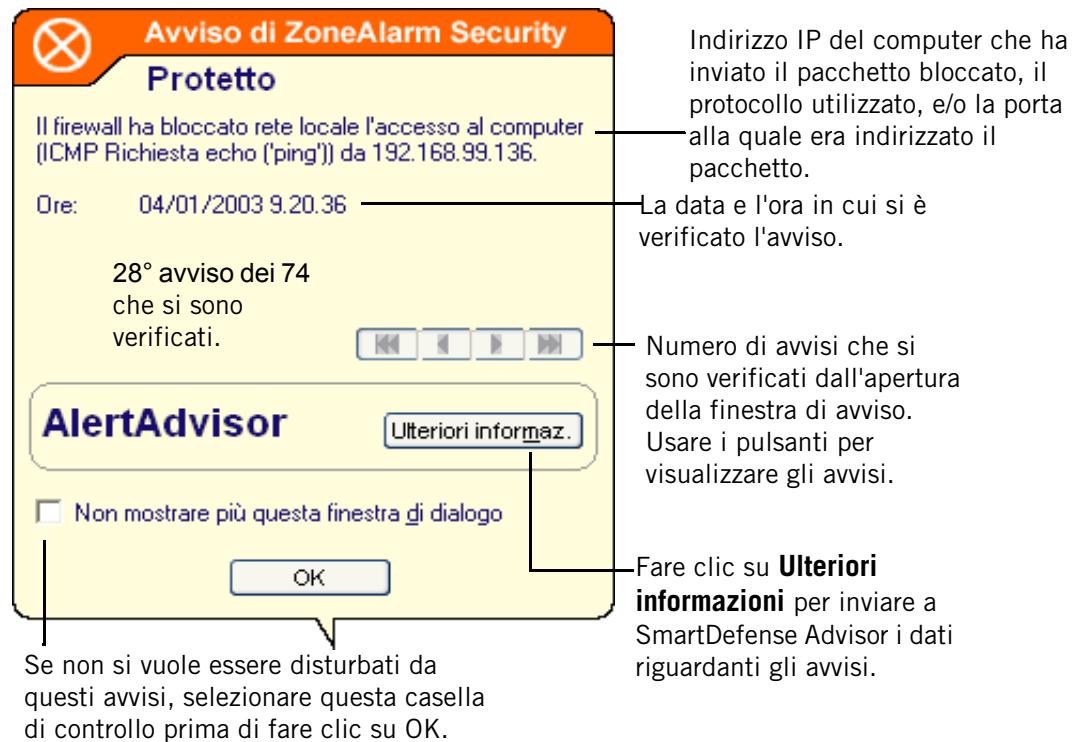
Gli avvisi del software di sicurezza Zone Labs sono divisi in tre categorie di base: informativi, di programma e di rete. A seconda della versione del software di sicurezza Zone Labs in uso potrebbero apparire avvisi aggiuntivi che includono gli avvisi relativi al Blocco ID e a OSFirewall.



Per ulteriori informazioni sui tipi di avviso visualizzati e su come comportarsi, vedere l'Appendice A, "Guida di riferimento agli avvisi", a pagina 211.

### Avvisi informativi

Gli avvisi informativi indicano che il software di sicurezza Zone Labs ha bloccato una comunicazione non conforme alle impostazioni di sicurezza. Il tipo di avviso informativo più comune è l'avviso del firewall.



**Figura 9-1: Avvisi del firewall**

Gli avvisi informativi non richiedono una decisione da parte dell'utente. È possibile chiudere l'avviso facendo clic sul pulsante **OK** che si trova nella parte inferiore dell'avviso. Facendo questo, non si sta indicando che il traffico può accedere al computer.

### Avvisi relativi ai programmi

Gli avvisi relativi ai programmi chiedono all'utente se desidera consentire l'accesso a Internet o alla rete locale a un programma, o agire come server. Questo tipo di avviso richiede una decisione da parte dell'utente (Consenti o Nega). I tipi di avvisi di programma più comuni sono Nuovo avviso di programma e Programma ripetuto.



**Figura 9-2: Avvisi Nuovo programma**

Facendo clic sul pulsante Consenti, vengono concesse le autorizzazioni al programma. Facendo clic sul pulsante Nega, vengono negate le autorizzazioni al programma.

### Avvisi Nuova rete

Gli avvisi Nuova rete vengono generati quando l'utente si connette a una rete qualsiasi (una rete domestica wireless, una rete LAN aziendale o la rete dell'ISP).

Tipo di rete (wireless o altro), indirizzo IP e subnet mask della rete rilevata.

Digitare qui un nome della rete. Questo nome compare nella scheda Zone e permette di riconoscere la rete successivamente.

Selezionare la zona a cui aggiungere la nuova rete. Aggiungere la rete alla zona attendibile solo se si è certi che sia la rete domestica o LAN aziendale e non la rete dell'ISP.

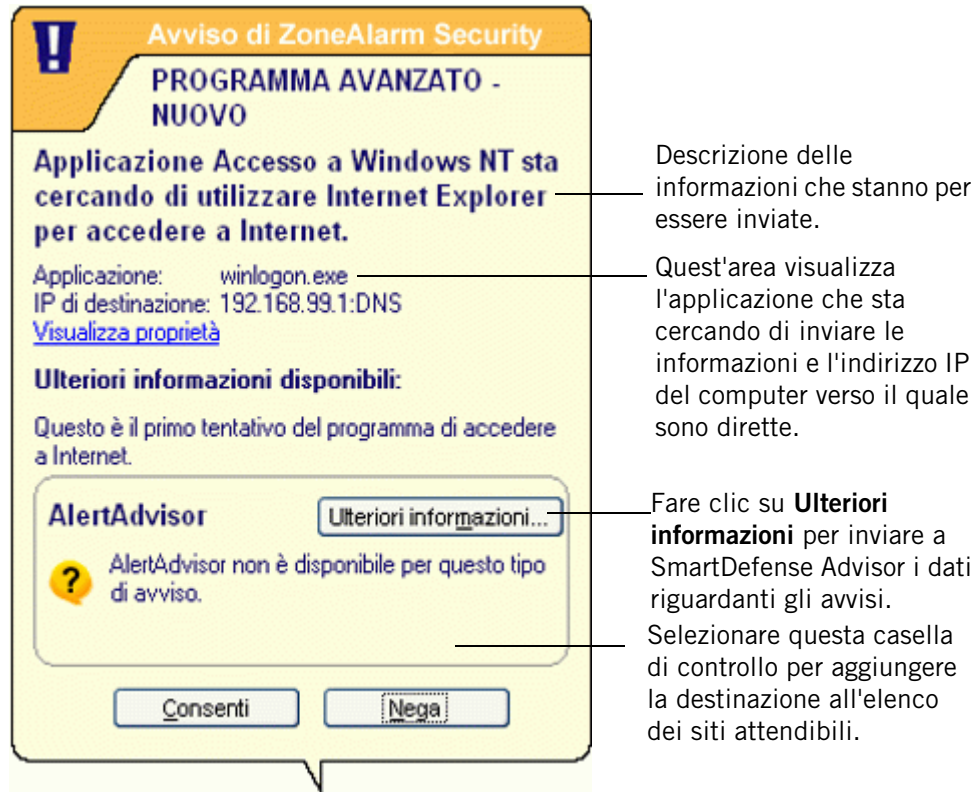
Fare clic su **OK** per aggiungere la rete alla zona selezionata e chiudere la finestra di avviso.

Per maggiore aiuto durante la configurazione della rete, accedere alla configurazione guidata Rete.

**Figura 9-3: Avviso Nuova rete**

### Avvisi Blocco ID

Se ha attivato la funzione Blocco ID, l'utente di ZoneAlarm Pro e di ZoneAlarm Security Suite può visualizzare avvisi Blocco ID nel caso in cui le informazioni personali salvate in myVAULT vengano inviate ad una destinazione che non è indicata nell'elenco dei siti attendibili.



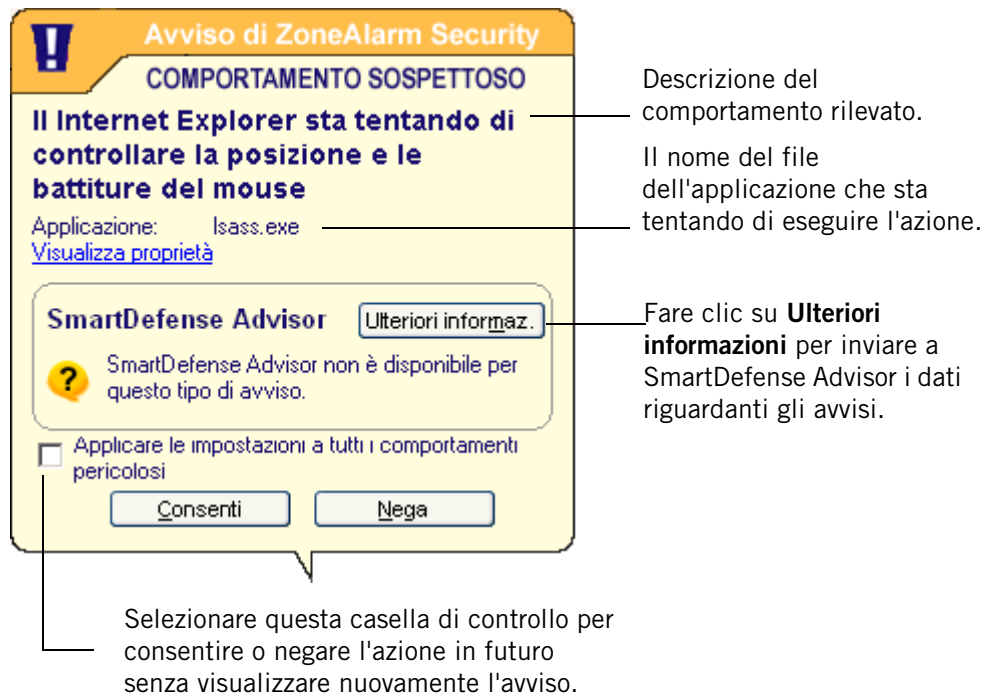
**Figura 9-4: Avvisi Blocco ID**

Facendo clic sul pulsante Sì, viene concessa l'autorizzazione di inviare le informazioni all'indirizzo IP che le richiede. Se la volta successiva non si desidera essere avvisati quando i dati di myVAULT vengono inviati a questa destinazione, selezionare la casella di controllo "**Memorizzare...**" per aggiungere la destinazione all'elenco dei siti attendibili.

### ***Avvisi di OSFirewall***

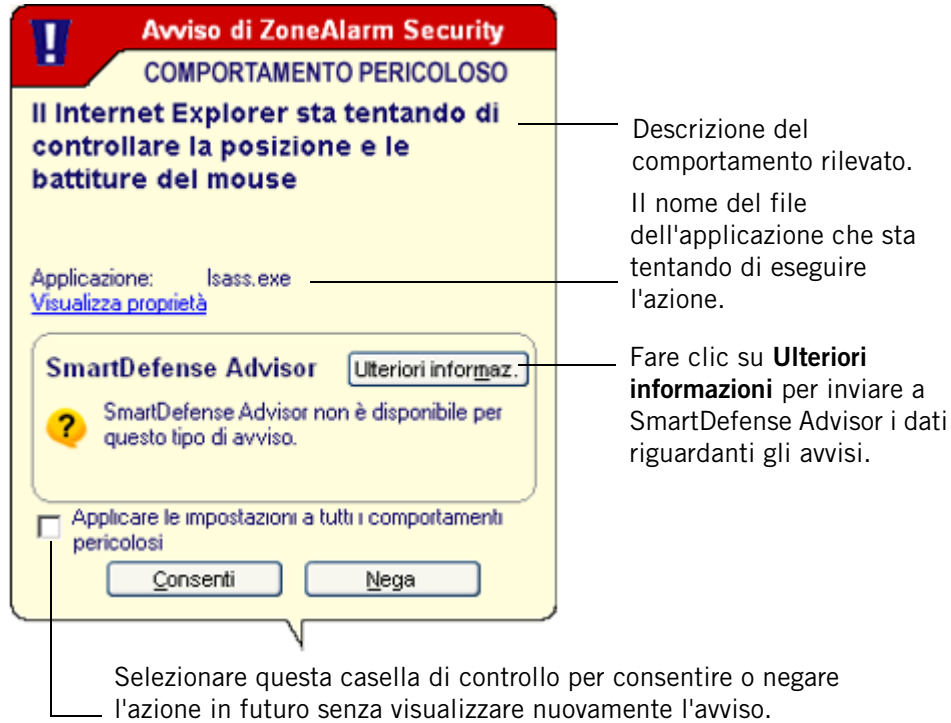
Esistono due tipi di avvisi di OSFirewall: Comportamento sospetto e Comportamento dannoso. Entrambi questi avvisi informano che ZoneALarm Security Suite ha rilevato che un programma sta eseguendo un'azione che potrebbe essere dannosa per i dati o per il computer.





**Figura 9-5: Avviso Comportamento sospetto**

Gli avvisi di tipo Comportamento sospetto informano delle azioni che potrebbero cambiare il comportamento di un programma, per esempio se un programma tenta di modificare la pagina iniziale predefinita del browser viene visualizzato un avviso di tipo Comportamento sospetto. Gli avvisi di tipo Comportamento pericoloso informano, invece, sulle azioni che potrebbero impedire un funzionamento corretto dei programmi o del sistema operativo o azioni di spyware che tenta di monitorare le attività dell'utente.



**Figura 9-6: Avviso Comportamento pericoloso**

Per ulteriori informazioni sugli avvisi di OSFirewall e dei tipi di comportamento rilevati, vedere l'Appendice D, "Comportamento dei programmi", a pagina 261.

## Informazioni sulla registrazione degli eventi

Per impostazione predefinita, il software di sicurezza Zone Labs crea una voce di log ogni volta che il traffico è bloccato, che venga visualizzato un avviso o meno. Le voci di log registrano l'origine e la destinazione del traffico, le porte, i protocolli e altri dettagli. Le informazioni vengono registrate in un file di testo con il nome ZALOG.txt, salvato nella cartella Internet Logs. Ogni 60 giorni, il file di log viene archiviato in un file separato in modo che non diventi di dimensioni troppo estese.

È possibile scegliere di impedire la registrazione nei log di categorie di eventi specifiche. Per esempio, si potrebbe voler creare le voci di log solo per gli avvisi del firewall, oppure disattivare le voci per un particolare tipo programma. Creando delle regole nella scheda Esperto e attivando la funzione di tracciamento, è anche possibile indicare al software di sicurezza Zone Labs di creare un log per un tipo specifico di traffico che si è scelto di consentire.

# Impostazione delle opzioni di base per avvisi e log

Le opzioni di base per avvisi e log consentono di specificare il tipo di evento per il quale il software di sicurezza Zone Labs visualizza un avviso e crea delle voci di log.

## Impostazione del livello di visualizzazione degli avvisi

Il controllo Eventi di avviso visualizzati, nella scheda Principale di Avvisi e log, consente di controllare la visualizzazione degli avvisi per livello. Gli avvisi Programma e Blocco ID vengono visualizzati sempre, perché richiedono di stabilire se concedere autorizzazioni o meno.

### Impostare il livello degli eventi di avviso

1. Selezionare **Avvisi e log** | **Principale**.
2. Nell'area Eventi di avviso visualizzati, selezionare l'impostazione desiderata.

Alta	Visualizza un avviso per ogni evento di sicurezza specifico che si verifica, sia di alto che di medio livello.
Media	Visualizza solamente avvisi di alto livello, che sono molto probabilmente il risultato dell'attività di hacker.
Disattivato	Visualizza solamente avvisi Programma e Blocco ID. Gli avvisi informativi non vengono visualizzati.

## Impostazione delle opzioni di registrazione dei log per eventi e programmi

Usare le aree Registrazione eventi e Registrazione programmi per selezionare i tipi di avvisi informativi e di programma che saranno registrati.

### Attivare o disattivare la registrazione dei log per eventi e programmi

1. Selezionare **Avvisi e log** | **Principale**.
2. Nell'area Registrazione eventi, selezionare l'impostazione desiderata.

Attivata	Crea una voce di log per tutti gli eventi.
Disattivato	Nessun evento registrato.

3. Nell'area Registrazione programmi, specificare il livello di log.

Alta	Crea una voce di log per tutti i programmi.
Media	Crea una voce di log solamente per avvisi di programma di alto livello.
Disattivato	Nessun evento di programma registrato.

# Mostrare o nascondere avvisi specifici

È possibile specificare se si desidera essere messi in guardia riguardo a tutti gli eventi di sicurezza e di programma, oppure se si desidera essere avvisati nel caso in cui gli eventi siano probabilmente il risultato dell'attività di hacker.

## Mostrare o nascondere gli avvisi del firewall

La scheda Eventi di avviso fornisce un controllo più dettagliato della visualizzazione degli avvisi consentendo di specificare i tipi di traffico bloccato per i quali gli avvisi del firewall e dei programmi vengono visualizzati.

### Mostrare o nascondere gli avvisi del firewall o dei programmi

1. Selezionare **Avvisi e log | Principale**, quindi fare clic su **Avanzate**.

Viene visualizzata la finestra di dialogo Impostazioni avvisi e log.

2. Selezionare la scheda Eventi di avviso
3. Nella colonna Avviso, selezionare il tipo di traffico bloccato per il quale il software di sicurezza Zone Labs deve visualizzare un avviso.
4. Fare clic su **Applica** per salvare le modifiche.

## Attivazione degli avvisi nell'area di notifica del sistema

Quando si decide di nascondere alcuni o tutti gli avvisi informativi, il software di sicurezza Zone Labs consente comunque di essere al corrente di quegli avvisi visualizzando una piccola icona 🚩 di avviso nell'area di notifica del sistema.

### Attivare gli avvisi nell'area di notifica del sistema

1. Selezionare **Avvisi e log | Principale**.
2. Fare clic su **Avanzate**, quindi fare clic sulla scheda **Avviso area di notifica del sistema**.
3. Selezionare la casella di controllo **Abilita avviso di icona nell'area di notifica del sistema**.

# Impostazione delle opzioni di log per eventi e programmi

Attivando o disattivando la registrazione per ogni tipo di avviso, è possibile specificare se il software di sicurezza Zone Labs deve tenere traccia degli eventi di sicurezza e dei programmi.

## Formattazione dei log

Usare questi controlli per determinare il separatore di campo per i file di log (txt).

### Formattare le voci di log

1. Selezionare **Avvisi e log**, quindi fare clic su **Avanzate**.

Viene visualizzata la finestra di dialogo Impostazioni avanzate avvisi e log.

2. Selezionare la scheda **Controllo log**.
3. Nell'area Aspetto archiviazione log, selezionare il formato da utilizzare per i log.

Scheda	Selezionare Tabulazione per separare i campi con un carattere di tabulazione.
Virgola	Selezionare Virgola per separare i campi con una virgola.
Punto e virgola	Selezionare Punto e virgola per separare i campi del log con un punto e virgola.

## Personalizzazione della registrazione degli eventi

Per impostazione predefinita, il software di sicurezza Zone Labs crea una voce di log quando si verifica un evento di alto livello relativo al firewall. È possibile personalizzare la registrazione degli avvisi del firewall abilitando o meno le voci di log per eventi di sicurezza specifici, come gli allegati messi in quarantena da MailSafe, pacchetti non IP bloccati, o violazioni del blocco.

### Creare o disattivare voci di log in base al tipo di evento

1. Selezionare **Avvisi e log** | **Principale**.
2. Fare clic su **Avanzate**.  
Viene visualizzata la finestra di dialogo Avvisi e log avanzati.
3. Selezionare **Eventi di avviso**.
4. Nella colonna Log, selezionare il tipo di evento per il quale il software di sicurezza Zone Labs deve creare una voce di log.
5. Fare clic su **Applica** per salvare le modifiche.
6. Fare clic su **OK** per chiudere la finestra di dialogo Impostazioni avvisi e log.

## Personalizzazione della registrazione di programma

Per impostazione predefinita, il software di sicurezza Zone Labs crea una voce di log quando si verifica un tipo qualsiasi di avviso di programma. È possibile personalizzare la registrazione dei log per gli avvisi di programma disattivando le voci di log per tipi di avviso di programma specifici, come gli avvisi Nuovo programma, Programma ripetuto o Programma server.

### Creare o disattivare voci di log in base al tipo di evento

1. Selezionare **Avvisi e log** | **Principale**.
2. Nell'area Registrazione programmi, fare clic su **Personalizza**.
3. Nella colonna Log di programma, selezionare il tipo di evento per il quale il software di sicurezza Zone Labs deve creare una voce di log.
4. Fare clic su **Applica** per salvare le modifiche.
5. Fare clic su **OK** per chiudere la finestra di dialogo Impostazioni avvisi e log.

### Visualizzazione delle voci di log

È possibile visualizzare le voci di log in due modi: in un file di testo usando un editor di testo, o nel Visualizzatore log. Nonostante il formato di ogni tipo di log sia leggermente diverso, le informazioni generali contenute in essi sono uguali.

### Visualizzare il log corrente nel Visualizzatore log

1. Selezionare **Avvisi e log** | **Visualizzatore log**.
2. Selezionare il numero di avvisi da visualizzare (da 1 a 999) nell'elenco degli avvisi.

È possibile ordinare l'elenco per qualsiasi campo, facendo clic sull'intestazione di colonna. La freccia (^) accanto al nome dell'intestazione indica l'ordine di disposizione. Fare di nuovo clic sulla stessa intestazione per invertire l'ordine.

3. Selezionare il tipo di avviso che si desidera visualizzare:

Antivirus	Visualizza le colonne Data/Ora, Tipo, Nome virus, Nome file, Azione eseguita, Modalità e Informazioni posta elettronica.
Firewall	Visualizza le colonne Livello, Data/Ora, Tipo, Protocollo, Programma, IP di origine, IP di destinazione, Direzione, Azione eseguita, Conteggio, DNS di origine e DNS di destinazione.
IM Security	Visualizza le colonne Data/Ora, Tipo, Origine, Programma, Utente locale, Utente remoto e Azione.
Firewall del sistema operativo	Visualizza le colonne Livello, Data/Ora, Tipo, Sottotipo, Dati, Programma, Direzione, Azione eseguita e Conteggio.
Programma	Visualizza le colonne Livello, Data/Ora, Tipo, Programma, IP di origine, IP di destinazione, Direzione, Azione eseguita, Conteggio, DNS di origine e DNS di destinazione.

Antispyware	Visualizza le colonne Data, Tipo, Nome spyware, Nome file, Azione e Attore.
-------------	---



Il Visualizzatore log mostra gli eventi di sicurezza che sono stati registrati nel log del software di sicurezza Zone Labs. Per visualizzare i dettagli dei campi del Visualizzatore log per ciascun tipo di avviso, consultare i capitoli relativi al firewall, al Controllo dei programmi, all'antivirus e a IM Security.

Campo	Informazioni
Descrizione	Descrizione dell'evento.
Direzione	La direzione del traffico bloccato. "In ingresso" significa che il traffico è stato inviato al proprio computer. "In uscita" significa che il traffico è stato inviato dal proprio computer.
Tipo	Il tipo di avviso: Firewall, Programma, Blocco ID o Blocco attivato.
DNS di origine	Il nome di dominio del computer che ha inviato il traffico che ha causato l'avviso.
IP di origine	L'indirizzo IP del computer che ha inviato il traffico bloccato dal software di sicurezza Zone Labs.
Livello	Ogni avviso è di livello alto o medio. Gli avvisi di alto livello sono quelli che probabilmente sono causati da attività di hacker. Gli avvisi di medio livello probabilmente sono causati da traffico di rete indesiderato ma inoffensivo.
Protocollo	Il protocollo di comunicazione utilizzato dal traffico che ha causato l'avviso.
Azione eseguita	Il modo in cui il traffico è stato gestito dal software di sicurezza Zone Labs.
DNS di destinazione	Il nome di dominio del destinatario a cui era diretto il traffico che ha causato l'avviso.
IP di destinazione	L'indirizzo del computer a cui era destinato il traffico bloccato.
Conteggio	Il numero di volte per cui un avviso dello stesso tipo, con la stessa origine, destinazione e protocollo si è verificato durante una singola sessione.

**Tabella 9-1: Campi del Visualizzatore log**



Campo	Informazioni
Data/Ora	La data e l'ora in cui si è verificato l'avviso.
Programma	Il nome del programma che sta tentando di inviare o ricevere dati (si applica solo ad avvisi Programma e Blocco ID).

**Tabella 9-1: Campi del Visualizzatore log**

## Visualizzazione del file di log

Per impostazione predefinita, gli avvisi generati dal software di sicurezza Zone Labs vengono registrati nel file *ZAlog.txt*. Se si utilizza Windows 95, Windows 98 o Windows Me, il file si trova nella cartella seguente: (x):\Windows\Internet Logs. Se si utilizza Windows NT o Windows 2000, il file si trova nella cartella seguente: (x):\Winnt\Internet Logs.

### Visualizzare il log corrente come file di testo

1. Selezionare **Avvisi e log** | **Principale**.
2. Fare clic su **Avanzate**.

Si apre la finestra di dialogo Impostazioni avanzate avvisi e log.

3. Selezionare la scheda **Controllo log**.

Nell'area Posizione archiviazione log, fare clic su **Visualizza log**.

### Campi del file di testo del log

Le voci di log contengono una combinazione dei campi descritti nella tabella seguente.

Campo	Descrizione	Esempio
Tipo	Tipo di evento registrato.	FWIN
Data	Data dell'avviso, in formato aaa/mm/gg	2001/12/31 (31 dicembre, 2001)
Ora	L'ora locale dell'avviso. In questo campo viene anche visualizzata la differenza tra l'ora locale e quella di Greenwich (GMT).	17:48:00 -8:00GMT (17:48, otto ore in meno rispetto a Greenwich. L'ora di Greenwich sarebbe 01:48.)
Nome virus	Nome del virus che ha causato l'evento. Questo campo viene visualizzato solamente per gli eventi relativi all'antivirus.	iloveyou

<b>Campo</b>	<b>Descrizione</b>	<b>Esempio</b>
Nome file	Nome del file che ha causato l'evento. Questo campo viene visualizzato solamente per gli eventi relativi all'antivirus.	iloveyou.exe
Azione	Modo in cui è stato gestito l'evento. Il valore per questo campo dipenderà dal tipo di evento che si è verificato.	Antivirus: Rinominato IM Security: Crittografato MailSafe: In quarantena Blocco ID: Bloccato
Categoria	Categoria di informazioni Blocco ID che sono state rilevate nell'evento. Questo campo viene visualizzato solamente per gli eventi Blocco ID.	PIN di accesso
Programma	Programma che invia o riceve il messaggio di posta elettronica contenente le informazioni Blocco ID. Questo campo viene visualizzato solamente per gli eventi Blocco ID.	Outlook.exe
Origine	Indirizzo IP del computer che ha inviato il pacchetto bloccato, e la porta utilizzata, OPPURE il programma sul computer che ha richiesto le autorizzazioni di accesso.	192.168.1.1:7138 Outlook.exe
Destinazione	Indirizzo IP e porta del computer a cui era indirizzato il pacchetto bloccato.	192.168.1.101:0
Trasporto	Protocollo (tipo di pacchetto) in questione.	UDP

## Archiviazione delle voci di log

A intervalli regolari, i contenuti di ZALog.txt vengono archiviati in un file il cui nome contiene la data corrente, per esempio ZALog2004.06.04.txt per il 4 giugno 2004. Questo serve a evitare che ZALog.txt diventi di dimensioni troppo estese.

Per visualizzare i file di log archiviati, usare Esplora risorse per aprire la cartella in cui sono salvati i log.

### Impostare la frequenza di archiviazione

1. Selezionare **Avvisi e log** | **Principale**, quindi fare clic su **Avanzate**.
2. Selezionare la scheda **Controllo log**.

3. Selezionare la casella di controllo **Frequenza archiviazione log** .



Se la casella di controllo Frequenza archiviazione log non è selezionata, il software di sicurezza Zone Labs continua a registrare eventi per la visualizzazione nella scheda Visualizzatore log, ma non li archivia nel file ZALog.txt.

4. Nell'area Frequenza log, specificare la frequenza di archiviazione dei log (da 1 a 60 giorni), quindi fare clic su **Applica**.

#### ***Specificare la posizione di archiviazione***

Il file ZALog.txt e tutti i file log archiviati vengono salvati nella stessa directory.

#### **Modificare la posizione del file di log e dei file archiviati**

1. Selezionare **Avvisi e log | Principale**.

2. Fare clic su **Avanzate**.

Si apre la finestra di dialogo Impostazioni avanzate avvisi e log.

3. Selezionare la scheda **Controllo log**.

4. Nell'area Posizione archiviazione log, fare clic su **Sfoggia**.

Selezionare una posizione per i file di log e di archiviazione.

# Utilizzo di SmartDefense Advisor e Hacker ID

Zone Labs SmartDefense Advisor è un servizio che consente di analizzare istantaneamente le possibili cause di un avviso, e aiuta a decidere come rispondere. SmartDefense Advisor fornisce suggerimenti relativi a come rispondere agli avvisi Programma, quando questi sono disponibili. Se non è disponibile alcun suggerimento, fare clic su **Ulteriori informazioni** nell'avviso per ricevere ulteriori informazioni riguardo all'avviso. SmartDefense Advisor invia in risposta un testo in cui sono presenti una spiegazione dell'avviso e dei suggerimenti su ciò che è necessario fare per garantire sicurezza.

Per determinare la posizione fisica e altre informazioni sull'indirizzo IP di origine o di destinazione in un avviso, fare clic sulla scheda Hacker ID. In questa scheda sono visualizzate le informazioni sull'indirizzo IP che è stato inviato.



Se l'utente visita frequentemente eBay e ha ricevuto in avviso Blocco ID che ha bloccato la password di eBay, è possibile utilizzare SmartDefense Advisor per inviare un rapporto sulla frode a eBay. Per ulteriori informazioni sul modo in cui il software di sicurezza Zone Labs protegge l'identità eBay dell'utente, vedere "Creazione di un profilo di protezione dalle frodi online", a pagina 26.

## Inviare un avviso ad SmartDefense Advisor

1. Selezionare **Avvisi e log** | **Visualizzatore log**.
2. Fare clic col pulsante destro del mouse nel record di avviso che si vuole inviare.
3. Selezionare **Ulteriori informazioni** dal menu di scelta rapida.



Con l'acquisto di ZoneAlarm Anti-virus, ZoneAlarm Pro o ZoneAlarm Security Suite è incluso uno o due anni di accesso ad aggiornamenti, supporto e servizi; per accedervi oltre questo periodo è necessario un contratto di assistenza annuale. Zone Labs si riserva il diritto di rimuovere in qualsiasi momento le funzioni e i servizi disponibili tramite ZoneAlarm.

# Capitolo

## Protezione dei dati

# 10

Grazie a Internet, molte operazioni che prima dovevano essere svolte di persona o al telefono, come pagare le bollette, chiedere un prestito o prenotare un volo aereo, possono ora essere svolte online. Ciò offre una gradita comodità a molti, e uno spiacevole rischio per alcuni. Sfortunatamente, la crescita commercio elettronico ha avuto come conseguenza anche un aumento degli episodi di furto d'identità.

La caratteristica Blocco ID del software di sicurezza Zone Labs mette le informazioni personali al sicuro da hacker e da furti di identità.

### Argomenti:

- "Comprensione della funzione Blocco ID", a pagina 180
- "Informazioni su myVAULT", a pagina 183
- "Utilizzo dell'elenco dei siti attendibili", a pagina 186

# Comprensione della funzione Blocco ID

Ogni volta che l'utente o un'altra persona utilizza il computer, può inserire delle informazioni personali in un messaggio di posta elettronica o in un modulo Web, per esempio numeri di carte di credito, numeri di telefono o indirizzi. È possibile che queste informazioni vengano rubate. Per cercare di impedire che questo succeda, la funzione Blocco ID garantisce l'invio esclusivo delle informazioni personali verso siti considerati attendibili.

La funzione Blocco ID fornisce un'area protetta chiamata myVAULT, dove è possibile salvare le informazioni personali che si desidera proteggere. La trasmissione dei contenuti di myVAULT verso destinazioni non autorizzate, che sia stata disposta dall'utente, da un'altra persona che sta utilizzando il computer oppure da un Trojan horse che sta cercando di trasmettere le informazioni personali dell'utente, viene bloccata.

La funzione Blocco ID è disponibile in ZoneAlarm Pro e ZoneAlarm Security Suite.

## Come vengono protette le informazioni personali

Il software di sicurezza Zone Labs impedisce alle informazioni personali dell'utente di essere trasmesse senza autorizzazione, sia all'interno di un messaggio di posta elettronica che sul Web.

### *Trasmissione mediante posta elettronica*

Quando l'utente o un'altra persona che utilizza il computer cerca di inviare dati di myVAULT all'interno di un messaggio di posta elettronica, il software di sicurezza Zone Labs visualizza un avviso che chiede se consentire l'invio delle informazioni. Se si desidera consentire sempre o bloccare sempre l'invio delle informazioni verso questa destinazione, prima di fare clic su Sì o No, selezionare la casella di controllo "**Memorizzare questa risposta...**" per aggiungere la destinazione all'elenco dei siti attendibili con le corrispondenti autorizzazioni automaticamente impostate. Per esempio, selezionando la casella di controllo "Memorizzare questa risposta..." e facendo clic su **Si**, la destinazione viene aggiunta all'elenco dei siti attendibili con le autorizzazioni impostate su **Consenti**. Al contrario, facendo clic su **No**, le autorizzazioni vengono impostate su **Blocca**.



Quando si risponde a un avviso Blocco ID generato in seguito all'invio di un messaggio di posta elettronica, selezionando la casella di controllo "**Memorizzare questa risposta...**" si aggiunge all'elenco dei siti attendibili il dominio del server di posta elettronica del destinatario del messaggio (e non il destinatario del messaggio). Per esempio, se l'utente consente l'invio di dati di myVAULT al contatto john@example.com, e decide di memorizzare la risposta, gli invii successivi di dati di myVAULT sono consentiti a QUALUNQUE contatto presente sul server di posta di example.com, senza che alcun avviso venga visualizzato.

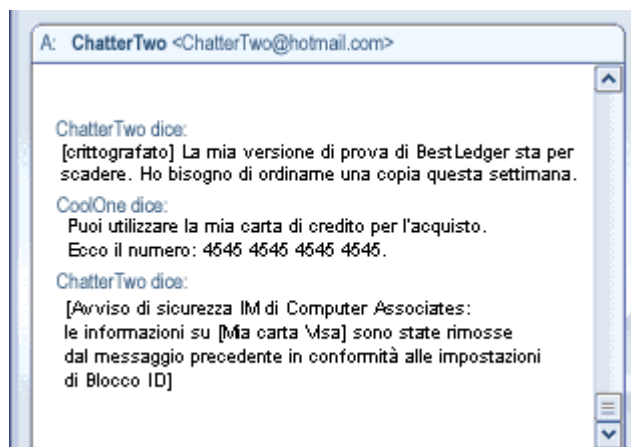
### ***Trasmissione di dati sul Web***

Quando si trasmettono dati myVAULT sul Web, il software di sicurezza Zone Labs consente o blocca la trasmissione a seconda delle autorizzazioni per il dominio presenti nell'elenco dei siti attendibili. Come avviene per la trasmissione dei contenuti myVAULT mediante posta elettronica, se l'utente decide di memorizzare la risposta per un avviso Blocco ID per un particolare sito Web, questo sito verrà aggiunto automaticamente all'elenco dei siti attendibili con le autorizzazioni impostate secondo le decisioni prese.

### ***Trasmissione di dati mediante messaggistica immediata***

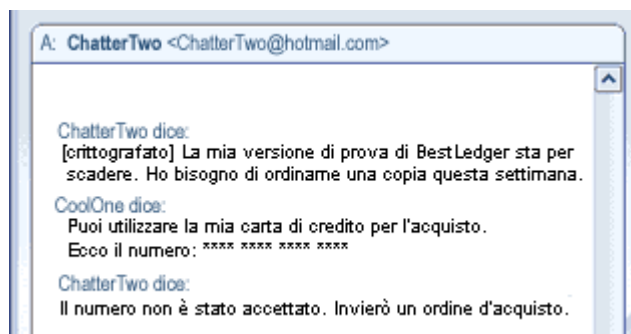
Quando si trasmettono dati di myVAULT durante una conversazione di messaggistica immediata, il software di sicurezza Zone Labs impedisce che le informazioni vengano ricevute.

In Figura 10-1 viene mostrata una conversazione in cui vengono trasmesse delle informazioni salvate in myVAULT. La descrizione dell'elemento salvato in myVAULT (nell'esempio, La mia carta Visa) è visualizzata tra parentesi quadre.



**Figura 10-1: Trasmissione di contenuti di myVAULT**

In Figura 10-2 viene mostrato come le informazioni trasmesse vengono visualizzate sul computer del destinatario. Le informazioni protette vengono sostituite con asterischi in modo da non essere leggibili.



**Figura 10-2: Ricezione di contenuti di myVAULT da parte del destinatario**

## Impostazione del livello di protezione di Blocco ID

La funzione di Blocco ID è disattivata per impostazione predefinita. Attivando il Blocco ID, si garantisce la protezione dei dati inseriti in myVAULT.

1. Selezionare **Blocco ID | Principale**.
2. Nell'area Blocco ID, specificare il livello di protezione desiderato.

Alta	Impedisce che i contenuti di myVAULT vengano inviati verso destinazioni non autorizzate. Il software di sicurezza Zone Labs blocca automaticamente la trasmissione dei dati dell'utente. Se si utilizza un computer condiviso, quest'impostazione è consigliata per avere la massima sicurezza.
Medio	Avvisa l'utente quando le informazioni sull'identità stanno per essere inviate verso destinazioni non presenti nell'elenco dei siti attendibili. Questa è l'impostazione predefinita.
Disattivato	La protezione dell'identità è disattivata. I contenuti di myVAULT possono essere inviati verso qualunque destinazione, che sia presente nell'elenco dei siti attendibili o meno.

## Monitoraggio dello stato di Blocco ID

La sezione Stato del software di sicurezza Zone Labs tiene traccia del numero di elementi salvati in myVAULT e visualizza il numero di occasioni in cui le informazioni dell'utente sono state protette.

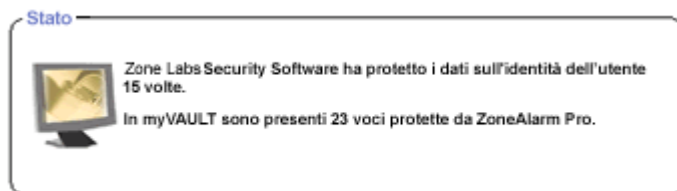


Figura 10-3: Sezione Stato di Blocco ID



# Informazioni su myVAULT

myVAULT fornisce un'area protetta in cui inserire i propri dati personali importanti, quelli che si desidera proteggere dall'attacco di hacker e da furti di identità. Quando il software di sicurezza Zone Labs rileva un tentativo di invio di dati salvati in myVAULT verso una destinazione, determina se queste informazioni devono essere bloccate oppure consentite. Per impostazione predefinita, il software di sicurezza Zone Labs crittografa i dati myVAULT durante il loro inserimento, salvando solamente il valore di hash dei dati invece dei dati stessi. La crittografia dei dati li protegge, poiché non possono essere recuperati usando il valore di hash.

## Aggiungere dati a myVAULT

Anche se è possibile salvare qualsiasi tipo di informazione in myVAULT, è preferibile salvare solamente le informazioni che si desidera proteggere, per esempio il numero di carta di credito e le informazioni di identificazione. Nel caso in cui l'utente salvasse informazioni come lo stato in cui vive (per esempio California) in myVAULT separatamente dal resto dell'indirizzo, digitando "California" in un modulo Web online, il software di sicurezza Zone Labs bloccherebbe ogni volta la trasmissione dei dati.



Se non si è certi del tipo di informazioni da inserire in myVAULT, usare come riferimento le categorie predefinite. Per accedere all'elenco delle categorie, selezionare **Blocco ID | myVAULT**, quindi fare clic su **Aggiungi**.

### Aggiungere informazioni a myVAULT

1. Selezionare **Blocco ID | myVAULT**.
2. Fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo **Aggiunta di informazioni a myVAULT**.

Per la massima protezione, il software di sicurezza Zone Labs crittografa i dati myVAULT per impostazione predefinita. Se non si desidera che i dati vengano crittografati durante l'inserimento, deselezionare la casella di controllo "**Utilizza crittografia one-way...**".

3. Inserire una descrizione dell'elemento che si sta aggiungendo.



Il software di sicurezza Zone Labs visualizza la descrizione dell'elemento negli avvisi Blocco ID. Assicurarsi che la descrizione inserita sia diversa dal valore dell'elemento che si sta aggiungendo, e viceversa. Se le informazioni da proteggere e la descrizione contengono alcuni o tutti i dati, si potrebbero ricevere degli avvisi Blocco ID multipli.

## 4. Selezionare una categoria dall'elenco a discesa.

PIN di accesso	Codice d'accesso personale o altro numero identificativo. Lunghezza massima 6 caratteri. Per una maggiore sicurezza, gli ID d'accesso sono sempre crittografati.
Indirizzo	Lunghezza massima 30 caratteri.
Carta American Express	Per una maggiore sicurezza, il software di sicurezza Zone Labs non registra gli ultimi 5 caratteri del numero di carta American Express dell'utente.
Conto bancario	Lunghezza massima 14 caratteri.
Carta di credito	Per una maggiore sicurezza, il software di sicurezza Zone Labs non registra gli ultimi 4 caratteri del numero di carta di credito dell'utente.
Patente di guida	Lunghezza massima 15 caratteri.
Password eBay	Password che si utilizza per accedere al sito di eBay. La password di eBay può essere inviata solamente al sito di eBay. Lunghezza massima 20 caratteri.
Indirizzo di posta elettronica	Lunghezza massima 60 caratteri.
ID International Tax	Lunghezza massima 15 caratteri.
Nome della madre da nubile	Lunghezza massima 30 caratteri.
Nome	Lunghezza massima 30 caratteri.
Numero di passaporto	Numero di passaporto (Stati Uniti) o altri numeri di identificazione internazionali. Lunghezza massima 30 caratteri.
Password	Inserire la password da proteggere. Lunghezza massima 20 caratteri.
Telefono	I caratteri di separazione come la parentesi e il trattino non sono consentiti. Lunghezza massima 13 caratteri.
Numero di previdenza sociale (Stati Uniti)	Lunghezza minima 9 caratteri.
Altro	Usare questo campo per inserire elementi che non corrispondono a nessuna delle categorie predefinite, oppure che superano il limite di caratteri consentiti per la categoria corrispondente. Lunghezza massima 30 caratteri.

### 5. Inserire i dati da proteggere.



La crittografia dei dati è attivata per impostazione predefinita. Se non si desidera che i dati vengano crittografati, deselezionare la casella di controllo **"Utilizza crittografia one-way...."** A causa della natura sensibile di questi dati, i numeri PIN, le password, le ultime quattro cifre del numero di previdenza sociale e della carta di credito vengono sempre visualizzati come asterischi, che si decida di crittografarli o meno.

Per disattivare la conferma della crittografia che appare per impostazione predefinita, selezionare **Blocco ID | myVAULT**, quindi fare clic su **Opzioni**. Deselezionare la casella di controllo **Mostra finestra di conferma crittografia**.

Al posto dei dati inseriti compariranno degli asterischi e in myVAULT i dati saranno memorizzati in forma crittografata. Il software di sicurezza Zone Labs confronterà i dati crittografati con i testi dei messaggi di posta elettronica in uscita.

6. Specificare se le informazioni devono essere protette quando si utilizza il Web, la posta elettronica e la messaggistica immediata (solo in ZoneAlarm Security Suite).
7. Fare clic su **OK** per salvare le modifiche.

## Modifica e rimozione dei contenuti di myVAULT

All'interno della scheda myVAULT è possibile modificare le impostazioni di crittografia, rimuovere i contenuti myVAULT e modificare i dati non crittografati. Poiché i dati crittografati vengono visualizzati sotto forma di asterischi, sono illeggibili e perciò non possono essere modificati.

### Modificare i contenuti di myVAULT

1. Selezionare **Blocco ID | myVAULT**.
2. Selezionare l'elemento che si desidera modificare, quindi fare clic su **Modifica**.  
Viene visualizzata la finestra di dialogo Modifica di informazioni da myVAULT.
3. Modificare i dati come opportuno, quindi fare clic su **OK** per salvare le modifiche.

### Rimuovere contenuti da myVAULT



Selezionare l'elemento che si desidera rimuovere, quindi fare clic su **Rimuovi**.



Se si rimuove l'ultimo elemento in myVAULT, il livello di protezione Blocco ID viene impostato su Disattivato. Se successivamente si aggiungono altri elementi a myVAULT, viene ripristinato il livello di protezione predefinito, Medio.

# Utilizzo dell'elenco dei siti attendibili

myVAULT fornisce un'area protetta in cui inserire i propri dati personali importanti, quelli che si desidera proteggere dall'attacco di hacker e da furti di identità. Quando il software di sicurezza Zone Labs rileva un tentativo di invio di dati salvati in myVAULT verso una destinazione, determina se queste informazioni devono essere bloccate oppure consentite, verificando che quella destinazione sia considerata attendibile.

L'elenco dei siti attendibili visualizza due tipi di siti: i siti Security Alliance e quelli personalizzati. I siti Security Alliance sono siti Web che Zone Labs, Inc. ha autenticato per garantire che non siano fraudolenti. I siti personalizzati sono i siti che l'utente aggiunge all'elenco.

## Visualizzazione elenco dei siti attendibili

Oltre ai siti considerati attendibili insieme per le informazioni personali, all'elenco è possibile aggiungere dei siti che *non* si vuole considerare attendibili, per esempio siti di spam e di chat, impedendo così che le informazioni vengano loro inviate.

L'elenco dei siti attendibili consente anche di specificare quali siti sono autorizzati per l'invio della password come *testo in chiaro*. Poiché le password in chiaro non sono crittografate, possono essere visualizzate facilmente da altre persone se vengono intercettate durante la trasmissione.

Autorizzazione di accesso	Sito	Tipo	Autorizzazione per le password in chiaro
✓	computerassociates.com	Personalizzato	✓
✓	eBay & PayPal	Security Alliance	?
✗	msn.com	Personalizzato	✗

Figura 10-4: Elenco dei siti attendibili

### **Autorizzazione di accesso**

Specifica se il software di sicurezza Zone Labs deve consentire, bloccare, o avvisare l'utente prima di inviare contenuti myVAULT alle destinazioni elencate. Per modificare le autorizzazioni per un sito, fare clic nella colonna Autorizzazione accanto al sito e selezionare **Consenti**, **Blocca**, o **Chiedi**.

### **Sito**

Visualizza il dominio del sito.

### **Tipo**

Specifica se il sito è un partner di Security Alliance o un sito personalizzato.

### ***Password in chiaro***

Specifica se il software di sicurezza Zone Labs deve consentire, bloccare o avvisare l'utente prima di inviare password come testo in chiaro alle destinazioni elencate. Per modificare le autorizzazioni per un sito, fare clic nella colonna Password in chiaro accanto al sito e selezionare **Consenti**, **Blocca**, o **Chiedi**.

### ***Dettagli per il sito***

Oltre al nome e al tipo di sito, nella casella Dettagli voce vengono visualizzati l'indirizzo IP e la data e l'ora dell'ultimo accesso al sito.

## **Aggiunta all'elenco dei siti attendibili**

L'elenco dei siti attendibili visualizza due tipi di siti: i siti personalizzati e quelli Security Alliance. I siti personalizzati sono i siti che l'utente aggiunge all'elenco. I siti partner di Security Alliance sono i siti di cui Zone Labs ha verificato la legittimità e che sono stati aggiunti automaticamente.

I siti personalizzati sono attendibili a livello di dominio, perciò ogni sottodominio che si desidera considerare attendibile deve essere aggiunto separatamente. Per esempio, [www.msn.com](http://www.msn.com) e [shopping.msn.com](http://shopping.msn.com) dovrebbero essere aggiunti separatamente. I siti di Security Alliance considerano esplicitamente attendibili tutti i sottodomini, non è quindi necessario creare una voce per ogni sottodominio che si desidera considerare attendibile.

### **Aggiungere un sito all'elenco dei siti attendibili**

1. Selezionare **Blocco ID | Siti attendibili**, quindi fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo Aggiungi sito attendibile.

2. Digitare l'URL del sito (omettendo <http://>), quindi fare clic su **OK**.

Facendo clic su OK, il software di sicurezza Zone Labs verifica l'indirizzo del sito e registra l'indirizzo IP. Questo processo potrebbe durare alcuni secondi.

3. Modificare le autorizzazioni del sito a piacimento.

Per impostazione predefinita, le autorizzazioni di accesso e delle password in chiaro per i siti personalizzati vengono impostate su Chiedi.

## **Modifica e rimozione dei siti attendibili**

Nella scheda Siti attendibili, è possibile modificare le autorizzazioni di accesso per un sito, e modificare o rimuovere i siti personalizzati. Anche se è possibile modificare le autorizzazioni per i siti di Security Alliance, non è possibile modificare o rimuovere la voce del sito.


### **Modificare un sito personalizzato**

1. Fare doppio clic sul sito che si desidera modificare.

Viene visualizzata la finestra di dialogo Modifica sito attendibile.

2. Modificare il sito come opportuno, quindi fare clic su **OK** per salvare le modifiche.

**Rimuovere un sito personalizzato**

 Fare clic con il pulsante destro del mouse sul sito che si desidera rimuovere, quindi selezionare **Rimuovi**.

# Capitolo

---

## Controllo genitori



Il Controllo genitori protegge la famiglia dai siti Web che contengono violenza, pornografia o altro contenuto non desiderabile. È possibile scegliere quali categorie di siti Web bloccare e utilizzare il filtro intelligente per classificare e filtrare in modo istantaneo siti non classificati in precedenza.

La funzione Controllo genitori è disponibile solo in ZoneAlarm Security Suite.

### Argomenti:

- "Comprendere il Controllo genitori", a pagina 190
- "Attivazione del Controllo genitori e del filtro intelligente", a pagina 191
- "Scegliere quali categorie bloccare", a pagina 193

---

# Comprendere il Controllo genitori

Quando il browser accede a un sito Web o ad altro contenuto basato sul Web, il ZoneAlarm Security Suite contatta i server *Blue Coat™* Parental Control per vedere in che modo è stato classificato il contenuto di tale sito. Se il sito che il browser sta tentando di raggiungere è stato posto da Blue Coat™ in una categoria che si è deciso di bloccare, l'accesso a tale sito viene negato. Questo processo richiede normalmente meno di un secondo. Viene visualizzata la pagina Violazione del Controllo genitori, con la spiegazione del motivo per cui il sito è stato bloccato. Se non si è d'accordo con questa classificazione, è possibile richiedere una rivalutazione del sito facendo clic sulla pagina Violazione filtro Web che appare quando il sito viene bloccato.

La funzione Controllo genitori è disponibile solo in ZoneAlarm Security Suite.



## Attivazione del Controllo genitori e del filtro intelligente

Quando si attiva il Controllo genitori, si bloccano immediatamente i siti Web che, secondo quanto rilevato da Blue Coat, contengono nudità, pornografia, informazioni su droghe illegali, testo o immagini razziste e altro contenuto ai quali non si desidera esporre i propri figli. Se si attiva il filtro intelligente, i siti nuovi e non classificati vengono istantaneamente classificati e filtrati, migliorando la protezione.



Per impedire che i bambini modifichino le impostazioni del Controllo genitori, impostare una password per il software di sicurezza Zone Labs. Vedere "Impostazione della password", a pagina 22.

La funzione Controllo genitori è disponibile solo in ZoneAlarm Security Suite.

### Attivazione o disattivazione del Controllo genitori

Il Controllo genitori consente di bloccare i siti impostati su Blocca nell'elenco delle categorie. Se il Controllo genitori non è attivato, le impostazioni Categoria e Filtro intelligente vengono ignorate.

#### Attivare o disattivare il controllo genitori

1. Selezionare **Controllo genitori | Principale**.
2. Nella sezione Controllo genitori, selezionare **Attivato** o **Disattivato**.

### Attivazione o disattivazione del filtro intelligente

Il filtro intelligente DRTR (Dynamic Real-Time Rating) consente di bloccare i siti indesiderati anche se sono nuovi e non sono stati ancora classificati. Quando questa funzione è attivata e il computer accede a contenuto non classificato, Blue Coat™ analizza istantaneamente il contenuto del sito Web e lo pone in una categoria. Il sito viene quindi bloccato o consentito in base alle impostazioni in Controllo genitori. Questo processo richiede normalmente dai due ai quattro secondi.

#### Attivare o disattivare il filtro intelligente

1. Selezionare **Controllo genitori | Principale**.
2. Nella sezione Filtro intelligente, selezionare **Attivato** o **Disattivato**.

Per accedere a questa opzione, il Controllo genitori deve essere attivato.

## Impostazione delle opzioni di timeout

Le opzioni di timeout determinano per quanto tempo il software di sicurezza Zone Labs tenta di ottenere la classificazione di un sito Web e cosa fare nel caso non sia in grado di ottenerla.

### Impostare le opzioni di timeout

1. Selezionare **Controllo genitori** | **Principale**, quindi fare clic su **Avanzate**.

Viene visualizzata la finestra di dialogo Opzioni Controllo genitori.

2. Specificare le preferenze di timeout.

Timeout Controllo genitori (sec)	L'intervallo, in secondi, per il quale il software di sicurezza Zone Labs tenterà di ottenere una classificazione quando il filtro intelligente è disattivato.
Timeout quando DRTR è attivato (sec)	L'intervallo, in secondi, per il quale il software di sicurezza Zone Labs tenterà di ottenere una classificazione quando il filtro intelligente è attivato.
Quando i livelli non sono disponibili	Specifica se il software di sicurezza Zone Labs deve consentire o bloccare i siti per i quali la classificazione non è disponibile.

3. Fare clic su **OK**.



Se l'opzione **Quando i livelli non sono disponibili** è impostata su **consenti l'accesso al sito**, impostare le opzioni di timeout su un valore molto basso potrebbe determinare l'accesso a siti indesiderati. Si consiglia di mantenere le opzioni di timeout predefinite.

# Scegliere quali categorie bloccare

La funzione Controllo genitori è disponibile solo in ZoneAlarm Security Suite.

La funzione Controllo genitore fornisce numerose categorie per filtrare il contenuto Web. Nella Tabella 11-1 seguente è fornita la descrizione di ciascuna categoria, insieme all'impostazione predefinita.

## Modificare l'impostazione di una categoria

1. Selezionare **Controllo genitori | Categorie**.
2. Nella colonna Categorie di siti da bloccare, selezionare o deselezionare la casella di controllo accanto alla categoria.

Un segno di spunta rosso indica che il contenuto appartenente a tale categoria verrà bloccato. Una casella di controllo vuota indica che il contenuto appartenente a tale categoria verrà consentito.



Per bloccare tutte le categorie dei siti, fare clic su **Seleziona tutto**. Per consentire tutte le categorie dei siti, fare clic su **Cancella tutto**. Per ripristinare le impostazioni predefinite, fare clic sul collegamento **Ripristina predefiniti**.

Categoria	Definizione	Impostazione predefinita
Oscenità	Sito che fornisce informazioni o argomenti in favore o contro l'aborto, descrive le procedure dell'aborto, offre aiuto per ottenere o evitare l'aborto, fornisce informazioni sull'effetto fisico, sociale, mentale, morale o emotivo dell'aborto o della mancanza di questo.	Consentito
Adulti: abbigliamento intimo/costumi da bagno	Siti che offrono immagini di modelle in lingerie, costumi da bagno o altri tipi di indumenti allusivi. Questo non include siti che vendono abbigliamento intimo come sottosezione di altri prodotti offerti.	Consentito
Adulti: nudità	Siti contenenti raffigurazioni di nudità o semi-nudità o immagini del corpo umano. Queste raffigurazioni non hanno necessariamente intento o effetto sessuale ma possono comprendere siti che contengono dipinti di nudo o rassegne fotografiche di natura artistica. Include inoltre siti di nudisti o naturisti che contengono immagini di persone nude.	Bloccato
Adulti: pornografia	Siti contenenti materiale sessualmente esplicito allo scopo di sollecitare interesse sessuale.	Bloccato

**Tabella 11-1: Categorie Controllo genitori**

<b>Categoria</b>	<b>Definizione</b>	<b>Impostazione predefinita</b>
Adulti: educazione sessuale	Siti che forniscono informazioni sulla riproduzione, lo sviluppo sessuale, le malattie trasmesse sessualmente, la contraccezione, le pratiche di sesso sicuro, la sessualità e l'orientamento sessuale. Questo non comprende i siti che offrono suggerimenti o consigli su come praticare il sesso in modo migliore.	Consentito
Alcol/Tabacco	Siti che promuovono o che offrono prodotti alcolici o per fumatori o che forniscono i mezzi per crearli. Possono essere compresi i siti che esaltano, reclamizzano o incoraggiano altrimenti il consumo di alcol o tabacco.	Bloccato
Chat/ Messaggistica immediata	Siti che offrono funzionalità di chat e messaggistica immediata.	Consentito
Azioni criminali/ Azioni illegali/ Imbrogli	Siti che patrocinano o forniscono consigli sull'esecuzione di atti illegali, quali il furto di un servizio, la violazione delle leggi in vigore, le frodi, le tecniche di svaligiamento e il plagio. Siti che forniscono istruzioni o promuovono il crimine, il comportamento non etico e disonesto o evadere l'accusa.	Bloccato
Culto/Occulto	Importanti gruppi religiosi moderni organizzati che vengono identificati come "culti" da tre o più fonti autorevoli. Siti che promuovono o che offrono metodi, mezzi di istruzione o altre risorse per influire su eventi reali attraverso l'uso di incantesimi, maledizioni, poteri magici o essere soprannaturali.	Consentito
Relazioni e incontri	Siti che promuovono relazioni interpersonali. Non include quelli pertinenti alle tendenze gay o lesbico.	Consentito
Droghe: droghe illegali	Siti che promuovono, offrono, vendono, forniscono, incoraggiano o altrimenti patrocinano l'uso illegale, la coltivazione, la produzione o la distribuzione di farmaci, sostanze farmaceutiche, piante intossicanti o altre sostanze chimiche e i relativi accessori.	Bloccato
Posta elettronica	Siti che offrono servizi di posta elettronica basati sul Web.	Consentito
Freeware/ Download di software	Siti che promuovono o che offrono software o prodotti gratuiti per il download generale o per scopi di prova.	Consentito

**Tabella 11-1: Categorie Controllo genitori**

<b>Categoria</b>	<b>Definizione</b>	<b>Impostazione predefinita</b>
Gioco d'azzardo	Siti in cui l'utente può piazzare una scommessa o partecipare a un pool di scommesse (incluse le lotterie) online, ottenere informazioni, assistenza o consigli su come piazzare una scommessa; ricevere istruzioni, assistenza o formazione sulla partecipazione nei giochi d'azzardo. Non comprende i siti che vendono prodotti o macchine relativi ai giochi d'azzardo.	Bloccato
Gay e lesbiche	Siti che forniscono informazioni o che si rivolgono allo stile di vita gay e lesbico. Non comprende i siti di orientamento sessuale.	Consentito
Glamour/Stile di vita	Siti che enfatizzano o forniscono informazioni o notizie su come l'utente può migliorare l'aspetto fisico, il fascino, la bellezza o lo stile in relazione al proprio aspetto.	Consentito
Governo: forze armate	Siti che promuovono o forniscono informazioni sui rami militari o sulle forze armate.	Consentito
Hacking/ Aggiramento sistemi proxy	Siti che forniscono informazioni sull'accesso o sull'uso illegale o discutibile di apparecchiature/software di telecomunicazione o che forniscono informazioni su come eludere funzioni di server proxy oppure ottenere l'accesso a URL in qualsiasi modo eludendo il server proxy.	Bloccato
Umore/Barzellette	Siti incentrati principalmente sulla comicità, le barzellette, il divertimento e così via. Non comprende i siti che contengono barzellette per adulti.	Consentito
Vendite all'asta su Internet	Siti che supportano l'offerta e l'acquisto di beni tra privati.	Consentito
MP3/Streaming	Siti che supportano e/o consentono agli utenti di scaricare musica e file multimediali quali MP3, MPG, MOV e così via. Comprende anche i siti che forniscono flussi multimediali (radio, film, TV).	Consentito
Newsgroup	Siti che offrono l'accesso a newsgroup di Usenet o siti simili.	Consentito
News e mezzi di informazione	Siti che riportano principalmente informazioni o commenti sugli eventi attuali o sulle questioni contemporanee del giorno. Voci quali il tempo, gli editoriali e gli interessi umani sono considerati target nell'ambito del contesto dei siti informativi principali.	Consentito

**Tabella 11-1: Categorie Controllo genitori**

<b>Categoria</b>	<b>Definizione</b>	<b>Impostazione predefinita</b>
Giochi online	Siti che forniscono informazioni e supportano la partecipazione a giochi o il download, videogame, giochi per computer, giochi elettronici, suggerimenti e consigli sui giochi o su come ottenerne i codici, giornali e riviste dedicati ai giochi, giochi online, nonché i siti che supportano oppure ospitano giochi online che includono lotterie e omaggi.	Consentito
Siti a pagamento	Siti che offrono di pagare gli utenti se fanno clic su specifici collegamenti o posizioni.	Bloccato
Politici/attivisti	Siti sponsorizzati da specifici partiti o gruppi politici e che contengono informazioni a essi relative. Siti sponsorizzati o dedicati a organizzazioni che promuovono cambio o riforme nella politica pubblica, nella pubblica opinione, nella pratica sociale, nelle attività e relazioni economiche. Esclude i siti sponsorizzati commercialmente dedicati alla politica o alla legislazione elettorale.	Consentito
Religione	Siti che promuovono e forniscono informazioni su buddismo, baha'I, cristianesimo, scienza cristiana, induismo, islam, giudaismo, mormonismo, shintoismo, sikhismo, ateismo, altre religioni convenzionali o non convenzionali o soggetti quasi religiosi, nonché chiese, sinagoghe, altri luoghi di culto, qualsiasi fede o credo religioso incluse le religioni "alternative" quali Wicca e arti magiche.	Consentito
Motori di ricerca/ Portali	Siti che supportano la ricerca sul Web, indici ed elenchi in linea.	Consentito
Shopping	Siti che forniscono i mezzi per ottenere prodotti e servizi che soddisfano le esigenze o i desideri umani. Questo non comprende prodotti o servizi che sono principalmente commercializzati per soddisfare esigenze industriali o commerciali.	Consentito
Sport/Svago/ Passatempo	Siti che promuovono o forniscono informazioni su sport per spettatori.	Consentito

**Tabella 11-1: Categorie Controllo genitori**

Categoria	Definizione	Impostazione predefinita
Violenza/Odio/ Razzismo	Siti che patrocinano o forniscono istruzioni che causano lesioni personali a persone o danni a cose attraverso l'uso di armi, esplosivi, scherzi o altri tipi di violenza. Siti che patrocinano ostilità o aggressione nei confronti di singoli o gruppi in base a razza, religione, genere, nazionalità, origine etnica o altre caratteristiche involontarie; un sito che denigra gli altri in base a tali caratteristiche o che giustifica l'ineguaglianza sulla base di tali caratteristiche; un sito che ha la pretesa di utilizzare metodi scientifici o altri metodi comunemente accreditati per giustificare l'aggressione, l'ostilità o la denigrazione succitate.	Bloccato
Armi	Siti che vendono, recensiscono o descrivono armi, quali pistole, coltelli o dispositivi di arti marziali o che forniscono informazioni sul loro utilizzo, sugli accessori o altre modifiche.	Bloccato
Comunicazione Web/Message board	Siti che consentono oppure offrono comunicazione basata sul Web mediante qualsiasi metodo tra quelli seguenti: posta elettronica (basata sul Web), chat, messaggistica immediata, Message Board e così via.	Consentito
Hosting Web/ Pagine Web personali	Siti di organizzazioni che forniscono pagine di dominio di livello superiore di comunità Web o servizi di hosting. Siti che ospitano servizi di chat Web, chat room su IRC, siti chat tramite HTTP, home page dedicate a IRC, nonché i siti che offrono forum o gruppi di discussione. Siti che promuovono o forniscono i mezzi per praticare atti illegali o non autorizzati mediante competenze di programmazione informatica (hacking).  Anche i siti contenenti TUTTI i tipi di contenuto quale GEO Cities.	Consentito

**Tabella 11-1: Categorie Controllo genitori**



Se si utilizza il ZoneAlarm Security Suite e si sceglie di bloccare nuove categorie, è opportuno cancellare la cache del browser per rimuovere le pagine dai siti appena bloccati che possono esservi memorizzati. Altrimenti, chiunque utilizza il computer avrà accesso al contenuto bloccato che è stato memorizzato nella cache del browser.





# Capitolo

---

## IM Security (Instant Messaging Security)

12

IM Security di Zone Labs è la difesa di prima linea contro le minacce della messaggistica immediata. I livelli di sicurezza predefiniti di IM Security forniscono un'immediata protezione contro gli hacker e lo spam e forniscono i controlli che impediscono l'invio inopportuno di contenuti Web al client di messaggistica immediata.

La funzione IM Security è disponibile solo in ZoneAlarm Security Suite.

Argomenti:

- "Panoramica di IM Security", a pagina 200
- "Impostazione delle opzioni di IM Security", a pagina 206

# Panoramica di IM Security

Il software di sicurezza Zone Labs fornisce una sicurezza completa per la messaggistica immediata (IM) per la maggior parte dei prodotti che offrono questi servizi, tra cui MSN Messenger e Yahoo! Messenger, AOL Instant Messenger e ICQ. IM Security supporta anche programmi di terzi che vengono eseguiti su questi servizi, quale Trillian. IM Security mantiene private le conversazioni di messaggistica immediata e protegge i computer da spammer IM, ladri di identità, hacker e predatori che sfruttano connessioni IM vulnerabili.

IM Security include le funzioni seguenti:

- **Controllo accesso** - Controlla a quali servizi IM è possibile accedere mediante il computer.
- **Blocco spam** - Blocca i messaggi inviati da utenti non presenti nell'elenco dei contatti.
- **Controllo caratteristica** - Determina quali funzioni IM sono consentite sul computer.
- **Protezione in entrata** - Protegge il computer contro gli attacchi filtrando messaggi non validi, script pericolosi e URL eseguibili.
- **Crittografia messaggi** - Protegge il traffico IM da possibili intercettazioni e lettura da parte di terzi.



Le funzioni di protezione descritte in precedenza sono pertinenti solo alle conversazioni uno a uno. Il software di sicurezza Zone Labs non protegge le conversazioni con più partecipanti (per esempio, conversazioni in una chat room).

## Accesso

Mediante il controllo dell'accesso è possibile consentire o bloccare il traffico di un particolare servizio di messaggistica immediata.

### Bloccare o consentire il traffico IM per un particolare servizio

1. Selezionare **Sicurezza | Impostazioni**.
2. Nella colonna **Accesso**, fare clic accanto al servizio di messaggistica immediata per il quale si desidera bloccare o consentire il traffico.
3. Selezionare **Consenti** o **Blocca**.

## Bloccare lo spam

Blocco spam esclude le comunicazioni non desiderate di mittenti non presenti nell'elenco dei contatti. Per impostazione predefinita, Blocco spam è attivato solo quando il livello di IM Security è impostato su Alto. In ogni caso, è possibile

personalizzare le impostazioni per attivare Blocco spam per un particolare servizio a prescindere dal livello di protezione.



Non viene visualizzata alcuna conferma che il software di sicurezza Zone Labs ha bloccato un messaggio in arrivo, tuttavia è possibile consultare il log per stabilire l'identità del mittente. Se si desidera ricevere in futuro i messaggi da questo mittente, accertarsi di aggiungere il relativo ID all'elenco contatti dei programmi di messaggistica immediata. I messaggi bloccati appaiono nel Visualizzatore log con la dicitura "È stato bloccato un messaggio proveniente da un mittente non incluso nell'elenco contatti" nella colonna Tipo.

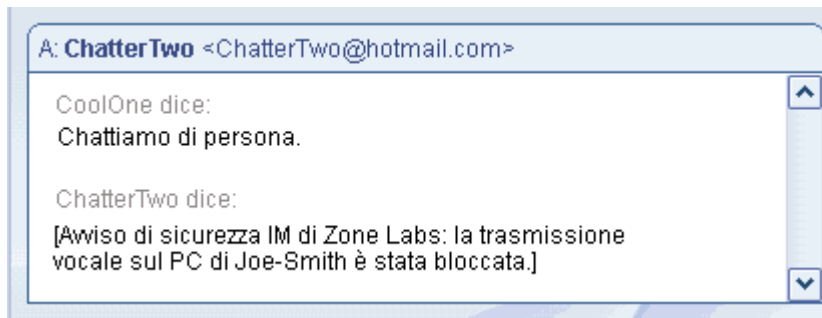
### **Attivare o disattivare Blocco spam per un particolare servizio**

1. Selezionare **Sicurezza | Impostazioni**.
2. Individuare il servizio di messaggistica immediata che si desidera personalizzare, quindi fare clic sulla colonna **Blocco spam**.
3. Selezionare **Attivato** o **Disattivato**.

## Controllo caratteristica

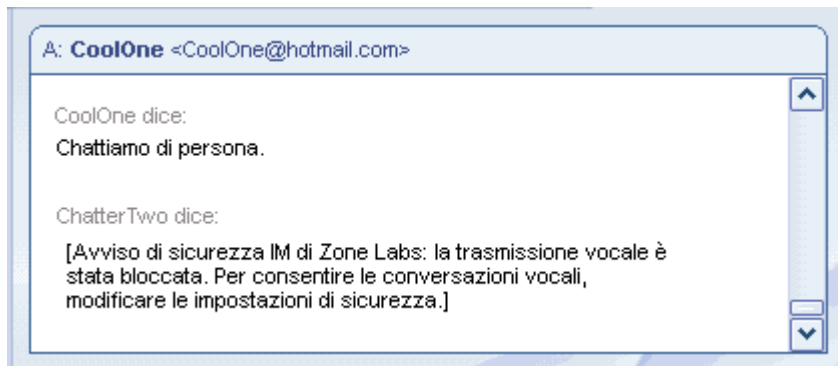
Le impostazioni di Controllo caratteristica consentono di limitare i tipi di elementi multimediali che è possibile ricevere durante la sessione di messaggistica immediata. Poiché potrebbe essere inviato contenuto inopportuno in molte forme, il software di sicurezza Zone Labs consente ai genitori di proteggere i bambini bloccando tipi specifici di elementi multimediali dalle sessioni di messaggistica immediata, tra cui trasmissioni audio, video e vocali.

Quando un messaggio è bloccato, il mittente viene avvisato, come illustrato nella Figura 12-1.



**Figura 12-1: Invio di una trasmissione vocale bloccata**

Anche il destinatario riceve un avviso, come illustrato nella Figura 12-2.



**Figura 12-2: Blocco di una trasmissione vocale in arrivo**

### Personalizzare le impostazioni di Controllo caratteristica

1. Selezionare **Sicurezza | Impostazioni**.
2. Individuare il servizio di messaggistica immediata che si desidera personalizzare, quindi fare clic sulla colonna **Controllo caratteristica**.
3. Fare clic su **Audio**, **Video** o **File**, quindi scegliere **Consenti** o **Blocca**.

## Protezione in entrata

Le impostazioni della protezione in entrata consentono di specificare a quali servizi di messaggistica immediata è consentito trasmettere collegamenti attivi e tag di formattazione, quali JavaScript, nei messaggi in entrata. I collegamenti attivi e i tag di formattazione possono contenere virus in grado di attaccare il computer quando si fa clic su un collegamento in un messaggio.

L'impostazione dei "tag" in entrata rimuove la formattazione supplementare che potrebbe contenere script e altro codice potenzialmente dannoso. L'impostazione dei tag rimuove anche la formattazione innocua, come grassetto, sottolineato, corsivo, e così via.

L'impostazione "Attivo" blocca i collegamenti che, se selezionati, possono eseguire codice o scaricare file pericolosi sul computer.

Quando si invia un collegamento attivo a un contatto, questo appare come illustrato nella Figura 12-3.

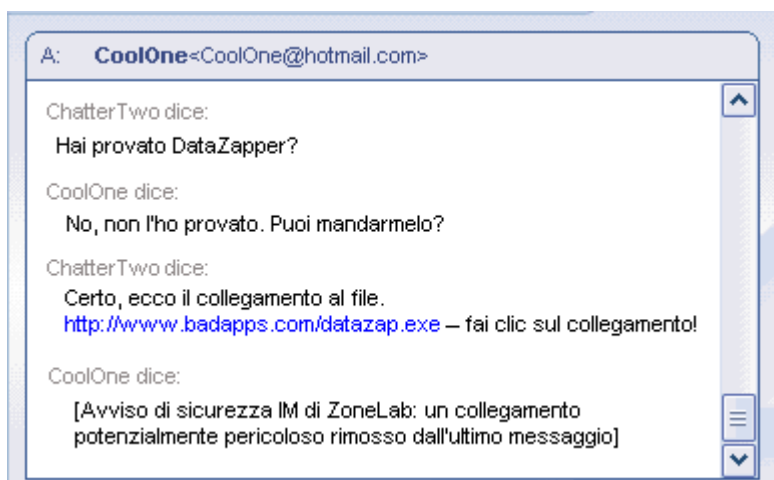


Figura 12-3: Invio di un URL eseguibile a un contatto

Quando un collegamento attivo viene filtrato da un messaggio, il destinatario viene avvisato, come illustrato nella Figura 12-4.

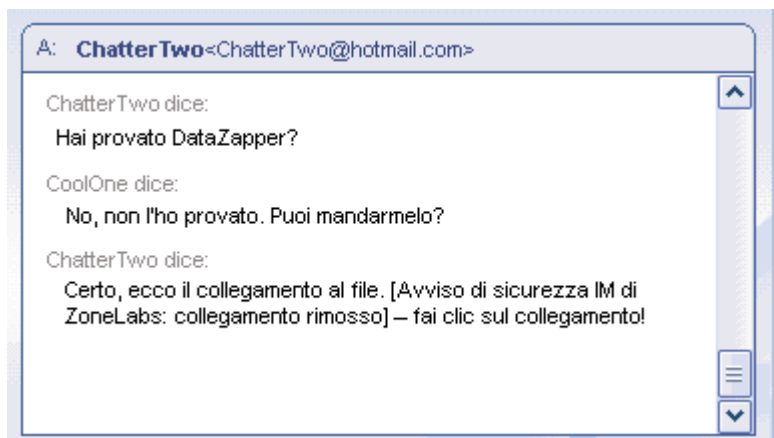


Figura 12-4: Collegamento potenzialmente dannoso rimosso

### Personalizzare le impostazioni di protezione in entrata

1. Selezionare **Sicurezza | Impostazioni**.
2. Individuare il servizio di messaggistica immediata che si desidera personalizzare, quindi fare clic sulla colonna **In entrata**.
3. Fare clic sotto **Tag** o **Attivo**, quindi scegliere **Consenti** o **Blocca**.

### Crittografia del traffico di messaggistica immediata

La crittografia impedisce a terzi di intercettare e leggere le conversazioni di messaggistica immediata dell'utente. Per crittografare le conversazioni di messaggistica immediata, entrambe le parti devono avere installato ZoneAlarm Security Suite e avere un account sullo stesso servizio IM. Le conversazioni non verranno crittografate se le parti non sono reciprocamente presenti nell'elenco contatti, anche se hanno installato ZoneAlarm Security Suite.

Quando si avvia una conversazione con un altro utente di ZoneAlarm Security Suite ed entrambi gli interlocutori hanno attivato la funzione di crittografia per il servizio IM al quale si è connessi, il termine **crittografia** appare tra parentesi dopo l'ID di messaggistica immediata del contatto. Se si avvia una conversazione con un contatto che non utilizza ZoneAlarm Security Suite o che non ha attivato la funzione di crittografia, apparirà il termine **non crittografato** dopo l'ID di messaggistica immediata del contatto.

Nella Figura 12-5 è illustrata una conversazione crittografata.

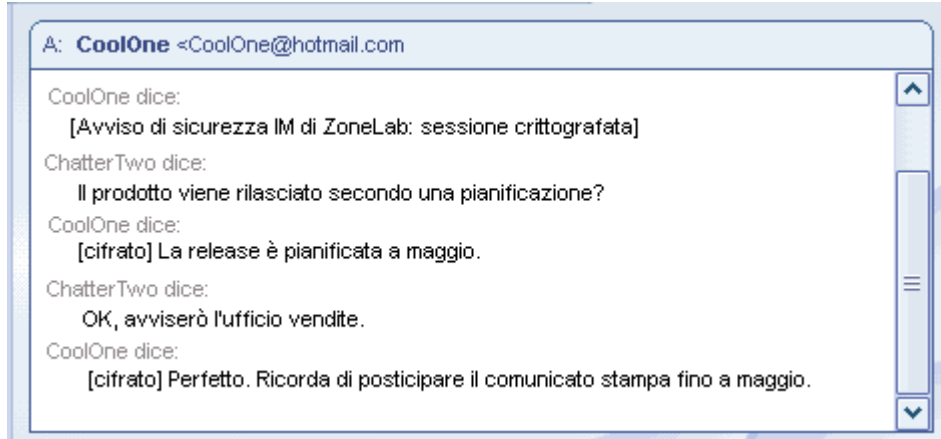


Figura 12-5: Esempio di conversazione crittografata.

Qui è riportata la stessa conversazione illustrata in precedenza, ma questa volta in modalità non crittografata.

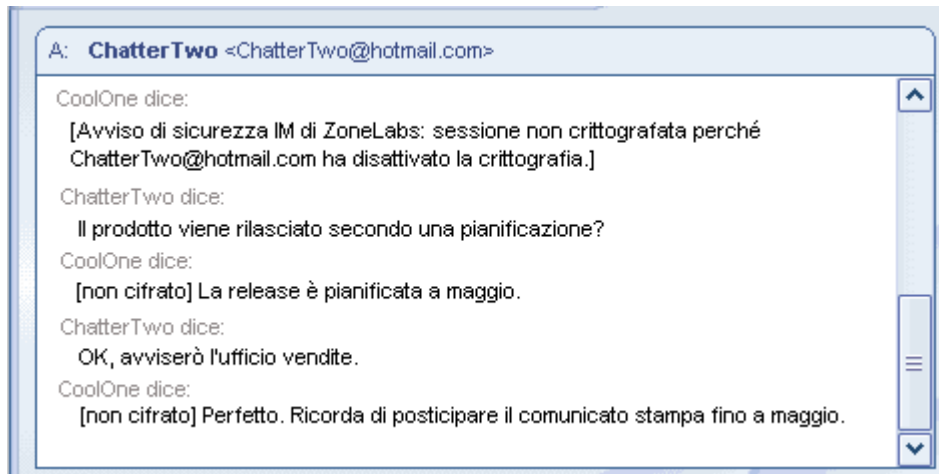


Figura 12-6: Esempio di conversazione non crittografata

### Attivare o disattivare la crittografia di un particolare servizio IM

1. Selezionare **Sicurezza | Impostazioni**.
2. Nella colonna Crittografia, fare clic accanto al servizio che si desidera crittografare.
3. Selezionare **Consenti** o **Blocca**.

### *Come vengono crittografati i messaggi immediati*

ZoneAlarm Security Suite si affida alla libreria *OpenSSL* per i servizi di crittografia. Il testo di ciascun messaggio in una sessione sicura è crittografato con codice a *3DES* 168-bit. ZoneAlarm Security Suite crea in modo automatico e trasparente un *certificato autofirmato* per ciascuno degli account IM dell'utente al primo accesso. All'inizio della prima conversazione IM tra due utenti di ZoneAlarm Security Suite dopo l'installazione del programma, i certificati vengono scambiati in modo trasparente tra gli utenti e memorizzati nel computer. La chiave pubblica di uno dei certificati viene utilizzata per crittografare la chiave di sessione da utilizzare per la durata di sessione.

# Impostazione delle opzioni di IM Security

Il software di sicurezza Zone Labs protegge il computer applicando limitazioni al software di messaggistica immediata, filtro dello spam e crittografia del traffico dei messaggi immediati. In abbinamento alla funzione Blocco ID, il software di sicurezza Zone Labs impedisce la trasmissione dei dati personali durante una sessione di messaggistica immediata senza l'autorizzazione dell'utente. È possibile specificare il livello di protezione desiderato mediante opzioni predefinite oppure personalizzando manualmente le singole impostazioni di sicurezza.

- ☞ Impostazione del livello di protezione
- ☞ Visualizzazione dello stato di protezione di IM Security
- ☞ Personalizzazione delle impostazioni di protezione
- ☞ Impostazione delle opzioni avanzate di IM Security
- ☞ Visualizzazione del log degli eventi relativi a IM Security

## Impostazione del livello di protezione

Il livello di protezione Medio predefinito rappresenta un compromesso tra sicurezza e convenienza, che consente le funzioni di messaggistica immediata, mentre assicura che tali comunicazioni siano sicure.

### Impostare il livello di protezione globale

1. Selezionare **IM Security | Principale**.
2. Nella sezione **Livello della protezione**, trascinare il dispositivo di scorrimento sull'impostazione desiderata.

Alta	Impedisce ai programmi di messaggistica immediata di inviare file multimediali di tutti i tipi, filtra messaggi spam, URL eseguibili e crittografa il traffico di messaggistica immediata.
Medio	Questa è l'impostazione predefinita. Crittografa il traffico di messaggistica immediata e filtra gli URL eseguibili.
Disattivato	Protezione messaggistica immediata disattivata.

## Visualizzazione dello stato di protezione di IM Security

È possibile visualizzare lo stato della protezione di IM Security dalla scheda Principale. La sezione Protezione fornisce le statistiche del numero di messaggi bloccati che hanno violato le impostazioni di sicurezza delle opzioni In entrata, Blocco spam e Controllo caratteristica.



Il Log cronologia programma elenca tutti i programmi IM attivi e visualizza data e ora più recenti in cui i programmi sono stati utilizzati.



Se si avvia un programma IM prima di avviare il software di sicurezza Zone Labs, il programma IM non appare nel Log cronologia. Per riflettere in modo preciso tutta l'attività IM, avviare i programmi IM dopo aver avviato il software di sicurezza Zone Labs.

## Personalizzazione delle impostazioni di protezione

Impostando il livello di protezione su Alto, Medio o Disattivato, si specifica globalmente se i programmi di messaggistica immediata possono inviare file, JavaScript e collegamenti al proprio client IM. In alcuni casi, si potrebbe voler specificare per un singolo servizio impostazioni diverse da queste impostazioni globali.

### Personalizzare le impostazioni di protezione

1. Selezionare **IM Security | Impostazioni**.
2. Individuare il servizio che si desidera modificare, quindi fare clic con il pulsante destro del mouse nella colonna del contenuto da personalizzare.

Accesso	Se impostato su Blocca, il traffico di messaggistica immediata proveniente da qualsiasi programma che utilizza il servizio selezionato viene bloccato.
Blocco spam	Se impostato su Attivato, blocca i messaggi inviati da persone che non sono presenti nell'elenco contatti.
Controllo caratteristica	Se impostato su Blocca, la trasmissione di audio, video o file è bloccata.
In entrata	Specifica se i tag di formattazione, quali JavaScript o collegamenti eseguibili, possono essere contenuti nei messaggi in entrata.
Crittografa	Specifica se il traffico di messaggistica immediata è crittografato.



Per tornare al livello di protezione Medio predefinito, selezionare **IM Security | Principale**, quindi fare clic su **Ripristina predefiniti**.

## Impostazione delle opzioni avanzate di IM Security

Per impostazione predefinita, il software di sicurezza Zone Labs avvisa l'utente quando del contenuto dannoso viene filtrato dalla conversazione IM e lo informa se le sessioni sono crittografate o meno. Mediante la finestra di dialogo Avanzate, è possibile modificare queste e altre impostazioni.

### Impostare le opzioni avanzate di IM Security

1. Selezionare **IM Security | Impostazioni**, quindi fare clic su **Avanzate**.

## 2. Specificare le impostazioni.

Avvisa contatti che è attiva la protezione di Zone Labs IM Security	Quando si avvia una conversazione con un contatto dopo aver installato il software di sicurezza Zone Labs, il contatto riceverà un avviso che l'utente è protetto. <b>Nota:</b> questa notifica avviene solo durante la prima sessione dopo l'installazione. I contatti dell'utente non riceveranno notifica durante le sessioni successive.
Avvisa dello stato di crittografia di ogni sessione IM	Il software di sicurezza Zone Labs contrassegna l'inizio di ciascuna sessione IM con l'etichetta predefinita "crittografato" o "non crittografato".
Etichetta messaggi crittografati con	Allega l'etichetta specificata ai messaggi <b>crittografati</b> in arrivo. L'etichetta predefinita è "crittografato".
Etichetta messaggi non crittografati con	Allega l'etichetta specificata ai messaggi <b>non crittografati</b> in arrivo. L'etichetta predefinita è "non crittografato".
Avvisa quando viene filtrato contenuto dannoso	Il software di sicurezza Zone Labs visualizzerà un messaggio nella finestra del programma IM quando contenuto potenzialmente dannoso viene filtrato da una conversazione IM.
Blocca IRC	Nel caso in cui il computer venga compromesso, questa funzione blocca i tentativi di stabilire una connessione con i canali IRC. Ciò impedisce ai computer infetti di stabilire connessioni dannose. Se si utilizza IRC ed è necessario utilizzare applicazioni IRC, deselezionare questa opzione.
Blocca tutti i collegamenti	Filtra tutti gli URL, che possono essere utilizzati per diffondere virus worm.

3. Fare clic su **OK** per salvare le modifiche.**Visualizzazione del log degli eventi relativi a IM Security**

Per impostazione predefinita, tutti gli eventi relativi a IM Security sono registrati nel Visualizzatore log. Sebbene non si riceva alcuna notifica quando il software di sicurezza Zone Labs blocca lo spam, sarà possibile visualizzare i dettagli di qualsiasi messaggio bloccato nel Visualizzatore log.

## Visualizzare il log degli eventi relativi a IM Security

1. Selezionare **Avvisi e log** | **Visualizzatore log**.

2. Selezionare **IM Security** dall'elenco a discesa Tipo di avviso.

La tabella 12-6 fornisce una spiegazione dei campi del Visualizzatore log per gli eventi

Campo	Spiegazione
Livello	Livello dell'evento in base al <b>Livello della protezione</b> dell'opzione di sicurezza.
Data/Ora	Data e ora in cui si è verificato l'evento
Tipo	Breve descrizione dell'evento. In funzione delle impostazioni di sicurezza che sono state violate (per esempio, Blocco spam, Blocco ID e così via), questo campo può contenere qualsiasi descrizione tra quelle seguenti: <ul style="list-style-type: none"> <li>• Connessione bloccata</li> <li>• È stato bloccato un messaggio proveniente da un mittente non incluso nell'elenco contatti</li> <li>• Trasmissioni contenuti multimediali</li> <li>• Il contenuto potenzialmente pericoloso è stato rimosso</li> <li>• È stato rimosso un collegamento a contenuto attivo</li> <li>• Sessione crittografata avviata</li> <li>• Sessione non crittografata</li> <li>• Dati riservati rimossi</li> </ul>
Servizio	Il servizio sul quale si è verificato l'evento.
Programma	Il programma di messaggistica immediata (visualizzato come file di applicazione) che era connesso quando si è verificato l'evento.
Utente locale	L'ID utente del contatto di messaggistica immediata che ha ricevuto il messaggio.
Utente remoto	L'ID utente del contatto di messaggistica immediata che innescato l'evento.
Azione	Descrive l'azione intrapresa. I valori comuni di questa colonna sono crittografato, crittografia disattivata, audio/video/file bloccati, script bloccati.

**Tabella 12-1: Spiegazioni dei campi del Visualizzatore log** relativi a IM Security.



# Appendice

---

## Guida di riferimento agli avvisi



Questo capitolo offre informazioni dettagliate sui diversi tipi di avvisi visualizzati nel software di sicurezza Zone Labs. Leggere questo capitolo per scoprire come si verificano gli avvisi, che cosa significano e come gestirli.

Argomenti:

- "Avvisi informativi", a pagina 212
- "Avvisi relativi ai programmi", a pagina 217
- "Avvisi di OSFirewall", a pagina 226
- "Avvisi blocco ID", a pagina 228
- "Avvisi Nuova rete", a pagina 229
- "Avvisi Messaggistica immediata", a pagina 230

# Avvisi informativi

Gli avvisi informativi indicano che il software di sicurezza Zone Labs ha bloccato una comunicazione non conforme alle impostazioni di sicurezza. Non richiedono una decisione da parte dell'utente.

## Avvisi del firewall o di protezione

Gli avvisi del firewall sono i tipi di avvisi informativi più comuni. Informano l'utente che il firewall del software di sicurezza Zone Labs ha bloccato il traffico in base a restrizioni di porta e di protocollo oppure in base ad altre regole dello stesso firewall.

### *Perché si verificano questi avvisi*

Gli avvisi del firewall con una banda rossa nella parte superiore indicano avvisi di alto livello. Questi tipi di avvisi si verificano spesso come risultato dell'attività di hacker.

Gli avvisi del firewall con una banda arancione nella parte superiore indicano avvisi di medio livello. Questi tipi di avvisi sono spesso il risultato di traffico di rete innocuo, per esempio quando l'ISP utilizza *ping* per verificare se l'utente è ancora collegato. È comunque possibile che siano provocati da un hacker che cerca di individuare le porte non protette sul computer.

### *Come comportarsi*

Se si lavora su una rete domestica o aziendale e la sicurezza della zona attendibile è impostata ad Alta, il normale traffico della LAN, come i broadcast NetBIOS, potrebbe anch'esso generare degli avvisi del firewall. Provare ad abbassare la sicurezza della zona attendibile a Media.

Per impostazione predefinita, il software di sicurezza Zone Labs visualizza solamente gli avvisi del firewall di alto livello. Se le impostazioni predefinite sono state modificate, verranno visualizzati molti avvisi di medio livello. Provare ad abbassare a medio il livello di visualizzazione degli avvisi.

Se si ricevono numerosi avvisi del firewall e si lavora su una rete LAN domestica o aziendale, è possibile che le normali comunicazioni di rete vengano bloccate. In questo caso, è possibile eliminare gli avvisi aggiungendo la rete alla zona attendibile.

### *Come visualizzare meno avvisi*

Gli avvisi ripetuti potrebbero indicare che una risorsa che si vuole considerare attendibile sta cercando ripetutamente di contattare l'utente. Se si ricevono molti avvisi del firewall, ma non si sospetta di un attacco, provare la seguente procedura:

- Determinare se l'origine degli avvisi è attendibile.
  - Inviare gli avvisi ripetuti ad SmartDefense Advisor per determinare l'indirizzo IP che ha generato gli avvisi.
  - Se gli avvisi sono stati generati da un'origine che si vuole considerare attendibile, aggiungerla alla zona attendibile.
- Determinare se l'ISP sta inviando all'utente messaggi "heartbeat".

- Provare le procedure suggerite per la gestione dei messaggi heartbeat dell'ISP. Vedere "Consentire messaggi heartbeat dell'ISP", a pagina 249.

## Avvisi di MailSafe

Gli avvisi di MailSafe informano l'utente che il software di sicurezza Zone Labs ha messo in quarantena un allegato potenzialmente dannoso di un messaggio di posta in arrivo. Facendo clic su OK, non si concede nessun tipo di autorizzazione.

### *Perché si verificano questi avvisi*

Gli avvisi di MailSafe possono verificarsi a causa di violazioni delle impostazioni di protezione di MailSafe in entrata o in uscita. Per esempio, si verifica una violazione in entrata quando l'utente apre un messaggio di posta elettronica con un allegato avente un'estensione presente nell'elenco di estensioni da mettere in quarantena nella scheda Allegati del pannello Protezione posta elettronica. In questi casi, l'avviso informa che il software di sicurezza Zone Labs ha modificato l'estensione per evitare che l'allegato venga aperto senza avvertire l'utente. Una violazione delle impostazioni di protezione di MailSafe in uscita, come un messaggio di posta con troppi destinatari, o troppi messaggi ricevuti in poco tempo, genera un avviso di MailSafe.

### *Come comportarsi*

Il modo in cui si risponde agli avvisi di MailSafe dipende dal fatto che l'avviso sia stato causato da una violazione in entrata o in uscita delle impostazioni di protezione di MailSafe.

Se l'avviso è stato provocato da una violazione in entrata, attenersi alla procedura seguente:

- Esaminare attentamente il messaggio di posta elettronica. Proviene da una persona conosciuta e attendibile? Ricordare che gli hacker riescono a falsificare i messaggi di posta proprio come se provenissero da un amico. Inoltre, se un amico ha aperto per errore un file contenente un worm, quest'ultimo potrebbe aver inviato copie di se stesso utilizzando il client di posta elettronica dell'amico.
- Contattare il mittente per telefono o per posta elettronica prima di aprire l'allegato in modo da essere certi che si tratta di un messaggio attendibile.
- Aprire l'allegato solo se si è certi che è inoffensivo. Aprire l'allegato facendo clic sull'icona della quarantena (che sostituisce la normale icona del file).



Quando si cerca di aprire un allegato in quarantena, il software di sicurezza Zone Labs visualizza una finestra di messaggio che ricorda all'utente la potenziale pericolosità dell'allegato.

Se l'avviso è stato provocato da una violazione in uscita, attenersi alla procedura seguente:

- Esaminare attentamente l'avviso. L'attività rilevata descrive azioni che si sono effettuate di recente? In questo caso, modificare le impostazioni di uscita di MailSafe per rispondere meglio alle proprie necessità di lavoro. Vedere "Protezione di MailSafe in uscita", a pagina 121. In caso contrario, l'avviso potrebbe essere il risultato di un virus. Di conseguenza, non autorizzare la posta elettronica in uscita ed eseguire una scansione del computer con un programma antivirus.
- Verificare che l'indirizzo di posta elettronica sia presente nell'elenco dei mittenti approvati. Se è stata selezionata l'opzione **L'indirizzo del mittente non è in questo elenco** e se il proprio indirizzo non è presente in quell'elenco oppure è stato digitato in modo sbagliato, aggiungere all'elenco l'indirizzo valido.

#### *Come visualizzare meno avvisi*

La protezione della posta in uscita è un aspetto importante del sistema di sicurezza per Internet e si consiglia di lasciarla attiva. Tuttavia, se si ricevono molti di questi messaggi di errore, si potrebbe regolare questa funzionalità oppure disattivarla del tutto. Vedere "Protezione di MailSafe in uscita", a pagina 121.

## **Avvisi Programma bloccato**

Gli avvisi Programma bloccato indicano che il software di sicurezza Zone Labs ha impedito a un'applicazione sul computer di accedere alle risorse su Internet o nella zona attendibile. Facendo clic su OK, si indica semplicemente al programma che l'avviso è stato letto.

#### *Perché si verificano questi avvisi*

Gli avvisi Programma bloccato si verificano quando un programma cerca di accedere a Internet o alla zona attendibile, anche quando l'utente ha negato esplicitamente l'autorizzazione.

#### *Come comportarsi*

Se si desidera che il programma bloccato possa accedere alla zona Internet o alla zona attendibile, ricorrere alla scheda Programmi per concedere al programma autorizzazioni di accesso.



### *Come visualizzare meno avvisi*

Per disattivare gli avvisi Programma bloccato, effettuare una delle seguenti operazioni:

- Quando si riceve un avviso Programma bloccato, selezionare **Non visualizzare più questa finestra di dialogo** prima di fare clic su **OK**. Da questo momento, tutti gli avvisi Programma bloccato verranno nascosti. Notare che questa operazione non avrà effetto sugli avvisi Nuovo programma, Programma ripetuto o Programma server.
- Nel pannello Controllo dei programmi, fare clic su **Avanzate** per accedere alla scheda Avvisi e funzionalità, quindi deselezionare la casella di controllo **Mostra avvisi quando l'accesso a Internet viene negato**.



La disattivazione degli avvisi Programma bloccato non ha effetto sul livello di sicurezza.

## **Avvisi Blocco Internet**

Gli avvisi Blocco Internet informano l'utente che il software di sicurezza Zone Labs ha bloccato il traffico in ingresso o in uscita perché è stato attivato il Blocco Internet (o è stato fatto clic sul pulsante Interrompi). Facendo clic su OK, si indica semplicemente al programma che l'avviso è stato letto.

Se il Blocco Internet è stato attivato automaticamente (o per errore), disattivarlo per non visualizzare altri avvisi. Vedere "Comprendere le zone", a pagina 18.

### *Perché si verificano questi avvisi*

Questi avvisi si verificano solo quando è attivo il Blocco Internet.

### *Come comportarsi*

Fare clic su **OK** per chiudere la finestra di avviso.

Se il Blocco Internet è stato attivato automaticamente (o per errore), disattivarlo per non visualizzare altri avvisi. Vedere "Comprendere le zone", a pagina 18.

Si potrebbe concedere a determinati programmi (per esempio il browser) l'autorizzazione a ignorare il blocco, in modo da continuare a svolgere alcune operazioni lasciando attivato il blocco. Vedere "Impostazione dell'autorizzazione Ignora blocco a un programma", a pagina 89.

### *Come visualizzare meno avvisi*

Se si ricevono molti avvisi Blocco Internet, è possibile che le impostazioni di Blocco automatico Internet attivino il Blocco Internet dopo ogni breve periodo di inattività.

Per ridurre il numero di avvisi, effettuare una delle seguenti operazioni:

- Disattivare il Blocco automatico Internet.

- Aumentare l'intervallo di inattività richiesto per attivare il Blocco automatico Internet. Per ulteriori informazioni, vedere "Attivazione del Blocco automatico", a pagina 75.

## Avvisi remoti

Gli avvisi remoti sono visualizzati su un computer client ICS quando il software di sicurezza Zone Labs ha bloccato tutto il traffico sul gateway ICS. Se non si lavora su un computer impostato come client di una rete ICS, non si riceverà mai questo avviso.

### *Perché si verificano questi avvisi*

Gli avvisi remoti si verificano quando:

- Il software di sicurezza Zone Labs viene avviato sul gateway ICS. L'avviso visualizza il messaggio "Il firewall remoto è stato attivato".
- Il software di sicurezza Zone Labs viene arrestato sul gateway ICS. L'avviso visualizza il messaggio "Il firewall remoto è stato interrotto".
- Il Blocco Internet è stato attivato sul gateway ICS, impedendo così al computer client di effettuare alcune operazioni. L'avviso visualizza il messaggio "Il firewall remoto ha attivato il blocco Internet".
- Il Blocco Internet è stato disattivato sul gateway ICS. L'avviso visualizza il messaggio "Il firewall remoto ha attivato il blocco Internet".

### *Come comportarsi*

Fare clic su **OK** per chiudere la finestra di avviso. Non sono necessarie altre operazioni.

### *Come visualizzare meno avvisi*

Se non si desidera visualizzare gli avvisi remoti sul computer client ICS:

1. Selezionare **Firewall | Principale**, quindi fare clic su **Avanzate**.
2. Nella sezione Condivisione connessione Internet, deselezionare la casella di controllo **Inoltra gli avvisi dal gateway a questo computer**.

# Avvisi relativi ai programmi

Gli avvisi Programma vengono visualizzati quando si utilizza un programma. Per esempio, se subito dopo aver installato il software di sicurezza Zone Labs l'utente apre Microsoft Outlook e cerca di inviare un messaggio, verrà visualizzato un avviso Programma che chiede se autorizzare Outlook ad accedere a Internet. Tuttavia, gli avvisi di programma possono anche verificarsi se un virus trojan o worm sul computer tenta di diffondersi o se un programma sul computer tenta di modificare il sistema operativo.

## Avvisi Nuovo programma

Gli avvisi Nuovo programma consentono di impostare autorizzazioni di accesso per programmi che non hanno mai chiesto prima d'ora di accedere a Internet o alla zona attendibile. Facendo clic su **Consenti**, il programma è autorizzato all'accesso. Facendo clic su **Nega**, il programma non è autorizzato all'accesso.

### *Perché si verificano questi avvisi*

Gli avvisi Nuovo programma si verificano quando un programma sul computer cerca di stabilire una connessione con un computer della zona attendibile o Internet e quel programma non ha ancora ricevuto autorizzazioni d'accesso.

Quando si inizia a lavorare con il software di sicurezza Zone Labs, si riceverà almeno un avviso Nuovo programma.

### *Come comportarsi*

Fare clic su **Consenti** o **Nega** nella finestra di avviso dopo aver risposto a queste domande:

- È stato avviato un programma o un processo che potrebbe richiedere l'autorizzazione? Se la risposta è sì, fare clic su **Consenti**. Se la risposta è no, continuare.
- Si riconosce il nome del programma nella finestra di avviso? In questo caso, si tratta di un programma che necessita dell'autorizzazione? Se la risposta è sì, fare clic su **Consenti**. Se la risposta è no, oppure se non si è sicuri, continuare.
- Fare clic sul pulsante **Ulteriori informazioni** nella finestra di avviso. In questo modo, le informazioni sull'avviso (come il nome del programma e l'indirizzo che cerca di raggiungere) vengono inviate a SmartDefense Advisor, che aprirà una pagina Web contenente informazioni sull'avviso e il programma. Utilizzare queste informazioni per decidere se consentire l'accesso.



Se il browser non è autorizzato ad accedere a Internet, l'utente verrà indirizzato a questo file della Guida in linea. Per accedere a SmartDefense Advisor, concedere al browser autorizzazioni di accesso a Internet.

- Se non si è sicuri di come agire, fare clic su **Nega**. Sarà possibile concedere autorizzazioni in seguito visualizzando la scheda Programmi. "Impostazione delle autorizzazioni d'accesso per i nuovi programmi", a pagina 79.

### *Come visualizzare meno avvisi*

È normale ricevere molti avvisi Nuovo programma subito dopo l'installazione del software di sicurezza Zone Labs. A mano a mano che vengono assegnate autorizzazioni a ogni nuovo programma, il numero di avvisi diminuirà. Per non visualizzare avvisi Programma ripetuto, selezionare **Memorizza impostazione** prima di fare clic su **Consenti** o **Nega**.

## Avvisi Programma ripetuto

Gli avvisi Programma ripetuto si verificano quando un programma sul computer cerca di stabilire una connessione con un computer della zona attendibile o Internet e quel programma ha già richiesto autorizzazioni d'accesso.

### *Perché si verificano questi avvisi*

Se si risponde Consenti o Nega a un avviso Nuovo programma senza selezionare la casella di controllo **Memorizza impostazione**, si riceverà un avviso Programma ripetuto alla prossima occasione in cui il programma chiederà autorizzazioni d'accesso.

### *Come comportarsi*

Rispondere agli avvisi Programma ripetuto come agli avvisi Nuovo programma. Vedere "Avvisi Nuovo programma", a pagina 218.

### *Come visualizzare meno avvisi*

Per non ricevere più avvisi Programma ripetuto, selezionare la casella di controllo **Ricorda la risposta la prossima volta che uso il programma** prima di fare clic su Consenti o Nega nell'avviso Nuovo programma o Programma ripetuto. In questo modo, il programma viene impostato come autorizzato o bloccato nella scheda Programmi.

## Avvisi Programma modificato

Gli avvisi Programma modificato informano che un programma che ha richiesto in precedenza autorizzazioni di accesso o server è stato in qualche modo modificato. Facendo clic su Consenti, il programma modificato è autorizzato all'accesso. Facendo clic su Nega, il programma non è autorizzato all'accesso.

### *Perché si verificano questi avvisi*

Gli avvisi Programma modificato si verificano se è stato aggiornato un programma dall'ultima volta che si è effettuato l'accesso a Internet. Possono anche verificarsi se un hacker è riuscito in qualche modo ad alterare il programma.

Ricordare che alcuni programmi sono configurati per accedere regolarmente a Internet alla ricerca di aggiornamenti disponibili. Consultare la documentazione del programma o fare riferimento ai siti Web di supporto dei produttori per sapere se includono funzionalità di aggiornamento automatico.

### *Come comportarsi*

Per decidere come rispondere a un avviso Programma modificato, rispondere a queste domande:

- Il programma che chiede l'autorizzazione è stato aggiornato di recente dall'utente (o dall'amministratore di sistema se si lavora in un ambiente di rete)?
- Si tratta di un programma che necessita dell'autorizzazione?

Se la risposta è sì a entrambe le domande, fare clic su **Consenti**.



Se non si è sicuri, fare clic su **Nega**. Sarà possibile concedere autorizzazioni in seguito visualizzando la scheda Programmi. Vedere "Impostazione di autorizzazioni per programmi specifici", a pagina 81.

### *Come visualizzare meno avvisi*

Gli avvisi Programma modificato vengono sempre visualizzati perché richiedono una risposta Consenti o Nega da parte dell'utente. Se si utilizza un programma il cui checksum cambia di frequente, si può evitare di ricevere molti avvisi impostando il software di sicurezza Zone Labs per controllare solo il nome di file del programma. "Aggiunta di un programma all'elenco dei programmi", a pagina 84.

## **Avvisi Componente di programma**

Utilizzare gli avvisi Componente di programma per consentire o negare l'accesso a Internet a un programma che impiega uno o più componenti che non sono ancora stati riconosciuti dal software di sicurezza Zone Labs. Ciò protegge l'utente da hacker che cercano di utilizzare componenti falsi o modificati per aggirare le restrizioni di controllo dei programmi.

Facendo clic su Consenti, il programma è autorizzato ad accedere a Internet utilizzando i componenti nuovi o modificati. Facendo clic su Nega, si impedisce al programma di accedere a Internet utilizzando quei componenti.

### *Perché si verificano questi avvisi*

Gli avvisi Componente di programma si verificano quando un programma che accede a Internet o alla rete locale utilizza uno o più componenti che il software di sicurezza Zone Labs non ha ancora riconosciuto o che sono stati modificati dopo essere stati considerati sicuri.

Il software di sicurezza Zone Labs protegge automaticamente i componenti che un programma utilizza nel momento in cui viene autorizzato all'accesso. Ciò impedisce la visualizzazione di un avviso per ogni componente caricato dal browser. Per informazioni su come il software di sicurezza Zone Labs protegge i componenti dei programmi, vedere "Gestione dei componenti dei programmi", a pagina 90.

### *Come comportarsi*

La risposta a un avviso Componente di programma dipende dalla situazione specifica. Rispondere alle seguenti domande:

- Le seguenti condizioni sono vere?
  - È stato appena installato o reinstallato il software di sicurezza Zone Labs.
  - È stata aggiornata di recente l'applicazione che carica il componente (per il nome dell'applicazione, vedere sotto Informazioni tecniche nella finestra di avviso).

- L'applicazione che carica il componente prevede una funzione di aggiornamento automatico.
- Un altro utente (per esempio, l'amministratore di sistema) può avere aggiornato un programma sul computer senza renderlo noto agli utenti.
- L'applicazione che carica il componente viene utilizzata attivamente?

Se si risponde "sì" a entrambe le domande, è probabile che il software di sicurezza Zone Labs abbia rilevato componenti legittimi che vengono usati dal browser o da altri programmi. È, quindi, possibile rispondere Consenti agli avvisi Componente di programma.

Facendo clic su Consenti, il programma è autorizzato ad accedere a Internet utilizzando i componenti nuovi o modificati. Se non si risponde "sì" a entrambe le domande o se non si è sicuri della validità del componente, fare clic su Nega.

Facendo clic su Nega, si impedisce al programma di accedere a Internet utilizzando quei componenti.



Se non si è sicuri di cosa fare o se si decide di fare clic su **Nega**, analizzare il componente per determinare di che cosa si tratta.

### *Come visualizzare meno avvisi*

Si potrebbero ricevere numerosi avvisi di componente se si imposta il livello Autenticazione programma ad Alta subito dopo aver installato il software di sicurezza Zone Labs. Con l'autenticazione impostata ad Alta, il software di sicurezza Zone Labs non può proteggere automaticamente i numerosi file DLL o gli altri componenti utilizzati comunemente dai browser e da altri programmi.

Per ridurre il numero di avvisi, abbassare il livello di autenticazione a Media nei primi giorni dopo l'installazione di software di sicurezza Zone Labs.

Se si utilizza il software di sicurezza Zone Labs già da qualche giorno, è poco probabile ricevere molti avvisi Programma.

## **Avvisi Programma server**

Gli avvisi Programma server consentono di impostare autorizzazioni server per i programmi sul computer.

### *Perché si verificano questi avvisi*

Gli avvisi Programma server si verificano quando un programma sul computer richiede per la prima volta autorizzazione server per la zona Internet o la zona attendibile.

Generalmente, sono pochi i programmi che richiedono autorizzazione server. Tra questi, i più comuni sono relativi a:

- Chat

- Chiamate in attesa su Internet
- Condivisione di file musicali (come Napster)
- Trasmissione di flussi multimediali (come RealPlayer)
- Voice-over-Internet
- Riunioni sul Web

Se si utilizzano i programmi suddetti, che richiedono autorizzazioni server per funzionare correttamente, concedere l'autorizzazione prima di avviare il programma. Vedere "Concessione a un programma dell'autorizzazione ad agire come server", a pagina 85.



Se il browser non è autorizzato ad accedere a Internet, l'utente verrà indirizzato a questo file della Guida in linea. Per accedere a SmartDefense Advisor, concedere al browser autorizzazioni di accesso a Internet. Vedere "Concessione dell'autorizzazione di accesso a Internet per un programma", a pagina 85.

### *Come comportarsi*

Prima di rispondere all'avviso Programma server, rispondere alle seguenti domande:

- È stato avviato un programma o un processo che potrebbe richiedere l'autorizzazione? Se la risposta è sì, fare clic su Consenti. Se la risposta è no, continuare.
- Si riconosce il nome del programma nella finestra di avviso e, in questo caso, è comprensibile che richieda l'autorizzazione? Se la risposta è sì, fare clic su Consenti.
- Fare clic sul pulsante **Ulteriori informazioni** nella finestra di avviso. In questo modo, le informazioni sull'avviso (come il nome del programma e l'indirizzo che cerca di raggiungere) vengono inviate a SmartDefense Advisor, che aprirà una pagina Web contenente informazioni sull'avviso e il programma. Utilizzare queste informazioni per decidere se consentire l'accesso. Per ulteriori informazioni, vedere "Utilizzo di SmartDefense Advisor e Hacker ID", a pagina 178.
- Se ancora non si è certi della legittimità del programma e della necessità di concedere l'autorizzazione server, fare clic su Nega. Qualora fosse necessario, si potrà successivamente concedere l'autorizzazione server al programma nella scheda Programmi. Vedere "Concessione a un programma dell'autorizzazione ad agire come server", a pagina 85.

### *Come visualizzare meno avvisi*

Se si utilizzano i programmi suddetti, che richiedono autorizzazioni server per funzionare correttamente, concedere l'autorizzazione prima di avviare il programma nella scheda Programmi del software di sicurezza Zone Labs. Se si ricevono molti avvisi Programma server, come misura di sicurezza aggiuntiva scaricare e installare un programma antivirus o uno strumento antispyware.



## Avvisi Programma avanzato

Gli avvisi Programma avanzato sono simili ad altri avvisi Programma (Nuovo programma, Programma ripetuto e Programma modificato) che informano che un programma sta cercando di accedere alla rete.

Sono, tuttavia, diversi da altri avvisi Programma in quanto il programma cerca di utilizzare un altro programma per connettersi a Internet oppure cerca di alterare la funzionalità di un altro programma.

### *Perché si verificano questi avvisi*

Gli avvisi Programma avanzato si verificano in due situazioni: quando un programma sul computer cerca di stabilire una connessione a un computer nella zona Internet o attendibile indicando a un altro programma di connettersi, oppure quando un programma cerca di impossessarsi dei processi di un altro programma chiamando la funzione OpenProcess.

Esistono alcuni programmi legittimi associati al sistema operativo che potrebbero richiedere l'accesso a un altro programma. Per esempio, quando si utilizza il Task Manager di Windows per chiudere Internet Explorer, il Task Manager deve chiamare la funzione OpenProcess per poter chiudere Internet Explorer.

### *Come comportarsi*

La risposta a un avviso Programma avanzato dipende dalla causa dell'avviso. Se l'avviso è stato causato da una chiamata alla funzione OpenProcess, determinare se la funzione è stata chiamata da un programma legittimo o dannoso. Verificare che il programma indicato nell'avviso sia un programma attendibile che può chiamare questa funzione. Per esempio, se si cercava di chiudere un programma usando il Task Manager di Windows quando è stato ricevuto l'avviso Programma avanzato, rispondere facendo clic su **Consenti**. Allo stesso modo, se l'avviso è stato causato da un programma che utilizza un altro programma per accedere a Internet e quel programma richiede ogni volta l'autorizzazione, rispondere facendo clic su **Consenti**. Se non si è sicuri della causa dell'avviso o del comportamento del programma che ha inoltrato la richiesta, fare clic su **Nega**. Dopo aver negato l'autorizzazione avanzata al programma, condurre una ricerca su Internet riguardante il nome di file del programma. Se il programma è dannoso, saranno probabilmente disponibili delle informazioni su esso, tra cui come rimuoverlo dal computer.

### *Come visualizzare meno avvisi*

Non è normale ricevere numerosi avvisi Programma avanzato. Se si ricevono avvisi ripetuti, cercare il nome o i nomi del programma e decidere se rimuoverlo dal computer o concedergli i diritti di accesso necessari.

## Avvisi Configurazione VPN automatica

Gli avvisi Configurazione VPN automatica si verificano quando il software di sicurezza Zone Labs rileva attività VPN. In base al tipo di attività VPN rilevata e se software di sicurezza Zone Labs ha potuto configurare la connessione VPN automaticamente, si può ricevere uno di più avvisi Configurazione VPN automatica.

### ***Perché si verificano questi avvisi***

Gli avvisi Configurazione VPN automatica si verificano quando il software di sicurezza Zone Labs rileva attività VPN non ancora autorizzata all'accesso.

### ***Come comportarsi***

La risposta a un avviso Configurazione VPN automatica dipende dal tipo di avviso ricevuto, se è in esecuzione software VPN e se si desidera configurare il software di sicurezza Zone Labs per consentire la connessione VPN.



Se è stata creata una regola della scheda Esperto che blocca il traffico VPN, sarà necessario modificare tale regola per consentire il traffico VPN. Vedere "Creazione di regole firewall nella scheda Esperto", a pagina 58.

- Se si esegue software VPN sul computer e si desidera configurare la connessione, selezionare:

**Configura il software di sicurezza Zone Labs per supportare la connessione VPN**, oppure

**Eseguo software VPN e desidero configurare il software di sicurezza Zone Labs per supportarlo.**

- Se si esegue software VPN ma non si desidera impostare il software di sicurezza Zone Labs per configurare la connessione, selezionare **Non configurare il software di sicurezza Zone Labs per supportare la connessione VPN**.
- Se non si esegue software VPN, selezionare **Non eseguo software VPN**.

### ***Come visualizzare meno avvisi***

Se si esegue software VPN, l'unico modo per ricevere meno avvisi è configurare il software di sicurezza Zone Labs per autorizzare il software VPN e le risorse da esso richieste. Vedere "Configurazione manuale della connessione VPN", a pagina 38.

## **Avvisi Azione manuale obbligatoria**

Un avviso Azione manuale obbligatoria informa l'utente che sono necessari altri passaggi prima che il software di sicurezza Zone Labs sia configurato correttamente per supportare la connessione VPN.

### ***Perché si verificano questi avvisi***

Gli avvisi Azione manuale obbligatoria si verificano quando il software di sicurezza Zone Labs non riesce a configurare la connessione VPN automaticamente, oppure se sono necessarie ulteriori modifiche manuali prima di completare la configurazione automatica.

### ***Come comportarsi***

Gli avvisi Azione manuale obbligatoria non richiedono una risposta da parte dell'utente. Per configurare una connessione VPN manualmente, vedere "Configurazione manuale della connessione VPN", a pagina 38 e seguire le istruzioni.

***Come visualizzare meno avvisi***

Non è normale ricevere molti avvisi Azione manuale obbligatoria. Se si visualizzano troppi avvisi, eseguire la procedura richiesta per configurare correttamente il software di sicurezza Zone Labs per supportare la connessione VPN, oppure rimuovere il software VPN dal computer.

# Avvisi di OSFirewall

Gli avvisi OSFirewall sono avvisi visualizzati quando programmi o processi sul computer tentano di modificare impostazioni o programmi dello stesso.

Vi sono due tipi di avvisi OSFirewall che richiedono una risposta da parte dell'utente: Comportamento sospetto, Comportamento pericoloso e Comportamento dannoso.

La protezione OSFirewall è disponibile in ZoneAlarm Pro e ZoneAlarm Security Suite.

## Avvisi Comportamento sospetto

Un avviso Comportamento sospetto informa l'utente che un programma sul computer sta tentando un'attività considerata sospetta. Facendo clic su **Consenti**, il programma è autorizzato a eseguire l'attività. Se si fa clic su **Nega**, viene impedito al programma di eseguire l'attività e viene concesso accesso limitato, con il significato che qualsiasi comportamento futuro sospetto e pericoloso verrà negato.

### *Perché si verificano questi avvisi*

Gli hacker utilizzano spesso programmi attendibili per modificare altri programmi, quali le impostazioni del browser o per compromettere il sistema operativo del computer.

### *Come comportarsi*

Fare clic su **Consenti** o **Nega** per rispondere. Se non si è sicuri se consentire o negare l'azione, fare clic sul pulsante **Ulteriori informazioni** nella finestra dell'avviso. In questo modo, le informazioni sull'avviso (come il nome del programma e l'attività che cerca di eseguire) vengono inviate a SmartDefense Advisor, che aprirà una pagina Web contenente informazioni sull'avviso e il comportamento. Utilizzare le informazioni di SmartDefense Advisor per decidere se consentire o negare l'azione. Per ulteriori informazioni sulle cause degli avvisi Comportamento sospetto, vedere "Comportamento sospetto", a pagina 262.



Selezionando la **casella di controllo Memorizza impostazione** prima di fare clic su **Consenti** o **Nega**, il programma o il componente sarà in grado di eseguire **QUALSIASI** funzione sospetta in futuro e non si riceverà alcun avviso.

## Avvisi Comportamento pericoloso

Un avviso Comportamento pericoloso informa l'utente che un programma sul computer sta tentando un'attività considerata pericolosa. Facendo clic su **Consenti**, il programma è autorizzato a eseguire l'attività. Se si fa clic su **Nega**, viene impedito al programma di eseguire l'attività e viene concesso accesso limitato, con il significato che qualsiasi comportamento futuro sospetto e pericoloso verrà negato.

### *Perché si verificano questi avvisi*

Questi avvisi si verificano quando viene rilevato un programma o un componente sul computer che tenta di dirottare un processo o programma sul computer o di alterare le impostazioni predefinite del computer o di uno dei suoi programmi.

### ***Come comportarsi***

A causa della natura delle azioni che determinano la visualizzazione di un avviso Comportamento pericoloso, la cosa più sicura è fare clic su **Nega** nella finestra dell'avviso. Se non si è sicuri, fare clic sul pulsante **Ulteriori informazioni** nella finestra dell'avviso. In questo modo, le informazioni sull'avviso (come il nome del programma e l'attività che cerca di eseguire) vengono inviate a SmartDefense Advisor, che aprirà una pagina Web contenente informazioni sull'avviso e il comportamento. Utilizzare le informazioni di SmartDefense Advisor per decidere se consentire o negare l'azione. Per ulteriori informazioni sulle cause degli avvisi di comportamento pericoloso, vedere "Comportamento pericoloso", a pagina 263.



Selezionando la **casella di controllo Memorizza impostazione** prima di fare clic su **Consenti** o **Nega**, il programma o il componente sarà in grado di eseguire **QUALSIASI** funzione pericolosa in futuro e non si riceverà alcun avviso.

## **Avvisi Comportamento dannoso**

Un avviso Comportamento dannoso informa l'utente che è in corso il tentativo di esecuzione di un programma dannoso sul computer. I programmi designati dagli esperti di sicurezza di Zone Labs tendono a essere worm, virus, trojan e altro malware noto.

### ***Perché si verificano questi avvisi***

Questo avviso appare per informare l'utente che un programma sul computer verrà terminato (chiuso).

### ***Come comportarsi***

Gli avvisi relativi a comportamenti dannosi non richiedono una risposta da parte dell'utente. Sono semplicemente informazioni su un'azione in corso di esecuzione. Se un programma attendibile viene terminato per errore, è possibile attivarlo dall'elenco dei programmi.

# Avvisi blocco ID

Gli avvisi Blocco ID informano l'utente che stanno per essere inviate informazioni memorizzate in myVAULT a una destinazione non presente nell'elenco dei siti attendibili.

## ***Perché si verificano questi avvisi***

Si riceve un avviso Blocco ID quando le informazioni memorizzate in myVAULT vengono inserite in una pagina Web o messaggio di posta, oppure quando la propria password viene inviata a una destinazione con un modulo in chiaro (non crittografato) senza l'autorizzazione da parte dell'utente.

## ***Come comportarsi***

Determinare se il sito che ha richiesto le informazioni è attendibile. Se consentire o bloccare le informazioni dipende dalla loro importanza, dalla legittimità della richiesta e dalla autenticità del sito. Se si sta per effettuare un acquisto online su un sito attendibile quando si riceve l'avviso, è possibile consentire l'invio delle informazioni. Se si riceve un avviso riguardante le informazioni mentre non si stanno effettuando transazioni, si consiglia di bloccare l'invio.

Inoltre, sono pochi i siti che trasmettono le password in chiaro. Se si bloccano le password in chiaro per un sito, visitare quel sito e digitare la password: si riceverà un avviso Blocco ID.

## ***Come visualizzare meno avvisi***

Si potrebbero visualizzare molti avvisi Blocco ID se si inviano spesso contenuti myVAULT a siti non presenti nell'elenco dei siti attendibili, oppure se sono state bloccate le password in chiaro per un sito che utilizza questo tipo di autenticazione. Per ridurre il numero di avvisi Blocco ID, aggiungere all'elenco dei siti attendibili i siti con cui si condividono spesso informazioni personali e consentire l'invio di password in chiaro per i siti che le richiedono.

# Avvisi Nuova rete

Gli avvisi Nuova rete appaiono quando il software di sicurezza Zone Labs rileva che l'utente si è collegato a una rete per la prima volta. Utilizzare la finestra di avviso per consentire la condivisione di file e stampanti con quella rete. Gli avvisi Nuova rete vengono generati quando l'utente si connette a qualsiasi rete, che sia una rete domestica wireless, una rete LAN aziendale o la rete dell'ISP dell'utente.

Al primo utilizzo del software di sicurezza Zone Labs, viene sicuramente visualizzato un avviso Nuova rete. Niente di preoccupante; questo avviso è un utile strumento progettato per aiutare l'utente nella configurazione del software di sicurezza Zone Labs.

## *Perché si verificano questi avvisi*

Gli avvisi Nuova rete vengono generati quando l'utente si connette a qualsiasi rete, che sia una rete domestica wireless, una rete LAN aziendale o la rete dell'ISP dell'utente.

## *Come comportarsi*

La risposta a un avviso Nuova rete dipende dalla situazione di rete specifica.

Se si è connessi a una rete locale domestica o aziendale e si desidera condividere le risorse con gli altri computer in rete, aggiungere la rete alla zona attendibile.

## **Aggiungere la rete alla zona attendibile**

1. Nella finestra di avviso Nuova rete, digitare il nome della rete (per esempio "LAN domestica") nella casella Nome.
2. Selezionare **Zona attendibile** dall'elenco a discesa Zona.
3. Fare clic su **OK**.



Se non si è certi della rete che il software di sicurezza Zone Labs ha rilevato, prendere nota dell'indirizzo IP visualizzato nella finestra di avviso. Quindi, consultare la documentazione della rete domestica, l'amministratore di sistema o l'ISP per determinare di che rete si tratta.

Fare attenzione se il software di sicurezza Zone Labs rileva una rete wireless. È possibile che la scheda di rete wireless rilevi una rete diversa dalla propria. Controllare che l'indirizzo IP visualizzato nell'avviso Nuova rete sia l'indirizzo della propria rete prima di aggiungerla alla zona attendibile.

Se si è connessi a Internet con una connessione remota mediante modem analogico, una linea di tipo DSL (Digital Subscriber Line) o un modem via cavo, fare clic su **OK** nella finestra di avviso Nuova rete.



Facendo clic su Annulla, il software di sicurezza Zone Labs bloccherà la connessione a Internet. Non aggiungere la rete dell'ISP alla zona attendibile.

## *Come visualizzare meno avvisi*

Non è normale ricevere molti avvisi Nuova rete.

# Avvisi Messaggistica immediata

Questa sezione offre una spiegazione dei tipi di messaggi di avviso che possono apparire durante una sessione di messaggistica immediata protetta dal software di sicurezza Zone Labs.

La tabella seguente riepiloga i messaggi di avviso visualizzati quando si utilizza il software di sicurezza Zone Labs. Consultare la tabella per una spiegazione del perché si ricevono questi avvisi e determinare se è richiesta un'azione da parte dell'utente. Tutti i messaggi di avviso appaiono tra parentesi quadre [ ] nella finestra di messaggistica immediata.

Testo dell'avviso	Spiegazione
Sessione non crittografata perché [ID IM del contatto] ha disattivato la crittografia	Questo avviso appare quando la crittografia è attivata sul computer dell'utente e disattivata sul computer del contatto.
Sessione non crittografata perché [ID IM del contatto] non è protetto da ZoneAlarm Security Suite	Questo avviso appare nella finestra di messaggistica immediata quando si conversa con un contatto che non utilizza ZoneAlarm Security Suite.
Le informazioni su [descrizione] sono state rimosse dal messaggio precedente in conformità alle impostazioni di Blocco ID	Questo avviso appare quando si cerca di trasmettere informazioni memorizzate in myVAULT. La descrizione dell'elemento, così come appare in myVAULT, è visualizzata tra parentesi.
Collegamento rimosso	Questo avviso appare nella finestra del destinatario del messaggio al posto di un collegamento rimosso.
Sessione crittografata	Questo avviso appare all'inizio di una conversazione immediata crittografata.
Contenuto potenzialmente dannoso rimosso dal messaggio	Questo avviso è aggiunto al messaggio filtrato.
Il messaggio è stato bloccato perché l'utente non è presente nell'elenco dei contatti di [ID IM del contatto]	Questo avviso appare quando si cerca di inviare un messaggio a qualcuno che ha attivato Blocco spam, ma che non ha aggiunto l'utente al proprio elenco dei contatti.
Un trasferimento di file sul PC di [ID IM del contatto] è stato bloccato	Questo avviso appare quando si cerca di inviare un file a un contatto, ma quest'ultimo ha bloccato il trasferimento di file in ZoneAlarm Security Suite.
La trasmissione di video sul PC di [ID IM del contatto] è stata bloccata	Questo avviso appare quando si cerca di trasmettere un video a un contatto, ma quest'ultimo ha bloccato il trasferimento di file video.

**Tabella A-1: Messaggi di avviso IM**



<b>Testo dell'avviso</b>	<b>Spiegazione</b>
Formattazione o script potenzialmente dannosi rimossi dall'ultimo messaggio	Questo avviso appare quando il contatto ha impostato la protezione in entrata per Tag a Blocca e si cerca di inviare un messaggio al contatto che include formattazione o script.
Collegamento potenzialmente dannoso rimosso dall'ultimo messaggio	Questo avviso appare quando il contatto ha impostato la protezione in entrata per Attivo a Blocca e si cerca di inviare un messaggio al contatto che include un collegamento eseguibile.

**Tabella A-1: Messaggi di avviso IM**



# Appendice

---

## Tasti di scelta rapida

# B

È possibile accedere a numerose funzioni del software di sicurezza Zone Labs utilizzando i tasti di scelta rapida.

- "Tasti di scelta rapida per lo spostamento nel programma", a pagina 234
- "Tasti di scelta rapida per funzioni globali", a pagina 236
- "Comandi per le finestre di dialogo", a pagina 238
- "Tasti di scelta rapida per pulsanti", a pagina 239

# Tasti di scelta rapida per lo spostamento nel programma

Utilizzare i tasti indicati di seguito per spostarsi tra pannelli, schede e finestre di dialogo del software di sicurezza Zone Labs. Utilizzare F6 per raggiungere l'elemento desiderato. Utilizzare poi le frecce SU, GIÙ, SINISTRA e DESTRA per arrivare alla selezione desiderata all'interno di un gruppo.

Per esempio:

## Visualizzare la scheda Zone del pannello Firewall

1. Premere **F6** finché viene selezionata la barra dei menu a sinistra.
2. Premere **freccia GIÙ** finché viene selezionato il pannello Firewall.
3. Premere **F6** finché vengono selezionate le schede.
4. Premere **freccia SU**, **freccia GIÙ**, **freccia SINISTRA** o **freccia DESTRA** finché viene selezionata la scheda Zone.

Tasti	Funzione
F1	Visualizza la Guida in linea del pannello corrente.
F6	Consente di spostarsi tra le aree dell'interfaccia nell'ordine seguente: selezione di pannelli, selezione di schede, area del pannello, controlli di interruzione e blocco.
TAB	Consente di spostarsi tra le aree dell'interfaccia nello stesso ordine di F6. Tuttavia, se si preme TAB quando è attiva un'area di un pannello, è possibile spostarsi tra i gruppi di controlli all'interno del pannello.
Frecce SU e GIÙ	Consentono di spostarsi tra singoli controlli all'interno di un gruppo.

**Tabella B-1: Tasti di scelta rapida per lo spostamento**

<b>Tasti</b>	<b>Funzione</b>
Frecce SINISTRA e DESTRA	Anche questi tasti consentono di spostarsi tra singoli controlli all'interno di un gruppo. Nelle visualizzazioni a elenco, consentono lo scorrimento orizzontale.
ALT+BARRA SPAZIATRICE	Apre il menu di controllo Windows (che consente di ingrandire, ridurre a icona e chiudere la finestra del programma).

**Tabella B-1: Tasti di scelta rapida per lo spostamento**

# Tasti di scelta rapida per funzioni globali

Utilizzare i tasti riportati di seguito per attivare funzioni da più posizioni dell'interfaccia. Notare che alcuni tasti e sequenze di tasti potrebbero avere funzioni diverse in base ai pannelli. Tali casi sono elencati nella sezione "Tasti di scelta rapida per pulsanti" riportata in seguito.

Tasti	Funzione
CTRL+S	Attiva e disattiva il pulsante Interrompi (Blocco di emergenza).
CTRL+L	Attiva e disattiva il blocco Internet.
ALT+T	Nasconde e visualizza il testo esplicativo.
ALT+D	Ripristina le impostazioni predefinite.
ALT+C	Visualizza una finestra di dialogo di personalizzazione, quando è disponibile.
ALT+U	Visualizza una seconda finestra di dialogo di personalizzazione quando sono presenti due pulsanti Personalizza (per esempio, nella scheda Principale del pannello Controllo dei programmi).
ALT+A	Visualizza una finestra di dialogo di impostazioni avanzate, quando è disponibile.
ALT+FRECCIA GIÙ	Apri la casella dell'elenco a discesa attivo. Nelle visualizzazioni a elenco, apre il menu di scelta rapida visualizzabile facendo clic con il pulsante sinistro del mouse, se è disponibile.

**Tabella B-2: Tasti di scelta rapida per funzioni globali**

<b>Tasti</b>	<b>Funzione</b>
MAIUSC+F10	Nelle visualizzazioni a elenco, apre il menu di scelta rapida visualizzabile facendo clic con il pulsante destro del mouse, se è disponibile.
ESC	Equivale a fare clic su un pulsante Annulla.
INVIO	Equivale a fare clic sul pulsante attivo.
ALT+P	Equivale a fare clic su un pulsante Applica.
CANC	Rimuove un elemento selezionato da una visualizzazione a elenco.
ALT+F4	Chiude il software di sicurezza Zone Labs.
ALT+K	Nasconde tutto eccetto il dashboard.
ALT+A	Equivale a fare clic su un pulsante Aggiungi, quando è disponibile.
ALT+R	Equivale a fare clic su un pulsante Rimuovi.
ALT+E	Equivale a fare clic su un pulsante Modifica.
ALT+M	Equivale a fare clic su un pulsante Ulteriori informazioni, quando è disponibile.

**Tabella B-2: Tasti di scelta rapida per funzioni globali**

# Comandi per le finestre di dialogo

Utilizzare i tasti riportati di seguito quando è visualizzata una finestra di dialogo.

Tasti	Funzione
Scheda	Attiva il controllo successivo nella finestra di dialogo.
MAIUSC+TAB	Attiva il controllo precedente nella finestra di dialogo.
CTRL+TAB	Visualizza la scheda successiva in una finestra di dialogo con più schede.
CTRL+MAIUSC+TAB	Visualizza la scheda precedente in una finestra di dialogo con più schede.
ALT+FRECCIA GIÙ	Apri la casella dell'elenco a discesa attivo.
BARRA SPAZIATRICE	Equivalente a fare clic su un pulsante attivo. Seleziona/deseleziona una casella di controllo attiva.
INVIO	Equivalente a fare clic sul pulsante attivo.
ESC	Equivalente a fare clic sul pulsante Annulla.

**Tabella B-3: Tasti di scelta rapida per le finestre di dialogo**



# Tasti di scelta rapida per pulsanti

Utilizzare le sequenze di tasti riportate di seguito per fare clic sui pulsanti disponibili nella finestra attiva.

Pannello	Scheda	Tasti	Equivale a fare clic su
Panoramica	Scheda Stato	ALT+R	Esercitazione
Panoramica	Scheda Stato	ALT+M	Novità di Zone Labs
Panoramica	Informazioni sul prodotto	ALT+I	Cambia licenza
Panoramica	Informazioni sul prodotto	ALT+B	Compra adesso
Panoramica	Informazioni sul prodotto	ALT+N	Rinnova
Panoramica	Informazioni sul prodotto	ALT+R	Modifica reg.
Panoramica	Preferenze	ALT+P	Imposta password
Panoramica	Preferenze	ALT+B	Backup
Panoramica	Preferenze	ALT+R	Ripristina
Panoramica	Preferenze	ALT+O	Accedi/Disconnetti
Panoramica	Preferenze	ALT+U	Ricerca aggiornamenti
Firewall	Principale	ALT+C	Personalizzato in Zona Internet
Firewall	Principale	ALT+U	Personalizzato in Zona attendibile
Firewall	Principale	ALT+A	Utente di livello avanzato
Firewall	zone	ALT+A	Aggiungi
Firewall	zone	ALT+R	Rimuovi
Firewall	zone	ALT+E	Modifica
Firewall	zone	ALT+P	Applica
Firewall	Esperto	ALT+A	Aggiungi
Firewall	Esperto	ALT+R	Rimuovi
Firewall	Esperto	ALT+E	Modifica
Firewall	Esperto	ALT+P	Applica
Firewall	Esperto	ALT+G	Gruppi
Controllo dei programmi	Principale	ALT+C	Personalizzato in Controllo dei programmi

**Tabella B-4: Sequenze di tasti per attivare pulsanti**

Pannello	Scheda	Tasti	Equivale a fare clic su
Controllo dei programmi	Principale	ALT+U	Personalizzato in Blocco automatico
Controllo dei programmi	Principale	ALT+A	Utente di livello avanzato
Controllo dei programmi	Programmi	ALT+A	Aggiungi
Controllo dei programmi	Programmi	ALT+O	Opzioni
Controllo dei programmi	Componenti	ALT+M	Ulteriori informazioni
Antivirus/Antispyware	Principale	ALT+S	Scansione di virus/spyware
Antivirus/Antispyware	Principale	ALT+U	Aggiorna ora
Antivirus/Antispyware	Principale	ALT+A	Opzioni avanzate
Antivirus/Antispyware	Principale	ALT+V	Scansione di virus
Antivirus/Antispyware	Principale	ALT+W	Scansione di spyware
Antivirus/Antispyware	Quarantena	ALT+D	CANC
Antivirus/Antispyware	Quarantena	ALT+E	Ripristina
Antivirus/Antispyware	Quarantena	ALT+M	Ulteriori informazioni
Protezione posta elettronica	Principale	ALT+A	Utente di livello avanzato
Protezione posta elettronica	Allegati	ALT+C	Seleziona tutto
Protezione posta elettronica	Allegati	ALT+R	Cancella tutto
Protezione posta elettronica	Allegati	ALT+A	Aggiungi
Protezione posta elettronica	Allegati	ALT+P	Applica
Privacy	Principale	ALT+C	Personalizzato in Controllo cookie
Privacy	Principale	ALT+U	Personalizzato in Blocco annunci
Privacy	Principale	ALT+S	Personalizzato in Controllo codice mobile
Privacy	Elenco siti	ALT+A	Aggiungi
Privacy	Elenco siti	ALT+O	Opzioni
Privacy	Cache Cleaner	ALT+N	Cancella ora
Privacy	Cache Cleaner	ALT+U	Personalizzato

**Tabella B-4: Sequenze di tasti per attivare pulsanti**

<b>Pannello</b>	<b>Scheda</b>	<b>Tasti</b>	<b>Equivale a fare clic su</b>
Privacy	Disco rigido IE/MSN Netscape	ALT+D	Ripristina predefiniti
Privacy	Disco rigido IE/MSN Netscape	ALT+P	Applica
Privacy	IE/MSN Netscape	ALT+S	Seleziona
Blocco ID	myVAULT	ALT+A	Aggiungi
Blocco ID	myVAULT	ALT+O	Opzioni
Blocco ID	myVAULT	ALT+N	Crittografa
Blocco ID	myVAULT	ALT+E	Modifica
Blocco ID	myVAULT	ALT+R	Rimuovi
Blocco ID	Siti attendibili	ALT+A	Aggiungi
Blocco ID	Siti attendibili	ALT+R	Rimuovi
Controllo genitori	Principale	ALT+A	Utente di livello avanzato
Controllo genitori	Categorie	ALT+C	Seleziona tutto
Controllo genitori	Categorie	ALT+R	Cancella tutto
Avvisi e log	Principale	ALT+D	Ripristina predefiniti
Avvisi e log	Principale	ALT+C	Personalizzato
Avvisi e log	Principale	ALT+A	Utente di livello avanzato
Avvisi e log	Visualizzatore log	ALT+M	Ulteriori informazioni
Avvisi e log	Visualizzatore log	ALT+D	Cancella elenco
Avvisi e log	Visualizzatore log	ALT+A	Aggiungi a zona
Avvisi e log	Controllo log	ALT+B	Sfoggia
Avvisi e log	Controllo log	ALT+E	Elimina log

**Tabella B-4: Sequenze di tasti per attivare pulsanti**



# Appendice

---

## Risoluzione dei problemi



Questo capitolo fornisce indicazioni per risolvere eventuali problemi sorti durante l'utilizzo del software di sicurezza Zone Labs.

Argomenti:

- "VPN",
- "Rete",
- "Connessione a Internet",
- "IM Security",
- "Antivirus",
- "Problemi legati a software di terzi",

# VPN

In caso di difficoltà nell'utilizzo del software VPN con il software di sicurezza Zone Labs, fare riferimento alla tabella seguente, che riporta i suggerimenti per la risoluzione di problemi forniti in questa sezione.

Se...	Vedere...
È impossibile connettersi alla rete privata virtuale (VPN)	"Configurazione del software di sicurezza Zone Labs per il traffico VPN", in questa pagina
Sono state create regole firewall nella scheda Esperto	"Configurazione automatica della VPN e regole della scheda Esperto", in questa pagina
Si utilizza un client VPN supportato e il software di sicurezza Zone Labs non lo rileva automaticamente alla prima connessione	"Ritardo del rilevamento automatico della VPN",

**Tabella C-1: Risoluzione di problemi con il software VPN**

## Configurazione del software di sicurezza Zone Labs per il traffico VPN

Se non è possibile connettersi alla VPN, potrebbe essere necessario configurare il software di sicurezza Zone Labs in modo che accetti il traffico proveniente dalla VPN.

### Configurare il software di sicurezza Zone Labs per consentire il traffico VPN

1. Aggiungere le risorse di rete relative alla VPN alla zona attendibile.  
Vedere "Aggiunta alla zona attendibile", .
2. Autorizzare l'accesso al computer al client VPN e agli altri programmi relativi alla VPN.  
Vedere "Impostazione di autorizzazioni per programmi specifici", .
3. Consentire l'utilizzo dei protocolli VPN.  
Vedere "Aggiunta di un gateway VPN e altre risorse alla zona attendibile", .

## Configurazione automatica della VPN e regole della scheda Esperto

Se sono state create regole firewall della scheda Esperto che bloccano protocolli VPN, il software di sicurezza Zone Labs non potrà rilevare automaticamente la VPN quando si stabilisce una connessione. Per configurare la connessione VPN, si dovrà verificare che il client VPN e i componenti relativi alla VPN siano nella zona attendibile e che dispongano dell'autorizzazione per accedere a Internet. Vedere "Configurazione della connessione VPN", .

## **Ritardo del rilevamento automatico della VPN**

Il software di sicurezza Zone Labs esamina periodicamente il computer per determinare se sono attivati protocolli VPN supportati. Dopo il rilevamento, il software di sicurezza Zone Labs richiede all'utente di configurare automaticamente la connessione. Se si è appena installato un client VPN e si è tentato di connettersi, il software di sicurezza Zone Labs potrebbe non avere rilevato la configurazione VPN. Se si preferisce che il software di sicurezza Zone Labs configuri la connessione automaticamente, è possibile attendere dieci minuti, quindi riprovare a connettersi. Se si preferisce connettersi subito, è possibile configurare la connessione manualmente. Vedere "Configurazione della connessione VPN", .

# Rete

In caso di difficoltà nel collegamento alla rete o nell'utilizzo di servizi di rete, fare riferimento alla tabella di seguito che riporta ai suggerimenti per la risoluzione di problemi forniti in questa sezione.

Se...	Vedere...
Non è possibile vedere gli altri computer nella rete, o se gli altri computer non possono vedere il computer dell'utente	"Rendere visibile il computer sulla rete locale", in questa pagina
Non è possibile condividere file o stampanti sulla rete domestica o sulla LAN aziendale	"Condivisione di file e stampanti in una rete locale", in questa pagina
Il computer dell'utente si trova su una LAN e l'avvio richiede molto tempo quando è installato il software di sicurezza Zone Labs	"Risoluzione del problema dell'avvio lento",

**Tabella C-2: Risoluzione di problemi di rete**

## Rendere visibile il computer sulla rete locale

Se non è possibile vedere gli altri computer sulla rete locale, o se gli altri computer non riescono a vedere il computer dell'utente, è possibile che il software di sicurezza Zone Labs stia bloccando il traffico NetBIOS necessario per la visibilità della rete Windows.

### Rendere visibile il computer sulla rete locale

1. Aggiungere la subnet della rete (o, in una rete di piccole dimensioni, l'indirizzo IP di ogni computer della rete) alla zona attendibile. Vedere "Aggiunta alla zona attendibile", .
2. Impostare la sicurezza della zona attendibile a Media e la sicurezza della zona Internet ad Alta. Tali impostazioni consentono ai computer attendibili di accedere ai file condivisi e impediscono l'accesso agli altri computer. Vedere "Impostazione delle opzioni di sicurezza avanzate", .



Il software di sicurezza Zone Labs rileverà automaticamente la rete e visualizzerà l'avviso Nuova rete. È possibile utilizzare l'avviso per aggiungere la subnet della rete alla zona attendibile. Per ulteriori informazioni, vedere "Avvisi Nuova rete", .

## Condivisione di file e stampanti in una rete locale

Il software di sicurezza Zone Labs consente di condividere in modo facile e veloce le risorse del computer affinché i computer attendibili della rete vi possano accedere, senza permettere a intrusi provenienti da Internet di compromettere il sistema.



**Configurare il software di sicurezza Zone Labs per una condivisione sicura**

1. Aggiungere la subnet della rete (o, in una rete di piccole dimensioni, l'indirizzo IP di ogni computer della rete) alla zona attendibile. Vedere "Aggiunta alla zona attendibile", .
2. Impostare la sicurezza della zona attendibile su Media. Questa impostazione consente a computer attendibile di accedere ai file condivisi. Vedere "Scelta dei livelli di sicurezza", .
3. Impostare la sicurezza della zona Internet ad Alta. Questa impostazione rende invisibile il computer a computer non attendibili. Vedere "Impostazione del livello di sicurezza per una zona", .

**Risoluzione del problema dell'avvio lento**

Se il software di sicurezza Zone Labs è configurato per essere caricato all'avvio, ad alcuni utenti collegati alla LAN potrebbe capitare di dover attendere diversi minuti prima del completamento del processo di avvio.

Nella maggior parte dei casi, questo problema è dovuto al fatto che il computer deve accedere al controller di dominio della rete per completare il processo di avvio e di autenticazione e il software di sicurezza Zone Labs blocca l'accesso perché il controller non è stato aggiunto alla zona attendibile.

Per risolvere questo problema, aggiungere il nome host o l'indirizzo IP del controller di dominio della rete alla zona attendibile.

# Connessione a Internet

In caso di difficoltà nella connessione a Internet, fare riferimento alla tabella di seguito che riporta ai suggerimenti per la risoluzione di problemi forniti in questa sezione.

Se...	Vedere...
Non è possibile connettersi a internet	"La connessione a Internet non riesce dopo l'installazione", in questa pagina
È possibile connettersi a Internet ma si viene disconnessi dopo breve tempo	"Consentire messaggi heartbeat dell'ISP",
Il computer è un client ICS (Condivisione connessione Internet) e non è possibile connettersi a internet	"Connessione tramite un client ICS",
Il computer utilizza un server proxy per connettersi a Internet e non è possibile connettersi a Internet	"Connessione tramite un server proxy",
In un avviso del programma è visualizzato il messaggio "Impossibile contattare il server di programmi automatico".	"Impossibile connettersi a un server per consigli sui programmi",

**Tabella C-3: Risoluzione di problemi relativi al software antivirus**

## La connessione a Internet non riesce dopo l'installazione

Se non è possibile connettersi a Internet dopo l'installazione del software di sicurezza Zone Labs, è necessario innanzitutto determinare se la causa è il software di sicurezza Zone Labs. Se è impossibile seguire i passaggi riportati di seguito, per esempio se non si può deselezionare la casella di controllo **Carica software di sicurezza Zone Labs all'avvio**, contattare il supporto tecnico di Zone Labs.

### Determinare se il software di sicurezza Zone Labs è la causa dei problemi di connessione

1. Selezionare **Panoramica | Preferenze**.
2. Nella sezione Impostazioni generali, deselezionare la casella di controllo **Carica software di sicurezza Zone Labs all'avvio**.

Viene visualizzata una finestra di dialogo di avviso Servizio TrueVector di Zone Labs.

3. Fare clic su **Consenti**.
4. Riavviare il computer e riprovare a connettersi a Internet.

Se è possibile connettersi	Le impostazioni del software di sicurezza Zone Labs potrebbero essere la causa dei problemi di connessione. Verificare che il browser disponga dell'autorizzazione di accesso.
Se non è possibile connettersi	Le impostazioni del software di sicurezza Zone Labs non sono la causa dei problemi di connessione.

## Consentire messaggi heartbeat dell'ISP

I provider di servizi Internet (ISP) inviano periodicamente messaggi heartbeat ai propri clienti che usano connessioni remote per verificare che siano ancora presenti. Se l'ISP non riesce a determinare se l'utente è ancora attivo, potrebbe disconnetterlo e fornire il suo indirizzo IP a un altro utente.

Per impostazione predefinita, il software di sicurezza Zone Labs blocca i protocolli più utilizzati per questi messaggi heartbeat e in questo modo potrebbe causare la disconnessione dell'utente da Internet. Per evitare che si verifichi tale situazione, è possibile identificare il server che invia i messaggi e aggiungerlo alla zona attendibile, oppure configurare la zona Internet per consentire i messaggi ping.

### *Identificazione dell'origine dei messaggi heartbeat*

Si tratta della soluzione migliore perché è adatta indipendentemente dal fatto che l'ISP utilizzi NetBIOS o ICMP (*Internet Control Message Protocol*) per controllare la connessione, e consente di mantenere una sicurezza elevata per la zona Internet.

### Identificare il server utilizzato dall'ISP per controllare la connessione

1. Quando l'ISP disconnette l'utente, fare clic su **Avvisi e log** | **Visualizzatore log**.
2. Nell'elenco degli avvisi, individuare l'avviso generato al momento della disconnessione.
3. Nella sezione Dettagli voce, annotare il DNS di origine rilevato.

Se non è possibile identificare il server in questo modo, contattare l'ISP per determinare quali server necessitano dell'autorizzazione di accesso.

4. Dopo avere identificato il server, aggiungerlo alla zona attendibile.

Vedere "Aggiunta alla zona attendibile", .

### *Configurazione del software di sicurezza Zone Labs per consentire i messaggi ping*

Se l'ISP utilizza messaggi echo ICMP (o ping) per controlli della connettività, configurare il software di sicurezza Zone Labs per consentire i messaggi ping dalla zona Internet.

### Configurare il software di sicurezza Zone Labs per consentire i messaggi ping

1. Selezionare **Firewall** | **Principale**.
2. Nella sezione Sicurezza zona Internet, fare clic su **Personalizza**.
3. Selezionare la casella di controllo **Consenti ping in arrivo (echo ICMP)**.
4. Fare clic su **OK**.
5. Impostare la sicurezza per la zona Internet a Media.

Vedere "Scelta dei livelli di sicurezza", .

## Connessione tramite un client ICS

Se è attiva l'opzione Condivisione connessione Internet (ICS) di Windows o si utilizza un programma di condivisione della connessione di terze parti, e non è possibile connettersi a Internet, verificare che il software di sicurezza Zone Labs sia configurato correttamente per i computer con funzione di client e gateway. Vedere "Protezione di una connessione a Internet condivisa", .

Non configurare il software di sicurezza Zone Labs per la condivisione della connessione a Internet se si utilizza una soluzione hardware (come un server o un router) anziché un PC host.

## Connessione tramite un server proxy

Se si prova a connettersi a Internet tramite un server proxy ma la connessione non riesce, verificare che l'indirizzo IP del server proxy sia nella zona attendibile. Vedere "Aggiunta alla zona attendibile", .

## Impossibile connettersi a un server per consigli sui programmi

Se si riceve un avviso Programma con il messaggio "Impossibile contattare il server di programmi automatico", nella sezione SmartDefense Advisor, verificare che la connessione a Internet funzioni correttamente.

- Verificare che il computer sia collegato correttamente alla rete o al modem.
- Se si è connessi a Internet tramite modem via cavo o DSL, potrebbe essersi verificata una temporanea interruzione del servizio.
- Spesso è sufficiente riprovare in seguito senza modificare la configurazione.
- Avviare il browser. Se non si riesce a collegarsi ad alcun sito su Internet, è possibile che il software di sicurezza Zone Labs sia configurato per bloccare l'accesso a Internet. Fornendo la corretta autorizzazione al browser è possibile risolvere il problema.

Se non si tratta di alcuno di questi casi, è possibile che il server non sia momentaneamente disponibile.

# IM Security

In caso di difficoltà con la funzionalità IM Security, fare riferimento alla tabella di seguito che riporta ai suggerimenti per la risoluzione di problemi forniti in questa sezione.

Se...	Vedere...
Un programma IM attivo non appare nella tabella Stato della protezione	"I programmi IM non appaiono nella tabella Stato della protezione", in questa pagina

**Tabella C-4: Risoluzione di problemi di IM Security**

## I programmi IM non appaiono nella tabella Stato della protezione

Se si dispone di un programma di messaggistica immediata in esecuzione ma tale programma non appare nella tabella Stato della protezione nel pannello di IM Security, chiudere il programma di messaggistica immediata e riavviarlo.

Questo problema si può verificare se i programmi di messaggistica immediata e il software di sicurezza Zone Labs sono impostati per essere aperti all'avvio. Per evitare che ciò avvenga, modificare le impostazioni per i programmi di messaggistica immediata consentendo un avvio manuale.

# Antivirus

In caso di difficoltà nella connessione con l'utilizzo del software antivirus, fare riferimento alla tabella di seguito che riporta ai suggerimenti per la risoluzione di problemi forniti in questa sezione.

Se...	Vedere...
La funzione antivirus non è disponibile	"Problema di installazione della funzione antivirus", in questa pagina
La funzione Monitoraggio antivirus non è disponibile	"Avviso Monitoraggio Antivirus", in questa pagina
Si riceve un avviso riguardante prodotti in conflitto	"Risoluzione di conflitti tra prodotti antivirus",
È impossibile attivare le funzioni di sicurezza antivirus o IM	"Scansione della posta elettronica o IM Security non disponibile",

**Tabella C-5: Risoluzione dei problemi di Zone Labs Anti-virus**

## Problema di installazione della funzione antivirus

In alcuni casi, la caratteristica Antivirus non è disponibile dopo l'installazione se si sono verificati dei problemi nell'installazione. Questo può avvenire se il file `av.dll` non viene registrato correttamente durante l'installazione oppure se si verifica un errore durante un'operazione di aggiornamento. In questi casi, sarà visualizzato un avviso "Azione necessaria: Reinstallare ZoneAlarm Security Suite (o ZoneAlarm Anti-virus)".

Per risolvere questo problema, chiudere il software di sicurezza Zone Labs ed eseguire di nuovo il programma di installazione. Quando viene richiesto durante l'installazione, selezionare **Aggiorna** anziché **Nuova installazione**. Se dopo la reinstallazione del prodotto il pannello Antivirus non funziona ancora correttamente, è possibile provare a disinstallare il prodotto ed eseguire una nuova installazione. Se non si riesce a risolvere il problema con queste soluzioni, contattare il supporto clienti di Zone Labs.

## Avviso Monitoraggio Antivirus

L'avviso Monitoraggio antivirus consente di sapere quando la protezione antivirus sul computer non protegge completamente dai virus. Questo avviso potrebbe essere visualizzato quando l'antivirus è disattivato, quando le firme dell'antivirus non sono aggiornate o quando non è in esecuzione alcun software antivirus.

Notare che non tutti i prodotti antivirus vengono monitorati, quindi l'assenza di un avviso non significa necessariamente che il computer è protetto. Per assicurare la protezione del computer, aprire il software antivirus (se installato) ed effettuare un aggiornamento o rinnovare la sottoscrizione se è scaduta.

## Risoluzione di conflitti tra prodotti antivirus

Se si utilizza ZoneAlarm Security Suite e sul computer è installato anche un altro prodotto antivirus, si potrebbe ricevere un avviso di conflitto che informa che occorre disinstallare tale prodotto prima di utilizzare l'antivirus di Zone Labs. L'avviso elenca i prodotti software antivirus rilevati e specifica se ZoneAlarm Security Suite è in grado di disinstalarli automaticamente o se è necessario disinstallarli manualmente. Se i prodotti elencati non possono essere disinstallati automaticamente, consultare la documentazione dei singoli produttori per avere istruzioni sulla disinstallazione dei prodotti.

## Scansione della posta elettronica o IM Security non disponibile

Se si prova ad attivare l'opzione di scansione della posta elettronica del software antivirus di Zone Labs o la caratteristica IM Security e non si riesce a farlo, è possibile che sul computer sia installato un prodotto che utilizza la tecnologia LSP (Layered Service Provider), che non è compatibile con ZoneAlarm Security Suite. Per porre rimedio a questa situazione, sarà necessario disinstallare il prodotto o i prodotti in conflitto.

Quando si verifica un conflitto, viene creato un file `lspconflict.txt` che viene inserito nella directory `C:\Windows\Internet Logs`. Questo file contiene il nome del prodotto o dei prodotti che hanno causato il conflitto. È possibile rimuovere manualmente i prodotti oppure inviare un messaggio di posta elettronica a [lsupport@zonelabs.com](mailto:lsupport@zonelabs.com) allegando il file. Consultare la documentazione dei singoli produttori per avere istruzioni sulla disinstallazione dei prodotti.

# Problemi legati a software di terzi

Molti dei programmi più comuni possono essere configurati automaticamente per accedere a Internet. Pur essendo possibile in alcuni casi configurare automaticamente l'accesso a Internet, molti programmi necessitano anche di diritti di accesso server.

Se si utilizzano programmi che il software di sicurezza Zone Labs non è in grado di riconoscere e configurare automaticamente, sarà necessario configurare manualmente le autorizzazioni. software di sicurezza Zone Labs. Fare riferimento alle sezioni seguenti per informazioni su come configurare i programmi per l'utilizzo con il software di sicurezza Zone Labs.

## Antivirus

Affinché il software antivirus possa ricevere gli aggiornamenti, deve avere l'autorizzazione di accesso alla zona attendibile.

### *Aggiornamenti automatici*

Per poter ricevere gli aggiornamenti automatici dal sito del software antivirus, aggiungere il dominio che contiene gli aggiornamenti (per esempio, update.avsupdate.com) alla zona attendibile. Vedere "Aggiunta alla zona attendibile", .

### *Protezione posta elettronica*

In alcuni casi, la funzione MailSafe del software di sicurezza Zone Labs potrebbe entrare in conflitto con le funzionalità di protezione della posta del software antivirus. In questi casi, regolare le impostazioni del software di sicurezza Zone Labs e dell'antivirus in modo da trarre beneficio da entrambe le protezioni.

## Configurare il software antivirus

1. Impostare il programma antivirus per eseguire la scansione di tutti i file all'accesso e disattivare l'opzione di scansione della posta elettronica.
2. Nel software di sicurezza Zone Labs, attivare la protezione di MailSafe in entrata.  
Vedere "Attivazione della protezione di MailSafe in entrata", .
3. Disattivare la visualizzazione di avvisi per gli allegati di MailSafe in quarantena.  
Vedere "Mostrare o nascondere avvisi specifici", .



Con questa configurazione, MailSafe continuerà a mettere in quarantena gli allegati sospetti e avviserà l'utente quando cercherà di aprirli. Se si decide di aprire comunque un allegato, il software antivirus lo sottoporrà a scansione.



## Browser

Affinché il browser possa funzionare correttamente, deve ricevere l'autorizzazione di accesso alla zona attendibile e alla zona Internet. Prima di concedere l'autorizzazione, accertarsi di aver compreso come configurare la sicurezza del browser per una protezione ottimale e aver installato gli ultimi service pack per il browser utilizzato.

Per concedere l'autorizzazione di accesso al browser, effettuare una delle seguenti operazioni:

- Consentire l'accesso direttamente al programma. Vedere "Concessione dell'autorizzazione di accesso a Internet per un programma", .
- Selezionare **Consenti** quando viene visualizzato un avviso relativo al browser.

### *Internet Explorer*

Se si usa Windows 2000, potrebbe essere necessario consentire diritti di accesso a Services and Controller App (il cui nome di file è generalmente services.exe).

### **Concedere l'autorizzazione di accesso a Services and Controller App**

1. Selezionare **Controllo dei programmi | Programmi**.
2. Nella colonna Programmi, individuare **Services and Controller App**.
3. Nella colonna Accesso, selezionare **Consenti** dal menu di scelta rapida.

### *Netscape*

Le versioni di Netscape Navigator successive alla 4.73 non dovrebbero avere problemi se eseguite assieme al software di sicurezza Zone Labs. Se, tuttavia, si utilizza Navigator versione 4.73 o versione successiva e si hanno comunque delle difficoltà ad accedere al Web con il software di sicurezza Zone Labs attivo, controllare le preferenze del browser perché potrebbe essere configurato l'accesso proxy.

## **Programmi di chat e messaggistica immediata**

I programmi di chat e messaggistica immediata (per esempio, AOL Instant Messenger) potrebbero richiedere l'autorizzazione del server per poter funzionare correttamente.

Per concedere l'autorizzazione server al programma di chat, effettuare una delle seguenti operazioni:

- Rispondere Consenti all'avviso Programma server generato dal programma.
- Concedere l'autorizzazione server al programma.

Vedere "Concessione a un programma dell'autorizzazione ad agire come server", .



Si consiglia di impostare il software di chat per consentire i trasferimenti di file solo dopo aver chiesto conferma. Il trasferimento di file nei programmi chat è, infatti, un mezzo utilizzato per distribuire programmi malware come worm, virus e Trojan horse. Fare riferimento alla Guida in linea del software di chat per istruzioni su come configurare il programma per la massima sicurezza. Se si utilizza ZoneAlarm Security Suite, impostare il livello di IM Security su Alta per bloccare il trasferimento dei file.

## Programmi di posta elettronica

Affinché il client di posta elettronica (per esempio, Microsoft Outlook) possa inviare e ricevere posta, deve ricevere l'autorizzazione di accesso per la zona a cui appartiene il server di posta. Inoltre, alcuni client di posta elettronica potrebbero includere più componenti che necessitano dell'autorizzazione server. Per esempio, Microsoft Outlook richiede che l'applicazione base (OUTLOOK.EXE) e il sottosistema di invio dei messaggi (MAPISP32.exe) abbiano entrambi l'autorizzazione server.

Sebbene sia possibile lasciare il server di posta nella zona Internet e concedere al client di posta l'autorizzazione di accesso a Internet, è consigliabile inserire il server nella zona attendibile e limitare l'accesso del programma solo a quella zona. Una volta che il client di posta può accedere alla zona attendibile, aggiungere il server di posta remoto (host) alla zona attendibile.

Per conoscere come assegnare a un programma l'autorizzazione ad accedere o ad agire come server nella zona attendibile, vedere "Impostazione manuale delle autorizzazioni per i programmi", .

Per sapere come aggiungere un host alla zona attendibile, vedere "Gestione delle origini di traffico", .

## Programmi di segreteria telefonica Internet

Per utilizzare i programmi di segreteria Internet (come CallWave) con il software di sicurezza Zone Labs, effettuare le seguenti operazioni:

- Concedere al programma l'autorizzazione server e di accesso per la zona Internet.
- Aggiungere l'indirizzo IP dei server del produttore alla zona attendibile.



Per conoscere l'indirizzo IP del server, contattare il supporto tecnico del produttore.

- Impostare la sicurezza per la zona Internet a Media.

## Programmi di condivisione file

I programmi di condivisione di file, come Napster, Limewire, AudioGalaxy e i client Gnutella, devono ricevere l'autorizzazione server per la zona Internet affinché possano operare con il software di sicurezza Zone Labs.

## Programmi FTP

Per utilizzare i programmi FTP (File Transfer Protocol), potrebbe essere necessario apportare le seguenti modifiche alle impostazioni del client FTP e nel software di sicurezza Zone Labs:

- Attivare la modalità passiva o PASV nel client FTP

Ciò indica al client di utilizzare la stessa porta di comunicazione in entrambe le direzioni. Se non si attiva la modalità PASV, il software di sicurezza Zone Labs potrebbe bloccare il tentativo del server FTP di contattare una nuova porta sul computer per il trasferimento dei file.

- Aggiungere i siti FTP utilizzati alla zona attendibile
- Concedere l'autorizzazione di accesso alla zona attendibile al client FTP.

Per sapere come aggiungere un programma alla zona attendibile e concedere l'autorizzazione di accesso, vedere "Impostazione delle opzioni di sicurezza avanzate", .

## Giochi

Per poter giocare su Internet utilizzando il software di sicurezza Zone Labs, potrebbe essere necessario regolare le seguenti impostazioni.

### *Autorizzazione per i programmi*

Per poter funzionare, molti giochi su Internet necessitano dell'autorizzazione di accesso e/o server per la zona Internet.

Il modo più semplice per concedere l'accesso è rispondere "Consenti" all'avviso generato dal programma del gioco. Tuttavia, molti giochi vengono eseguiti in modalità schermo intero "esclusiva", che non visualizza l'avviso. Per risolvere questo problema, utilizzare uno dei seguenti metodi.

- Impostare il gioco per essere eseguito in una finestra

In questo modo, sarà possibile vedere l'avviso se il gioco viene eseguito in una finestra di dimensioni inferiori del desktop. Se l'avviso appare ma non è possibile rispondere perché il mouse è bloccato dal gioco, premere il tasto Windows sulla tastiera.

Dopo aver concesso al programma del gioco l'accesso a Internet, reimpostare la modalità a schermo intero.

- Utilizzare la modalità di rendering software

Impostando la modalità di rendering a "software", si consente a Windows di visualizzare l'avviso sopra la schermata del gioco. Dopo aver consentito al gioco l'accesso a Internet, è possibile riattivare le impostazioni di rendering preferite.

- Utilizzare Alt+Tab

Premere **Alt+Tab** per tornare a Windows. La combinazione di tasti lascia il gioco in esecuzione, ma consente all'utente di rispondere all'avviso. Dopo aver consentito l'accesso a Internet, premere di nuovo **Alt+Tab** per ritornare al gioco.



L'ultimo metodo potrebbe mandare in blocco alcune applicazioni, soprattutto se si utilizza Glide o OpenGL; tuttavia, il problema dovrebbe essere corretto al successivo avvio del gioco. A volte, si può premere Alt+Invio al posto di Alt+Tab.

### ***Livello di sicurezza e zona***

Alcuni giochi su Internet, in particolare quelli che utilizzano Java, applet o altra funzionalità fornita da un portale su Internet, potrebbero non funzionare correttamente quando l'impostazione di sicurezza della zona Internet è Alta. Questo livello potrebbe anche impedire ai server di gioco remoti di "vedere" il computer. Per risolvere questi problemi, è possibile:

- Impostare il livello di sicurezza della zona Internet a Media, oppure
- Aggiungere l'indirizzo IP del server di gioco a cui ci si connette alla zona attendibile. La documentazione del produttore del gioco dovrebbe indicare l'indirizzo IP o il nome host del server.

Per sapere come aggiungere un host o un indirizzo IP alla zona attendibile, vedere "Aggiunta alla zona attendibile", .



Fidarsi dei server di gioco significa fidarsi degli altri giocatori. Il software di sicurezza Zone Labs non protegge l'utente dagli attacchi provocati dai compagni di gioco in un ambiente attendibile. Accertarsi di aver compreso come configurare la sicurezza del browser per una protezione ottimale e aver installato gli ultimi service pack per il browser utilizzato.

## **Programmi di controllo remoto**

Se il computer è l'host o il client di un sistema di controllo remoto come PCAnywhere o Timbuktu:

- Aggiungere alla zona attendibile l'indirizzo IP degli host o dei client a cui si accede. Vedere "Aggiunta alla zona attendibile", .
- Aggiungere la subnet della rete a cui si accede da remoto alla zona attendibile. Vedere "Aggiunta alla zona attendibile", .

- Se viene assegnato un indirizzo IP dinamico al computer remoto, aggiungere l'indirizzo o l'intervallo di indirizzi del server DHCP alla zona attendibile.



Se l'host o il client di controllo remoto si trova su una rete non controllata dall'utente (per esempio, una LAN aziendale o universitaria), i firewall o altre caratteristiche della rete potrebbero impedire la connessione. Se si verificano ancora dei problemi con la connessione dopo aver seguito le suddette istruzioni, chiedere assistenza all'amministratore della rete.

## Programmi VNC

Affinché i programmi VNC e il software di sicurezza Zone Labs possano operare assieme, seguire questi passaggi.

1. Sul computer server e client, effettuare una delle seguenti operazioni:

- Se si conosce l'indirizzo IP o la subnet del client che si utilizzerà per l'accesso remoto, e si tratterà sempre dello stesso computer, aggiungerlo alla zona attendibile. Vedere "Aggiunta alla zona attendibile", .

Se non si conosce l'indirizzo IP del client, oppure non si utilizza sempre lo stesso computer, concedere al programma l'autorizzazione di accesso e server per le zone attendibile e Internet. Vedere "Impostazione delle autorizzazioni d'accesso per i nuovi programmi", .

Quando richiesto da VNC Viewer sul computer client, immettere il nome o l'indirizzo IP del server, seguito dalla password. Dovrebbe essere così possibile stabilire una connessione.



Se è stato attivato l'accesso VNC concedendo l'autorizzazione server e di accesso, ricordarsi di impostare e utilizzare la password VNC per poter mantenere la sicurezza. È consigliabile aggiungere l'indirizzo IP del server e del client alla zona attendibile, invece di concedere l'autorizzazione di accesso alla zona Internet.

2. Sul computer client, eseguire VNC Viewer per stabilire la connessione al server. Non eseguirlo in modalità "di ascolto".

### *Telnet*

Per accedere a un server remoto via Telnet, aggiungere l'indirizzo IP del server alla zona attendibile.

## Programmi per flussi multimediali

Le applicazioni che ricevono flussi multimediali audio e video, come RealPlayer, Windows Media Player, QuickTime o altri, devono ricevere l'autorizzazione server per la zona Internet affinché possano operare con il software di sicurezza Zone Labs.

Per sapere come concedere l'autorizzazione server a un programma, vedere "Concessione a un programma dell'autorizzazione ad agire come server", .

## Programmi Voice over IP

Per utilizzare programmi Voice over IP (VoIP) con il software di sicurezza Zone Labs, è necessario effettuare una o entrambe le operazioni seguenti, in base al programma specifico:

1. Concedere all'applicazione VoIP l'autorizzazione server e di accesso.
2. Aggiungere i server del provider della soluzione VoIP alla zona attendibile. Per conoscere l'indirizzo IP di questi server, rivolgersi al supporto clienti del provider della soluzione VoIP.

## Programmi per conferenze sul Web

Se si hanno dei problemi nell'utilizzo di programmi per conferenze sul Web, come Microsoft NetMeeting, provare quanto segue:

1. Aggiungere alla zona attendibile il dominio o l'indirizzo IP a cui ci si connette per tenere la conferenza. Vedere "Aggiunta alla zona attendibile", .
2. Disattivare l'opzione di condivisione del desktop remoto del programma per conferenze.

# Appendice

---

## Comportamento dei programmi

D

Questa appendice fornisce le istruzioni per determinare se consentire o negare ai programmi l'autorizzazione a eseguire attività sospette o pericolose.

- "Comportamento sospetto", a pagina 262
- "Comportamento pericoloso", a pagina 263

## Comportamento sospetto

La tabella seguente fornisce alcune informazioni utili per capire come rispondere agli avvisi di tipo Comportamento sospetto. Le informazioni elencate qui servono solo da riferimento. Ricordare che alcuni programmi "legittimi" hanno la necessità di eseguire le azioni elencate nella tabella. L'autorizzazione o meno del comportamento sospetto deve essere determinata in base alla situazione specifica.

Comportamento rilevato	Che cosa significa	Che cosa fare
Modifiche alla directory di avvio	Un programma si sta impostando per l'esecuzione all'avvio del computer.	È opportuno negare questa azione, a meno che non si stia installando un programma, poiché potrebbe trattarsi di uno malware.
Modifica delle impostazioni di ricerca predefinite del browser	La ricerca predefinita del browser viene modificata.	È opportuno negare questa azione, a meno che non si stia modificando la funzione di ricerca del browser.
Modifica delle impostazioni predefinite delle pagine del browser	La pagina iniziale del browser predefinito viene modificata.	È opportuno negare questa azione, a meno che non si stia modificando la pagina iniziale.
Scaricare un driver	Un programma sta cercando di scaricare il driver di un altro programma.	Questo comportamento non è giustificato. È opportuno negare questa azione.

**Tabella D-1: Guida sul comportamento sospetto**



# Comportamento pericoloso

La tabella seguente fornisce alcune informazioni utili per capire come rispondere agli avvisi di tipo Comportamento pericoloso. Le informazioni elencate qui servono solo da riferimento. Ricordare che pochi programmi "legittimi" hanno la necessità di eseguire le azioni elencate nella tabella.

Comportamento rilevato	Che cosa significa	Che cosa fare
Trasmissione di input DDE (Dynamic Data Exchange)	Un programma sta cercando di inviare input DDE a un altro programma e questo potrebbe consentirgli l'accesso a Internet o potrebbe provocare la perdita di dati.	Questo comportamento è usato spesso per aprire URL in Internet Explorer. Se l'applicazione in questione è nota e attendibile, probabilmente è possibile consentire l'azione. In caso contrario, fare clic su Nega.
Invio di messaggi di Windows	Un programma sta cercando di inviare un messaggio a un altro programma.	Un programma potrebbe cercare di costringere un altro programma a eseguire determinate funzioni. È opportuno negare questa azione, a meno che non si stia installato un software che deve comunicare con un altro programma.
Un programma sta tentando di bloccare un altro programma.	Un programma sta tentando di terminare un altro programma.	Un programma potrebbe cercare di terminare un programma attendibile. È opportuno negare questa azione, a meno che sia stato usato Task Manager per terminare un programma o un processo oppure è appena stato installato un software che richiede il riavvio del computer.
Aprire processi/thread	Un programma sta tentando di controllare un altro programma. È normale che le applicazioni di sistema si comportino così.	È opportuno negare questa azione, a meno che il programma sia attendibile.

**Tabella D-2: Guida sul comportamento pericoloso**

<b>Comportamento rilevato</b>	<b>Che cosa significa</b>	<b>Che cosa fare</b>
Monitoraggio dell'utilizzo di tastiera e mouse	Un programma sta tentando di monitorare i tasti premuti sulla tastiera e l'input tramite mouse.	È opportuno negare questa azione, a meno che non si stia eseguendo un programma speciale che ha la necessità di monitorare queste attività, come i software di narrazione.
Controllo remoto dell'input da tastiera e tramite mouse	Un programma sta tentando di controllare a distanza la tastiera e il mouse.	È opportuno negare questa azione, a meno che non si stia eseguendo un software di accesso remoto, quale PC Anywhere o VNC.
Installazione di driver	Un programma sta tentando di caricare un <i>driver</i> . Il caricamento di un driver consente a un programma di eseguire qualsiasi cosa sul computer.	È opportuno negare questa azione, a meno che non si stia installando un software antivirus o antispyware, un firewall, una rete VPN o altri tipi di strumenti di sistema.
Modifica della <i>memoria fisica</i>	Un programma potrebbe tentare di modificare o leggere informazioni appartenenti a un altro programma.	È opportuno negare questa azione, a meno che non si stia eseguendo un software di gioco, video o utilità di sistema.
Introduzione di codice in un programma o in un servizio di sistema	Un programma sta tentando di inserire in un altro programma del codice, che potrebbe essere usato per disattivare il programma o il servizio.	È opportuno negare questa azione, a meno che non si stia eseguendo un software speciale per cambiare l'aspetto o il comportamento di un programma.
Modifica dei parametri di rete	Un programma sta tentando di modificare le impostazioni di rete, probabilmente per dirottare l'utente verso siti Web pericolosi e monitorarne il traffico sul Web.	È opportuno negare questa azione, a meno che non si stia eseguendo un software di regolazione TCP/IP.

**Tabella D-2: Guida sul comportamento pericoloso**

<b>Comportamento rilevato</b>	<b>Che cosa significa</b>	<b>Che cosa fare</b>
Avvio di un programma sconosciuto o maligno da uno valido	Un programma sta tentando di modificare un altro programma.	È opportuno negare questa azione, a meno che un programma che si sta utilizzando debba legittimamente aprirne un altro (per esempio un documento Word con un collegamento al browser o un programma IM con collegamenti ad altri programmi).
Accesso al registro di sistema	Il processo sta cercando di accedere alle impostazioni del registro di sistema.	Generalmente, questo comportamento viene bloccato automaticamente. Se il controllo dei programmi è impostato alla modalità manuale, negare questa azione.
Eliminazione di una chiave di esecuzione	Un programma ha cercato di eliminare la voce di una chiave di esecuzione.	Se il programma è stato impostato per l'apertura all'avvio del computer, ma è stato rimosso, sarà rimossa anche la chiave di esecuzione. Negare l'azione in tutti gli altri casi.
Modifica di ZoneAlarm	Un programma sta cercando di modificare il programma ZoneAlarm, probabilmente per impedirne l'esecuzione o per eseguire gli aggiornamenti del prodotto.	Negare questa azione, a meno che non si stia aggiornando il client ZoneAlarm.

**Tabella D-2: Guida sul comportamento pericoloso**



# Appendice

---

## Errata corrige della documentazione



Questa appendice descrive le modifiche apportate alla versione Inglese della documentazione per la versione 6.1 che non sono state incluse nel corpo principale del manuale utente per le versioni localizzate.

- “Modifica agli avvisi OSFirewall”, a pagina 267
- “La scansione della posta elettronica supporta IMAP in Outlook”, a pagina270
- “Interrompere la scansione dei virus”, a pagina270
- “Controllo dei componenti”, a pagina 271
- “Modifiche alla funzione Controllo dei programmi”, a pagina272
- “Altre modifiche”, a pagina272

## Modifica agli avvisi OSFirewall

Gli avvisi di tipo Comportamento pericoloso di OSFirewall sono stati rinominati in avvisi di tipo Comportamento sospetto di alto livello. Questi avvisi presentano un indicatore di avviso rosso. Il motivo per cui vengono visualizzati questi avvisi è invariato: vengono visualizzati quando un programma sconosciuto tenta di eseguire operazioni tipiche di software dannosi. Tuttavia, alcuni software autorizzati potrebbero eseguire queste operazioni sospette come parte del loro normale funzionamento. Per questo l'utente deve decidere se consentire o negare il comportamento sospetto in base alle proprie conoscenze sull'applicazione e sull'affidabilità del produttore.

Le tabelle seguenti sono state modificate rispetto alle versioni dell'Appendice D per riflettere la modifica da Comportamento pericoloso a Comportamento sospetto di alto livello. La tabella seguente fornisce alcune informazioni utili per capire come rispondere agli avvisi di tipo Comportamento sospetto di medio livello (indicatore giallo).

Comportamento rilevato	Che cosa significa	Che cosa fare
Modifiche alla directory di avvio	Un programma si sta impostando per l'esecuzione all'avvio del computer.	È opportuno negare questa azione, a meno che non si stia installando un programma, poiché potrebbe trattarsi di uno spyware.
Modifica delle impostazioni di ricerca predefinite del browser	La ricerca predefinita del browser viene modificata.	È opportuno negare questa azione, a meno che non si stia modificando la funzione di ricerca del browser.
Modifica delle impostazioni predefinite delle pagine del browser	La pagina iniziale del browser predefinito viene modificata.	È opportuno negare questa azione, a meno che non si stia modificando la pagina iniziale.
Scaricare un driver	Un programma sta cercando di scaricare il driver di un altro programma.	Questo comportamento non è giustificato. È opportuno negare questa azione.

**Tabella E-1: Guida al comportamento sospetto di medio livello**

La tabella seguente fornisce alcune informazioni utili per capire come rispondere agli avvisi di tipo Comportamento sospetto di alto livello (indicatore rosso). Le informazioni

elencate qui servono solo da riferimento. Ricordare che pochi programmi "legittimi" hanno la necessità di eseguire le azioni elencate nella tabella.

<b>Comportamento rilevato</b>	<b>Che cosa significa</b>	<b>Che cosa fare</b>
Trasmissione di input DDE (Dynamic Data Exchange)	Un programma sta cercando di inviare input DDE a un altro programma e questo potrebbe consentirgli l'accesso a Internet o potrebbe provocare la perdita di dati.	Questo comportamento è usato spesso per aprire URL in Internet Explorer. Se l'applicazione in questione è nota e attendibile, probabilmente è possibile consentire l'azione. In caso contrario, fare clic su Nega.
Invio di messaggi di Windows	Un programma sta cercando di inviare un messaggio a un altro programma.	Un programma potrebbe cercare di costringere un altro programma a eseguire determinate funzioni. È opportuno negare questa azione, a meno che non si stia installando un software che deve comunicare con un altro programma.
Un programma sta tentando di bloccare un altro programma.	Un programma sta tentando di terminare un altro programma.	Un programma potrebbe cercare di terminare un programma attendibile. È opportuno negare questa azione, a meno che sia stato usato Task Manager per terminare un programma o un processo oppure è appena stato installato un software che richiede il riavvio del computer.
Aprire processi/thread	Un programma sta tentando di controllare un altro programma. È normale che le applicazioni di sistema si comportino così.	È opportuno negare questa azione, a meno che il programma sia attendibile.
Monitoraggio dell'utilizzo di tastiera e mouse	Un programma sta tentando di monitorare i tasti premuti sulla tastiera e l'input tramite mouse.	È opportuno negare questa azione, a meno che non si stia eseguendo un programma speciale che ha la necessità di monitorare queste attività, come i software di narrazione.

**Tabella E-2: Guida al comportamento sospetto di alto livello**

<b>Comportamento rilevato</b>	<b>Che cosa significa</b>	<b>Che cosa fare</b>
Controllo remoto dell'input da tastiera e tramite mouse	Un programma sta tentando di controllare a distanza la tastiera e il mouse.	È opportuno negare questa azione, a meno che non si stia eseguendo un software di accesso remoto, quale PC Anywhere o VNC.
Installazione di driver	Un programma sta tentando di caricare un <i>driver</i> . Il caricamento di un driver consente a un programma di eseguire qualsiasi cosa sul computer.	È opportuno negare questa azione, a meno che non si stia installando un software antivirus o antispysware, un firewall, una rete VPN o altri tipi di strumenti di sistema.
Modifica della <i>physical memory</i>	Un programma potrebbe tentare di modificare o leggere informazioni appartenenti a un altro programma.	È opportuno negare questa azione, a meno che non si stia eseguendo un software di gioco, video o utilità di sistema.
Introduzione di codice in un programma o in un servizio di sistema	Un programma sta tentando di inserire in un altro programma del codice, che potrebbe essere usato per disattivare il programma o il servizio.	È opportuno negare questa azione, a meno che non si stia eseguendo un software speciale per cambiare l'aspetto o il comportamento di un programma.
Modifica dei parametri di rete	Un programma sta tentando di modificare le impostazioni di rete, probabilmente per dirottare l'utente verso siti Web pericolosi e monitorarne il traffico sul Web.	È opportuno negare questa azione, a meno che non si stia eseguendo un software di regolazione TCP/IP.
Avvio di un programma sconosciuto o maligno da uno valido	Un programma sta tentando di modificare un altro programma.	È opportuno negare questa azione, a meno che un programma che si sta utilizzando debba legittimamente aprirne un altro (per esempio un documento Word con un collegamento al browser o un programma IM con collegamenti ad altri programmi).

**Tabella E-2: Guida al comportamento sospetto di alto livello**



<b>Comportamento rilevato</b>	<b>Che cosa significa</b>	<b>Che cosa fare</b>
Accesso al registro di sistema	Il processo sta cercando di accedere alle impostazioni del registro di sistema.	Generalmente, questo comportamento viene bloccato automaticamente. Se il controllo dei programmi è impostato alla modalità manuale, negare questa azione.
Eliminazione di una chiave di esecuzione	Un programma ha cercato di eliminare la voce di una chiave di esecuzione.	Se il programma è stato impostato per l'apertura all'avvio del computer, ma è stato rimosso, sarà rimossa anche la chiave di esecuzione. Negare l'azione in tutti gli altri casi.
Modifica di ZoneAlarm	Un programma sta cercando di modificare il programma ZoneAlarm, probabilmente per impedirne l'esecuzione o per eseguire gli aggiornamenti del prodotto.	Negare questa azione, a meno che non si stia aggiornando il client ZoneAlarm.

**Tabella E-2: Guida al comportamento sospetto di alto livello**

## **La scansione della posta elettronica supporta IMAP in Outlook**

In passato, IMAP non era supportato in Outlook per la scansione degli account di posta elettronica. Questo protocollo è ora supportato.

### **Interrompere la scansione dei virus**

Nella documentazione corrente per la versione 6.1, il testo afferma che facendo clic su Pausa durante la scansione di virus si può interrompere la scansione corrente e disattivare la scansione all'accesso. Questa affermazione non è corretta. Anche se la scansione corrente viene interrotta, la scansione all'accesso rimane inalterata. Facendo di nuovo clic su Pausa la scansione corrente viene ripresa.

## Controllo dei componenti

Nella documentazione fornita con la versione 6.1 erano state omesse le istruzioni per attivare il controllo dei componenti. Queste sono state poi aggiunte alla documentazione di aggiornamento della release per la versione Inglese.

### Per attivare il controllo dei componenti:

1. Selezionare **Controllo dei programmi| Principale**.
2. Nell'area Controllo dei programmi, fare clic su **Personalizza**.  
Viene visualizzata la finestra di dialogo Impostazioni personalizzate Controllo dei programmi.
3. Nell'area Controllo dei componenti, selezionare la casella di controllo **Attiva controllo dei componenti**.
4. Fare clic su **OK**.

## Modifiche al filtro della posta indesiderata

Sono state aggiunte due nuove caselle di controllo al filtro della posta indesiderata. Una nuova casella di controllo per consentire la scansione di più cartelle Posta in arrivo di Outlook e una nuova casella di controllo per consentire la segnalazione automatica della posta fraudolenta.

### Per attivare la segnalazione automatica della posta elettronica fraudolenta:

1. Aprire il programma di posta Outlook o Outlook Express.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm | Configura preferenze | Impostazioni**.
3. Nella sezione **E-mail rapporto automatico sulla frode**, selezionare **Attiva il rapporto automatico**.
4. Fare clic su **Chiudi**.

### Per attivare la scansione di più cartelle Posta in arrivo:

1. Aprire il programma di posta Outlook o Outlook Express.
2. Nella barra degli strumenti del filtro della posta indesiderata, fare clic su **Opzioni di ZoneAlarm | Configura preferenze | Impostazioni**.
3. Nell'area Supporto per più cartelle Posta in arrivo di Outlook, selezionare Supporto scansione di più cartelle Posta in arrivo in Microsoft Outlook.



Questa funzione è supportata solo per Outlook 2000, 2002 (XP) e 2003 ed è attivata per impostazione predefinita.

## Modifiche alla funzione Controllo dei programmi

Nella sezione "Impostazione del livello di Controllo dei programmi (capitolo relativo al Controllo dei programmi), le definizioni di ALTA, MEDIA E BASSA ora sono le seguenti:

Impostazione	Descrizione
ALTA	Il programma avanzato è attivato. Con questa impostazione, saranno visualizzati numerosi avvisi. I programmi devono richiedere l'accesso a Internet e i diritti di agire da server. OSFirewall monitorerà il computer alla ricerca di comportamenti sospetti e pericolosi.
MEDIA	Questa è l'impostazione predefinita. I programmi devono richiedere l'accesso a Internet e i diritti di agire da server. OSFirewall monitorerà il computer alla ricerca di comportamenti sospetti e pericolosi. Controllo dei componenti disattivato.
BASSA	Il Controllo dei programmi è in modalità di apprendimento (non vengono visualizzati avvisi). OSFirewall è disattivato. Controllo dei componenti disattivato.

**Tabella E-3: Modifiche alla funzione Controllo dei programmi**

Inoltre è stata aggiunta una nuova opzione di Controllo dei programmi: Attiva OSFirewall; questa opzione attiva la protezione OSFirewall, che monitora i programmi alla ricerca di comportamenti sospetti che potrebbero compromettere il sistema operativo del computer.

### Altre modifiche

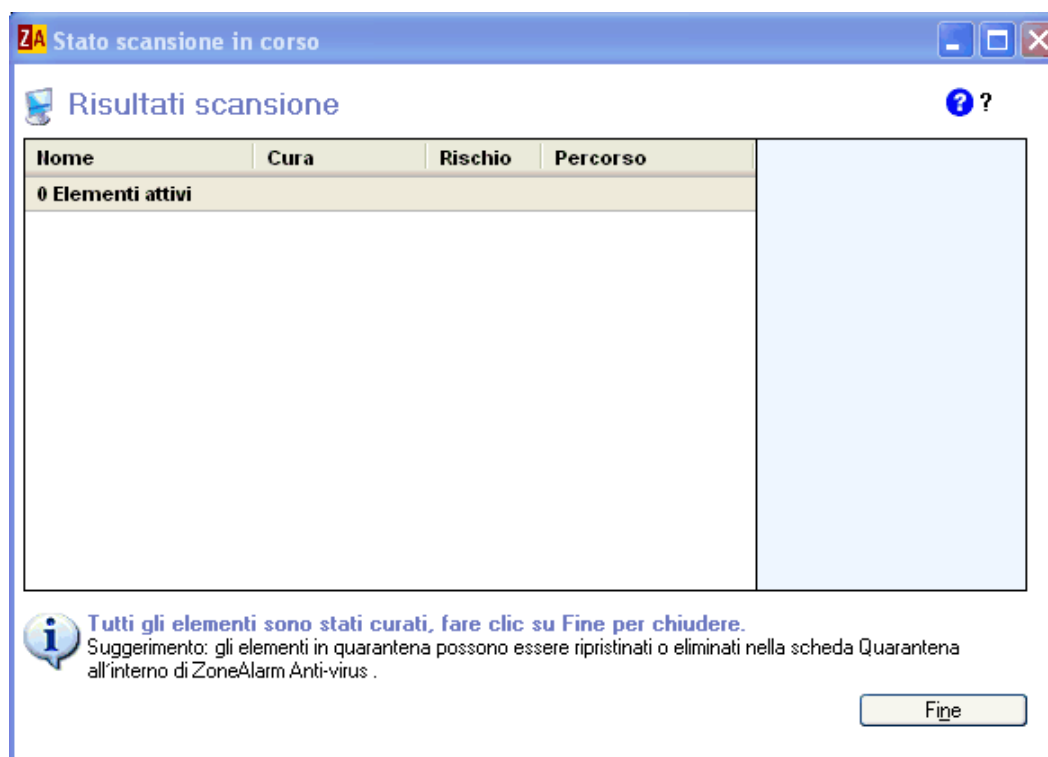
Sono state apportate le seguenti modifiche non funzionali alla documentazione:

- Nella Prefazione è stata aggiunta la descrizione seguente di ZoneAlarm Anti-Spyware in sostituzione di ZoneAlarm Wireless Security:

Include le stesse funzioni disponibili in ZoneAlarm gratuito, più la protezione anti-spyware, la protezione MailSafe in arrivo e in uscita, il Controllo dei programmi con SmartDefense Advisor e la protezione OSFirewall.

- La protezione della posta elettronica in uscita è stata rinominata in protezione MailSafe in uscita.

- L'immagine che mostra i risultati delle scansioni dei virus è stata sostituita con l'immagine seguente:



# Glossario

---

## **3DES**

Acronimo di Triple Data Encryption Standard, un metodo di crittografia a chiave simmetrica basato su standard che utilizza una chiave a 168 bit. 3DES è una variante più efficace del precedente standard di crittografia DES a 56 bit.

## **AGIRE COME SERVER**

Un programma agisce come server quando "ascolta" le richieste di connessione provenienti da altri computer. Molti tipi di applicazioni comuni, come i programmi di chat, i client di posta elettronica e i programmi di chiamate in attesa su Internet, potrebbero richiedere di agire come server per funzionare correttamente. Tuttavia, alcuni programmi concepiti da hacker agiscono come server per ricevere istruzioni dai loro creatori. Il software di sicurezza Zone Labs impedisce ai programmi sul computer di agire come server, a meno che ricevano l'autorizzazione server.

## **ANNUNCIO ANIMATO**

Un annuncio pubblicitario che contiene immagini in movimento.

## **ANNUNCIO POP-UNDER**

Un annuncio pubblicitario che appare in una nuova finestra del browser che si apre sotto la finestra correntemente visualizzata, in modo che l'annuncio sia visibile solo quando si chiude la finestra del browser originale.

## **ANNUNCIO POP-UP**

Un annuncio pubblicitario che appare in una nuova finestra del browser che si apre sopra alla finestra correntemente visualizzata.

## **ANNUNCIO SU BANNER**

Un annuncio pubblicitario che appare su un banner orizzontale lungo una pagina Web.

## **ANNUNCIO VERTICALE**

Un annuncio pubblicitario che appare in una colonna verticale lungo il lato di una pagina Web.

## **APPLET JAVA**

Un programma di piccole dimensioni basato su Internet e scritto in Java che è generalmente incorporato in una pagina HTML di un sito Web e può essere eseguito da un browser.

**AUTORIZZAZIONE DI ACCESSO**

L'autorizzazione di accesso consente a un programma sul computer di avviare la comunicazione con un altro computer. L'autorizzazione server, invece, consente a un programma di "ascoltare" le richieste di connessione provenienti da altri computer. È possibile concedere un'autorizzazione di accesso per la zona attendibile, la zona Internet o entrambe.

**AUTORIZZAZIONE SERVER**

L'autorizzazione server consente a un programma sul computer di "ascoltare" le richieste di connessione provenienti da altri computer, offrendo a questi ultimi la possibilità di avviare una comunicazione con il computer dell'utente. L'autorizzazione di accesso, invece, consente a un programma di avviare una sessione di comunicazione con un altro computer.

**AVVISI DI ALTO LIVELLO**

Un avviso causato probabilmente dall'attività di un hacker. Gli avvisi del firewall di alto livello presentano una banda rossa nella parte superiore della finestra di avviso. Nel Visualizzatore log, è possibile controllare se un avviso era di alto livello osservando la colonna Livello.

**AVVISI INFORMATIVI**

Il tipo di avvisi che viene visualizzato quando il software di sicurezza Zone Labs blocca una comunicazione che non corrisponde alle impostazioni di sicurezza. Gli avvisi informativi non richiedono una risposta da parte dell'utente.

**AVVISO DI MEDIO LIVELLO**

Un avviso causato probabilmente da attività di rete non pericolosa, piuttosto che dall'attacco di un hacker.

**BLOCCO ANNUNCI**

Una funzione del software di sicurezza Zone Labs che consente di bloccare banner, pop-up e altri tipi di annunci pubblicitari.

**BLUE COAT**

Blue Coat è una società di servizi di applicazione e di sviluppo software che si occupa di filtraggio, monitoraggio e report sull'utilizzo di Internet e le attività svolte. La funzione Controllo genitori di ZoneAlarm Pro utilizza categorie di contenuto di Blue Coat per stabilire se l'accesso ai siti Web visitati dall'utente sarà consentito o bloccato.

**BROADCAST/MULTICAST DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)**

Un tipo di messaggio utilizzato da un computer client su una rete che utilizza l'assegnazione dinamica degli indirizzi IP. Se il computer si connette online e richiede un indirizzo IP, emette un messaggio di broadcast per eventuali server DHCP sulla rete. Quando un server DHCP riceve il messaggio di broadcast, assegna un indirizzo IP al computer.

**CACHE CLEANER**

Funzione di privacy che consente di rimuovere i file e i cookie indesiderati dal computer a richiesta o in modo pianificato.

**CAMPO INTESTAZIONE PROVENIENZA HTTP**

Un campo facoltativo nel messaggio che apre una pagina Web contenente informazioni sul "documento di provenienza". Usato in modo corretto, questo campo aiuta i Webmaster ad amministrare i loro siti Web. Usato in modo scorretto, può divulgare l'indirizzo IP, il nome della workstation, il nome di accesso dell'utente o persino il suo numero di carta di credito (in un sito di commercio elettronico implementato male). Selezionando Rimuovi informazioni di intestazione private nella scheda Cookie, si impedisce che questo campo di intestazione trasferisca informazioni personali.

**CAPACITÀ DISTRUTTIVA**

Si riferisce all'estensione del danno causato da un virus. Il livello di capacità distruttiva suggerisce il grado di reversibilità del danno. Un livello di capacità distruttiva basso indica che l'estensione dell'interruzione è stata contenuta e che l'eventuale danno causato è reversibile. Un livello di capacità distruttiva medio o alto indica che il danno causato potrebbe essere irreversibile o che ha provocato un'interruzione estesa.

**CERTIFICATO AUTOFIRMATO**

Un certificato con chiave pubblica in cui la chiave pubblica associata al certificato e la chiave privata utilizzata per firmarlo sono componenti della stessa coppia di chiavi, che appartiene all'utente firmatario.

**CODICE MOBILE**

Contenuto eseguibile che può essere incorporato nelle pagine Web o nella posta elettronica HTML. Il codice mobile favorisce l'interattività dei siti Web, ma quello dannoso può essere utilizzato per modificare o rubare dati e per altri scopi illeciti.

**COMPONENTE**

Un piccolo programma o un set di funzioni che i programmi utilizzano per eseguire attività specifiche. Alcuni componenti potrebbero essere utilizzati da vari programmi diversi contemporaneamente. I sistemi operativi Windows forniscono molti componenti DLL (Dynamic Link Library) utilizzabili da tutta una serie di applicazioni Windows.

**CONNESSIONE REMOTA**

Connessione a Internet che utilizza un modem e una linea telefonica analogica. Il modem si connette a Internet componendo il numero di telefono del provider di servizi Internet. Questa è la differenza con altri metodi di connessione, come le connessioni DSL (Digital Subscriber Line), che non utilizzano modem analogici e non compongono numeri di telefono.

**CONTROLLI ACTIVEX**

Un set di tecnologie sviluppato da Microsoft che può essere scaricato ed eseguito automaticamente da un browser Web. Dato che hanno pieno accesso al sistema operativo Windows, i controlli ActiveX rappresentano un rischio potenziale per il software o i dati sul computer di un utente.

**CONTROLLO CODICE MOBILE**

Una funzione del software di sicurezza Zone Labs che consente di bloccare controlli e script attivi sui siti Web visitati. Nonostante il codice mobile sia comune su Internet e presenti molti impieghi onesti, gli hacker talvolta possono utilizzarlo per scopi illeciti.

**CONTROLLO COOKIE**

Funzione di privacy che consente di impedire la memorizzazione dei cookie sul proprio computer.

**CONTROLLO DEI PROGRAMMI AVANZATO**

Controllo dei programmi avanzato è una funzione di sicurezza avanzata che aumenta la sicurezza impedendo a programmi sconosciuti di utilizzare programmi attendibili per accedere a Internet.

**COOKIE**

Un piccolo file di dati utilizzato da un sito Web per personalizzare il contenuto, ricordare l'utente tra una visita e l'altra e/o tenere traccia della sua attività su Internet. Nonostante i numerosi utilizzi onesti, alcuni cookie possono essere sfruttati per divulgare informazioni sull'utente senza il suo consenso.

**COOKIE DI SESSIONE**

Un cookie memorizzato nella cache del browser che scompare appena si chiude la finestra del browser. Sono i cookie più sicuri perché di breve durata.

**COOKIE DI TERZE PARTI**

Un cookie permanente posizionato sul computer non dal sito Web che si sta visitando, ma da un autore di pubblicità o da "terzi". Questi cookie sono comunemente usati per trasmettere informazioni sull'attività Internet a quelle terze parti. Noti anche come cookie di tracciamento.

**COOKIE PERMANENTE**

Un cookie collocato sul disco rigido da un sito Web visitato. Questi cookie potranno essere rilevati dal sito Web alla visita successiva. Benché utili, sono fonte di vulnerabilità perché memorizzano in un file di testo informazioni personali, sul computer o sull'utilizzo di Internet.

**CRITTOGRAFIA**

Processo che modifica i dati da trasmettere, così che possano leggerli solo i destinatari autorizzati. Per esempio, la crittografia è utilizzata per proteggere le informazioni sulle carte di credito quando si fanno acquisti su Internet.



**DES**

Acronimo di Data Encryption Standard, un noto metodo di crittografia a chiave simmetrica che utilizza una chiave a 56 bit. DES è stato soppiantato da 3DES, una sua variante più robusta.

**DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)**

Un protocollo utilizzato per supportare la distribuzione dinamica degli indirizzi IP. Anziché fornire un indirizzo IP statico, l'ISP potrebbe assegnare un indirizzo IP diverso in occasione di ogni connessione. Ciò permette al provider di servire un elevato numero di clienti con un numero relativamente contenuto di indirizzi IP.

**DLL (DYNAMIC LINK LIBRARY)**

Una libreria di funzioni a cui si può accedere in modo dinamico (cioè quando occorre) tramite un'applicazione Windows.

**DNS (DOMAIN NAME SYSTEM)**

Un servizio generalmente utilizzato su Internet per convertire nomi host o nomi di dominio (come `www.miosito.com`) in indirizzi Internet (come `123.456.789.0`).

**DRIVER**

Programma che controlla una periferica. In ambienti Windows, i driver hanno spesso estensione `.DRV`. Un driver agisce come una sorta di traduttore fra la periferica e i programmi che la utilizzano. Ogni periferica ha un proprio set di comandi specifici noti soltanto al driver. Dall'altra parte, la maggior parte dei programmi accede alle periferiche utilizzando comandi generici. Il driver accetta comandi generici da un programma e li converte in comandi specifici per la periferica.

**ELENCO DEI PROGRAMMI**

L'elenco dei programmi a cui si possono assegnare le autorizzazioni server e di accesso a Internet. L'elenco è visualizzato nella scheda Programmi del pannello Controllo dei programmi. È possibile aggiungere o rimuovere programmi dall'elenco.

**FILTRI DEI MESSAGGI**

Una funzione del filtro della posta indesiderata del software di sicurezza Zone Labs. I filtri dei messaggi utilizzano regole euristiche per l'analisi delle caratteristiche della posta elettronica comuni a vari tipi di posta indesiderata.

**FILTRI LINGUE STRANIERE**

Una funzione del filtro della posta indesiderata del software di sicurezza Zone Labs. I filtri delle lingue straniere bloccano la posta elettronica contenente lingue non europee.

**FILTRO COLLABORATIVO**

Una funzione del filtro della posta indesiderata del software di sicurezza Zone Labs'. Il filtro collaborativo utilizza le informazioni estratte dalla segnalazione della posta indesiderata inviata dall'utente e da altri utenti del software di sicurezza Zone Labs per determinare la probabilità che nuovi messaggi provenienti da mittenti sconosciuti siano spam.

**FIRMA MD5**

Una "impronta" digitale utilizzata per verificare l'integrità di un file. Se un file è stato modificato in qualsiasi modo (per esempio, se un programma è stato compromesso da un hacker), cambierà anche la sua firma MD5.

**GATEWAY**

Nelle connessioni di rete, una combinazione di hardware e software che collega due tipi di reti diverse. Per esempio, se ci si trova su una rete domestica o su una LAN aziendale, il gateway consente ai computer in rete di comunicare con Internet.

**HASH**

L'hash è un numero generato mediante una formula a partire da una stringa di testo; il sistema è studiato in modo che sia molto improbabile che un altro testo produca lo stesso valore. I valori hash sono utilizzati per garantire che i messaggi trasmessi non siano stati alterati.

**ICMP (INTERNET CONTROL MESSAGE PROTOCOL)**

Un'estensione del protocollo IP che supporta il controllo degli errori e messaggi informativi. Il messaggio "ping" è un comune messaggio ICMP utilizzato per testare una connessione a Internet.

**ICS (CONDIVISIONE CONNESSIONE INTERNET)**

ICS è un servizio fornito dal sistema operativo Windows che consente ai computer in rete di condividere un'unica connessione a Internet.

**IGNORA BLOCCO**

Quando il Blocco Internet viene attivato, i programmi a cui viene concessa l'autorizzazione Ignora blocco possono continuare ad accedere a Internet. L'autorizzazione di accesso e l'autorizzazione server per tutti gli altri programmi sono revocate fino alla disattivazione del blocco.

**INDEX.DAT**

I file Index.dat conservano delle copie di tutto ciò che era contenuto nelle cartelle dei file temporanei di Internet, dei cookie e della cronologia anche DOPO che questi file sono stati eliminati.

**INDIRIZZO IP**

Il numero che identifica il computer su Internet, così come un numero telefonico identifica un telefono su una rete telefonica. Si tratta di un indirizzo numerico, in genere visualizzato con quattro numeri tra 0 e 255 separati da punti. Per esempio, 172.16.100.100 potrebbe essere un indirizzo IP.

L'indirizzo IP assegnato al computer può essere sempre lo stesso. Tuttavia, il provider di servizi Internet (ISP) potrebbe utilizzare il protocollo DHCP (Dynamic Host Configuration Protocol) per assegnare al computer un indirizzo IP diverso ogni volta che si connette a Internet.

**ISP (PROVIDER DI SERVIZI INTERNET)**

Una società che fornisce l'accesso a Internet. Gli ISP forniscono a privati e aziende molti tipi di connessioni a Internet, fra cui le connessioni remote (mediante una normale linea telefonica e un modem), DSL ad alta velocità e con modem via cavo.

**JAVASCRIPT**

Un noto linguaggio di scripting per sviluppare parte del contenuto interattivo più comune nei siti Web. Alcune delle funzioni JavaScript utilizzate più spesso comprendono i collegamenti Indietro e Cronologia, il cambiamento delle immagini al passaggio del mouse e l'apertura e la chiusura delle finestre del browser. Le impostazioni predefinite del software di sicurezza Zone Labs consentono l'esecuzione di codice JavaScript perché è molto comune e perché la maggior parte dei suoi impieghi non implica rischi.

**LIVELLI DI SICUREZZA**

Le impostazioni Alta, Media e Bassa che regolano il tipo di traffico che può passare sul computer in entrata o in uscita.

**MEMORIA FISICA**

Il componente hardware di memoria (normalmente RAM) installato su un computer.

**MESSAGGI HEARTBEAT**

Messaggi inviati da un provider di servizi Internet (ISP) per assicurarsi che la connessione remota sia ancora in uso. Se risulta che il cliente non è presente, l'ISP potrebbe scollegarlo per assegnare il suo indirizzo IP a un altro utente.

**MODALITÀ DI APPRENDIMENTO DEI COMPONENTI**

Il periodo successivo all'installazione in cui il controllo del programma è impostato a Medio. Quando è in modalità di apprendimento dei componenti, il software di sicurezza Zone Labs può apprendere velocemente le firme MD5 dei componenti più usati senza interrompere il lavoro dell'utente con troppi avvisi.

**MODALITÀ INVISIBILE**

Quando il software di sicurezza Zone Labs pone il computer in modalità invisibile, qualsiasi traffico non richiesto non riceve risposta, non permettendo ad altri di rilevare l'esistenza del computer in rete. Questa modalità rende il computer invisibile ad altri computer su Internet finché un programma autorizzato sul computer stabilisce un contatto.

**MOTORE DI SICUREZZA DI TRUEVECTOR**

Il componente principale della sicurezza del software di sicurezza Zone Labs. TrueVector esamina il traffico di Internet e applica le regole di sicurezza.

**NETBIOS (NETWORK BASIC INPUT/OUTPUT SYSTEM)**

Un programma che consente alle applicazioni su computer diversi di comunicare in una rete locale. Per impostazione predefinita, il software di sicurezza Zone Labs consente il traffico NetBIOS nella zona attendibile, ma lo blocca nella zona Internet. Ciò consente la condivisione dei file sulle reti locali, proteggendo il computer dalle vulnerabilità di NetBIOS su Internet.

**OGGETTO INCORPORATO**

Un oggetto, come un file audio o un file di immagine, che è incorporato in una pagina Web.

**OGGETTO INTEGRATO DI TIPO MIME**

Un oggetto come un file di immagine, audio o video che è integrato in un messaggio di posta elettronica. MIME è l'acronimo di Multipurpose Internet Mail Extension.

**OPENSSL**

OpenSSL è un protocollo di sicurezza open source basato sulla libreria SSL sviluppata da Eric A. Young e Tim J. Hudson.

**PACCHETTO**

Una singola unità di traffico di rete. Sulle reti "a commutazione di pacchetto" come Internet, i messaggi in uscita sono suddivisi in piccole unità, inviati e indirizzati alle loro destinazioni, quindi riassembleati all'arrivo. Ogni pacchetto include l'indirizzo IP del mittente e l'indirizzo IP e il numero di porta di destinazione.

**PERVASIVITÀ**

La pervasività si riferisce al potenziale di diffusione di un virus. A un virus dei settori di avvio che si diffonde tramite la condivisione manuale dei dischi floppy sarà assegnato un livello di pervasività basso, mentre a un worm in grado di auto-inviarsi a un elevato numero di utenti sarà assegnato un livello di pervasività alto.

**PHISHING**

L'atto di inviare un messaggio di posta elettronica ingannevole presentandosi come un'azienda o un'agenzia legittima. Un messaggio di phishing tenta di indurre i destinatari a fornire informazioni personali che poi potranno essere utilizzate per scopi fraudolenti.

**PING**

Un tipo di messaggio ICMP (formalmente noto come "echo ICMP") utilizzato per determinare se un computer specifico è connesso a Internet. Una piccola utilità invia un semplice messaggio "echo request" all'indirizzo IP di destinazione, quindi attende una risposta. Se un computer a quell'indirizzo riceve il messaggio, invia un "echo" di risposta. Alcuni provider Internet inviano regolarmente "ping" ai propri clienti per controllare se sono ancora connessi.

**PORTA**

Un canale associato all'utilizzo di TCP o UDP. Alcune porte sono associate a protocolli di rete standard; per esempio, il protocollo HTTP (Hypertext Transfer Protocol) è tradizionalmente indirizzato alla porta 80. I numeri di porta vanno da 0 a 65535.

**PRIVACY ADVISOR**

Un piccolo avviso che mostra quando il software di sicurezza Zone Labs blocca cookie o codice mobile e permette di sbloccare tali elementi per una determinata pagina.

**PROTOCOLLO**

Un formato standardizzato per inviare e ricevere dati. Protocolli diversi servono per scopi diversi; per esempio, SMTP (Simple Mail Transfer Protocol) serve per inviare messaggi di posta elettronica; FTP (File Transfer Protocol) serve per inviare file di grandi dimensioni di tipi diversi. Ogni protocollo è associato a una porta specifica; per esempio, i messaggi FTP sono indirizzati alla porta 21.

**QUARANTENA**

MailSafe del software di sicurezza Zone Labs mette in quarantena gli allegati di posta in arrivo le cui estensioni del nome di file (per esempio .EXE o .BAT) indicano la possibile presenza di un codice auto-eseguibile. Modificando l'estensione del nome di file, la funzione di quarantena impedisce che gli allegati si aprano senza che vengano controllati. Ciò favorisce la protezione del computer da worm, virus e altro malware che gli hacker distribuiscono sotto forma di allegati di posta elettronica.

**RETE PRIVATA**

Una rete domestica o LAN (Local Area Network). Le reti private vengono aggiunte alla *zona attendibile* per impostazione predefinita.

**RETE PUBBLICA**

Una rete estesa, come quella gestita da un ISP. Le reti pubbliche vengono aggiunte alla *zona Internet* per impostazione predefinita.

**SCANSIONE DELLE PORTE**

Una tecnica utilizzata dagli hacker per trovare computer non protetti su Internet. Utilizzando strumenti automatizzati, l'hacker esegue sistematicamente la scansione delle porte su tutti i computer in un intervallo di indirizzi IP, cercando porte non protette o "aperte". Una volta individuata una porta aperta, l'hacker la può utilizzare come punto di accesso per entrare nel computer non protetto.

**SCRIPT**

Una serie di comandi da eseguire automaticamente, senza intervento dell'utente. In genere sono utilizzati per banner, menu che cambiano al passaggio del mouse (rollover) e annunci pop-up.

**SERVER DI POSTA**

Il computer remoto da cui il programma di posta elettronica sul computer dell'utente recupera i messaggi inviati a quest'ultimo.

**SERVIZIO DI AGGIORNAMENTO DEL PRODOTTO**

Servizio a sottoscrizione di Zone Labs che fornisce aggiornamenti gratuiti per il software di sicurezza Zone Labs. Quando si acquista il software di sicurezza Zone Labs, si riceve automaticamente una sottoscrizione di un anno al servizio di aggiornamento del prodotto.

**SHA1**

Un algoritmo utilizzato per creare un valore hash dei dati.

**SMARTDEFENSE ADVISOR**

Zone Labs SmartDefense Advisor è un'utilità online che consente di analizzare all'istante le possibili cause di un avviso, aiutando a decidere se rispondere Concedi o Nega a un avviso di programma. Per utilizzare SmartDefense Advisor, fare clic sul pulsante Ulteriori informazioni in una finestra di avviso. Il software di sicurezza Zone Labs invia informazioni sull'avviso a SmartDefense Advisor. SmartDefense Advisor invia in risposta un testo in cui sono presenti una spiegazione dell'avviso e dei suggerimenti su ciò che è necessario fare per garantire sicurezza.

**SOFTWARE DI REGISTRAZIONE DELLA PRESSIONE DEI TASTI**

Una forma di spyware che registra i tasti premuti sulla tastiera del computer e spesso invia i dati a un server remoto. Questi tipi di programmi sono in grado di raccogliere qualsiasi immissione di testo tramite tastiera, tra cui i numeri di carta di credito o altri dati personali riservati, e utilizzarli per commettere furti di identità.

**SPAM**

Tentativo non corretto di utilizzare una mailing list, USENET o altra struttura di comunicazione in rete come mezzo di trasmissione per inviare messaggi non richiesti a un numero elevato di persone.

**TCP (TRANSMISSION CONTROL PROTOCOL)**

Uno dei protocolli principali nelle reti TCP/IP, che garantisce la ricezione dei dati da parte del destinatario e che i pacchetti arrivino a destinazione nello stesso ordine in cui sono stati inviati.

**TESTO IN CHIARO**

I dati in chiaro sono quei dati che vengono trasmessi in formato di "testo" senza essere crittografati. Non essendo crittografati, i dati potrebbero essere intercettati e letti da altri durante la trasmissione.

**UDP (USER DATAGRAM PROTOCOL)**

Un protocollo "senza connessione" che viene utilizzato sulle reti IP, principalmente per il broadcast dei messaggi.

**VIRUS DEI SETTORI DI AVVIO**

Tipo di virus che infetta il primo o i primi settori del disco rigido di un computer o di un disco floppy e si attiva quando si avvia il computer dal disco rigido o dall'unità disco floppy.

**VIRUS DI TIPO TROJAN**

Programma dannoso che assume le sembianze di un elemento utile o innocuo, come uno screen saver. Alcuni virus di tipo Trojan funzionano installandosi come server sul computer dell'utente, ascoltando le connessioni provenienti dall'esterno. Se un hacker riesce a contattare il programma, potrà prendere il controllo effettivo del computer. Questo è il motivo per cui è importante concedere l'autorizzazione server solo a programmi noti e attendibili. Altri virus di tipo Trojan tentano di contattare automaticamente un indirizzo remoto.

**WEB BEACON**

Un file di immagine, spesso di 1 x 1 pixel, concepito per monitorare le visite alla pagina (o al messaggio di posta elettronica HTML) che lo contiene. I Web beacon sono utilizzati per scoprire quali annunci pubblicitari e pagine Web sono stati visualizzati dall'utente. Se si bloccano i Web beacon utilizzando il controllo della privacy, al loro posto saranno visualizzate delle aree vuote.

**WILD**

Con il termine "in the wild" (letteralmente, "allo stato selvaggio") ci si riferisce a un virus che si sta diffondendo tra i computer di utenti ignari di questo come conseguenza delle normali operazioni quotidiane che essi svolgono. Il livello "wild" si riferisce al numero di report dei clienti in relazione al virus. Un livello "wild" basso si rifletterà in un basso numero di report dei clienti, mentre un livello "wild" medio o alto si rifletterà in un numero di report dei clienti più elevato.

**ZONA ATTENDIBILE**

La zona attendibile contiene i computer considerati attendibili con cui l'utente desidera condividere delle risorse.

Per esempio, se si possiedono tre PC domestici collegati insieme tramite una rete Ethernet, è possibile aggiungere ciascuno di essi o l'intera subnet della scheda di rete alla zona attendibile del software di sicurezza Zone Labs. L'impostazione predefinita di sicurezza Media della zona attendibile consente di condividere in tutta sicurezza file, stampanti e altre risorse sulla rete domestica. Gli hacker sono relegati nella zona Internet, dove l'impostazione di sicurezza Alta garantisce la protezione.

**ZONA BLOCCATA**

La zona bloccata contiene computer con cui non si desidera avere contatti. Il software di sicurezza Zone Labs impedisce qualsiasi comunicazione tra il computer dell'utente e i computer in questa zona.

**ZONA INTERNET**

La zona Internet contiene tutti i computer del mondo, a eccezione di quelli che sono stati aggiunti dall'utente alla zona attendibile o alla zona bloccata.

Il software di sicurezza Zone Labs applica la sicurezza più rigorosa alla zona Internet, proteggendo il computer dell'utente dagli hacker. Nello stesso tempo, le impostazioni di sicurezza media della zona attendibile consentono di comunicare facilmente con i computer o le reti note e attendibili, per esempio i PC della propria rete domestica o la propria rete aziendale.



# Indice

---

## SIMBOLI

.z16, estensione di file 139

## A

Address Mask Reply, Address Mask Request, messaggi

ICMP 63

adware 112

aggiornamento del software 22

aggiungere

alla zona attendibile 50

alla zona bloccata 51

porte personalizzate 54

programmi all'elenco dei programmi 84

regole della scheda Esperto ai programmi 91

reti alla zona attendibile 47

reti wireless alla zona Internet 48

agire da server 19

definizione 267

AH (Authenticating Header), protocollo 37

allegati, elenco di

accedere 122

modificare 122

Alt, messaggio ICMP 63

Alta, impostazione di sicurezza

autorizzazioni di porta predefinite per 53–54

Alta, livello di sicurezza

Blocco annunci e 143

condivisione di file e stampanti 35

consentire protocolli non comuni 40

Controllo cookie 143

Controllo dei programmi e 73

informazioni su 18

per Blocco ID 182

per la zona attendibile 43

per la zona Internet 43

protezione della privacy e 143

protezione firewall e 43

alto livello, avvisi di 212

Alto, livello di protezione

eventi di avviso visualizzati in 170

opzioni di registrazione e 170

animati, annunci

bloccare 143

riempire il vuoto lasciato da 152

antivirus, funzioni di protezione 93–116

antivirus, software

protezione della posta elettronica e 254

AOL

elenco della privacy e 147

in regole Esperto 63

Instant Messenger, utilizzo 255

AOL Instant Messenger 200

applet Java, bloccare 154

area di sistema 14

ARP (Address Resolution Protocol), attivare 46

asterischi, utilizzo di 185

Attendibile, accesso 84

autorizzazione

Ignora blocco 14, 75

password e 23

server 19

autorizzazione di accesso

browser e 255

client di posta elettronica e 256

concedere ai programmi 40, 71

configurazione per i programmi 7

giochi e 257

password e 79

per la zona attendibile 19

per le porte, impostare 54

programmi FTP e 257

software antivirus e 254

autorizzazione Ignora blocco

concedere a un programma 89

autorizzazione per i programmi 83

autorizzazione server

avvisi e 221

client di posta elettronica e 256

colonna in elenco dei programmi 84

concedere ai programmi 85

giochi e 257

predefinita per tipi di traffico 53

programmi di chat e 255

programmi di condivisione file e 257

programmi di ricezione di flussi multimediali e 260

programmi Voice over Internet e 260

regole Esperto e 91

zone e 19

## avvisi

- Blocco ID 228
- Blocco Internet 215
- come rispondere agli 20, 37
- di alto livello 212
- di medio livello 212
- guida di riferimento 211–229
- Nuova rete 229
- OSFirewall 226
- preferenze per 80
- Programma
  - Aviso Programma ripetuto 72
  - Azione manuale obbligatoria, avvisi 224
  - Configurazione VPN automatica, avvisi 37, 223
  - MailSafe 120
  - Nuovo programma 218, 226, 227
  - Programma avanzato, avvisi 223
  - Programma bloccato 214
  - Programma modificato, avvisi 219
  - Programma ripetuto, avvisi 173
  - Programma server, avvisi 71, 173, 215, 255
- registrazione di 169
- avvisi informativi 163, 212
- Avvisi relativi ai programmi
  - come rispondere agli 75
- Aviso Programma ripetuto 72, 219
- Azione
  - in regola Esperto 58, 67
  - in Visualizzatore log 52
- azione
  - in Visualizzatore log 174

**B**

- backup e ripristino delle impostazioni di sicurezza 23
- banner, annunci su
  - bloccare 143
  - riempire il vuoto lasciato da 152
- barra degli strumenti del filtro della posta elettronica 127
- Bassa, impostazione di sicurezza
  - autorizzazioni di porta predefinite per 53–54
- Basso livello, impostazione di sicurezza
  - condivisione di file e stampanti e 43
  - Controllo dei programmi e 74
  - modalità di apprendimento 74
  - opzione Cambia di frequente 85
  - zone e 43

## bloccare

- allegati di posta elettronica 120–121
  - annunci 152–153
  - contenuto Web inappropriato 193–197
  - contenuto Web per categoria 191–197
  - cookie 149–151
  - frammenti di pacchetto 46
  - oggetti incorporati 154
  - porte 53–55
  - programmi 46
  - script 154
  - trasferimenti di file 230
  - trasmissioni video 230
  - URL eseguibili 230
  - bloccare un programma 84
  - Blocco annunci
    - informazioni su 142
  - Blocco automatico
    - attivare 75
    - impostare le opzioni per 76
  - Blocco ID 179–188
    - monitoraggio stato di 182
    - panoramica 180
    - vedere anche* myVAULT
  - Blocco ID, avvisi 228
  - Blocco Internet 14, 15
    - icona 15
  - Blocco Internet, avviso 215
  - Blocco spam
    - citato 200
    - impostare le opzioni per 207
    - informazioni su 200–201
  - Blue Coat 190, 191
  - Blue Coat, citato 191
  - browser help object 112
  - browser, utilizzare 255
- 
- C**
- Cache Cleaner 156–159
    - eseguire manualmente 156
    - informazioni su 142, 156
    - opzioni di ripulitura del browser, impostare 157–159
    - opzioni di ripulitura del disco rigido, impostare 157
  - cache del browser, ripulire 158, 197
  - Cambia di frequente 85
  - cartella Posta indesiderata 130
  - categorie 197
    - consentire e bloccare 191, 193–??, 197
  - Centro di controllo 12
  - Centro di controllo, panoramica 12–14
  - Cerberian, citato 190
  - certificato autofirmato 205
  - chat, programmi di
    - avvisi Programma server e 255
    - utilizzare 255
  - chiaro, password in 228
  - chiusura dell'applicazione del software di sicurezza Zone Labs 15

- classifica delle regole firewall Esperto 57, 66
- codice di licenza
  - aggiornamento 28
- collegamenti dannosi, rimuovere 230
- combinazione di colori, modificare 24, 26
- come rispondere agli avvisi 20, 37, 162
- completamento automatico, cancellare i dati *vedere*
  - Cache Cleaner
- Componente di programma, avvisi 220
- componenti
  - autenticare 74
  - firma MD5 di 73
  - gestire 90
  - relativi a VPN 37
- componenti di programma
  - gestire 90
- componenti di sicurezza
  - gestire 206
  - personalizzare 207
- comportamento pericoloso
  - tipi di 263
- Comportamento pericoloso, avviso 226
- comportamento sospetto dei programmi
  - tipi di 262
- Comportamento sospetto, avviso 226
- computer host remoti
  - configurazione VPN e 39
- Condivisione connessione Internet (ICS)
  - attivare 36
  - impostare le opzioni di sicurezza per 45–46
  - opzioni degli avvisi per 216
- condivisione di file e stampanti
  - accesso server e 222
  - attivare 35, 229
  - risoluzione dei problemi 257
  - sicurezza di rete e 47
- configurazione guidata Rete
  - disabilitare 33, 34
  - informazioni su 32
- Configurazione VPN automatica, avvisi 223
- connessione remota
  - configurare 229
- conservare i cookie 158
- contenuto per adulti, bloccare 193
- contenuto violento, bloccare 197
- contenuto Web, filtrare 88
- contribuire alla posta elettronica fraudolenta 131
- contribuire alla posta indesiderata 129
- controllo accesso
  - impostare le opzioni per 207
  - informazioni su 200
- Controllo caratteristica
  - citato 200
  - impostare le opzioni per 207
  - informazioni su 202
- Controllo codice mobile
  - informazioni su 142
  - personalizzare 147, 154

- Controllo cookie
  - informazioni su 142
- Controllo dei programmi 69–258
  - Blocco Internet e 76
  - impostare il livello per 73
  - impostazione Medio 73
  - informazioni su 70
  - zone e 19
- Controllo genitori 189–197
  - attivare 191
  - consentire e bloccare 197
  - consentire e bloccare categorie 193–??
  - filtro intelligente e 191
  - impostare le opzioni di timeout per 192
  - impostare le preferenze per 192
  - informazioni su 190
- Controllo interazione applicazioni 74
- conversazioni chat, protezione di 200
- cookie 112
  - bloccare 142, 149–150
  - conservare e rimuovere 157
  - impostare una data di scadenza per 150
- CreateProcess 87
- criterio 75
- crittografia 200
  - attivare e disattivare 205
  - esempi 204–205
  - impostare le opzioni per 207
  - informazioni su 204
- crittografia messaggi 200
- cura dei virus 99

## D

- dashboard
  - tasti di scelta rapida per 237
  - utilizzare 13
- data di scadenza
  - impostare per i cookie 150
  - sottoscrizione ai servizi e 17
- Data/Ora
  - in Visualizzatore log 175
- dati dei moduli, rimuovere dalla cache *vedere* Cache Cleaner
- DefenseNet 7
- destinazione
  - in regole Esperto 56, 58, 59
- DHCP (Dynamic Host Configuration Protocol), messaggi
  - autorizzazioni di porta predefinite per 53
  - in gruppo di giorni/ore 63
  - programmi di controllo remoto e 259
- dialer 112
- disabilitare
  - Windows Firewall 47
- disco rigido, ripulire 157

DNS (Domain Name System)  
definizione 271  
in regole Esperto 63  
messaggi in arrivo  
determinare l'origine di 174  
messaggi in uscita  
autorizzazioni di porta predefinite per 53  
determinare la destinazione di 52, 174  
risolvere problemi di connessione a Internet 249  
risorse VPN necessarie 39  
domestica, rete  
avvisi del firewall e 212  
driver, caricamento 264  
driver, evento 78  
DRTR (Dynamic Real-time rating) 192

**E**

EBay, bloccare 195  
Echo Request, messaggio ICMP  
in regole Esperto 63  
Elenco dei componenti 90  
elenco dei programmi  
accedere 81  
aggiungere e rimuovere programmi 84  
elenco dei siti attendibili 186–188  
esecuzione, evento 78  
ESP (Encapsulating Security Payload), protocollo  
protocolli VPN e 37, 47  
Eudora, posta elettronica infetta e 139  
eventi di sicurezza, registrazione 208–209

**F**

file di archivio  
virus e 105  
file infetti  
valutazione dei rischi di 104, 109  
file, evento 78  
filtrare il contenuto Web 193  
filtri dei messaggi 131  
filtri lingue straniere 131  
filtro collaborativo 131  
filtro della posta elettronica, barra degli strumenti 127

filtro della posta indesiderata  
barra degli strumenti 127  
bloccare elenchi di distribuzione 129  
bloccare nomi di società 128  
blocco dei mittenti 127  
cartella Posta contestata 134  
cartella Posta indesiderata 130  
cartelle di Outlook speciali 127–137  
contribuire alla posta indesiderata 129  
e privacy 134  
filtri dei messaggi 131  
filtri lingue straniere 131  
filtro collaborativo 131  
Hotmail, e 127, 136  
opzione di segnalazione automatica 135  
opzioni di filtro del messaggi 131  
Posta fraudolenta, cartella 131  
proteggere la privacy 130, 131  
report 137  
segnalazione di posta elettronica fraudolenta 130, 135  
segnalazione di posta indesiderata 129  
supporto periferica wireless 135  
filtro della posta indesiderata, vedere filtro della posta elettronica indesiderata 127  
filtro intelligente  
attivare 191  
impostare le opzioni di timeout per 192  
informazioni su 190  
firewall, avvisi 163  
come rispondere agli 212  
determinare l'origine di 212  
registrazione di 172  
firewall, protezione 41–68  
bloccare e sbloccare porte 53  
impostare il livello di sicurezza per 43–44  
informazioni su 42  
mantenere aggiornata 17  
opzioni di sicurezza avanzate 45–51  
regole Esperto e 56–57  
FireWire 47  
firma MD5 73, 85  
definizione 272  
formattazione file di log 172  
frammenti di file, rimuovere *vedere* Cache Cleaner 157  
frammenti, bloccare 46  
FTP  
programmi, utilizzare 257  
protocolli, aggiungere a regole Esperto 62

## G

gateway  
aggiungere alla zona attendibile 50  
applicazione della sicurezza del 45  
come tipo di posizione 61  
Condivisione connessione Internet (ICS) e 36  
autorizzazioni di porta predefinite 53  
inoltrare o disattivare avvisi 45

giochi  
  online, bloccare l'accesso ai 195  
  uso con il software di sicurezza Zone Labs 257–258  
giorni/ore  
  aggiungere a regole Esperto 59  
  creare un gruppo di intervalli di 64  
GRE (Generic Routing Encapsulation), protocollo  
  citato 47  
  protocolli VPN e 37, 40  
gruppi  
  aggiungere a regole Esperto 61–65

## H

Hacker ID  
  informazioni su 178  
heartbeat, messaggi  
  connessione remota, risolvere problemi 249  
  consentire 249  
  definizione 273  
host, nome  
  aggiungere alla zona attendibile 247  
  nell'elenco della privacy 147  
  nell'elenco delle origini di traffico 49  
hosts, bloccare il file 47  
Hotmail, cartelle speciali 127, 136  
HTTP (Hypertext Transfer Protocol)  
  in regole firewall Esperto 63  
HTTPS (Secure Hypertext Transfer Protocol) 62

## I

ICMP (Internet Control Messaging Protocol)  
  autorizzazioni di porta predefinite per 53  
  in regole firewall Esperto 56  
  risolvere problemi di connessione a Internet 249  
  tipi di messaggio 63  
ie3.proxy.aol.com 147  
IGMP  
  autorizzazioni di porta predefinite per 53  
  in regole Esperto 56, 92  
IKE (Internet Key Exchange), protocollo  
  protocolli VPN e 37  
IM Security  
  panoramica 200–205  
IMAP4  
  in regole Esperto 62  
impostazioni di sicurezza  
  backup e ripristino 23  
  condividere con Zone Labs *vedere* DefenseNet  
impostazioni di sicurezza predefinite 206, 207  
impostazioni per la ricerca degli aggiornamenti 22  
impostazioni predefinite del browser, modifica 262  
Index.dat, rimuovere i file *vedere* Cache Cleaner  
Indicatore del traffico in entrata/in uscita 13  
indicatore delle reti 13, 14

indirizzo IP  
  aggiungere alla zona attendibile 35, 50  
  determinare il tipo di rete da 32, 33  
  in regole Esperto 56  
  nascondere nelle comunicazioni con Zone Labs 25  
  nell'elenco delle origini di traffico 49  
Information reply, messaggio ICMP 63  
Information request, messaggio ICMP 63  
installazione  
  ZoneAlarm 4  
installazione del software di sicurezza Zone Labs 1–5  
Interazione delle applicazioni 87  
Internet Explorer  
  cache, ripulire 158  
  concedere l'autorizzazione di accesso a 255  
  impostare le opzioni di ripulitura per 157  
  protezione della privacy e 143  
Internet Relay Chat, bloccare 208  
Interrompi, pulsante 15  
  icone nell'area di notifica del sistema 15  
  informazioni su 13  
  quando fare clic 13  
  tasti di scelta rapida per 236  
intervallo di indirizzi IP  
  aggiungere alla zona attendibile 50  
  in regole firewall Esperto 58  
introduzione di codice *vedere* comportamento pericoloso  
  tipi di 264  
Intrusioni bloccate, area 16  
invio della posta, autorizzazione 86  
  protezione di MailSafe in uscita e 121  
invisibile, modalità  
  definizione 273  
  livello di sicurezza Alta e 43  
IPSec (IP Security), protocollo  
  protocolli VPN e 37  
isafe.exe 139  
ISP (provider di servizi Internet)  
  messaggi heartbeat 14, 249  
  nei dettagli degli avvisi 165  
  nell'elenco delle origini di traffico 49

## J

JavaScript  
  protezione della posta elettronica e 120

## L

L2TP (Layer 2 Tunneling), protocollo  
  protocolli VPN e 37  
LDAP (Lightweight Directory Access), protocollo  
  protocolli VPN e 37  
limitare l'accesso ai programmi 84  
Livelli di attendibilità 83, 84  
livello di protezione  
  impostare 206  
  personalizzare 207

locali, bloccare server 46  
loopback  
  aggiungere alla zona attendibile 37  
lsass.exe 20  
lucchetto, icona  
  nell'area di notifica del sistema 15

**M**

MailFrontier 130  
MailSafe  
  protezione in uscita  
    indirizzo del mittente, verifica 28  
MailSafe, avvisi di 120, 213  
matita, icona 147  
Media, impostazione di sicurezza  
  autorizzazioni di porta predefinite per 53–54  
Media, impostazione di sicurezza definita 206  
medio livello, avvisi di 212  
Medio, livello di protezione  
  accesso di porta e 54  
  avvisi e 212, 221  
  Blocco annunci e 143  
  Blocco ID e 182  
  condivisione di file e stampanti e 35  
  condivisione di risorse e 247  
  connessioni di rete e 35  
  Controllo dei programmi e 74, 256  
  eventi di avviso 170  
  informazioni su 18  
  modalità di apprendimento 73, 74  
  opzioni di registrazione e 170  
  personalizzare 19  
  protezione della privacy e 143  
  protocolli non comuni e 47  
  zona attendibile e 43, 50, 246  
  zona Internet e 43, 249, 256  
memoria fisica, evento 78  
memoria fisica, modifica *vedere* comportamento  
  pericoloso  
  tipi di 264  
menu di scelta rapida 15  
messaggio, evento 78  
MIME, oggetti integrati di tipo  
  bloccare 155  
  definizione 274  
modalità di apprendimento 73, 74  
modalità di blocco, specificare 76  
modalità di rendering software 257  
modulo, evento 78  
motore di sicurezza di TrueVector 79, 248  
MSN Messenger 200  
myVAULT 183–185  
  aggiungere dati a 183  
  modifica e rimozione dati 185

**N**

NetBIOS  
  autorizzazioni di porta predefinite per 53  
  avvisi del firewall e 212  
  definizione 274  
  in regole firewall Esperto 62  
  livello di sicurezza Alta e 43  
  messaggi heartbeat e 249  
  visibilità della rete e 246  
Netscape  
  cache, ripulire 158  
  impostare le opzioni di ripulitura per 157  
  rimuovere i cookie 159  
  versione 4.73 255  
NNTP (Network News Transfer Protocol) 62  
Nuova rete, avviso 229  
Nuovo programma, avvisi 218, 226, 227

**O**

oggetti incorporati, bloccare 154  
OpenGL  
  blocco del sistema e 258  
OpenProcess 87  
opzioni filtro, impostare 88  
origine  
  conservare cookie di una 157  
  di traffico, determinare 49, 169  
  in regole firewall Esperto 56  
OSFirewall, eventi  
  tipi di 78  
Outlook e filtro della posta indesiderata 127

**P**

pacchetto  
  definizione 274  
  in avvisi 163  
  origine del  
    determinare 176  
  regole firewall Esperto 56  
  tipi, blocco di 46  
Parameter Problem, messaggio ICMP  
  in regole Esperto 63  
password  
  cancellare dalla cache 158  
  Controllo dei programmi e 79  
  creare 22  
  VNC Viewer e 259  
PC Anywhere  
  comportamento pericoloso 264  
PCAnywhere *vedere* programmi di controllo remoto,  
  utilizzare  
permanenti, cookie 143  
  impostare una data di scadenza per 150  
personalizzate, aggiungere porte 54  
phishing 130

- ping, messaggi
  - autorizzazioni di porta predefinite per 53
  - consentire in zona Internet 249
  - e avvisi 212
- POP3
  - in regole firewall Esperto 62
- porte
  - 1394 47
  - aggiungere 54
  - autorizzazioni predefinite per 53
  - bloccare e sbloccare 53–54
  - in regole firewall Esperto 56
  - livello di sicurezza Alta e 43
  - protezione firewall e 42
- posizione 61
- posizioni
  - aggiungere a regole firewall Esperto 59
  - creare gruppi di 61
- Posta contestata 134
- Posta contestata ZoneAlarm, vedere filtro della posta indesiderata
- posta elettronica
  - fraudolenta, segnalazione 131
  - indesiderata, segnalazione 129
- posta elettronica fraudolenta, vedere filtro della posta indesiderata
- posta elettronica, protezione 119–126
  - allegati, elenco di 122
  - in entrata 120, 121
  - in uscita 121
  - informazioni su 120
  - stato di 254
- posta eliminata, cancellare *vedere* Cache Cleaner
- Posta fraudolenta ZoneAlarm, *vedere* filtro della posta indesiderata
- Posta fraudolenta, cartella 131
- Posta indesiderata ZoneAlarm, *vedere* filtro della posta indesiderata, cartelle speciali di Outlook
- PPTP (Point-to-Point Tunneling), protocollo protocolli VPN e 37
- preferenze
  - caricare all'avvio 248
  - per Controllo dei programmi 80
  - per il Controllo genitori 192
  - per la protezione firewall 45
  - tasti di scelta rapida 239
- preferenze di visualizzazione, impostare 24
- preferenze, impostare 24
- Privacy Advisor
  - utilizzare 145
- privacy, elenco della 146
  - accedere 146
  - aggiungere siti Web a 147
  - AOL e 147
  - software per il blocco di annunci e 147
- privacy, protezione della
  - Blocco annunci
    - personalizzare 152–153
  - Cache Cleaner 156–159
  - Controllo cookie 149–151
    - personalizzare 149–151
- privata, rete
  - configurazione guidata Rete e 32
  - definizione 275
  - virtuale *vedere* VPN (rete privata virtuale)
- processo, evento 78
- profilo di protezione Amazon, creare 26
- profilo di protezione eBay, creare 26
- Programma avanzato, avvisi 223
- Programma bloccato, avviso 214
- Programma modificato, avvisi 219
- Programma ripetuto, avvisi
  - opzioni di registrazione e 173
- Programma server, avvisi 71, 79, 215, 255
  - opzioni di registrazione e 173
- Programma, avvisi 217–223
- programmi
  - aggiungere all'elenco dei programmi 84
  - bloccare 84
  - creare regole della scheda Esperto per 91
  - livello attendibilità di 84
- programmi attivi, area 14
- programmi di accesso remoto
  - risoluzione dei problemi 24
- programmi di controllo remoto, utilizzare 258
- programmi per conferenze sul Web, utilizzare 260
- programmi VNC, utilizzare 259
- protezione antivirus
  - stato, visualizzare 113
- Protezione della privacy
  - attivare per programma 143
  - Blocco annunci
    - impostare il livello per 143
  - Cache Cleaner
    - eseguire manualmente 156
  - Controllo codice mobile
    - attivare e disattivare 143
    - personalizzare 154
  - Controllo cookie
    - impostare il livello per 143
  - impostare livelli per 143
- protezione di MailSafe in uscita
  - attivare 121
  - indirizzo del mittente, verifica 28
  - personalizzare 125–126
- protezione in entrata
  - citato 200
  - impostare le opzioni per 207
  - informazioni su 203–204
- Protezione in uscita, area 16

## protocolli

- autorizzazioni predefinite per 53
  - creare gruppi di 61
  - in regole Esperto 47
  - in regole firewall Esperto 56
  - posta 35
  - protezione firewall e 46
  - VPN 37, 40
- proxy, server
- risolvere problemi di connessione a Internet 248
  - sistemi di elusione, bloccare l'accesso a 195
- pubblica, rete
- configurazione guidata Rete e 32
  - definizione 275

**Q**

## quarantena

- aprire allegati in 124, 254
- icona 213
- modificare l'impostazione dei tipi di allegato 122
- protezione di MailSafe in entrata e 120

**R**

## Real Networks

- in regole firewall Esperto 63
- Redirect, messaggio ICMP 63
- registrazione eventi
- attivazione e disattivazione 170
  - informazioni su 169
  - personalizzare 172
- registro, evento 78
- regole firewall Esperto
- applicazione di 56–57
  - classificare 66
  - creare 58–59
  - gestire 66–68
  - informazioni su 56
  - modificare 67
  - opzioni di traccia per 67
  - per programmi 91
- rete wireless non sicura
- configurazione guidata Rete wireless e 33
- rete wireless sicura
- configurazione guidata Rete wireless e 33
- rete wireless, impostazioni
- impostare 48
- rete, impostazioni
- impostare 47
- Ricerca, pulsante 61
- ripristinare le impostazioni di sicurezza 23
- ripristino delle impostazioni predefinite 207
- Risoluzione dei problemi 243–250
- Risorse del computer 58
- risorse di rete, condivisione 32
- Router Advertisement, messaggio ICMP 63
- Router Solicitation, messaggio ICMP 63
- RTSP 62

**S**

- scansione approfondita 101
- scansione completa del sistema 101
- scansione di virus 103–106
- scansione rapida intelligente 101
- scansioni, pianificazione 94
- Scheda Chi è *vedere* Hacker ID
- screenlogger 112
- script, bloccare 154
- segnalazione
- posta elettronica fraudolenta 131
  - posta elettronica indesiderata 129
- segreteria Internet, programmi 256
- server di posta, connessione ai 35
- services.exe 20
- servizi di messaggistica immediata
- bloccare l'accesso ai 200
  - crittografare il traffico 204
- sessione, cookie di
- bloccare 149
  - livello di sicurezza Alta e 143
- sicurezza di rete wireless, impostare le opzioni di 48
- sicurezza di rete, impostare le opzioni di 47
- siti a pagamento, bloccare 196
- siti di aste su Internet, bloccare 195
- siti di attivisti, bloccare 196
- siti di glamour e stile di vita, bloccare 195
- siti di news e mezzi di informazione, bloccare 195
- siti governativi, bloccare 195
- siti militari, bloccare 195
- siti MP3, bloccare 195
- siti umoristici, bloccare 195
- SKIP 37
- SmartDefense 83
- SmartDefense Advisor 212
- autorizzazione del browser e 222
  - definizione 276
  - impostare il livello per 75
  - informazioni su 178
  - invio di avvisi a 164, 166
- SMTP
- in regole firewall Esperto 63
- software antivirus
- protezione della posta elettronica e 254
- software di gioco
- comportamento pericoloso 264
- software di registrazione della pressione dei tasti 112
- software di sicurezza Zone Labs 4
- aggiornamento 17, 22
  - caricare all'avvio 24
  - chiusura dell'applicazione 15
  - informazioni su 15
  - installazione 1–5
  - programmi di condivisione file e 257
  - programmi FTP e 257
- software video
- comportamento pericoloso 264
- spoolsv.exe 20



spy cookie 112  
spyware  
  prevenire 81  
  scansione di 101  
  tipi di 112  
stampanti *vedere* risorse di rete, condivisione  
Stato, scheda 16  
subnet  
  aggiungere alla zona attendibile 50  
  configurazione VPN e 39  
  tipo di voce 49  
Super, accesso 84  
svchost.exe 20

**T**

tasti di scelta rapida 233–241  
tastiera e mouse  
  monitoraggio 264  
TCP (Transmission Control Protocol)  
  autorizzazione di porta predefinita per 53  
  in regole firewall Esperto 56  
Telnet 62, 259  
terze parti, bloccare cookie di 150  
TFTP 63  
Timbuktu *vedere* programmi di controllo remoto,  
  utilizzare  
Time Exceeded, messaggio ICMP 63  
Timestamp, Timestamp reply, messaggi ICMP 63  
traccia, opzioni di  
  per regole firewall Esperto 58, 67  
Traceroute, messaggio ICMP 63  
traffico, origini di  
  autorizzazioni di porta predefinite per 53  
  elenco delle 49  
  gestire 49  
trasferimento di file, bloccare 230  
trasmissione vocale  
  bloccare 202  
  esempio 202  
trasmissioni video, bloccare 207, 230  
Trojan 72  
Trojan, virus di tipo 72, 112  
  Controllo dei programmi e 85  
  proteggere il software di sicurezza Zone Labs da 79  
  protezione della posta elettronica e 120

**U**

UDP  
  autorizzazioni di porta predefinite per 53  
  in regole firewall Esperto 56  
Ulteriori informazioni, pulsante 163, 164, 166, 167,  
  168, 222  
  tasti di scelta rapida per 237, 241  
URL, bloccare 208  
URL, cancellare la cronologia *vedere* Cache Cleaner

**V**

valutazione dei rischi di infezioni 104, 109  
verticali, annunci  
  riempire il vuoto lasciato da 152  
virus  
  cura 99, 105  
  e file di archivio 105  
  file delle firme, aggiornare 95  
  scansione di 103–106  
Visualizzatore log  
  accedere 173  
  utilizzare 208–209  
VNC  
  comportamento pericoloso 264  
voci di log  
  archiviazione 176–177  
  campi in 175  
  formattazione 172  
  informazioni su 169  
  opzioni per 172  
  per avvisi di programma 173  
  per programmi 173  
  regole Esperto e 91  
  visualizzazione 173, 175  
VoIP, programmi, utilizzare 260  
VPN (rete privata virtuale)  
  avvisi 37, 223  
  Azione manuale obbligatoria, avvisi 224  
  configurare la connessione 37–40, 244  
  Configurazione automatica, avvisi 223  
  risolvere problemi di connessione 244

**W**

Windows 98 139  
Windows Firewall, disabilitare 47  
Windows Media  
  cancellare la cronologia 157  
  in regole Esperto 62  
winlogon.exe 20  
worm 112

**Y**

Yahoo! Messenger 200

**Z**

Zona attendibile  
  aggiungere a 50  
  aggiungere automaticamente reti alla 47  
  aggiungere reti automaticamente 32  
  aggiungere risorse VPN 37  
  autorizzazioni 19  
  Condivisione connessione Internet (ICS) e 36  
  indicatore delle reti 14

zona bloccata  
  aggiungere a 51  
  informazioni su 18  
Zona Internet 14  
  aggiungere automaticamente reti alla 47, 48  
  aggiungere reti automaticamente 32  
  autorizzazioni 19  
zone  
  aggiungere a 50–51  
  informazioni su 18  
  protezione firewall e 49  
  tasti di scelta rapida 234  
ZoneAlarm, installazione 4