

Kaspersky Embedded Systems Security

Manuale dell'Amministratore

Versione applicazione: 2.2.0.605

Gentile utente,

grazie per aver scelto il software di protezione Kaspersky Lab. Ci auguriamo che la presente documentazione agevoli l'utilizzo del prodotto.

Attenzione! Questo documento è di proprietà di AO Kaspersky Lab (di seguito denominata anche Kaspersky Lab). Tutti i diritti relativi a questo documento sono riservati dalle leggi sul copyright della Federazione Russa e dai trattati internazionali. La riproduzione e la distribuzione non autorizzate del presente documento, interamente o in parte, possono comportare gravi responsabilità civili, amministrative e penali, in conformità alle leggi applicabili.

Qualsiasi riproduzione o distribuzione del materiale, incluse le traduzioni, è consentita solo previa autorizzazione scritta concessa da Kaspersky Lab.

Il presente documento e le immagini correlate possono essere utilizzati solo a scopo informativo, non commerciale e personale.

Kaspersky Lab si riserva il diritto di apportare modifiche al documento senza ulteriori notifiche.

Kaspersky Lab non si assume responsabilità per il contenuto, la qualità, la pertinenza o la precisione del materiale utilizzato in questo documento i cui diritti appartengono a terze parti o per eventuali danni potenziali associati all'utilizzo del documento.

I marchi registrati e i marchi di servizi utilizzati in questo documento appartengono ai rispettivi proprietari.

Data di revisione del documento: 29.10.2018

© 2018 AO Kaspersky Lab. Tutti i diritti riservati.

<https://www.kaspersky.it>
<https://support.kaspersky.it/>

Sommario

Informazioni sulla guida	10
Contenuto del documento.....	10
Convenzioni utilizzate nella documentazione.....	12
Fonti di informazioni su Kaspersky Embedded Systems Security 2.2	13
Fonti per il recupero di informazioni in autonomia.....	13
Discussione delle applicazioni Kaspersky Lab nel forum.....	14
Kaspersky Embedded Systems Security 2.2.....	15
Informazioni su Kaspersky Embedded Systems Security 2.2	15
Novità.....	17
Kit di distribuzione.....	18
Requisiti hardware e software	20
Installazione e rimozione dell'applicazione	22
Componenti software di Kaspersky Embedded Systems Security 2.2 e relativi codici per il servizio Windows Installer.....	22
Componenti software di Kaspersky Embedded Systems Security 2.2	23
Set di componenti software "Strumenti di amministrazione"	25
Modifiche al sistema dopo l'installazione di Kaspersky Embedded Systems Security 2.2	25
Processi di Kaspersky Embedded Systems Security 2.2.....	29
Impostazioni di installazione e disinstallazione e opzioni della riga di comando per il servizio Windows Installer.....	29
Log di installazione e disinstallazione di Kaspersky Embedded Systems Security 2.2	36
Pianificazione dell'installazione	36
Selezione degli strumenti di amministrazione	37
Selezione del tipo di installazione	38
Installazione e disinstallazione dell'applicazione tramite procedura guidata	39
Installazione tramite l'Installazione guidata	40
Installazione di Kaspersky Embedded Systems Security 2.2	40
Installazione della console di Kaspersky Embedded Systems Security 2.2	42
Impostazioni avanzate dopo l'installazione della console dell'applicazione in un altro computer	43
Azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2	46
Modifica del set di componenti e ripristino di Kaspersky Embedded Systems Security 2.2	48
Disinstallazione tramite l'Installazione guidata	49
Disinstallazione di Kaspersky Embedded Systems Security 2.2	49
Disinstallazione della console di Kaspersky Embedded Systems Security 2.2	50
Installazione e disinstallazione dell'applicazione dalla riga di comando	51
Informazioni sull'installazione e la disinstallazione di Kaspersky Embedded Systems Security 2.2 dalla riga di comando	51
Comandi di esempio per l'installazione di Kaspersky Embedded Systems Security 2.2.....	52
Azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2	53
Aggiunta/rimozione di componenti. Comandi di esempio	54

Disinstallazione di Kaspersky Embedded Systems Security 2.2. Comandi di esempio	55
Codici restituiti	55
Installazione e disinstallazione dell'applicazione tramite Kaspersky Security Center	56
Informazioni generali sull'installazione tramite Kaspersky Security Center	57
Diritti per l'installazione o la disinstallazione di Kaspersky Embedded Systems Security 2.2	57
Procedura di installazione di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center	58
Azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2	59
Installazione della console dell'applicazione tramite Kaspersky Security Center	60
Disinstallazione di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center	60
Installazione e disinstallazione tramite i criteri di gruppo di Active Directory	61
Installazione di Kaspersky Embedded Systems Security 2.2 tramite i criteri di gruppo di Active Directory	61
Azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2	62
Disinstallazione di Kaspersky Embedded Systems Security 2.2 tramite i criteri di gruppo di Active Directory	62
Verifica delle funzioni di Kaspersky Embedded Systems Security 2.2. Utilizzo del virus di prova EICAR	63
Informazioni sul virus di prova EICAR	63
Test di Protezione in tempo reale e Scansione su richiesta	64
Interfaccia dell'applicazione	66
Licensing dell'applicazione	67
Informazioni sul Contratto di licenza con l'utente finale	67
Informazioni sulla licenza	67
Informazioni sul certificato di licenza	68
Informazioni sul codice di attivazione	69
Informazioni sulla chiave	69
Informazioni sul file chiave	69
Informazioni sulla trasmissione dei dati	70
Attivazione dell'applicazione con una chiave	71
Visualizzazione delle informazioni sulla licenza corrente	71
Limitazioni delle funzionalità alla scadenza della licenza	73
Rinnovo della licenza	74
Eliminazione della chiave	74
Avvio e arresto del plug-in di Kaspersky Embedded Systems Security 2.2	76
Avvio del plug-in di amministrazione di Kaspersky Embedded Systems Security 2.2	76
Avvio e arresto del servizio di Kaspersky Security	76
Autorizzazioni di accesso per le funzioni di Kaspersky Embedded Systems Security 2.2	77
Informazioni sulle autorizzazioni per la gestione di Kaspersky Embedded Systems Security 2.2	77
Informazioni sulle autorizzazioni per la gestione del servizio di Kaspersky Security	79
Informazioni sulle autorizzazioni di accesso per il servizio di gestione di Kaspersky Security	81
Configurazione delle autorizzazioni di accesso per Kaspersky Embedded Systems Security 2.2 e il servizio di Kaspersky Security	81

Accesso protetto tramite password alle funzioni di Kaspersky Embedded Systems Security 2.2	83
Abilitazione delle connessioni di rete per il servizio di gestione di Kaspersky Security	85
Creazione e configurazione dei criteri	86
Informazioni sui criteri	86
Creazione di un criterio	87
Configurazione di un criterio	88
Configurazione dell'avvio pianificato delle attività locali di sistema	93
Creazione e configurazione delle attività tramite Kaspersky Security Center	95
Informazioni sulla creazione di attività in Kaspersky Security Center	95
Creazione di un'attività tramite Kaspersky Security Center	96
Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center	100
Configurazione di attività di gruppo in Kaspersky Security Center	101
Attività Generazione regole per Controllo dell'avvio delle applicazioni e Generazione regole per Controllo dispositivi	106
Attività Attivazione dell'applicazione	108
Attività Aggiornamento	108
Verifica dell'integrità dei moduli software	110
Creazione di un'attività Scansione su richiesta	111
Configurazione dell'attività Scansione su richiesta	114
Assegnazione dello stato Scansione aree critiche all'attività Scansione su richiesta	115
Scansione dei file in un archivio cloud	115
Configurazione delle impostazioni di diagnostica degli arresti anomali in Kaspersky Security Center	117
Gestione delle pianificazioni delle attività	119
Configurazione delle impostazioni della pianificazione di avvio delle attività	119
Abilitazione e disabilitazione delle attività pianificate	121
Gestione delle impostazioni dell'applicazione	122
Gestione di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center	122
Configurazione delle impostazioni generali dell'applicazione in Kaspersky Security Center	123
Configurazione della scalabilità e dell'interfaccia in Kaspersky Security Center	123
Configurazione delle impostazioni di sicurezza in Kaspersky Security Center	125
Configurazione delle impostazioni di connessione tramite Kaspersky Security Center	127
Configurazione delle funzionalità avanzate	128
Configurazione delle impostazioni dell'area attendibile in Kaspersky Security Center	129
Aggiunta di processi attendibili	130
Applicazione della maschera not-a-virus	132
Scansione unità rimovibili	133
Configurazione delle autorizzazioni di accesso in Kaspersky Security Center	135
Configurazione delle impostazioni di quarantena e backup in Kaspersky Security Center	136
Configurazione di log e notifiche	137
Configurazione delle impostazioni dei log	138
Log di sicurezza	139

Configurazione delle impostazioni di integrazione SIEM	139
Configurazione delle impostazioni di notifica	142
Configurazione dell'interazione con Administration Server	143
Protezione del computer in tempo reale	144
Protezione dei file in tempo reale	144
Informazioni sull'attività Protezione dei file in tempo reale	144
Configurazione delle impostazioni dell'attività Protezione dei file in tempo reale	145
Utilizzo dell'analizzatore euristico	147
Selezione della modalità di protezione	147
Ambito della protezione nell'attività Protezione dei file in tempo reale	149
Ambiti della protezione predefiniti	149
Selezione dei livelli di sicurezza predefiniti	150
Configurazione manuale delle impostazioni di sicurezza	152
Configurazione delle impostazioni generali dell'attività	153
Configurazione delle azioni	156
Configurazione delle prestazioni	158
Utilizzo di KSN	159
Informazioni sull'attività Utilizzo di KSN	159
Configurazione dell'attività Utilizzo di KSN	161
Configurazione dell'elaborazione dei dati	163
Configurazione del trasferimento di dati aggiuntivi	165
Prevenzione exploit	166
Informazioni su Prevenzione exploit	166
Configurazione delle impostazioni di protezione della memoria processo	167
Aggiunta di un processo per la protezione	169
Tecniche di prevenzione exploit	170
Controllo attività locali	172
Gestione dell'avvio delle applicazioni da Kaspersky Security Center	172
Utilizzo di un profilo per configurare le attività Controllo dell'avvio delle applicazioni in un criterio di Kaspersky Security Center	172
Configurazione delle impostazioni dell'attività Controllo dell'avvio delle applicazioni	173
Informazioni su Controllo distribuzione software	178
Configurazione di Controllo distribuzione software	180
Abilitazione della modalità Default allow	183
Informazioni sulla generazione delle regole di Controllo dell'avvio delle applicazioni per tutti i computer in Kaspersky Security Center	184
Creazione di regole di permesso dagli eventi di Kaspersky Security Center	185
Importazione delle regole di Controllo dell'avvio delle applicazioni da un file XML	186
Importazione delle regole dal file di un rapporto sulle applicazioni bloccate di Kaspersky Security Center	188
Gestione delle connessioni dei dispositivi tramite Kaspersky Security Center	190
Informazioni sull'attività Controllo dispositivi	190

Informazioni sulla generazione delle regole di Controllo dispositivi per tutti i computer in Kaspersky Security Center	191
Generazione delle regole in base ai dati di sistema sui dispositivi esterni connessi ai computer della rete	193
Creazione delle regole utilizzando l'attività Generazione regole per Controllo dispositivi	193
Creazione delle regole di permesso in base ai dati del sistema in un criterio di Kaspersky Security Center	195
Generazione delle regole per i dispositivi connessi	195
Importazione delle regole dal file di un rapporto sui dispositivi bloccati di Kaspersky Security Center	196
Controllo attività di rete	198
Gestione firewall	198
Informazioni sull'attività Gestione firewall	198
Informazioni sulle regole del firewall	199
Attivazione e disattivazione delle regole del firewall	200
Aggiunta manuale delle regole del firewall	201
Eliminazione delle regole del firewall	203
Analisi sistema	204
Monitoraggio integrità file	204
Informazioni sull'attività Monitoraggio integrità file	204
Informazioni sulle regole di monitoraggio operazioni file	205
Configurazione dell'attività Monitoraggio integrità file	207
Configurazione delle regole di monitoraggio	209
Analisi log	212
Informazioni sull'attività Analisi log	212
Configurazione delle regole predefinite dell'attività	213
Configurazione delle regole di analisi log	215
Generazione dei rapporti in Kaspersky Security Center	217
Utilizzo di Kaspersky Embedded Systems Security 2.2 dalla riga di comando	219
Comandi della riga di comando	219
Visualizzazione della Guida per i comandi di Kaspersky Embedded Systems Security 2.2. KAVSHELL HELP	221
Avvio e arresto del servizio di Kaspersky Security. KAVSHELL START, KAVSHELL STOP	222
Scansione dell'area selezionata. KAVSHELL SCAN	222
Avvio dell'attività Scansione aree critiche. KAVSHELL SCANCritical	226
Gestione dell'attività specificata in modo asincrono. KAVSHELL TASK	227
Avvio e arresto delle attività Protezione in tempo reale. KAVSHELL RTP	228
Gestione dell'attività Controllo dell'avvio delle applicazioni KAVSHELL APPCONTROL /CONFIG	229
Generazione regole per Controllo dell'avvio delle applicazioni KAVSHELL APPCONTROL /GENERATE	230
Compilazione dell'elenco delle regole di Controllo dell'avvio delle applicazioni KAVSHELL APPCONTROL	232
Compilazione dell'elenco delle regole di Controllo dispositivi. KAVSHELL DEVCONTROL	233

Avvio dell'attività di aggiornamento dei database di Kaspersky Embedded Systems Security 2.2. KAVSHELL UPDATE	233
Rollback degli aggiornamenti dei database di Kaspersky Embedded Systems Security 2.2. KAVSHELL ROLLBACK.....	236
Gestione di Analisi log. KAVSHELL TASK LOG-INSPECTOR	237
Attivazione dell'applicazione. KAVSHELL LICENSE	237
Abilitazione, configurazione e disabilitazione del log di traccia. KAVSHELL TRACE	238
Deframmentazione dei file di log di Kaspersky Embedded Systems Security 2.2. KAVSHELL VACUUM	240
Pulizia del database di iSwift. KAVSHELL FBRESET	241
Abilitazione e disabilitazione della creazione del file di dump. KAVSHELL DUMP	241
Importazione delle impostazioni. KAVSHELL IMPORT	243
Esportazione delle impostazioni. KAVSHELL EXPORT	243
Integrazione con Microsoft Operations Management Suite. KAVSHELL OMSINFO.....	244
Codici restituiti dalla riga di comando	244
Codici restituiti per i comandi KAVSHELL START e KAVSHELL STOP	245
Codici restituiti per i comandi KAVSHELL SCAN e KAVSHELL SCANCritical	245
Codici restituiti per il comando KAVSHELL TASK LOG-INSPECTOR	246
Codici restituiti per il comando KAVSHELL TASK	246
Codici restituiti per il comando KAVSHELL RTP.....	246
Codici restituiti per il comando KAVSHELL UPDATE	247
Codici restituiti per il comando KAVSHELL ROLLBACK	247
Codici restituiti per il comando KAVSHELL LICENSE	248
Codici restituiti per il comando KAVSHELL TRACE.....	248
Codici restituiti per il comando KAVSHELL FBRESET	248
Codici restituiti per il comando KAVSHELL DUMP	249
Codici restituiti per il comando KAVSHELL IMPORT	249
Codici restituiti per il comando KAVSHELL EXPORT	249
Integrazione con sistemi di terze parti	251
Monitoraggio delle prestazioni. Contatori di Kaspersky Embedded Systems Security 2.2.....	251
Contatori delle prestazioni per Monitor di sistema	251
Informazioni sui contatori SNMP di Kaspersky Embedded Systems Security 2.2.....	252
Numero totale di richieste negate.....	252
Numero totale di richieste ignorate	253
Numero di richieste non elaborate a causa della mancanza di risorse di sistema	254
Numero di richieste inviate per l'elaborazione.....	254
Numero medio di flussi del dispatcher di intercettazione dei file	255
Numero massimo di flussi del dispatcher di intercettazione dei file.....	255
Numero di elementi nella coda degli oggetti infetti.....	256
Numero di oggetti elaborati al secondo.....	256
Contatori e trap SNMP di Kaspersky Embedded Systems Security 2.2	257
Informazioni su contatori e trap SNMP di Kaspersky Embedded Systems Security 2.2	257

Contatori SNMP di Kaspersky Embedded Systems Security 2.2	258
Trap SNMP	260
Integrazione con WMI.....	265
Come contattare il Servizio di assistenza tecnica	269
Come ottenere assistenza tecnica	269
Assistenza tecnica tramite Kaspersky CompanyAccount	269
Utilizzo di file di traccia e script AVZ.....	270
AO Kaspersky Lab	271
Informazioni sul codice di terze parti	272
Note relative ai marchi	273
Glossario	274
Indice	279

Informazioni sulla guida

Il Manuale dell'Amministratore di Kaspersky Embedded Systems Security 2.2.0.605 (di seguito denominato "Kaspersky Embedded Systems Security 2.2" o "l'applicazione") è destinato agli specialisti che installano e amministrano Kaspersky Embedded Systems Security 2.2 in tutti i dispositivi protetti, nonché agli specialisti che offrono assistenza tecnica alle organizzazioni che utilizzano Kaspersky Embedded Systems Security 2.2.

Questo manuale contiene informazioni sulla configurazione e sull'utilizzo di Kaspersky Embedded Systems Security 2.2.

Vengono inoltre elencati le fonti di informazioni sull'applicazione e i modi per ottenere assistenza tecnica.

In questo capitolo

Contenuto del documento	10
Convenzioni utilizzate nella documentazione	12

Contenuto del documento

Il Manuale dell'Amministratore per Kaspersky Embedded Systems Security 2.2 contiene le seguenti sezioni:

Fonti di informazioni su Kaspersky Embedded Systems Security 2.2

Questa sezione elenca le fonti di informazioni sull'applicazione.

Kaspersky Embedded Systems Security 2.2

Questa sezione descrive le funzioni, i componenti e il kit di distribuzione di Kaspersky Embedded Systems Security 2.2 e fornisce un elenco di requisiti hardware e software di Kaspersky Embedded Systems Security 2.2.

Installazione e rimozione dell'applicazione

Questa sezione offre istruzioni dettagliate per l'installazione e la rimozione di Kaspersky Embedded Systems Security 2.2.

Interfaccia dell'applicazione

Questa sezione contiene informazioni sugli elementi dell'interfaccia Kaspersky Embedded Systems Security 2.2.

Licensing dell'applicazione

Questa sezione fornisce informazioni sui concetti principali correlati alla gestione delle licenze dell'applicazione.

Avvio e arresto di Kaspersky Embedded Systems Security 2.2

Questa sezione contiene informazioni sull'avvio e sull'arresto del plug-in di amministrazione di Kaspersky Embedded Systems Security 2.2 (di seguito denominato "plug-in di amministrazione") e del Servizio di Kaspersky Security.

Informazioni sulle autorizzazioni di accesso per le funzioni di Kaspersky Embedded Systems Security 2.2

Questa sezione contiene informazioni sulle autorizzazioni per gestire Kaspersky Embedded Systems Security 2.2 e i servizi di Windows® registrati dall'applicazione, nonché istruzioni su come configurare queste autorizzazioni.

Creazione e configurazione dei criteri

Questa sezione contiene informazioni sull'utilizzo dei criteri di Kaspersky Security Center per la gestione di Kaspersky Embedded Systems Security 2.2 in diversi computer.

Creazione e configurazione delle attività tramite Kaspersky Security Center

Questa sezione contiene informazioni sulle attività di Kaspersky Embedded Systems Security 2.2, su come crearle, configurarne le impostazioni, nonché su come avviarle e arrestarle.

Gestione delle impostazioni dell'applicazione

Questa sezione contiene informazioni sulla configurazione delle impostazioni generali di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center.

Protezione del computer in tempo reale

Questa sezione fornisce informazioni sulle attività di Protezione del computer in tempo reale (Protezione dei file in tempo reale e Utilizzo di KSN) e sulla funzionalità Prevenzione exploit. Vengono inoltre fornite istruzioni su come configurare le attività di Protezione in tempo reale e gestire le impostazioni di sicurezza di un computer protetto.

Controllo attività locali

Questa sezione fornisce informazioni sulla funzionalità di Kaspersky Embedded Systems Security 2.2 che controlla gli avvii delle applicazioni e le connessioni dei dispositivi esterni tramite USB.

Controllo attività di rete

Questa sezione contiene informazioni sull'attività Gestione firewall.

Analisi sistema

Questa sezione contiene informazioni sull'attività Monitoraggio integrità file e sulle funzionalità per l'analisi del log del sistema operativo.

Integrazione con sistemi di terze parti

In questa sezione viene descritta l'integrazione di Kaspersky Embedded Systems Security 2.2 con funzionalità e tecnologie di terze parti.

Utilizzo di Kaspersky Embedded Systems Security 2.2 dalla riga di comando

Questa sezione illustra l'utilizzo di Kaspersky Embedded Systems Security 2.2 dalla riga di comando.

Come contattare il Servizio di assistenza tecnica

Questa sezione descrive i modi e le condizioni per ottenere assistenza tecnica.

Glossario

Questa sezione contiene un elenco dei termini utilizzati nella documentazione e le relative definizioni.

AO Kaspersky Lab

Questa sezione contiene informazioni su AO Kaspersky Lab.

Informazioni sul codice di terze parti

Questa sezione contiene informazioni sul codice di terze parti utilizzato nell'applicazione.

Note relative ai marchi

Questa sezione elenca i marchi di proprietà di terze parti menzionati nel documento.

Indice

Questa sezione consente di trovare rapidamente le informazioni desiderate all'interno della documentazione.

Convenzioni utilizzate nella documentazione

Questo documento utilizza le seguenti convenzioni (vedere la tabella di seguito).

Tabella 1. Convenzioni utilizzate nella documentazione

Testo di esempio	Descrizione della convenzione
Si noti che...	Il testo degli avvisi è in rosso e racchiuso da un riquadro. Gli avvisi contengono informazioni sulle azioni che possono avere conseguenze indesiderate.
È consigliabile utilizzare...	Le note sono racchiuse da un riquadro. Le note contengono informazioni supplementari e di riferimento.
Esempio: ...	Gli esempi sono riportati in blocchi su sfondo blu e sotto l'intestazione "Esempio".
<i>Aggiornamento significa...</i> Si verifica l'evento I database non sono aggiornati.	I seguenti elementi sono in corsivo nel testo: <ul style="list-style-type: none"> • Nuovi termini • Nomi di stati ed eventi dell'applicazione
Premere INVIO. Premere ALT+F4.	I nomi dei tasti sono contrassegnati dalla formattazione in grassetto e in lettere maiuscole. I nomi dei tasti connessi da un segno più (+) indicano l'utilizzo di una combinazione di tasti. Tali tasti devono essere premuti contemporaneamente.
Fare clic sul pulsante Abilita .	I nomi degli elementi di interfaccia dell'applicazione, come caselle di testo, voci di menu e pulsanti, sono in grassetto.
► <i>Per configurare la pianificazione per un'attività:</i>	Le frasi introduttive delle istruzioni sono in corsivo e contrassegnate da un segno a forma di freccia.
Nella riga di comando digitare <code>help</code> . Verrà visualizzato il seguente messaggio: Specificare la data nel formato <code>gg:mm:aa</code> .	I seguenti tipi di testo sono visualizzati con uno speciale carattere: <ul style="list-style-type: none"> • Testo della riga di comando • Testo dei messaggi visualizzati dall'applicazione • Dati che devono essere immessi dalla tastiera
<Nome utente>	Le variabili sono racchiuse tra parentesi angolari. Al posto di una variabile deve essere immesso il valore corrispondente, senza le parentesi angolari.

Fonti di informazioni su Kaspersky Embedded Systems Security 2.2

Questa sezione elenca le fonti di informazioni sull'applicazione.

È possibile scegliere le risorse più adatte in base all'urgenza e all'importanza del quesito.

In questo capitolo

Fonti per il recupero di informazioni in autonomia.....	13
Discussione delle applicazioni Kaspersky Lab nel forum.....	14

Fonti per il recupero di informazioni in autonomia

È possibile utilizzare le seguenti risorse per trovare informazioni su Kaspersky Embedded Systems Security 2.2:

- Pagina di Kaspersky Embedded Systems Security 2.2 nel sito Web di Kaspersky Lab.
- Pagina di Kaspersky Embedded Systems Security 2.2 nel sito Web dell'Assistenza tecnica (Knowledge Base).
- Manuali.

Se non è possibile trovare una soluzione al problema, contattare l'Assistenza tecnica di Kaspersky Lab <https://support.kaspersky.it/>.

Per utilizzare le fonti di informazioni online, è necessaria una connessione a Internet.

Pagina di Kaspersky Embedded Systems Security 2.2 nel sito Web di Kaspersky Lab

Nella pagina di Kaspersky Embedded Systems Security 2.2

(<https://www.kaspersky.it/enterprise-security/embedded-systems>) sono disponibili informazioni generali sull'applicazione e le relative funzionalità e caratteristiche.

La pagina di Kaspersky Embedded Systems Security 2.2 contiene un collegamento al negozio online. Tramite il negozio online è possibile acquistare l'applicazione o rinnovare la licenza.

Pagina di Kaspersky Embedded Systems Security 2.2 nella Knowledge Base

La Knowledge Base è una sezione del sito Web dell'Assistenza tecnica.

La pagina di Kaspersky Embedded Systems Security 2.2 nella Knowledge Base

(<https://support.kaspersky.com/kess2>) contiene articoli che forniscono informazioni utili, suggerimenti e risposte a domande frequenti su come acquistare, installare e utilizzare l'applicazione.

Gli articoli della Knowledge Base possono rispondere a domande relative non solo a Kaspersky Embedded

Systems Security 2.2 ma anche ad altre applicazioni di Kaspersky Lab. Gli articoli della Knowledge Base possono inoltre includere notizie sull'Assistenza tecnica.

Documentazione su Kaspersky Embedded Systems Security 2.2

Il Manuale dell'Amministratore di Kaspersky Embedded Systems Security 2.2 contiene informazioni sull'installazione, la disinstallazione, la configurazione delle impostazioni e l'utilizzo dell'applicazione.

Discussione delle applicazioni Kaspersky Lab nel forum

Se la domanda non richiede una risposta immediata, è possibile sottoporla agli esperti di Kaspersky Lab e ad altri utenti nel forum Kaspersky <http://forum.kaspersky.com/>.

In questo forum è possibile visualizzare i thread esistenti, lasciare i propri commenti e creare nuovi thread di discussione.

Kaspersky Embedded Systems Security 2.2

Questa sezione descrive le funzioni, i componenti e il kit di distribuzione di Kaspersky Embedded Systems Security 2.2 e fornisce un elenco di requisiti hardware e software di Kaspersky Embedded Systems Security 2.2.

In questo capitolo

Informazioni su Kaspersky Embedded Systems Security 2.2	15
Novità.....	17
Kit di distribuzione.....	18
Requisiti hardware e software	19

Informazioni su Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 protegge i computer e altri sistemi integrati con Microsoft® Windows da virus e altre minacce. Gli utenti di Kaspersky Embedded Systems Security 2.2 sono amministratori di rete aziendali e specialisti responsabili della protezione anti-virus della rete aziendale.

È possibile installare Kaspersky Embedded Systems Security 2.2 in svariati sistemi integrati con Windows, inclusi i seguenti tipi di dispositivi:

- ATM (Automated Teller Machine);
- POS (Point of Sale).

Kaspersky Embedded Systems Security 2.2 può essere gestito nei seguenti modi:

- Tramite la console dell'applicazione, installata nello stesso computer in cui è installato Kaspersky Embedded Systems Security 2.2 o in un computer diverso.
- Utilizzando i comandi della riga di comando.
- Tramite Kaspersky Security Center Administration Console.

L'applicazione Kaspersky Security Center può anche essere utilizzata per l'amministrazione centralizzata di più computer che eseguono Kaspersky Embedded Systems Security 2.2.

È possibile esaminare i contatori delle prestazioni di Kaspersky Embedded Systems Security 2.2 per l'applicazione "Monitor di sistema", nonché i contatori e le trap SNMP.

Componenti e funzioni di Kaspersky Embedded Systems Security 2.2

L'applicazione include i seguenti componenti:

- **Protezione dei file in tempo reale.** Kaspersky Embedded Systems Security 2.2 esegue la scansione degli oggetti al momento dell'accesso. Kaspersky Embedded Systems Security 2.2 esamina i seguenti oggetti:
 - File
 - Flussi alternativi del file system (flussi NTFS)
 - Record di avvio principale e settori di avvio in unità disco rigido locali e unità rimovibili

- **Scansione su richiesta.** Kaspersky Embedded Systems Security 2.2 esegue una singola scansione dell'area specificata alla ricerca di virus e altre minacce per la sicurezza del computer. L'applicazione esamina i file, la RAM e gli oggetti di avvio in un computer protetto.
- **Controllo dell'avvio delle applicazioni.** Il componente tiene traccia dei tentativi di avvio delle applicazioni da parte degli utenti e controlla gli avvii delle applicazioni in un computer protetto.
- **Controllo dispositivi.** Il componente controlla la registrazione e l'utilizzo dei dispositivi di archiviazione di massa e delle unità CD/DVD per proteggere il computer dalle minacce per la sicurezza che possono sopraggiungere durante lo scambio di file con flash drive connesse tramite USB o altri tipi di dispositivi esterni.
- **Gestione firewall.** Questo componente offre la possibilità di gestire Windows Firewall, configurando le impostazioni e le regole del firewall del sistema operativo e bloccando qualsiasi possibilità di configurazione esterna del firewall.
- **Monitoraggio integrità file.** Kaspersky Embedded Systems Security 2.2 rileva le modifiche nei file all'interno degli ambiti del monitoraggio specificati nelle impostazioni dell'attività. Queste modifiche possono indicare una violazione di sicurezza nel computer protetto.
- **Analisi log.** Questo componente monitora l'integrità dell'ambiente protetto in base ai risultati di un'analisi dei log degli eventi di Windows.

Nell'applicazione sono implementate le seguenti funzioni:

- **Aggiornamento database e Aggiornamento moduli software.** Kaspersky Embedded Systems Security 2.2 scarica gli aggiornamenti dei database e dei moduli dell'applicazione dai server di aggiornamento FTP o HTTP di Kaspersky Lab, Kaspersky Security Center Administration Server o altre sorgenti degli aggiornamenti.
- **Quarantena.** Kaspersky Embedded Systems Security 2.2 mette gli oggetti potenzialmente infetti in quarantena, spostando tali oggetti dalla loro posizione originale in *Quarantena*. Per motivi di sicurezza, gli oggetti vengono archiviati in Quarantena in formato criptato.
- **Backup.** Kaspersky Embedded Systems Security 2.2 archivia copie criptate degli oggetti classificati come *Infetto* o *Potenzialmente infetto* in *Backup* prima di disinfettarli o di eliminarli.
- **Notifiche per amministratori e utenti.** È possibile configurare l'applicazione per inviare notifiche all'amministratore e agli utenti che accedono al computer protetto sugli eventi che si verificano durante l'esecuzione di Kaspersky Embedded Systems Security 2.2 e sullo stato della protezione anti-virus del computer.
- **Importazione ed esportazione di impostazioni.** È possibile esportare le impostazioni di Kaspersky Embedded Systems Security 2.2 in un file di configurazione XML e importare le impostazioni in Kaspersky Embedded Systems Security 2.2 dal file di configurazione. È possibile salvare tutte le impostazioni dell'applicazione o solo le impostazioni relative ai singoli componenti in un file di configurazione.
- **Applicazione di modelli.** È possibile configurare manualmente le impostazioni di sicurezza di un nodo nell'albero o in un elenco delle risorse file del computer, nonché salvare i valori delle impostazioni configurate come modello. Questo modello può quindi essere utilizzato per configurare le impostazioni di sicurezza di altri nodi nelle attività di protezione e di scansione di Kaspersky Embedded Systems Security 2.2.
- **Gestione delle autorizzazioni di accesso per le funzioni di Kaspersky Embedded Systems Security.** È possibile configurare i diritti per la gestione di Kaspersky Embedded Systems Security 2.2 e dei servizi di Windows registrati dall'applicazione per utenti e gruppi di utenti.
- **Scrittura di eventi nel log eventi dell'applicazione.** Kaspersky Embedded Systems Security 2.2 registra le informazioni sulle impostazioni dei componenti software, lo stato corrente delle attività, gli eventi che si verificano durante la loro esecuzione, gli eventi associati alla gestione di Kaspersky Embedded Systems

Security 2.2 e le informazioni richieste per diagnosticare gli errori in Kaspersky Embedded Systems Security 2.2.

- **Area attendibile.** È possibile generare l'elenco di esclusioni dall'ambito della protezione o della scansione che Kaspersky Embedded Systems Security 2.2 applicherà nelle attività di protezione su richiesta e in tempo reale.
- **Prevenzione exploit.** È possibile proteggere la memoria processo dagli exploit utilizzando un agente inoculato nel processo.

Novità

Kaspersky Embedded Systems Security 2.2 offre i seguenti miglioramenti e funzionalità:

- Supporto per le nuove versioni dei sistemi operativi Microsoft Windows.
Meccanismi di auto-difesa basati sulle tecnologie ELAM e PPL: ora durante l'installazione dell'applicazione viene registrato automaticamente un driver ELAM che consente di avviare il servizio di Kaspersky Security (kavfs.exe) con l'attributo PPL (Protected Process Light). In tal modo, è possibile rafforzare le funzionalità di auto-difesa dell'applicazione e impedire una vasta gamma di attacchi.
La funzionalità è disponibile quando l'applicazione è installata nei computer che eseguono Microsoft Windows 10 RS2 (build 15063) e versioni successive.
- Supporto per il controllo e l'elaborazione dei file cloud archiviati in Microsoft OneDrive.
- Le possibilità offerte dal sottosistema Controllo distribuzione software sono state migliorate.
Ora è possibile specificare i file di installazione che possono passare l'attributo del pacchetto di installazione attendibile per l'intera catena di file estratti da tale pacchetto. Questo consente di aumentare la stabilità dei processi di installazione del software in un computer in cui Controllo dell'avvio delle applicazioni è attivato, ma al tempo stesso estende l'area per un potenziale attacco aumentando il numero di avvii delle applicazioni autorizzati. È consigliabile utilizzare questa opzione durante le distribuzioni software complesse, ad esempio quando è necessario riavviare il computer durante il processo di distribuzione del software.
- Integrazione con gli strumenti WMI.
Ora durante l'installazione dell'applicazione, viene creato automaticamente uno spazio dei nomi di Kaspersky Security nello spazio dei nomi radice WMI nel computer locale. È possibile utilizzare soluzioni client che supportano query WMI per ottenere dati sull'applicazione e i relativi componenti.
- Il formato per la visualizzazione delle informazioni sull'applicazione e i relativi componenti è stato ampliato con il comando KAVSHELL OMSINFO: ora è possibile ottenere informazioni sullo stato dell'attività Controllo dell'avvio delle applicazioni, nonché sugli aggiornamenti critici installati dei moduli dell'applicazione.
- Sono state migliorate le possibilità di gestione e monitoraggio dello stato dell'applicazione tramite l'interfaccia diagnostica compatta:
 - Ora è possibile esaminare i contatori delle statistiche per i componenti installati nella scheda Statistiche dell'interfaccia diagnostica compatta.
 - La password non è necessaria per l'accesso all'interfaccia diagnostica compatta, anche se la protezione tramite password è attivata: l'applicazione limita l'accesso alle informazioni e agli elementi di controllo che sono disponibili nell'interfaccia diagnostica compatta solo in base alle autorizzazioni utente specificate per la gestione dell'applicazione.
- A partire dalla versione 2.2, l'applicazione implementa la possibilità di garantire la protezione di base del computer durante l'avvio del sistema operativo in modalità provvisoria.

Per impostazione predefinita, l'applicazione non funziona in un computer in esecuzione in modalità provvisoria. Per impostare l'applicazione per l'avvio quando il sistema operativo viene avviato in modalità

provvisoria, impostare il parametro LoadInSafeMode su 1 nella seguente chiave del Registro di sistema di Windows:

```
HKLM\SYSTEM\CurrentControlSet\services\klam\Parameters
```

Durante l'esecuzione in un computer in modalità provvisoria, la funzionalità dell'applicazione sarà limitata.

- Sono supportati i rapporti di Kaspersky Security Center: ora è possibile esaminare i rapporti sullo stato dei componenti dell'applicazione e due tipi di rapporti sulle applicazioni non consentite. Questa funzionalità è supportata solo quando si utilizza Kaspersky Security Center 11.
- Le autorizzazioni di accesso utente per la modifica della cartella di installazione e dei rami critici del Registro di sistema per i componenti dell'applicazione ora sono limitate.

Kit di distribuzione

Il kit di distribuzione include l'applicazione iniziale che consente di eseguire le seguenti operazioni:

- Avviare l'Installazione guidata di Kaspersky Embedded Systems Security 2.2.
- Avviare l'Installazione guidata della console di Kaspersky Embedded Systems Security 2.2.
- Avviare l'Installazione guidata per installare il plug-in di amministrazione di Kaspersky Embedded Systems Security 2.2, che consente di gestire l'applicazione tramite Kaspersky Security Center.
- Consultare il Manuale dell'Amministratore.
- Consultare il Manuale Utente.
- Visitare la pagina di Kaspersky Embedded Systems Security 2.2 nel sito Web di Kaspersky Lab.
- Visitare il sito dell'Assistenza tecnica (<https://support.kaspersky.it/>).
- Leggere le informazioni sulla versione corrente di Kaspersky Embedded Systems Security 2.2

La cartella \console contiene i file per l'installazione della console dell'applicazione (set di componenti "Strumenti di amministrazione di Kaspersky Embedded Systems Security 2.2").

La cartella \product contiene:

- I file per l'installazione dei componenti di Kaspersky Embedded Systems Security 2.2 in un computer con sistema operativo Microsoft Windows a 32 o 64 bit.
- Il file per l'installazione del plug-in di amministrazione per la gestione di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center.
- Archivio con la versione corrente dei database anti-virus al momento del rilascio dell'applicazione.
- Il file con il testo del Contratto di licenza con l'utente finale e dell'Informativa sulla privacy.

La cartella \product_no_avbases contiene i file di installazione per i componenti e i plug-in di Kaspersky Embedded Systems Security 2.2 senza i database anti-virus.

La cartella \setup contiene i file di avvio del programma iniziale.

I file del kit di distribuzione sono archiviati in cartelle diverse a seconda del relativo utilizzo (vedere la tabella di seguito).

Tabella 2. File del kit di distribuzione di Kaspersky Embedded Systems Security 2.2

File	Scopo
autorun.inf	File di esecuzione automatica per l'installazione guidata di Kaspersky Embedded Systems Security 2.2 durante l'installazione dell'applicazione da supporti rimovibili.
ess_admin_guide_it.pdf	Manuale dell'Amministratore.
ess_user_guide_it.pdf	Manuale Utente.
release_notes.txt	File che contiene le informazioni sulla release.
setup.exe	File di avvio del programma iniziale (avvia setup.hta).
\console\esstools_x86(x64).msi	Pacchetto di installazione di Windows Installer. Installa la console dell'applicazione nel computer protetto.
\console\setup.exe	File che avvia l'installazione guidata del set di componenti "Strumenti di amministrazione" (che include la console dell'applicazione). Avvia il file del pacchetto di installazione esstools.msi utilizzando le impostazioni specificate nell'installazione guidata.
\product\bases.cab	Archivio con la versione corrente dei database anti-virus al momento del rilascio dell'applicazione.
\product\setup.exe	File che avvia l'installazione guidata di Kaspersky Embedded Systems Security 2.2 nel computer protetto. Avvia il file del pacchetto di installazione ess.msi con le impostazioni di installazione specificate nella procedura guidata.
\product\ess_x86(x64).msi	Pacchetto di installazione di Windows Installer. Installa Kaspersky Embedded Systems Security 2.2 nel computer protetto.
\product\ess.kud	File nel formato Kaspersky Unicode Definition con una descrizione del pacchetto di installazione per l'installazione remota di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center.
\product\klcfginst.exe	Programma di installazione del plug-in di amministrazione per la gestione di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center. Installare il plug-in di amministrazione in ogni computer in cui è installata Kaspersky Security Center Administration Console, se si prevede di usarla per gestire Kaspersky Embedded Systems Security 2.2.
\product\license.txt	Testo del Contratto di licenza con l'utente finale e dell'Informativa sulla privacy.
\product\migration.txt	Il file descrive la migrazione dalle versioni precedenti dell'applicazione.
\setup\setup.hta	File di avvio del programma iniziale.

I file del kit di distribuzione possono essere eseguiti dal CD di installazione. Se si copiano i file del pacchetto di distribuzione nell'unità locale prima dell'installazione, assicurarsi di mantenere la struttura dei file del kit di distribuzione.

Requisiti hardware e software

Prima di installare Kaspersky Embedded Systems Security 2.2, è necessario disinstallare altre applicazioni anti-virus dal computer.

Requisiti hardware per il computer protetto

Requisiti generali:

- Sistemi compatibili con x86 in configurazioni singole e multiprocessore.
- Sistemi compatibili con x64 in configurazioni singole e multiprocessore.

Volume disco:

- Per installare il componente Controllo dell'avvio delle applicazioni - 50 MB.
- Per installare tutti i componenti di Kaspersky Embedded Systems Security 2.2 - 500 MB.

RAM:

- 256 MB per installare il componente Controllo dell'avvio delle applicazioni solo nei computer con sistema operativo Microsoft® Windows.
- 512 MB per eseguire l'installazione completa di tutti i componenti nei computer con sistema operativo Microsoft Windows.

Requisiti minimi a livello di processore:

- per sistemi operativi Microsoft Windows a 32 bit: Intel® Pentium® III.
- per sistemi operativi Microsoft Windows a 64 bit: Intel Pentium IV.

Requisiti software per il computer protetto

È possibile installare Kaspersky Embedded Systems Security 2.2 in un dispositivo con un sistema operativo Microsoft Windows a 32 o a 64 bit.

Per la corretta installazione e l'utilizzo dell'applicazione in un computer con Microsoft Windows XP, è necessario Windows Installer 3.1.

Per installare e utilizzare Kaspersky Embedded Systems Security 2.2 nei dispositivi con sistemi operativi integrati, sono richiesti i componenti Gestione filtri e Strumenti di amministrazione.

È possibile installare Kaspersky Embedded Systems Security 2.2 in un computer con uno dei seguenti sistemi operativi Microsoft Windows a 32 o 64 bit:

- Windows XP Embedded SP3
- Windows XP Pro SP2 / SP3
- Windows Embedded POSReady 2009
- Windows Embedded Standard 7 SP1
- Windows Embedded Enterprise 7 SP1
- Windows Embedded POSReady 7

- Windows 7 Professional / Enterprise SP1
- Windows Embedded 8.1 Industry Professional / Enterprise
- Windows Embedded 8.1 Professional
- Windows Embedded 8.0 Standard
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Professional / Enterprise
- Windows 10 IoT Enterprise
- Windows 10 Redstone 1 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 2 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 3 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 4 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 5 Professional / Enterprise / IoT Enterprise

Installazione e rimozione dell'applicazione

Questa sezione offre istruzioni dettagliate per l'installazione e la rimozione di Kaspersky Embedded Systems Security 2.2.

In questo capitolo

Componenti software di Kaspersky Embedded Systems Security 2.2 e relativi codici per il servizio Windows Installer	22
Modifiche al sistema dopo l'installazione di Kaspersky Embedded Systems Security 2.2	25
Processi di Kaspersky Embedded Systems Security 2.2	29
Impostazioni di installazione e disinstallazione e opzioni della riga di comando per il servizio Windows Installer	29
Log di installazione e disinstallazione di Kaspersky Embedded Systems Security 2.2	36
Pianificazione dell'installazione	36
Installazione e disinstallazione dell'applicazione tramite procedura guidata.....	39
Installazione e disinstallazione dell'applicazione dalla riga di comando	51
Installazione e disinstallazione dell'applicazione tramite Kaspersky Security Center	56
Installazione e disinstallazione tramite i criteri di gruppo di Active Directory	61
Verifica delle funzioni di Kaspersky Embedded Systems Security 2.2.Utilizzo del virus di prova EICAR	63
Interfaccia dell'applicazione.....	66

Componenti software di Kaspersky Embedded Systems Security 2.2 e relativi codici per il servizio Windows Installer

Per impostazione predefinita, i file `\server\ess_x86(x64).msi` sono utilizzabili per installare tutti i componenti di Kaspersky Embedded Systems Security 2.2. È possibile installare questo componente includendolo in un'installazione personalizzata.

I file `\client\esstools_x86(x64).msi` installano tutti i componenti software dal set "Strumenti di amministrazione".

Nelle sezioni seguenti sono elencati i codici dei componenti di Kaspersky Embedded Systems Security 2.2 per il servizio Windows Installer. Questi codici possono essere utilizzati per definire un elenco di componenti da installare durante l'installazione di Kaspersky Embedded Systems Security 2.2 dalla riga di comando.

In questa sezione

Componenti software di Kaspersky Embedded Systems Security 2.2.....	23
Set di componenti software "Strumenti di amministrazione"	25

Componenti software di Kaspersky Embedded Systems Security 2.2

La seguente tabella contiene i codici dei componenti software di Kaspersky Embedded Systems Security 2.2, con la relativa descrizione.

Tabella 3. Descrizione dei componenti software di Kaspersky Embedded Systems Security 2.2

Componente	Codice	Funzioni eseguite
Funzionalità di base	Core	Questo componente contiene il set di funzioni di base dell'applicazione e garantisce il relativo funzionamento.
Controllo dell'avvio delle applicazioni	AppCtrl	Questo componente monitora i tentativi dell'utente di eseguire le applicazioni e consente o impedisce l'avvio delle applicazioni in base alle regole di Controllo dell'avvio delle applicazioni impostate. È implementato nell'attività Controllo dell'avvio delle applicazioni.
Controllo dispositivi	DevCtrl	Questo componente tiene traccia dei tentativi di connettere dispositivi di archiviazione di massa USB a un computer protetto e consente o nega l'utilizzo di tali dispositivi in base alle regole di controllo dei dispositivi specificate. Il componente è implementato nell'attività Controllo dispositivi.
Protezione anti-virus	AVProtection	Questo componente garantisce la protezione anti-virus e contiene i seguenti componenti: <ul style="list-style-type: none"> • Scansione su richiesta • Protezione dei file in tempo reale
Scansione su richiesta	Ods	Questo componente installa i file di sistema di Kaspersky Embedded Systems Security 2.2 e le attività Scansione su richiesta (scansione degli oggetti sul computer protetto su richiesta). Se si specificano altri componenti di Kaspersky Embedded Systems Security 2.2 durante l'installazione di Kaspersky Embedded Systems Security 2.2 dalla riga di comando, ma il componente di base non è specificato, il componente di base viene installato automaticamente.
Protezione dei file in tempo reale	Oas	Questo componente esegue la scansione anti-virus dei file sul computer protetto al momento dell'accesso ai file. Implementa l'attività Protezione dei file in tempo reale.
Utilizzo di Kaspersky Security Network	KSN	Questo componente fornisce la protezione sulla base delle tecnologie cloud di Kaspersky Lab. Implementa l'attività Utilizzo di KSN (invio di richieste al servizio Kaspersky Security Network e ricezione delle relative conclusioni).
Monitoraggio integrità file	FIM	Questo componente registra le operazioni eseguite sui file nell'ambito del monitoraggio specificato. Il componente implementa l'attività Monitoraggio integrità file.

Componente	Codice	Funzioni eseguite
Prevenzione exploit	AntiExploit	Questo componente consente di gestire le impostazioni per proteggere la memoria utilizzata dai processi nella memoria di un computer protetto.
Gestione firewall	Firewall	Questo componente consente di gestire Windows Firewall attraverso l'interfaccia utente grafica di Kaspersky Embedded Systems Security 2.2. Il componente implementa l'attività Gestione firewall.
Modulo per l'integrazione con Kaspersky Security Center Network Agent	AKIntegration	Fornisce una connessione tra Kaspersky Embedded Systems Security 2.2 e Kaspersky Security Center Network Agent. È possibile installare questo componente nel computer protetto se si intende gestire l'applicazione tramite Kaspersky Security Center.
Analisi log	LogInspector	Questo componente monitora l'integrità dell'ambiente protetto in base ai risultati di un'analisi dei log degli eventi di Windows.
Set di contatori di performance "Monitor di sistema"	PerfMonCounters	Questo componente installa un set di contatori delle prestazioni di Monitor di sistema. I contatori delle prestazioni consentono di misurare le prestazioni di Kaspersky Embedded Systems Security 2.2 e di individuare potenziali colli di bottiglia durante l'utilizzo di Kaspersky Embedded Systems Security 2.2 con altri programmi.
Contatori e trap SNMP	SnmpSupport	Questo componente pubblica i contatori e le trap di Kaspersky Embedded Systems Security 2.2 tramite SNMP (Simple Network Management Protocol) in Microsoft Windows. Questo componente può essere installato nel computer protetto solo se Microsoft SNMP è installato nello stesso computer.
Icona di Kaspersky Embedded Systems Security 2.2 nell'area di notifica	TrayApp	Questo componente visualizza l'icona di Kaspersky Embedded Systems Security 2.2 nell'area di notifica della barra delle applicazioni del computer protetto. L'icona di Kaspersky Embedded Systems Security 2.2 visualizza lo stato della protezione del computer e può essere utilizzata per aprire la console di Kaspersky Embedded Systems Security 2.2 in Microsoft Management Console (se installato) e la finestra Informazioni sull'applicazione .
Utilità della riga di comando	Shell	Rende possibile controllare Kaspersky Embedded Systems Security 2.2 dalla riga di comando di un computer protetto.

Set di componenti software "Strumenti di amministrazione"

La seguente tabella contiene i codici e una descrizione del set di componenti software "Strumenti di amministrazione".

Tabella 4. Descrizione dei componenti software "Strumenti di amministrazione"

Componente	Codice	Funzioni dei componenti
Snap-in di Kaspersky Embedded Systems Security 2.2	MmcSnapin	Questo componente installa lo snap-in MMC (Microsoft Management Console) tramite la console di Kaspersky Embedded Systems Security 2.2. Se si specificano altri componenti durante l'installazione di "Strumenti di amministrazione" dalla riga di comando e il componente MmcSnapin non è specificato, il componente verrà installato automaticamente.
Guida	Help	File della Guida in formato .chm; salvato nella cartella con i file degli strumenti di amministrazione di Kaspersky Embedded Systems Security 2.2. È possibile aprire il file della Guida utilizzando il menu Start o premendo F1 mentre è aperta la finestra della console dell'applicazione.
Documentazione	Help	Kaspersky Embedded Systems Security 2.2 aggiunge un collegamento alla risorsa Web di Kaspersky Lab in cui sono disponibili il Manuale dell'Amministratore e il Manuale Utente in formato PDF. Il collegamento è disponibile nel menu Start.

Modifiche al sistema dopo l'installazione di Kaspersky Embedded Systems Security 2.2

Quando Kaspersky Embedded Systems Security 2.2 e la console dell'applicazione (set "Strumenti di amministrazione") vengono installati insieme, il servizio Windows apporta le seguenti modifiche sul computer protetto:

- Vengono create le cartelle di Kaspersky Embedded Systems Security 2.2 nel computer protetto e nel computer in cui è installata la console dell'applicazione.
- Vengono registrati i servizi di Kaspersky Embedded Systems Security 2.2.
- Viene creato un gruppo di utenti di Kaspersky Embedded Systems Security 2.2.
- Vengono registrate le chiavi di Kaspersky Embedded Systems Security 2.2 nel Registro di sistema.

Queste modifiche sono descritte nella seguente tabella.

Cartelle di Kaspersky Embedded Systems Security 2.2

Tabella 5. Cartelle di Kaspersky Embedded Systems Security 2.2 in un computer protetto

Cartella	File di Kaspersky Embedded Systems Security 2.2
<p>Cartella di installazione predefinita di Kaspersky Embedded Systems Security 2.2:</p> <p>Nella versione di Microsoft Windows a 32 bit - %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\ Nella versione di Microsoft Windows a 64 bit - %ProgramFiles(x86)%\Kaspersky Embedded Systems Security\ Security\</p>	<p>File eseguibili di Kaspersky Embedded Systems Security 2.2 (cartella di destinazione specificata durante l'installazione).</p>
<p>Cartella %Kaspersky Embedded Systems Security%\mibs</p>	<p>File MIB (Management Information Base). Questi file contengono una descrizione dei contatori e degli hook pubblicati da Kaspersky Embedded Systems Security 2.2 tramite il protocollo SNMP.</p>
<p>Cartella %Kaspersky Embedded Systems Security%\x64</p>	<p>File eseguibili delle versioni a 64 bit di Kaspersky Embedded Systems Security 2.2 (la cartella verrà creata solo durante l'installazione di Kaspersky Embedded Systems Security 2.2 nella versione a 64 bit di Microsoft Windows).</p>
<p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Data\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Settings\ %ALLUSERSPROFILE%\Application Data\Kaspersky Embedded Systems Security\2.2\Dskm\ \</p>	<p>File dei servizi di Kaspersky Embedded Systems Security 2.2.</p>
<p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\ \</p>	<p>File con le impostazioni delle sorgenti degli aggiornamenti.</p>
<p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\Distribution\ \</p>	<p>Aggiornamenti dei database e dei moduli software scaricati tramite l'attività Copia degli aggiornamenti (la cartella sarà creata la prima volta che gli aggiornamenti vengono scaricati utilizzando l'attività Copia degli aggiornamenti).</p>
<p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Reports\ \</p>	<p>Log delle attività e log di audit.</p>
<p>%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Current\ \</p>	<p>Set di database utilizzato al momento attuale.</p>

Cartella	File di Kaspersky Embedded Systems Security 2.2
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Backup\	Copia di backup dei database. Sarà sovrascritta ogni volta che i database vengono aggiornati.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Temp\	File temporanei creati durante l'esecuzione delle attività di aggiornamento.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Quarantine\	Oggetti in Quarantena (cartella predefinita).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Backup\	Oggetti in Backup (cartella predefinita).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored\	Oggetti ripristinati da Backup e Quarantena (cartella predefinita per gli oggetti ripristinati).

Tabella 6. Cartelle create durante l'installazione della console dell'applicazione

Cartella	File della console di Kaspersky Embedded Systems Security 2.2
Cartella di installazione predefinita della console dell'applicazione: <ul style="list-style-type: none"> • Nella versione di Microsoft Windows a 32 bit - %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\ • Nella versione di Microsoft Windows a 64 bit - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\ 	File di "Strumenti di amministrazione" (cartella di destinazione specificata durante l'installazione della console di Kaspersky Embedded Systems Security 2.2)

Servizi di Kaspersky Embedded Systems Security 2.2

I servizi di Kaspersky Embedded Systems Security 2.2 sono avviati utilizzando l'account Sistema locale (SYSTEM).

Tabella 7. Servizi di Kaspersky Embedded Systems Security 2.2

Servizio	Scopo
Servizio di Kaspersky Security (KAVFS)	Servizio essenziale di Kaspersky Embedded Systems Security 2.2 che gestisce le attività e i flussi di lavoro di Kaspersky Embedded Systems Security 2.2.
Servizio di gestione di Kaspersky Security (KAVFSGT)	Questo servizio consente la gestione dell'applicazione Kaspersky Embedded Systems Security 2.2 tramite la console dell'applicazione.

Gruppi di Kaspersky Embedded Systems Security 2.2

Tabella 8. Gruppi di Kaspersky Embedded Systems Security 2.2

Gruppo	Scopo
Amministratori ESS	Un gruppo nel computer protetto i cui utenti hanno accesso completo al servizio di gestione di Kaspersky Security e a tutte le funzioni di Kaspersky Embedded Systems Security 2.2.

Chiavi del Registro di sistema

Tabella 9. Chiavi del Registro di sistema

Chiave	Scopo
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Proprietà del servizio Kaspersky Embedded Systems Security 2.2.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]	Impostazioni del log eventi di Kaspersky Embedded Systems Security 2.2 (log eventi Kaspersky).
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Proprietà del servizio di gestione di Kaspersky Embedded Systems Security 2.2.
Nella versione di Microsoft Windows a 32 bit: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance] Nella versione di Microsoft Windows a 64 bit: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance].	Impostazioni dei contatori delle prestazioni.
Nella versione di Microsoft Windows a 32 bit: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\SnmpAgent] Nella versione di Microsoft Windows a 64 bit: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\SnmpAgent]	Impostazioni del componente di supporto del protocollo SNMP.

Chiave	Scopo
Nella versione di Microsoft Windows a 32 bit: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\CrashDump] Nella versione di Microsoft Windows a 64 bit: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\CrashDump]	Impostazioni di scrittura del file di dump.
Nella versione di Microsoft Windows a 32 bit: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\Trace] Nella versione di Microsoft Windows a 64 bit: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Trace]	Impostazioni del file di traccia.
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Environment]	Configurazione delle attività e delle funzioni dell'applicazione

Processi di Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 avvia i processi descritti nella seguente tabella.

Tabella 10. Processi di Kaspersky Embedded Systems Security 2.2

Nome del file	Scopo
kavswp.exe	Flusso di lavoro di Kaspersky Embedded Systems Security 2.2
kavtray.exe	Processo per l'icona nell'area di notifica
kavshell.exe	Processo dell'utilità della riga di comando
kavsrcn.exe	Processo di gestione remota di Kaspersky Embedded Systems Security 2.2
kavfs.exe	Processo del servizio di Kaspersky Security
kavsgt.exe	Processo del servizio di gestione di Kaspersky Security
kavswh.exe	Processo del servizio Prevenzione exploit di Kaspersky Security

Impostazioni di installazione e disinstallazione e opzioni della riga di comando per il servizio Windows Installer

Le tabelle riportate di seguito contengono le descrizioni delle impostazioni per l'installazione e la disinstallazione di Kaspersky Embedded Systems Security 2.2, i relativi valori predefiniti, le chiavi per la modifica dei valori delle impostazioni di installazione e i relativi valori possibili. Queste chiavi possono essere utilizzate in combinazione con le chiavi standard per il comando msixec del servizio Windows Installer durante l'installazione di Kaspersky Embedded Systems Security 2.2 dalla riga di comando.

Tabella 11. Parametri di installazione e opzioni della riga di comando in Windows Installer

Impostazione	Opzioni della riga di comando di Windows Installer e valori possibili	Valore predefinito	Descrizione
Accettazione delle condizioni del Contratto di licenza con l'utente finale	EULA=<valore> 0 - si rifiutano le condizioni del Contratto di licenza con l'utente finale. 1 - si accettano le condizioni del Contratto di licenza con l'utente finale.	0	È necessario accettare le condizioni del Contratto di licenza con l'utente finale per installare Kaspersky Embedded Systems Security 2.2.
Accettazione delle condizioni dell'Informativa sulla privacy	PRIVACYPOLICY=<valore> 0 – l'utente rifiuta le condizioni dell'Informativa sulla privacy. 1 – l'utente accetta le condizioni dell'Informativa sulla privacy.	0	È necessario accettare le condizioni dell'Informativa sulla privacy per installare Kaspersky Embedded Systems Security 2.2.
Cartella di destinazione	INSTALLDIR=<percorso completo della cartella>	Kaspersky Embedded Systems Security 2.2: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Strumenti di amministrazione: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools Nella versione x64 di Microsoft Windows: %ProgramFiles(x86)%.	Cartella in cui verranno salvati i file di Kaspersky Embedded Systems Security 2.2 durante l'installazione. È possibile specificare una cartella diversa.
Avvio dell'attività Protezione dei file in tempo reale all'avvio di Kaspersky Embedded Systems Security 2.2 (Abilita la protezione in tempo reale dopo l'installazione dell'applicazione)	RUNRTP=<valore> 1 - avviare. 0 - non avviare.	1	Attivare questa impostazione per avviare Protezione dei file in tempo reale all'avvio di Kaspersky Embedded Systems Security 2.2 (scelta consigliata).

Impostazione	Opzioni della riga di comando di Windows Installer e valori possibili	Valore predefinito	Descrizione
<p>Esclusioni dalla scansione consigliate da Microsoft Corporation (Aggiungi i file consigliati da Microsoft all'elenco di esclusioni)</p>	<p>ADDMSEXCLUSION=<valore > 1 - escludere. 0 - non escludere.</p>	<p>1</p>	<p>Nell'attività Protezione dei file in tempo reale escludere dall'ambito della protezione gli oggetti nel computer che Microsoft Corporation consiglia di escludere.</p> <p>Alcune applicazioni sul computer possono diventare instabili quando l'applicazione anti-virus intercetta o modifica i file utilizzati da tali applicazioni. Per esempio, Microsoft Corporation include alcune applicazioni del controller di dominio nell'elenco di tali oggetti.</p>
<p>Oggetti esclusi dall'ambito della scansione in base alle raccomandazioni di Kaspersky Lab (Aggiungi i file consigliati da Kaspersky Lab all'elenco di esclusioni)</p>	<p>ADDKLEXCLUSION=<valore > 1 - escludere. 0 - non escludere.</p>	<p>1</p>	<p>Nell'attività Protezione dei file in tempo reale escludere dall'ambito della protezione gli oggetti nel computer che Kaspersky Lab consiglia di escludere.</p>

Impostazione	Opzioni della riga di comando di Windows Installer e valori possibili	Valore predefinito	Descrizione
<p>Consentire la connessione remota alla console dell'applicazione.</p>	<p>ALLOWREMOTECON= <valore> 1 - consentire. 0 - non consentire.</p>	<p>0</p>	<p>Per impostazione predefinita, la connessione remota alla console dell'applicazione installata nel computer protetto non è consentita. Durante l'installazione, è possibile consentire la connessione. Kaspersky Embedded Systems Security 2.2 crea regole di permesso per il processo kavfsgt.exe utilizzando il protocollo TCP per tutte le porte.</p>
<p>Percorso del file chiave (Chiave)</p>	<p>LICENSEKEYPATH=<nome del file chiave></p>	<p>Directory \product nel kit di distribuzione</p>	<p>Per impostazione predefinita, il programma di installazione tenta di individuare il file con l'estensione .key nella cartella \product del kit di distribuzione. Se la cartella \product contiene diversi file chiave, il programma di installazione selezionerà il file chiave con la data di scadenza più lontana. Un file chiave può essere salvato in anticipo nella cartella \product o specificando un altro percorso del file chiave tramite l'impostazione Aggiungi chiave.</p>

Impostazione	Opzioni della riga di comando di Windows Installer e valori possibili	Valore predefinito	Descrizione
			<p>È possibile aggiungere una chiave dopo l'installazione di Kaspersky Embedded Systems Security 2.2 utilizzando lo strumento di amministrazione che si preferisce, come ad esempio la console dell'applicazione. Se non si aggiunge una chiave durante l'installazione dell'applicazione, Kaspersky Embedded Systems Security 2.2 non funzionerà.</p>
<p>Percorso del file di configurazione</p>	<p>CONFIGPATH=<nome del file di configurazione></p>	<p>Non specificato</p>	<p>Kaspersky Embedded Systems Security 2.2 importa le impostazioni dal file di configurazione specificato creato nell'applicazione.</p> <p>Kaspersky Embedded Systems Security 2.2 non importa le password dal file di configurazione, ad esempio le password dell'account per l'avvio delle attività o le password per la connessione a un server proxy. Una volta importate le impostazioni, sarà necessario immettere tutte le password manualmente.</p> <p>Se il file di configurazione non viene specificato, l'applicazione inizierà a funzionare con le impostazioni predefinite dopo l'installazione.</p>

Impostazione	Opzioni della riga di comando di Windows Installer e valori possibili	Valore predefinito	Descrizione
<p>Abilitazione delle connessioni di rete per la console</p>	<p>ADDWFEXCLUSION=<valore > 1 - consentire. 0 - non consentire.</p>	<p>0</p>	<p>Utilizzare questa opzione per installare Kaspersky Embedded Systems Security 2.2 in un altro computer. È possibile gestire in remoto la protezione di un computer da un altro dispositivo con la console di Kaspersky Embedded Systems Security 2.2 installata.</p> <p>La porta 135 (TCP) viene aperta in Microsoft Windows Firewall, sono consentite le connessioni di rete per il file eseguibile kavfsrcn.exe per la gestione remota di Kaspersky Embedded Systems Security 2.2 e viene concesso l'accesso alle applicazioni DCOM.</p> <p>Dopo il completamento dell'installazione, aggiungere gli utenti al gruppo Amministratori ESS per consentire loro di eseguire la gestione remota dell'applicazione e consentire le connessioni di rete al servizio di gestione di Kaspersky Security (file kavfsgt.exe) sul computer.</p> <p>È possibile consultare ulteriori informazioni sulla configurazione aggiuntiva durante l'installazione della console di Kaspersky Embedded Systems Security 2.2 in un altro</p>

Impostazione	Opzioni della riga di comando di Windows Installer e valori possibili	Valore predefinito	Descrizione
			computer (vedere la sezione "Impostazioni avanzate dopo l'installazione della console dell'applicazione in un altro computer" a pagina 43).
Disabilitazione della verifica della presenza di software incompatibile	SKIPINCOMPATIBLESW = <valore> 0 - Viene eseguita la verifica della presenza di software incompatibile. 1 - Non viene eseguita la verifica della presenza di software incompatibile.	0	Utilizzare questa impostazione per abilitare o disabilitare la verifica della presenza di software incompatibile durante l'installazione in background dell'applicazione nel dispositivo. Indipendentemente dal valore di questa impostazione, durante l'installazione di Kaspersky Embedded Systems Security 2.2 l'applicazione avvisa sempre della presenza di altre versioni dell'applicazione installate nel dispositivo.

Tabella 12. Impostazioni di disinstallazione e opzioni della riga di comando in Windows Installer

Impostazione	Opzioni della riga di comando di Windows Installer e valori possibili	Valore predefinito
Ripristino degli oggetti in quarantena	RESTOREQTN =<valore> 0 - rimuovere il contenuto della Quarantena. 1 - ripristinare il contenuto della Quarantena nella cartella specificata tramite il parametro RESTOREPATH nella sottocartella \Quarantine.	0 - Rimuovere
Ripristino del contenuto del backup	RESTOREBCK =<valore> 0 - rimuovere il contenuto del Backup. 1 - ripristinare il contenuto del Backup nella cartella specificata tramite il parametro RESTOREPATH nella sottocartella \Backup.	0 - Rimuovere

Impostazione	Opzioni della riga di comando di Windows Installer e valori possibili	Valore predefinito
Immettere la password corrente per confermare l'eliminazione (se la protezione tramite password è abilitata)	UNLOCK_PASSWORD=<password specificata>	Non specificato
Cartella per gli oggetti ripristinati	RESTOREPATH=<percorso completo della cartella> Gli oggetti ripristinati saranno salvati nella cartella specificata.	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored

Log di installazione e disinstallazione di Kaspersky Embedded Systems Security 2.2

Se Kaspersky Embedded Systems Security 2.2 viene installato o disinstallato utilizzando l'Installazione o la Disinstallazione guidata, il servizio Windows Installer crea un log di installazione (disinstallazione). Il file di log `ess_install_<uid>.log` (dove `<uid>` è un identificatore univoco del log di 8 caratteri) sarà salvato in una cartella `%temp%` dell'utente dal cui account è stato avviato il file `setup.exe`.

Se si esegue l'opzione **Modifica o rimuovi** per la console dell'applicazione o Kaspersky Embedded Systems Security 2.2 dal menu **Start**, viene creato automaticamente il file `ess_2.2_maintenance.log` nella cartella `%temp%`.

Se Kaspersky Embedded Systems Security 2.2 viene installato o disinstallato dalla riga di comando, il file di log dell'installazione per impostazione predefinita non sarà creato.

► *Per installare Kaspersky Embedded Systems Security 2.2 con il file di log creato sul disco C:*

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

Pianificazione dell'installazione

Questa sezione contiene una descrizione del set di strumenti di amministrazione di Kaspersky Embedded Systems Security 2.2 e degli aspetti speciali dell'installazione e della disinstallazione di Kaspersky Embedded Systems Security 2.2 tramite una procedura guidata (vedere la sezione "Installazione e disinstallazione dell'applicazione tramite procedura guidata" a pagina [39](#)), la riga di comando (vedere la sezione "Installazione e disinstallazione dell'applicazione dalla riga di comando" a pagina [51](#)), tramite Kaspersky Security Center (vedere la sezione "Installazione e disinstallazione dell'applicazione tramite Kaspersky Security Center" a pagina [56](#)) e tramite i criteri di gruppo di Active Directory® (vedere la sezione "Installazione e disinstallazione tramite i criteri di gruppo di Active Directory" a pagina [61](#)).

Prima di avviare l'installazione di Kaspersky Embedded Systems Security 2.2, pianificarne le fasi principali.

1. Determinare quali strumenti di amministrazione saranno utilizzati per gestire e configurare Kaspersky Embedded Systems Security 2.2.
2. Selezionare i componenti dell'applicazione necessari per l'installazione (vedere la sezione "Componenti software di Kaspersky Embedded Systems Security 2.2 e relativi codici per il servizio Windows Installer" a pagina [22](#)).
3. Selezionare il metodo di installazione.

In questa sezione

Selezione degli strumenti di amministrazione	37
Selezione del tipo di installazione	38

Selezione degli strumenti di amministrazione

Determinare gli strumenti di amministrazione che saranno utilizzati per configurare le impostazioni di Kaspersky Embedded Systems Security 2.2 e gestirlo. Kaspersky Embedded Systems Security 2.2 può essere gestito tramite la console dell'applicazione, l'utilità della riga di comando e Kaspersky Security Center Administration Console.

Console di Kaspersky Embedded Systems Security 2.2

La console di Kaspersky Embedded Systems Security 2.2 è uno snap-in isolato aggiunto a Microsoft Management Console. Kaspersky Embedded Systems Security 2.2 può essere gestito tramite la console dell'applicazione installata nel computer protetto o in un altro computer nella rete aziendale.

È possibile aggiungere più snap-in di Kaspersky Embedded Systems Security 2.2 a una console MMC aperta in modalità di modifica per utilizzarli per la gestione della protezione di più computer in cui è installato Kaspersky Embedded Systems Security 2.2.

La console dell'applicazione è inclusa nel set di componenti "Strumenti di amministrazione" dell'applicazione.

Utilità della riga di comando

È possibile gestire Kaspersky Embedded Systems Security 2.2 dalla riga di comando di un computer protetto.

L'utilità della riga di comando è inclusa nel gruppo di componenti software di Kaspersky Embedded Systems Security 2.2.

Kaspersky Security Center

Se si utilizza l'applicazione Kaspersky Security Center per la gestione centralizzata della protezione anti-virus dei computer dell'azienda, è possibile gestire Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center Administration Console.

Devono essere installati i seguenti componenti:

- **Modulo per l'integrazione con Kaspersky Security Center Network Agent.** Questo componente è incluso nel gruppo di componenti software di Kaspersky Embedded Systems Security 2.2. Garantisce la comunicazione di Kaspersky Embedded Systems Security 2.2 con Network Agent. Installare il modulo per l'integrazione con Kaspersky Security Center Network Agent nel computer protetto.
- **Kaspersky Security Center Network Agent.** Installare questo componente in ogni computer protetto.

Questo componente supporta l'interazione tra Kaspersky Embedded Systems Security 2.2 installato nel computer e Kaspersky Security Center Administration Console. Il file di installazione di Network Agent è incluso nella cartella del kit di distribuzione di Kaspersky Security Center.

- **Plug-in di amministrazione per Kaspersky Embedded Systems Security 2.2.** Installare inoltre il plug-in di amministrazione per la gestione di Kaspersky Embedded Systems Security 2.2 tramite Administration Console nel computer in cui è installato Kaspersky Security Center Administration Server. Questo consente di utilizzare l'interfaccia di gestione dell'applicazione tramite Kaspersky Security Center. Il file di installazione del plug-in di amministrazione, `\product\klcfinst.exe`, è incluso nel kit di distribuzione di Kaspersky Embedded Systems Security 2.2.

Selezione del tipo di installazione

Dopo avere specificato i componenti software per l'installazione di Kaspersky Embedded Systems Security 2.2 (vedere la sezione "Componenti software di Kaspersky Embedded Systems Security 2.2 e relativi codici per il servizio Windows Installer" a pagina [22](#)), è necessario selezionare il metodo di installazione dell'applicazione.

Selezionare il metodo di installazione in base all'architettura di rete e alle seguenti condizioni:

- Se sarà necessario configurare speciali impostazioni di installazione di Kaspersky Embedded Systems Security 2.2 o se saranno utilizzate le impostazioni di installazione consigliate (vedere la sezione "Impostazioni di installazione e disinstallazione e opzioni della riga di comando per il servizio Windows Installer" a pagina [29](#)).
- Se le impostazioni di installazione saranno le stesse per tutti i computer o specifiche per ogni computer.

Kaspersky Embedded Systems Security 2.2 può essere installato in modalità interattiva utilizzando l'Installazione guidata o in modalità invisibile all'utente e richiamato eseguendo il file del pacchetto di installazione con le impostazioni di installazione dalla riga di comando. Un'installazione remota centralizzata di Kaspersky Embedded Systems Security 2.2 può essere eseguita utilizzando i criteri di gruppo di Active Directory o tramite l'attività di installazione remota di Kaspersky Security Center.

Kaspersky Embedded Systems Security 2.2 può essere installato in un singolo computer, configurato per l'esecuzione e le relative impostazioni possono essere salvate in un file di configurazione. Il file creato può quindi essere utilizzato per installare Kaspersky Embedded Systems Security 2.2 in un altro computer (questa possibilità non si applica quando l'applicazione viene installata utilizzando i criteri di gruppo di Active Directory).

Avvio dell'Installazione guidata

L'Installazione guidata consente di installare quanto segue:

- I componenti di Kaspersky Embedded Systems Security 2.2 (vedere la sezione "Componenti software di Kaspersky Embedded Systems Security 2.2" a pagina [23](#)) in un computer protetto da un file `\product\setup.exe` incluso nel kit di distribuzione.
- La console di Kaspersky Embedded Systems Security 2.2 (vedere la sezione "Installazione della console di Kaspersky Embedded Systems Security 2.2" a pagina [42](#)) dal file `\client\setup.exe` del kit di distribuzione nel computer protetto o in un altro host della rete LAN.

Esecuzione del file del pacchetto di installazione dalla riga di comando con le impostazioni di installazione richieste

Se il file del pacchetto di installazione viene avviato senza opzioni della riga di comando, Kaspersky Embedded Systems Security 2.2 sarà installato con le impostazioni predefinite. Le opzioni di Kaspersky Embedded Systems Security 2.2 possono essere utilizzate per modificare le impostazioni di installazione.

La console dell'applicazione può essere installata nel computer protetto e/o nella workstation di amministrazione.

È inoltre possibile utilizzare comandi di esempio per l'installazione di Kaspersky Embedded Systems Security 2.2 e della console dell'applicazione (vedere la sezione "Installazione e disinstallazione dell'applicazione dalla riga di comando" a pagina [51](#)).

Installazione centralizzata tramite Kaspersky Security Center

Se si utilizza Kaspersky Security Center per gestire la protezione anti-virus dei computer della rete, Kaspersky Embedded Systems Security 2.2 può essere installato in più computer utilizzando l'attività di installazione remota di Kaspersky Security Center.

I computer in cui si desidera installare Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center (vedere la sezione "Installazione e disinstallazione dell'applicazione tramite Kaspersky Security Center" a pagina [56](#)) possono appartenere allo stesso dominio di Kaspersky Security Center, a un dominio diverso o non appartenere ad alcun dominio.

Installazione centralizzata tramite i criteri di gruppo di Active Directory

I criteri di gruppo di Active Directory possono essere utilizzati per installare Kaspersky Embedded Systems Security 2.2 nel computer protetto. La console dell'applicazione può essere installata nel computer protetto o nella workstation di amministrazione.

Kaspersky Embedded Systems Security 2.2 può essere installato utilizzando soltanto le impostazioni di installazione consigliate.

I computer in cui viene installato Kaspersky Embedded Systems Security 2.2 tramite i criteri di gruppo di Active Directory (vedere la sezione "Installazione e disinstallazione tramite i criteri di gruppo di Active Directory" a pagina [61](#)) devono appartenere allo stesso dominio e alla stessa unità organizzativa. L'installazione viene eseguita all'avvio del computer prima dell'accesso a Microsoft Windows.

Installazione e disinstallazione dell'applicazione tramite procedura guidata

Questa sezione contiene la descrizione dei processi di installazione e disinstallazione di Kaspersky Embedded Systems Security 2.2 e della console dell'applicazione per mezzo dell'installazione guidata, nonché informazioni sulla configurazione aggiuntiva di Kaspersky Embedded Systems Security 2.2 e sulle azioni da eseguire dopo l'installazione.

In questa sezione

Installazione tramite l'Installazione guidata	40
Modifica del set di componenti e ripristino di Kaspersky Embedded Systems Security 2.2	48
Disinstallazione tramite l'Installazione guidata	49

Installazione tramite l'Installazione guidata

Le sezioni seguenti contengono informazioni sull'installazione di Kaspersky Embedded Systems Security 2.2 e della console dell'applicazione.

► *Per installare e iniziare a utilizzare Kaspersky Embedded Systems Security 2.2, eseguire le seguenti operazioni:*

1. Installare Kaspersky Embedded Systems Security 2.2 in un computer protetto.
2. Installare la console dell'applicazione nei computer da cui si intende gestire Kaspersky Embedded Systems Security 2.2.
3. Se la console dell'applicazione è stata installata in un computer della rete diverso dal computer protetto, eseguire configurazioni aggiuntive per consentire agli utenti della console dell'applicazione di gestire Kaspersky Embedded Systems Security 2.2 in modalità remota.
4. Eseguire le operazioni dopo l'installazione di Kaspersky Embedded Systems Security 2.2.

In questa sezione

Installazione di Kaspersky Embedded Systems Security 2.2.....	40
Installazione della console di Kaspersky Embedded Systems Security 2.2	42
Impostazioni avanzate dopo l'installazione della console dell'applicazione in un altro computer	43
Azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2	46

Installazione di Kaspersky Embedded Systems Security 2.2

Prima di installare Kaspersky Embedded Systems Security 2.2, eseguire le seguenti operazioni:

- Verificare che nel computer non siano installati altri programmi anti-virus.
- Verificare che l'account che verrà utilizzato per avviare l'Installazione guidata sia registrato nel gruppo Administrators sul computer protetto.

Dopo avere completato le operazioni descritte in precedenza, continuare con la procedura d'installazione. Seguendo le istruzioni dell'Installazione guidata, specificare le impostazioni per l'installazione di Kaspersky Embedded Systems Security 2.2. Il processo di installazione di Kaspersky Embedded Systems Security 2.2 può essere interrotto durante qualsiasi passaggio dell'Installazione guidata. A tale scopo, fare clic sul pulsante **Annulla** nella finestra dell'Installazione guidata.

Sono disponibili ulteriori informazioni sulle impostazioni di installazione (disinstallazione) (vedere la sezione "Impostazioni di installazione e disinstallazione e opzioni della riga di comando per il servizio Windows Installer" a pagina [29](#)).

► *Per installare Kaspersky Embedded Systems Security 2.2 tramite l'Installazione guidata:*

1. Avviare il file della iniziale setup.exe nel computer.
2. Nella finestra visualizzata, nella sezione **Installazione**, fare clic sul collegamento **Installa Kaspersky Embedded Systems Security 2.2**.
3. Nella schermata iniziale dell'Installazione guidata di Kaspersky Embedded Systems Security 2.2 fare clic sul pulsante **Avanti**.
Verrà visualizzata la finestra **Contratto di licenza con l'utente finale e Informativa sulla privacy**.

4. Leggere le condizioni del criterio Contratto di licenza e dell'Informativa sulla privacy.
5. Se si accettano i termini e le condizioni del Contratto di licenza con l'utente finale e l'Informativa sulla privacy, selezionare le caselle di controllo **i termini e le condizioni del presente Contratto di licenza con l'utente finale e Informativa sulla privacy in cui viene descritta la gestione dei dati** per procedere con l'installazione.

Se non si accettano il Contratto di licenza con l'utente finale e/o l'Informativa sulla privacy, l'installazione verrà interrotta.

6. Fare clic sul pulsante **Avanti**.
Verrà visualizzata la finestra **Installazione personalizzata**.

7. Selezionare i componenti da installare.

Per impostazione predefinita, tutti i componenti di sicurezza di Kaspersky Embedded Systems Security 2.2 sono inclusi nel set di installazione raccomandato, ad eccezione del componente Gestione firewall.

Il componente di supporto del protocollo SNMP di Kaspersky Embedded Systems Security 2.2 comparirà nell'elenco dei componenti consigliati per l'installazione solo se il servizio SNMP di Microsoft Windows è installato nel computer.

8. Per annullare tutte le modifiche, fare clic sul pulsante **Reimposta** nella finestra **Installazione personalizzata**. Fare clic sul pulsante **Avanti**.
9. Nella finestra **Selezionare la cartella di destinazione**:
 - Se necessario, specificare una cartella in cui copiare i file di Kaspersky Embedded Systems Security 2.2.
 - Se necessario, esaminare le informazioni sullo spazio disponibile nelle unità locali facendo clic sul pulsante **Disco**.Fare clic sul pulsante **Avanti**.
10. Nella finestra **Impostazioni di installazione avanzate** configurare le seguenti impostazioni di installazione:
 - **Abilita la protezione in tempo reale dopo l'installazione dell'applicazione.**
 - **Aggiungi i file consigliati da Microsoft all'elenco di esclusioni.**
 - **Aggiungi i file consigliati da Kaspersky Lab all'elenco di esclusioni.**Fare clic sul pulsante **Avanti**.
11. Nella finestra **Importa impostazioni da file di configurazione** visualizzata:
 - a. Specificare il file di configurazione per importare le impostazioni di Kaspersky Embedded Systems Security 2.2 da un file di configurazione esistente creato in una versione precedente compatibile dell'applicazione.
 - b. Fare clic sul pulsante **Avanti**.
12. Nella finestra **Attivazione dell'applicazione** eseguire una delle seguenti operazioni:
 - Se si desidera attivare l'applicazione, specificare un file chiave di Kaspersky Embedded Systems Security 2.2 per l'attivazione dell'applicazione.
 - Se si desidera attivare l'applicazione in seguito, fare clic sul pulsante **Avanti**.
 - Se un file chiave è stato salvato in precedenza nella cartella \server del kit di distribuzione, il nome di

tale file sarà visualizzato nel campo **Chiave**.

Per aggiungere la chiave utilizzando un file chiave archiviato in un'altra cartella, specificare il file chiave.

Una volta aggiunto il file chiave, le informazioni sulla licenza saranno visualizzate nella finestra. Kaspersky Embedded Systems Security 2.2 visualizza la data calcolata di scadenza della licenza. Il periodo di validità della licenza inizia nel momento in cui si aggiunge una chiave e termina entro la data di scadenza del file chiave.

Fare clic sul pulsante **Avanti** per applicare la chiave nell'applicazione.

13. Nella finestra **Inizio dell'installazione** fare clic sul pulsante **Installa**. La procedura guidata avvierà l'installazione dei componenti di Kaspersky Embedded Systems Security 2.2.
14. Al termine dell'installazione, verrà visualizzata la finestra **Installazione completata**.
15. Selezionare la casella di controllo **Visualizza note sulla release** per visualizzare le informazioni sulla release al termine dell'Installazione guidata.
16. Fare clic su **OK**.

La finestra dell'Installazione guidata si chiuderà. Una volta completata l'installazione, Kaspersky Embedded Systems Security 2.2 è pronto per l'utilizzo se è stata aggiunta la chiave di attivazione.

Installazione della console di Kaspersky Embedded Systems Security 2.2

Seguire le istruzioni dell'Installazione guidata per modificare le impostazioni di installazione per la console dell'applicazione. Il processo di installazione può essere interrotto in qualsiasi passaggio della procedura guidata. A tale scopo, fare clic sul pulsante **Annulla** nella finestra dell'Installazione guidata.

► *Per installare la console dell'applicazione, eseguire le seguenti operazioni:*

1. Verificare che l'account utilizzato per avviare l'Installazione guidata sia incluso nel gruppo Administrators sul computer.
2. Eseguire il file setup.exe nel computer.
Verrà visualizzata la finestra iniziale.
3. Fare clic sul collegamento **Installa la console di Kaspersky Embedded Systems Security 2.2**.
Verrà visualizzata la finestra iniziale dell'Installazione guidata. Fare clic sul pulsante **Avanti**.
4. Leggere le condizioni del Contratto di licenza con l'utente finale e l'Informativa sulla privacy nella finestra visualizzata, quindi selezionare **i termini e le condizioni del presente Contratto di licenza con l'utente finale e Informativa sulla privacy in cui viene descritta la gestione dei dati** per procedere con l'installazione. Fare clic sul pulsante **Avanti**.
Verrà visualizzata la finestra **Impostazioni di installazione avanzate**.
5. Nella finestra **Impostazioni di installazione avanzate**:
 - Se si intende utilizzare la console dell'applicazione per gestire Kaspersky Embedded Systems Security 2.2 installato in un computer remoto, selezionare la casella di controllo **Consenti accesso remoto**.
 - Per aprire la finestra **Installazione personalizzata** e selezionare i componenti:
 - a. Fare clic sul pulsante **Avanzate**.
Verrà visualizzata la finestra **Installazione personalizzata**.

- b. Selezionare i componenti del set "Strumenti di amministrazione" dall'elenco.
Per impostazione predefinita, tutti i componenti sono installati.
- c. Fare clic sul pulsante **Avanti**.

Sono disponibili informazioni più dettagliate sui componenti di Kaspersky Embedded Systems Security 2.2 (vedere la sezione "Componenti software di Kaspersky Embedded Systems Security 2.2 e relativi codici per il servizio Windows Installer" a pagina [22](#)).

6. Nella finestra **Selezionare la cartella di destinazione**:
 - a. Se necessario, specificare una cartella diversa in cui devono essere salvati i file da installare.
 - b. Fare clic sul pulsante **Avanti**.
7. Nella finestra **Inizio dell'installazione** fare clic sul pulsante **Installa**.
La procedura guidata avvierà l'installazione dei componenti selezionati.
8. Fare clic su **OK**.

La finestra dell'Installazione guidata si chiuderà. La console dell'applicazione sarà installata in un computer protetto.

Se il set "Strumenti di amministrazione" è stato installato in un computer nella rete diverso dal computer protetto, modificare le impostazioni avanzate (vedere la sezione "Impostazioni avanzate dopo l'installazione della console dell'applicazione in un altro computer" a pagina [43](#)).

Impostazioni avanzate dopo l'installazione della console dell'applicazione in un altro computer

Se la console dell'applicazione è stata installata in un computer della rete diverso dal computer protetto, eseguire le operazioni descritte di seguito per consentire agli utenti di gestire Kaspersky Embedded Systems Security 2.2 in modalità remota:

- Aggiungere gli utenti di Kaspersky Embedded Systems Security 2.2 al gruppo Amministratori ESS nel computer protetto.
- Consentire le connessioni di rete per il servizio di gestione di Kaspersky Security (kavfsgt.exe) (vedere la sezione "Informazioni sulle autorizzazioni di accesso per il servizio di gestione di Kaspersky Security" a pagina [81](#)), se il computer protetto utilizza Windows Firewall o un firewall di terze parti.
- Se non si seleziona la casella di controllo **Consenti accesso remoto** durante l'installazione della console dell'applicazione in un computer con Microsoft Windows, è necessario consentire manualmente le connessioni di rete per la console dell'applicazione tramite il firewall del computer.

Autorizzazione delle connessioni di rete per la console dell'applicazione

I nomi delle impostazioni possono variare a seconda del sistema operativo Windows installato.

La console dell'applicazione nel computer remoto utilizza il protocollo DCOM per ricevere le informazioni sugli eventi di Kaspersky Embedded Systems Security 2.2 (ad esempio, oggetti esaminati, attività completate e così via) dal servizio di gestione di Kaspersky Security nel computer protetto. È necessario consentire le connessioni di rete per la console dell'applicazione nelle impostazioni di Windows Firewall perché possano essere stabilite le connessioni

tra la console dell'applicazione e il servizio di gestione di Kaspersky Security.

Nel computer remoto in cui è installata la console dell'applicazione eseguire le seguenti operazioni:

- Verificare che l'accesso remoto anonimo alle applicazioni COM sia consentito (ma non l'avvio e l'attivazione remoti delle applicazioni COM).
- In Windows Firewall aprire la porta TCP 135 e consentire le connessioni di rete per il file eseguibile del processo di gestione remota di Kaspersky Embedded Systems Security 2.2, kavfsrcn.exe.

Il computer client in cui è installata la console dell'applicazione utilizza la porta TCP 135 per accedere al computer protetto e per ricevere una risposta dal computer.

- Configurare la regola in uscita di Windows Firewall per l'autorizzazione della connessione.

A differenza dei servizi TCP/IP e UDP/IP tradizionali in cui un singolo protocollo ha una porta prefissata, DCOM assegna le porte in modo dinamico per gli oggetti COM remoti. Se è presente un firewall tra il client (in cui è installata la console dell'applicazione) e l'endpoint DCOM (il server protetto), è necessario aprire un ampio intervallo di porte.

Gli stessi passaggi devono essere applicati per la configurazione di qualsiasi altro firewall software o hardware.

Se la console dell'applicazione è stata aperta mentre era in corso la configurazione della connessione tra il computer protetto e il computer in cui è installata la console, chiudere la console dell'applicazione, attendere il completamento del processo di gestione remota di Kaspersky Embedded Systems Security 2.2 (kavfsrcn.exe) e riavviare la console dell'applicazione. Vengono applicate le nuove impostazioni di connessione.

► *Per consentire l'accesso remoto anonimo alle applicazioni COM, eseguire le seguenti operazioni:*

1. Nel computer remoto in cui è installata la console di Kaspersky Embedded Systems Security 2.2 aprire la console Servizi componenti.
2. Selezionare **Start > Esegui**.
3. Immettere il comando `dcomcnfg`.
4. Fare clic su **OK**.
5. Espandere il nodo **Computer** nella console **Servizi componenti** sul computer.
6. Aprire il menu di scelta rapida del nodo **Computer locale**.
7. Selezionare **Proprietà**.
8. Nella scheda **Sicurezza COM** della finestra **Proprietà** fare clic sul pulsante **Modifica limiti** nel gruppo di impostazioni **Autorizzazioni di accesso**.
9. Verificare che la casella di controllo **Consenti accesso remoto** sia selezionata per l'utente **ACCESSO ANONIMO** nella finestra **Consenti accesso remoto**.
10. Fare clic su **OK**.

► *Per aprire la porta TCP 135 in Windows Firewall e consentire le connessioni di rete per il file eseguibile del processo di gestione remota di Kaspersky Embedded Systems Security 2.2:*

1. Chiudere la console di Kaspersky Embedded Systems Security 2.2 nel computer remoto.

2. Eseguire una delle seguenti operazioni:
 - In Microsoft Windows XP o Microsoft Windows Vista®:
 - a. In Microsoft Windows XP SP2 o versioni successive selezionare **Start > Windows Firewall**.
In Microsoft Windows Vista selezionare **Start > Pannello di controllo > Windows Firewall** e nella finestra **Windows Firewall** selezionare il comando **Cambia impostazioni**.
 - b. Nella finestra Windows Firewall (o Impostazioni di Windows Firewall) fare clic sul pulsante **Aggiungi porta** nella scheda **Esclusioni**.
 - c. Nel campo **Nome** specificare il nome della porta RPC (TCP/135) o immettere un altro nome, ad esempio Kaspersky Embedded Systems Security 2.2 DCOM, e specificare il numero di porta (135) nel campo **Nome porta**.
 - d. Selezionare il protocollo **TCP**.
 - e. Fare clic su **OK**.
 - f. Fare clic sul pulsante **Aggiungi** nella scheda **Esclusioni**.
 - In Microsoft Windows 7 o versione successiva:
 - a. Selezionare **Start > Pannello di controllo > Windows Firewall**.
 - b. Nella finestra **Windows Firewall** selezionare **Consenti programma o funzionalità con Windows Firewall**.
 - c. Nella finestra **Consenti ai programmi di comunicare con Windows Firewall** fare clic sul pulsante **Consenti un altro programma...**
3. Specificare il file kavfsrnc.exe nella finestra **Aggiungi programma**. Questo file è disponibile nella cartella specificata come cartella di destinazione durante l'installazione della console di Kaspersky Embedded Systems Security 2.2 tramite Microsoft Management Console.
4. Fare clic su **OK**.
5. Fare clic sul pulsante **OK** nella finestra **Windows Firewall (o Impostazioni di Windows Firewall)**.

► *Aggiungere una regola in uscita di Windows Firewall:*

1. Selezionare **Start > Pannello di controllo > Windows Firewall**.
2. Nella finestra **Windows Firewall** fare clic sul collegamento **Impostazioni avanzate**.
Verrà visualizzata la finestra **Windows Firewall con sicurezza avanzata**.
3. Selezionare il nodo figlio **Regole in uscita**.
4. Fare clic sull'opzione **Nuova regola** nel riquadro **Azioni**.
5. Nella finestra **Creazione guidata nuova regola connessioni in uscita** visualizzata selezionare l'opzione **Porta** e fare clic su **Avanti**.
6. Selezionare il protocollo **TCP**.
7. Nel campo **Porte remote specifiche** specificare il seguente intervallo di porte per consentire le connessioni in uscita: 1024-65535.
8. Nella finestra **Azione** selezionare l'opzione **Consenti la connessione**.
9. Salvare la nuova regola e chiudere la finestra **Windows Firewall con sicurezza avanzata**.

Windows Firewall consentirà le connessioni di rete tra la console dell'applicazione e il servizio di gestione di Kaspersky Security.

Azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 avvia le attività di protezione e scansione subito dopo l'installazione se è stata attivata l'applicazione. Se è stata selezionata l'opzione predefinita **Abilita la protezione in tempo reale dopo l'installazione dell'applicazione** durante l'installazione di Kaspersky Embedded Systems Security 2.2, l'applicazione esamina gli oggetti del file system dei computer al momento dell'accesso. Kaspersky Embedded Systems Security 2.2 eseguirà l'attività Scansione aree critiche ogni venerdì alle 20:00.

È consigliabile eseguire le seguenti operazioni dopo l'installazione di Kaspersky Embedded Systems Security 2.2:

- Avviare l'attività Aggiornamento database dell'applicazione. Dopo l'installazione, Kaspersky Embedded Systems Security 2.2 esaminerà gli oggetti utilizzando il database incluso nel kit di distribuzione dell'applicazione.

È consigliabile aggiornare immediatamente i database di Kaspersky Embedded Systems Security 2.2 poiché potrebbero non essere aggiornati.

L'applicazione aggiornerà quindi i database ogni ora in base alla pianificazione predefinita configurata nell'attività.

- Eseguire una Scansione aree critiche del computer se nel computer protetto non era installato alcun software anti-virus con protezione dei file in tempo reale prima dell'installazione di Kaspersky Embedded Systems Security 2.2.
- Configurare le notifiche per l'amministratore degli eventi di Kaspersky Embedded Systems Security 2.2.

In questa sezione

Avvio e configurazione dell'attività di aggiornamento dei database di Kaspersky Embedded Systems Security 2.2	46
Scansione aree critiche	48

Avvio e configurazione dell'attività di aggiornamento dei database di Kaspersky Embedded Systems Security 2.2

► *Per aggiornare il database dell'applicazione dopo l'installazione, procedere come segue:*

1. Nelle impostazioni dell'attività Aggiornamento database configurare una connessione con una sorgente degli aggiornamenti: Server degli aggiornamenti HTTP o FTP di Kaspersky Lab.
2. Avviare l'attività Aggiornamento database.

► *Per configurare la connessione con i server di aggiornamento di Kaspersky Lab, nell'attività Aggiornamento database:*

1. Avviare la console dell'applicazione in uno dei seguenti modi:
 - Aprire la console dell'applicazione nel computer protetto. A tale scopo, selezionare **Start > Programmi > Kaspersky Embedded Systems Security 2.2 > Strumenti di amministrazione > Console di Kaspersky Embedded Systems Security 2.2.**

- Se la console dell'applicazione non è stata avviata in un computer protetto, stabilire la connessione al computer protetto:
 - a. Aprire il menu di scelta rapida del nodo **Kaspersky Embedded Systems Security** nell'albero della console dell'applicazione.
 - b. Selezionare l'elemento **Connetti a un altro computer**.
 - c. Nella finestra **Seleziona computer** selezionare **Altro computer** e indicare nel campo di testo il nome di rete del computer protetto.

Se l'account utilizzato per accedere a Microsoft Windows non dispone delle autorizzazioni di accesso per il servizio di gestione di Kaspersky Security (vedere la sezione "Informazioni sulle autorizzazioni di accesso per il servizio di gestione di Kaspersky Security" a pagina [81](#)), indicare un account che dispone delle autorizzazioni richieste.

Verrà visualizzata la finestra della console dell'applicazione.

2. Nell'albero della console dell'applicazione espandere il nodo **Aggiornamento**.
3. Selezionare il nodo figlio **Aggiornamento database**.
4. Fare clic sul collegamento **Proprietà** nel riquadro dei dettagli.
5. Nella finestra **Impostazioni attività** visualizzata aprire la scheda **Impostazioni di connessione**.
6. Eseguire le seguenti operazioni:
 - a. Se nella rete non è configurato il protocollo WPAD (Web Proxy Auto-Discovery) per rilevare automaticamente le impostazioni del server proxy nella rete LAN, specificare le impostazioni del server proxy: nella sezione **Impostazioni del server proxy** selezionare la casella di controllo **Usa le impostazioni del server proxy specificate**, immettere l'indirizzo nel campo **Indirizzo** e immettere il numero di porta per il server proxy nel campo **Porta**.
 - b. Se la rete richiede l'autenticazione per l'accesso al server proxy, selezionare il metodo di autenticazione necessario nell'elenco a discesa della sezione **Impostazioni di autenticazione del server proxy**:
 - **Usa l'autenticazione NTLM** se il server proxy supporta l'autenticazione NTLM predefinita di Microsoft Windows. Kaspersky Embedded Systems Security 2.2 utilizzerà l'account utente specificato nelle impostazioni dell'attività per l'accesso al server proxy. Per impostazione predefinita, l'attività verrà eseguita con l'account utente **Sistema locale (SYSTEM)**.
 - **Usa l'autenticazione NTLM con nome utente e password** se il server proxy supporta l'autenticazione NTLM predefinita di Microsoft Windows. Kaspersky Embedded Systems Security 2.2 utilizzerà l'account specificato per l'accesso al server proxy. Immettere un nome utente e una password o selezionare un utente dall'elenco.
 - **Applica nome utente e password** per selezionare l'autenticazione di base. Immettere un nome utente e una password o selezionare un utente dall'elenco.
7. Fare clic su **OK** nella finestra **Impostazioni attività**.

Le impostazioni per la connessione alla sorgente degli aggiornamenti nell'attività **Aggiornamento database** verranno salvate.

► *Per eseguire l'attività **Aggiornamento database**:*

1. Nell'albero della console dell'applicazione espandere il nodo **Aggiornamento**.
2. Nel menu di scelta rapida del nodo figlio **Aggiornamento database** selezionare l'elemento **Avvia**.

Verrà avviata l'attività **Aggiornamento database**.

Dopo il completamento dell'attività, è possibile visualizzare la data di rilascio degli ultimi aggiornamenti del database installati nel riquadro dei dettagli del nodo **Kaspersky Embedded Systems Security**.

Scansione aree critiche

Dopo avere aggiornato i database di Kaspersky Embedded Systems Security 2.2, esaminare il computer alla ricerca di malware utilizzando l'attività Scansione aree critiche.

► *Per eseguire l'attività Scansione aree critiche, eseguire le seguenti operazioni:*

1. Espandere il nodo **Scansione su richiesta** nell'albero della console dell'applicazione.
2. Nel menu di scelta rapida del nodo figlio **Scansione aree critiche** selezionare il comando **Avvia**.

L'attività verrà avviata e nell'area di lavoro sarà visualizzato lo stato dell'attività **In esecuzione**.

► *Per visualizzare il log dell'attività:*

Nel riquadro dei dettagli del nodo **Scansione aree critiche** fare clic sul collegamento **Apri log**.

Modifica del set di componenti e ripristino di Kaspersky Embedded Systems Security 2.2

I componenti di Kaspersky Embedded Systems Security 2.2 possono essere aggiunti o rimossi. È necessario interrompere l'attività Protezione dei file in tempo reale prima di poter rimuovere il componente Protezione dei file in tempo reale. Negli altri casi, non è necessario interrompere l'attività Protezione dei file in tempo reale o il servizio di Kaspersky Security.

Se l'accesso alla gestione dell'applicazione è protetto tramite password, Kaspersky Embedded Systems Security 2.2 richiede la password quando si tenta di eliminare o modificare il set di componenti nel passaggio successivo dell'Installazione guidata.

► *Per modificare il set di componenti di Kaspersky Embedded Systems Security 2.2:*

1. Nel menu **Start** selezionare **Tutti i programmi > Kaspersky Embedded Systems Security 2.2 > Modifica o rimuovi**.

Verrà visualizzata la finestra **Modifica, ripristino o rimozione dell'installazione** dell'Installazione guidata.

2. Selezionare **Modifica set di componenti**. Fare clic sul pulsante **Avanti**.

Verrà visualizzata la finestra **Installazione personalizzata**.

3. Nella finestra **Installazione personalizzata**, nell'elenco dei componenti disponibili, selezionare i componenti che si desidera aggiungere a Kaspersky Embedded Systems Security 2.2 o rimuovere. A tale scopo, eseguire le seguenti operazioni:
 - Per modificare il set di componenti, fare clic sul pulsante accanto al nome del componente selezionato e nel menu di scelta rapida selezionare:
 - **Il componente verrà installato sul disco rigido locale** se si desidera installare un solo componente;
 - **Il componente e i relativi componenti secondari verranno installati sul disco rigido locale** se

si desidera installare un gruppo di componenti.

- Per rimuovere i componenti precedentemente installati, fare clic sul pulsante accanto al nome del componente selezionato e nel menu di scelta rapida selezionare **Il componente non sarà disponibile**.

Fare clic sul pulsante **Installa**.

4. Nella finestra **Inizio dell'installazione** confermare la modifica del set di componenti software facendo clic sul pulsante **Installa**.
5. Nella finestra visualizzata a completamento dell'installazione fare clic sul pulsante **OK**.

Il set di componenti di Kaspersky Embedded Systems Security 2.2 sarà modificato in base alle impostazioni specificate.

Se si verificano problemi durante l'esecuzione di Kaspersky Embedded Systems Security 2.2 (arresti anomali di Kaspersky Embedded Systems Security 2.2; arresti anomali o mancato avvio delle attività), è possibile tentare di ripristinare Kaspersky Embedded Systems Security 2.2. È possibile eseguire un ripristino salvando le impostazioni correnti di Kaspersky Embedded Systems Security 2.2 oppure è possibile selezionare un'opzione per ripristinare i valori predefiniti di tutte le impostazioni di Kaspersky Embedded Systems Security 2.2.

► *Per ripristinare Kaspersky Embedded Systems Security 2.2 dopo un arresto anomalo dell'applicazione o di un'attività, eseguire le seguenti operazioni:*

1. Nel menu **Start** selezionare **Tutti i programmi > Kaspersky Embedded Systems Security 2.2 > Modifica o rimuovi**.

Verrà visualizzata la finestra **Modifica, ripristino o rimozione** dell'Installazione guidata.

2. Selezionare **Ripristina componenti installati**. Fare clic sul pulsante **Avanti**.

Verrà visualizzata la finestra **Ripristina componenti installati**.

3. Nella finestra **Ripristina componenti installati** selezionare la casella di controllo **Ripristina le impostazioni consigliate dell'applicazione** se si desidera reimpostare le impostazioni dell'applicazione configurate e ripristinare le impostazioni predefinite di Kaspersky Embedded Systems Security 2.2. Fare clic sul pulsante **Installa**.

4. Nella finestra **Inizio del ripristino** confermare l'operazione di ripristino facendo clic sul pulsante **Installa**.

5. Nella finestra visualizzata al completamento dell'operazione di ripristino fare clic sul pulsante **OK**.

Kaspersky Embedded Systems Security 2.2 sarà ripristinato in base alle impostazioni specificate.

Disinstallazione tramite l'Installazione guidata

Questa sezione contiene istruzioni per la rimozione di Kaspersky Embedded Systems Security 2.2 e della console dell'applicazione da un computer protetto utilizzando l'Installazione guidata.

Disinstallazione di Kaspersky Embedded Systems Security 2.2

I nomi delle impostazioni possono variare nei diversi sistemi operativi Windows.

Kaspersky Embedded Systems Security 2.2 può essere disinstallato dal computer protetto utilizzando l'Installazione/Disinstallazione guidata.

Dopo la disinstallazione di Kaspersky Embedded Systems Security 2.2 da un computer protetto può essere necessario un riavvio. Il riavvio può essere rimandato.

La disinstallazione, il ripristino e l'installazione dell'applicazione tramite il pannello di controllo di Windows non sono disponibili, se il sistema operativo utilizza la funzionalità Controllo dell'account utente o se l'accesso all'applicazione è protetto tramite password.

Se l'accesso alla gestione dell'applicazione è protetto tramite password, Kaspersky Embedded Systems Security 2.2 richiede la password quando si tenta di eliminare o modificare il set di componenti nel passaggio successivo dell'Installazione guidata.

► *Per disinstallare Kaspersky Embedded Systems Security 2.2:*

1. Nel menu **Start** selezionare **Tutti i programmi > Kaspersky Embedded Systems Security 2.2 > Modifica o rimuovi**.

Verrà visualizzata la finestra **Modifica, ripristino o rimozione dell'installazione** dell'Installazione guidata.

2. Selezionare **Rimuovi componenti software**. Fare clic sul pulsante **Avanti**.

Verrà visualizzata la finestra **Impostazioni avanzate di disinstallazione dell'applicazione**.

3. Se necessario, nella finestra **Impostazioni avanzate di disinstallazione dell'applicazione**:

- a. Selezionare la casella di controllo **Esporta oggetti in quarantena** per fare in modo che Kaspersky Embedded Systems Security 2.2 esporti gli oggetti che sono stati messi in quarantena. La casella di controllo è deselezionata per impostazione predefinita.
- b. Selezionare la casella di controllo **Esporta oggetti in Backup** per esportare gli oggetti dal Backup di Kaspersky Embedded Systems Security 2.2. La casella di controllo è deselezionata per impostazione predefinita.
- c. Fare clic sul pulsante **Salva in** e selezionare la cartella in cui esportare gli oggetti ripristinati. Per impostazione predefinita, gli oggetti saranno esportati in %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Uninstall.

Fare clic sul pulsante **Avanti**.

4. Nella finestra **Inizio della disinstallazione** confermare la disinstallazione facendo clic sul pulsante **Disinstalla**.
5. Nella finestra visualizzata al completamento della disinstallazione fare clic sul pulsante **OK**.

Kaspersky Embedded Systems Security 2.2 sarà disinstallato da un computer protetto.

Disinstallazione della console di Kaspersky Embedded Systems Security 2.2

I nomi delle impostazioni possono variare nei diversi sistemi operativi Windows.

È possibile disinstallare la console dell'applicazione dal computer utilizzando l'Installazione/Disinstallazione guidata.

Una volta disinstallata la console dell'applicazione, non è necessario riavviare il computer.

► *Per disinstallare la console dell'applicazione:*

1. Nel menu **Start** selezionare **Tutti i programmi > Kaspersky Embedded Systems Security > Strumenti di amministrazione > Modifica o rimuovi**.
2. Verrà visualizzata la finestra **Modifica, ripristino o rimozione** della procedura guidata.
Selezionare **Rimuovi componenti software** e fare clic sul pulsante **Avanti**.
3. Verrà visualizzata la finestra **Inizio della disinstallazione**. Fare clic sul pulsante **Rimuovi**.
Verrà visualizzata la finestra **Disinstallazione completata**.
4. Fare clic su **OK**.

La rimozione sarà completata e l'installazione guidata verrà chiusa.

Installazione e disinstallazione dell'applicazione dalla riga di comando

Questa sezione descrive i particolari dell'installazione e della disinstallazione di Kaspersky Embedded Systems Security 2.2 dalla riga di comando. Vengono inoltre forniti esempi di comandi per installare e disinstallare Kaspersky Embedded Systems Security 2.2 dalla riga di comando ed esempi di comandi per aggiungere e rimuovere i componenti di Kaspersky Embedded Systems Security 2.2 dalla riga di comando.

In questa sezione

Informazioni sull'installazione e la disinstallazione di Kaspersky Embedded Systems Security 2.2 dalla riga di comando	51
Comandi di esempio per l'installazione di Kaspersky Embedded Systems Security 2.2	52
Azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2	53
Aggiunta/rimozione di componenti. Comandi di esempio	54
Disinstallazione di Kaspersky Embedded Systems Security 2.2. Comandi di esempio.....	55
Codici restituiti.....	55

Informazioni sull'installazione e la disinstallazione di Kaspersky Embedded Systems Security 2.2 dalla riga di comando

Kaspersky Embedded Systems Security 2.2 può essere installato o disinstallato e i relativi componenti possono essere aggiunti o rimossi eseguendo i file del pacchetto di installazione `\product\ess_x86(x64).msi` dalla riga di comando dopo che le impostazioni di installazione sono state specificate utilizzando chiavi.

Il set "Strumenti di amministrazione" può essere installato nel computer protetto o in un altro computer della rete per l'utilizzo con la console dell'applicazione in locale o in remoto. A tale scopo, utilizzare il pacchetto di installazione `\client\esstools.msi`.

Eseguire l'installazione utilizzando i diritti di un account incluso nel gruppo degli amministratori nel computer in cui è installata l'applicazione.

Se uno dei file `\product\ess_x86(x64).msi` è eseguito nel computer protetto senza chiavi di riserva, Kaspersky Embedded Systems Security 2.2 verrà installato con le impostazioni di installazione consigliate.

Il set di componenti da installare può essere assegnato utilizzando l'opzione della riga di comando `ADDLOCAL` ed elencando i codici per i componenti o i set di componenti selezionati.

Comandi di esempio per l'installazione di Kaspersky Embedded Systems Security 2.2

Questa sezione fornisce esempi di comandi utilizzati per installare Kaspersky Embedded Systems Security 2.2.

Nei computer che eseguono una versione a 32 bit di Microsoft Windows eseguire i file con il suffisso `x86` nel kit di distribuzione. Nei computer che eseguono una versione a 64 bit di Microsoft Windows eseguire i file con il suffisso `x64` nel kit di distribuzione.

Informazioni dettagliate sull'utilizzo dei comandi standard di Windows Installer e sulle opzioni della riga di comando sono disponibili nella documentazione fornita da Microsoft.

Esempi per l'installazione di Kaspersky Embedded Systems Security 2.2 dal file `setup.exe`

- Per installare Kaspersky Embedded Systems Security 2.2 con le impostazioni di installazione consigliate senza interazione con l'utente, eseguire il seguente comando:

```
\product\setup.exe /s/p EULA=1 PRIVACYPOLICY=1
```

- Per installare Kaspersky Embedded Systems Security 2.2 con le seguenti impostazioni:

- installare solo i componenti Protezione dei file in tempo reale e Scansione su richiesta;
- non eseguire Protezione in tempo reale durante l'avvio di Kaspersky Embedded Systems Security 2.2;
- non escludere dalla scansione i file che Microsoft Corporation consiglia di escludere;

eseguire il seguente comando:

```
\product\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

Esempi di comandi utilizzati per l'installazione: esecuzione del file `.msi` di un pacchetto di installazione

- Per installare Kaspersky Embedded Systems Security 2.2 con le impostazioni di installazione consigliate senza interazione con l'utente, eseguire il seguente comando:

```
msiexec /i ess.msi /qn EULA=1 PRIVACYPOLICY=1
```

- ▶ Per installare Kaspersky Embedded Systems Security 2.2 con le impostazioni di installazione consigliate e visualizzare l'interfaccia di installazione, eseguire il seguente comando:

```
msiexec /i ess.msi /qf EULA=1 PRIVACYPOLICY=1
```

- ▶ Per installare Kaspersky Embedded Systems Security 2.2 eseguendo l'attivazione tramite il file chiave C:\0000000A.key:

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1  
PRIVACYPOLICY=1
```

- ▶ Per installare Kaspersky Embedded Systems Security 2.2 con una scansione preliminare dei processi attivi e dei settori di avvio dei dischi locali, eseguire il seguente comando:

```
msiexec /i ess.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

- ▶ Per installare Kaspersky Embedded Systems Security 2.2 salvandone i file nella cartella di destinazione C:\ESS, eseguire il seguente comando:

```
msiexec /i ess.msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
```

- ▶ Per installare Kaspersky Embedded Systems Security 2.2 e salvare il file di log dell'installazione con il nome ess.log nella cartella in cui è memorizzato il file msi del pacchetto di installazione di Kaspersky Embedded Systems Security 2.2, eseguire il seguente comando:

```
msiexec /i ess.msi /l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
```

- ▶ Per installare la console di Kaspersky Embedded Systems Security 2.2, eseguire il seguente comando:

```
msiexec /i esstools.msi /qn EULA=1 PRIVACYPOLICY=1
```

- ▶ Per installare Kaspersky Embedded Systems Security 2.2 eseguendo l'attivazione tramite il file chiave C:\0000000A.key, configurare Kaspersky Embedded Systems Security 2.2 in base alle impostazioni descritte nel file di configurazione C:\settings.xml ed eseguire il seguente comando:

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key  
CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

- ▶ Per installare la patch dell'applicazione quando Kaspersky Embedded Systems Security 2.2 è protetto tramite password, eseguire il seguente comando:

```
msiexec /p "<nome e percorso msp>" UNLOCK_PASSWORD=<password>
```

Azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 avvia le attività di protezione e scansione subito dopo l'installazione se è stata attivata l'applicazione. Se è stata selezionata l'opzione **Abilita la protezione in tempo reale dopo**

l'installazione dell'applicazione durante l'installazione di Kaspersky Embedded Systems Security 2.2, l'applicazione esamina gli oggetti del file system del computer al momento dell'accesso. Kaspersky Embedded Systems Security 2.2 eseguirà l'attività Scansione aree critiche ogni venerdì alle 20:00.

È consigliabile eseguire le seguenti operazioni dopo l'installazione di Kaspersky Embedded Systems Security 2.2:

- Avviare l'attività di aggiornamento dei database di Kaspersky Embedded Systems Security 2.2. Dopo l'installazione, Kaspersky Embedded Systems Security 2.2 esaminerà gli oggetti utilizzando il database incluso nel kit di distribuzione. È consigliabile aggiornare immediatamente il database di Kaspersky Embedded Systems Security 2.2. A tale scopo, è necessario eseguire l'attività Aggiornamento database. Il database sarà quindi aggiornato ogni ora in base alla pianificazione predefinita.

È ad esempio possibile eseguire l'attività Aggiornamento database eseguendo il seguente comando:

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456
```

In questo caso, gli aggiornamenti dei database di Kaspersky Embedded Systems Security 2.2 vengono scaricati dai server di aggiornamento di Kaspersky Lab. La connessione a una sorgente degli aggiornamenti viene stabilita tramite un server proxy (indirizzo del server proxy: proxy.company.com, porta: 8080) utilizzando l'autenticazione NTLM predefinita di Windows per l'accesso al server con un account (nome utente: inetuser; password: 123456).

- Eseguire una Scansione aree critiche del computer se nel computer protetto non era installato alcun software anti-virus con protezione dei file in tempo reale prima dell'installazione di Kaspersky Embedded Systems Security 2.2.

► *Per avviare l'attività Scansione aree critiche tramite la riga di comando:*

```
KAVSHELL SCANCritical /W:scancritical.log
```

Questo comando salva il log dell'attività in un file denominato scancritical.log contenuto nella cartella corrente.

- Configurare le notifiche per l'amministratore degli eventi di Kaspersky Embedded Systems Security 2.2.

Aggiunta/rimozione di componenti. Comandi di esempio

Il componente Controllo dell'avvio delle applicazioni viene installato automaticamente. Non è necessario specificarlo nell'elenco dei valori della chiave ADDLOCAL aggiungendo o eliminando i componenti di Kaspersky Embedded Systems Security 2.2.

► *Per aggiungere il componente Scansione su richiesta a componenti già installati, eseguire il seguente comando:*

```
msiexec /i ess.msi ADDLOCAL=Oas,Ods /qn
```

oppure

```
\server\setup.exe /s /p "ADDLOCAL=Oas,Ods"
```

Se si enumerano i componenti da installare insieme ai componenti già installati, Kaspersky Embedded Systems Security 2.2 reinstallerà i componenti esistenti.

- Per rimuovere i componenti installati eseguire il comando seguente:

```
msiexec /i ess.msi "ADDLOCAL=Oas,AppCntrl,Ksn,AntiExploit,DevCtrl,Firewall,LogInspector,AKIntegration,PerfMonCounters,SnmpSupport,Shell,TrayApp,AVProtection,RamDisk REMOVE=Ods,Fim" /qn
```

Disinstallazione di Kaspersky Embedded Systems Security 2.2. Comandi di esempio

- Per disinstallare Kaspersky Embedded Systems Security 2.2 dal computer protetto, eseguire il seguente comando:

```
msiexec /x ess.msi /qn
```

oppure

- Per sistemi operativi a 32 bit:

```
msiexec /x {D8279E25-E44F-4164-8651-10123E2E30EA} /qn
```

- Per sistemi operativi a 64 bit:

```
msiexec /x {E8584EDC-0675-4784-96E5-FD10C26A613E} /qn
```

- Per disinstallare la console di Kaspersky Embedded Systems Security 2.2, eseguire il seguente comando:

```
msiexec /x esstools.msi /qn
```

oppure

- Per sistemi operativi a 32 bit:

```
msiexec /x {A727008F-F8CC-4B35-848A-1AECCEF22178} /qn
```

- Per sistemi operativi a 64 bit:

```
msiexec /x {D978C311-2D2D-41A3-8158-BDF97149CCD4} /qn
```

- Per disinstallare Kaspersky Embedded Systems Security 2.2 da un computer protetto in cui è abilitata la protezione tramite password, eseguire il comando seguente:

- Per sistemi operativi a 32 bit:

```
msiexec /x {D8279E25-E44F-4164-8651-10123E2E30EA} UNLOCK_PASSWORD=*** /qn
```

- Per sistemi operativi a 64 bit:

```
msiexec /x {E8584EDC-0675-4784-96E5-FD10C26A613E} UNLOCK_PASSWORD=*** /qn
```

Codici restituiti

La tabella di seguito contiene un elenco di codici restituiti della riga di comando.

Tabella 13. Codici restituiti

Codice	Descrizione
1324	Il nome della cartella di destinazione contiene caratteri non validi.
25001	Diritti insufficienti per installare Kaspersky Embedded Systems Security 2.2. Per installare l'applicazione, avviare l'installazione guidata con diritti di amministratore locale.
25003	Kaspersky Embedded Systems Security 2.2 non può essere installato nei computer che eseguono questa versione di Microsoft Windows. Avviare l'installazione guidata per le versioni a 64 bit di Microsoft Windows.
25004	Rilevato software incompatibile. Per continuare l'installazione, disinstallare il seguente software: <elenco di software incompatibile>.
25010	Il percorso indicato non può essere utilizzato per salvare gli oggetti spostati in Quarantena.
25011	Il nome della cartella per il salvataggio degli oggetti spostati in Quarantena contiene caratteri non validi.
26251	Impossibile scaricare DLL dei contatori di performance
26252	Impossibile scaricare DLL dei contatori di performance
27300	Il driver non può essere installato.
27301	Il driver non può essere disinstallato.
27302	Il componente di rete non può essere installato. È stato raggiunto il numero massimo di dispositivi filtrati supportato.
27303	Database anti-virus non trovati.

Installazione e disinstallazione dell'applicazione tramite Kaspersky Security Center

Questa sezione contiene informazioni generali sull'installazione di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center. Vengono inoltre descritti come installare e disinstallare Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center e le azioni da eseguire dopo avere installato Kaspersky Embedded Systems Security 2.2.

In questa sezione

Informazioni generali sull'installazione tramite Kaspersky Security Center	57
Diritti per l'installazione o la disinstallazione di Kaspersky Embedded Systems Security 2.2	57
Procedura di installazione di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center	58
Azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2	59
Installazione della console dell'applicazione tramite Kaspersky Security Center	60
Disinstallazione di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center.....	60

Informazioni generali sull'installazione tramite Kaspersky Security Center

È possibile installare Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center utilizzando l'attività d'installazione remota.

Al termine dell'attività d'installazione remota, Kaspersky Embedded Systems Security 2.2 sarà installato con impostazioni identiche su vari computer.

È possibile unire tutti i computer in un gruppo di amministrazione solo e creare un'attività di gruppo per eseguire l'installazione di Kaspersky Embedded Systems Security 2.2 nei computer di questo gruppo.

È possibile creare un'attività per installare in remoto Kaspersky Embedded Systems Security 2.2 in un set di computer che non sono nello stesso gruppo di amministrazione. Durante la creazione di questa attività è necessario generare un elenco dei singoli computer in cui deve essere installato Kaspersky Embedded Systems Security 2.2.

Informazioni dettagliate sull'attività di installazione remota sono disponibili nella *Guida di Kaspersky Security Center*.

Diritti per l'installazione o la disinstallazione di Kaspersky Embedded Systems Security 2.2

L'account specificato nell'attività di installazione (rimozione) remota deve essere incluso nel gruppo Administrators in ciascuno dei computer protetti in tutti i casi tranne quelli descritti di seguito:

- Se Kaspersky Security Center Network Agent è già installato nei computer in cui deve essere installato Kaspersky Embedded Systems Security 2.2 (indipendentemente dal dominio in cui si trovano i computer e dal fatto che appartengano o meno a un dominio).

Se Network Agent non è ancora installato nei computer, è possibile installarlo con Kaspersky Embedded Systems Security 2.2 utilizzando un'attività di installazione remota. Prima di installare Network Agent, verificare che l'account che si desidera specificare nell'attività sia incluso nel gruppo Administrators in ciascuno dei computer.

- Tutti i computer in cui si desidera installare Kaspersky Embedded Systems Security 2.2 sono nello stesso dominio dell'Administration Server e l'Administration Server è registrato nell'account **Amministratore di dominio** (se questo account ha i diritti di amministratore locale sui computer nel dominio).

Per impostazione predefinita, quando si utilizza il metodo **Installazione forzata**, l'attività di installazione remota viene eseguita dall'account in cui è in esecuzione l'Administration Server.

Quando si lavora con attività di gruppo o con attività per set di computer nella modalità di installazione (disinstallazione) forzata, un account deve avere i diritti seguenti su un computer client:

- Diritto di eseguire le applicazioni in remoto.
- Diritti per la risorsa **Admin\$**.
- Diritto **Accesso come servizio**.

Procedura di installazione di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center

Informazioni dettagliate sulla generazione di un pacchetto di installazione e la creazione di un'attività di installazione remota sono disponibili nella Guida all'implementazione di Kaspersky Security Center.

Se si prevede di gestire Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center in futuro, verificare che le seguenti condizioni siano soddisfatte:

- Nel computer in cui è installato Kaspersky Security Center Administration Server è installato anche il plug-in di amministrazione (file \product\klcfginst.exe nel kit di distribuzione di Kaspersky Embedded Systems Security 2.2).
- Kaspersky Security Center Network Agent è installato nei computer protetti. Se Kaspersky Security Center Network Agent non è installato nei computer protetti, è possibile installarlo insieme a Kaspersky Embedded Systems Security 2.2 utilizzando un'attività di installazione remota.

I computer possono anche essere uniti in un gruppo di amministrazione per gestire successivamente le impostazioni di protezione tramite i criteri e le attività di gruppo di Kaspersky Security Center.

► *Per installare Kaspersky Embedded Systems Security 2.2 mediante l'attività di installazione remota:*

1. Avviare Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center espandere il nodo **Installazione remota** e nel nodo figlio **Pacchetti di installazione** selezionare l'opzione **Crea pacchetto di installazione per un'applicazione Kaspersky Lab**.
3. Immettere il nome del pacchetto di installazione.
4. Specificare il file ess.kud contenuto nel kit di distribuzione di Kaspersky Embedded Systems Security 2.2 come file del pacchetto di installazione.

Verrà visualizzata la finestra **Contratto di licenza con l'utente finale e Informativa sulla privacy**.

5. Se si accettano i termini e le condizioni del Contratto di licenza con l'utente finale e l'Informativa sulla privacy, selezionare le caselle di controllo **i termini e le condizioni del presente Contratto di licenza con l'utente finale e Informativa sulla privacy in cui viene descritta la gestione dei dati** per procedere con l'installazione.

Per procedere è necessario accettare il Contratto di licenza e l'Informativa sulla privacy.

6. Per modificare il set di componenti di Kaspersky Embedded Systems Security 2.2 da installare (vedere la sezione "Modifica del set di componenti e ripristino di Kaspersky Embedded Systems Security 2.2" a pagina [48](#)) e le impostazioni di installazione predefinite (vedere la sezione "Impostazioni di installazione e disinstallazione e opzioni della riga di comando per il servizio Windows Installer" a pagina [29](#)) nel pacchetto di installazione:
 - a. In Kaspersky Security Center espandere il nodo **Installazione remota**.
 - b. Nell'area di lavoro del nodo figlio **Pacchetti di installazione** aprire il menu di scelta rapida del pacchetto di installazione di Kaspersky Embedded Systems Security 2.2 creato e selezionare **Proprietà**.

- c. Nella finestra **Proprietà: <nome del pacchetto di installazione>**, nella sezione **Impostazioni**, eseguire le seguenti operazioni:
 - a. Nel gruppo di impostazioni **Componenti da installare** selezionare le caselle di controllo accanto ai nomi dei componenti di Kaspersky Embedded Systems Security 2.2 da installare.
 - b. Per indicare una cartella di destinazione diversa da quella predefinita, specificare il nome e il percorso della cartella nel campo **Cartella di destinazione**.
Il percorso della cartella di destinazione può contenere variabili di ambiente di sistema. Se la cartella non esiste nel computer, verrà creata.
 - c. Nel gruppo **Impostazioni di installazione avanzate** configurare le seguenti impostazioni:
 - Esegui una scansione anti-virus del computer prima dell'installazione.
 - Abilita la protezione in tempo reale dopo l'installazione dell'applicazione.
 - Aggiungi i file consigliati da Microsoft all'elenco di esclusioni.
 - d. Aggiungi i file consigliati da Kaspersky Lab all'elenco di esclusioni.
- d. Nella finestra di dialogo **Proprietà: <nome del pacchetto di installazione>** fare clic su **OK**.
7. Nel nodo **Pacchetti di installazione** creare un'attività per installare in remoto Kaspersky Embedded Systems Security 2.2 nei computer selezionati (gruppo di amministrazione). Configurare le impostazioni dell'attività.
Per ulteriori informazioni sulla creazione e sulla configurazione delle attività di installazione remota, vedere la *Guida di Kaspersky Security Center*.
8. Eseguire l'attività di installazione remota per Kaspersky Embedded Systems Security 2.2.
Kaspersky Embedded Systems Security 2.2 sarà installato nei computer specificati nell'attività.

Azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2

Dopo avere installato Kaspersky Embedded Systems Security 2.2, è consigliabile aggiornare i database di Kaspersky Embedded Systems Security 2.2 nei computer ed eseguire una Scansione aree critiche dei computer, se nei computer non era installata alcuna applicazione anti-virus con la funzione di Protezione in tempo reale abilitata prima dell'installazione di Kaspersky Embedded Systems Security 2.2.

Se i computer in cui è stato installato Kaspersky Embedded Systems Security 2.2 sono unificati in un singolo gruppo di amministrazione in Kaspersky Security Center, è possibile eseguire queste attività utilizzando i metodi seguenti:

1. Creare le attività Aggiornamento database per il gruppo di computer in cui è stato installato Kaspersky Embedded Systems Security 2.2. Impostare Kaspersky Security Center Administration Server come sorgente degli aggiornamenti.
2. Creare un'attività di gruppo Scansione su richiesta con lo stato Scansione aree critiche. Kaspersky Security Center valuta lo stato di sicurezza di ogni computer nel gruppo in base ai risultati dell'esecuzione di questa attività, non in base ai risultati dell'attività Scansione aree critiche.
3. Creare un nuovo criterio per il gruppo di computer. Nelle proprietà del criterio creato, nella scheda **Attività di sistema**, disattivare l'avvio pianificato delle attività di scansione del sistema in base alle esigenze e delle attività di aggiornamento database nei computer del gruppo di amministrazione.

È anche possibile configurare le notifiche per l'amministratore degli eventi di Kaspersky Embedded Systems Security 2.2.

Installazione della console dell'applicazione tramite Kaspersky Security Center

Informazioni dettagliate sulla creazione di un pacchetto di installazione e di un'attività di installazione remota sono disponibili nella *Guida all'implementazione di Kaspersky Security Center*.

► Per installare la console dell'applicazione mediante un'attività di installazione remota:

1. In Kaspersky Security Center Administration Console espandere il nodo **Installazione remota** e nel nodo figlio **Pacchetti di installazione** creare un nuovo pacchetto di installazione sulla base del file client\setup.exe. Durante la creazione di un nuovo pacchetto di installazione:
 - Nella finestra **Selezione del pacchetto di distribuzione per l'installazione** selezionare il file client\setup.exe dalla cartella del kit di distribuzione di Kaspersky Embedded Systems Security 2.2 e selezionare la casella di controllo **Copia aggiornamenti dall'archivio al pacchetto di installazione**.
 - Se richiesto, utilizzare l'opzione della riga di comando ADDLOCAL per modificare il set di componenti da installare nel campo **Impostazioni di avvio del file eseguibile (facoltativo)** e modificare la cartella di destinazione.

Ad esempio, per installare solo la console dell'applicazione nella cartella C:\KasperskyConsole senza installare il file della Guida e la documentazione, procedere come segue:

```
/s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1  
PRIVACYPOLICY=1"
```

2. Nel nodo **Pacchetti di installazione** creare un'attività per installare in remoto la console dell'applicazione nei computer selezionati (gruppo di amministrazione). Configurare le impostazioni dell'attività.

Per ulteriori informazioni sulla creazione e sulla configurazione delle attività di installazione remota, vedere la *Guida di Kaspersky Security Center*.

3. Eseguire l'attività di installazione remota creata.

La console dell'applicazione sarà installata nei computer specificati nell'attività.

Disinstallazione di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center

Se l'accesso alla gestione di Kaspersky Embedded Systems Security 2.2 nei computer della rete è protetto tramite password, immettere la password durante la creazione di un'attività di disinstallazione di più applicazioni. Se la protezione tramite password non è gestita a livello centralizzato dal criterio di Kaspersky Security Center, l'applicazione verrà disinstallata correttamente dai computer con accesso protetto in cui la password immessa corrisponde al valore impostato. Kaspersky Embedded Systems Security 2.2 non verrà disinstallato dai rimanenti computer.

► *Per disinstallare Kaspersky Embedded Systems Security 2.2, eseguire le seguenti operazioni in Kaspersky Security Center Administration Console:*

1. In Kaspersky Security Center Administration Console creare e avviare l'attività di rimozione dell'applicazione.
2. Nell'attività selezionare il metodo di disinstallazione (in modo analogo alla selezione del metodo di installazione illustrata nella sezione precedente) e specificare un account di cui Administration Server utilizzerà i diritti per gestire i computer. È possibile disinstallare Kaspersky Embedded Systems Security 2.2 solo con le impostazioni di disinstallazione predefinite (vedere la sezione "Impostazioni di installazione e disinstallazione e opzioni della riga di comando per il servizio Windows Installer" a pagina [29](#)).

Installazione e disinstallazione tramite i criteri di gruppo di Active Directory

Questa sezione descrive l'installazione e la disinstallazione di Kaspersky Embedded Systems Security 2.2 tramite i criteri di gruppo di Active Directory. Vengono inoltre fornite informazioni sulle azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2 tramite i criteri di gruppo.

In questa sezione

Installazione di Kaspersky Embedded Systems Security 2.2 tramite i criteri di gruppo di Active Directory.....	61
Azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2	62
Disinstallazione di Kaspersky Embedded Systems Security 2.2 tramite i criteri di gruppo di Active Directory.....	62

Installazione di Kaspersky Embedded Systems Security 2.2 tramite i criteri di gruppo di Active Directory

È possibile installare Kaspersky Embedded Systems Security 2.2 su vari computer tramite il criterio di gruppo di Active Directory. È possibile installare la console dell'applicazione nello stesso modo.

I computer in cui si desidera installare Kaspersky Embedded Systems Security 2.2 o la console dell'applicazione devono essere in un singolo dominio e un'unica unità organizzativa.

I sistemi operativi nei computer su cui si desidera installare Kaspersky Embedded Systems Security 2.2 mediante il criterio devono essere della stessa versione (32 bit o 64 bit).

È necessario disporre dei diritti di amministratore di dominio.

Per installare Kaspersky Embedded Systems Security 2.2, utilizzare i pacchetti di installazione `ess_x86(x64).msi`. Per installare la console dell'applicazione, utilizzare i pacchetti di installazione `esstools.msi`.

Informazioni dettagliate sull'utilizzo dei criteri di gruppo di Active Directory sono disponibili nella documentazione fornita da Microsoft.

► *Per installare Kaspersky Embedded Systems Security 2.2 (o la console dell'applicazione):*

1. Salvare il file msi del pacchetto di installazione che corrisponde alle dimensioni della parola (32 o 64 bit)

della versione installata del sistema operativo Microsoft Windows, nella cartella pubblica sul controller di dominio.

2. Nel controller di dominio creare un nuovo criterio per il gruppo a cui appartengono i computer.
3. Utilizzando l'**Editor oggetti Criteri di gruppo** creare un nuovo pacchetto di installazione nel nodo **Configurazione computer**. Specificare il percorso del file msi del pacchetto di installazione di Kaspersky Embedded Systems Security 2.2 (o della console dell'applicazione) nel formato UNC (Universal Naming Convention).
4. Selezionare la casella di controllo **Installa sempre con privilegi elevati** di Windows Installer, sia nel nodo **Configurazione computer** che nel nodo **Configurazione utente** del gruppo selezionato.
5. Applicare le modifiche con il comando `gpupdate / force`.

Kaspersky Embedded Systems Security 2.2 sarà installato nei computer del gruppo dopo il riavvio e prima dell'accesso a Microsoft Windows.

Azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2

Dopo avere installato Kaspersky Embedded Systems Security 2.2 nei computer protetti, è consigliabile aggiornare immediatamente i database dell'applicazione ed eseguire una Scansione aree critiche. È possibile eseguire queste azioni (vedere la sezione "Azioni da eseguire dopo l'installazione di Kaspersky Embedded Systems Security 2.2" a pagina [46](#)) dalla console dell'applicazione.

È anche possibile configurare le notifiche per l'amministratore degli eventi di Kaspersky Embedded Systems Security 2.2.

Disinstallazione di Kaspersky Embedded Systems Security 2.2 tramite i criteri di gruppo di Active Directory

Se è stata eseguita l'installazione di Kaspersky Embedded Systems Security 2.2 (o della console dell'applicazione) nei computer del gruppo utilizzando il criterio di gruppo di Active Directory, è possibile utilizzare questo criterio per disinstallare Kaspersky Embedded Systems Security 2.2 (o la console dell'applicazione).

È possibile disinstallare l'applicazione solo con i parametri di disinstallazione predefiniti.

Informazioni dettagliate sull'utilizzo dei criteri di gruppo di Active Directory sono disponibili nella documentazione fornita da Microsoft.

Se l'accesso alla gestione dell'applicazione è protetto tramite password, la disinstallazione di Kaspersky Embedded Systems Security 2.2 tramite i criteri di gruppo di Active Directory non è disponibile.

► *Per disinstallare Kaspersky Embedded Systems Security 2.2 (o la console dell'applicazione):*

1. Selezionare l'unità organizzativa nel controller di dominio dai cui computer si desidera eliminare Kaspersky Embedded Systems Security 2.2 o la console dell'applicazione.
2. Selezionare il criterio creato per l'installazione di Kaspersky Embedded Systems Security 2.2 e in **Editor**

oggetti Criteri di gruppo, nel nodo **Installazione software (Configurazione computer > Configurazione programma > Installazione software)** aprire il menu di scelta rapida del pacchetto di installazione di Kaspersky Embedded Systems Security 2.2 (o della console dell'applicazione) e selezionare il comando **Tutte le attività > Rimuovi**.

3. Selezionare il metodo di rimozione **Disinstalla immediatamente il software per utenti e computer**.
4. Applicare le modifiche con il comando `gpupdate / force`.

Kaspersky Embedded Systems Security 2.2 viene rimosso dai computer dopo il riavvio e prima dell'accesso a Microsoft Windows.

Verifica delle funzioni di Kaspersky Embedded Systems Security 2.2. Utilizzo del virus di prova EICAR

Questa sezione descrive il virus di prova EICAR e come utilizzarlo per verificare le funzionalità Protezione in tempo reale e Scansione su richiesta di Kaspersky Embedded Systems Security 2.2.

In questa sezione

Informazioni sul virus di prova EICAR	63
Test di Protezione in tempo reale e Scansione su richiesta	64

Informazioni sul virus di prova EICAR

Il virus di prova è progettato per verificare il funzionamento delle applicazioni anti-virus. È stato sviluppato da EICAR (European Institute for Computer Antivirus Research).

Il virus di prova non è un virus e non contiene codice di programma per il computer, tuttavia le applicazioni anti-virus della maggior parte dei produttori lo identificano come una minaccia.

Il file che contiene questo virus di prova è denominato `eicar.com`. È possibile scaricarlo dal sito Web di EICAR http://www.eicar.org/anti_virus_test_file.htm.

Prima di salvare il file in una cartella sul disco rigido del computer, verificare che Protezione dei file in tempo reale su tale unità sia disabilitata.

Il file `eicar.com` contiene una riga di testo. Durante la scansione del file, Kaspersky Embedded Systems Security 2.2 rileva una minaccia in questa riga di testo, assegna al file lo stato **Infetto** e lo elimina. Le informazioni sulla minaccia rilevata nel file verranno visualizzate nella console dell'applicazione e nel log delle attività.

È possibile utilizzare il file `eicar.com` per verificare in che modo Kaspersky Embedded Systems Security 2.2 disinfetta gli oggetti infetti e rileva gli oggetti potenzialmente infetti. A tale scopo, aprire il file utilizzando un editor di testo, aggiungere uno dei prefissi elencati nella tabella di seguito all'inizio della riga di testo nel file e salvare il file

con un nuovo nome, ad esempio eicar_cure.com.

Per assicurarsi che Kaspersky Embedded Systems Security 2.2 elabori il file eicar.com con un prefisso, nella sezione delle impostazioni di sicurezza **Protezione degli oggetti** impostare il valore **Tutti gli oggetti** per le attività Protezione dei file in tempo reale e Scansione su richiesta di Kaspersky Embedded Systems Security 2.2.

Tabella 14. Prefissi nei file EICAR

Prefisso	Stato del file dopo la scansione e l'azione di Kaspersky Embedded Systems Security 2.2
Nessun prefisso	Kaspersky Embedded Systems Security 2.2 assegna all'oggetto lo stato Infetto e lo elimina.
SUSP-	Kaspersky Embedded Systems Security 2.2 assegna all'oggetto (rilevato dall'analizzatore euristico) lo stato Potenzialmente infetto e lo elimina (gli oggetti potenzialmente infetti non vengono disinfettati).
WARN-	Kaspersky Embedded Systems Security 2.2 assegna all'oggetto lo stato Potenzialmente infetto (il codice dell'oggetto corrisponde parzialmente al codice di una minaccia nota) e lo elimina (gli oggetti potenzialmente infetti non vengono disinfettati).
CURE-	Kaspersky Embedded Systems Security 2.2 assegna all'oggetto lo stato Infetto e lo disinfetta. Se la disinfezione va a buon fine, l'intero testo nel file viene sostituito con la parola "CURE".

Test di Protezione in tempo reale e Scansione su richiesta

Dopo avere installato Kaspersky Embedded Systems Security 2.2, è possibile verificare che Kaspersky Embedded Systems Security 2.2 individui gli oggetti che contengono codice dannoso. Per eseguire la verifica, è possibile utilizzare un virus di prova di EICAR (vedere la sezione "Informazioni sul virus di prova EICAR" a pagina 63).

► Per verificare la funzionalità Protezione in tempo reale, eseguire le seguenti operazioni:

1. Scaricare il file eicar.com dal sito Web EICAR http://www.eicar.org/anti_virus_test_file.htm. Salvarlo nella cartella pubblica sull'unità locale di qualsiasi computer della rete.

Prima di salvare il file nella cartella, verificare che la funzionalità Protezione dei file in tempo reale sia disabilitata nella cartella.

2. Se si desidera verificare il funzionamento delle notifiche di rete per l'utente, assicurarsi che il servizio Messenger di Microsoft Windows sia abilitato nel computer protetto e nel computer in cui è stato salvato il file eicar.com.
3. Aprire la console dell'applicazione.
4. Copiare il file eicar.com salvato nell'unità locale del computer protetto utilizzando uno dei seguenti metodi:
 - Per testare le notifiche tramite la finestra Servizi terminal, copiare il file eicar.com nel computer dopo avere eseguito la connessione al computer mediante l'utilità Connessione Desktop remoto.
 - Per testare le notifiche attraverso il Servizio Messenger di Microsoft Windows, utilizzare le posizioni di rete del computer per copiare il file eicar.com dal computer in cui è stato salvato.

Protezione dei file in tempo reale funziona correttamente se le seguenti condizioni sono soddisfatte:

- Il file eicar.com è stato eliminato dal computer protetto.
- Nella console dell'applicazione al log delle attività è stato assegnato lo stato **Critico**. Nel log è stata aggiunta una riga con informazioni su una minaccia nel file eicar.com. Per visualizzare il log delle attività, nell'albero della console dell'applicazione espandere il nodo **Protezione del computer in tempo reale**, selezionare l'attività Protezione dei file in tempo reale e nel riquadro dei dettagli del nodo fare clic sul collegamento **Apri log**.
- Nel computer da cui è stato copiato il file sarà visualizzato un messaggio del servizio Messenger di Microsoft Windows, come segue: `Kaspersky Embedded Systems Security 2.2 ha bloccato l'accesso a <percorso del file nel computer> \eicar.com nel computer <nome di rete del computer> alle <ora in cui si è verificato l'evento>. Motivo: minaccia rilevata. Virus: EICAR-Test-File. Nome utente: <nome utente>. Nome computer: <nome di rete del computer da cui è stato copiato il file>.`

Verificare che il servizio Messenger di Microsoft Windows sia funzionante nel computer da cui è stato copiato il file eicar.com.

► Per verificare la funzionalità Scansione su richiesta, eseguire le seguenti operazioni:

1. Scaricare il file eicar.com dal sito Web di EICAR http://www.eicar.org/anti_virus_test_file.htm. Salvarlo nella cartella pubblica sull'unità locale di qualsiasi computer della rete.

Prima di salvare il file nella cartella, verificare che la funzionalità Protezione dei file in tempo reale sia disabilitata nella cartella.

2. Aprire la console dell'applicazione.
3. Eseguire le seguenti operazioni:
 - a. Espandere il nodo **Scansione su richiesta** nell'albero della console dell'applicazione.
 - b. Selezionare il nodo figlio **Scansione aree critiche**.
 - c. Nella scheda **Impostazioni ambito della scansione** aprire il menu di scelta rapida del nodo **Rete** e selezionare **Aggiungi file di rete**.
 - d. Immettere il percorso di rete del file eicar.com nel computer remoto nel formato UNC (Universal Naming Convention).
 - e. Selezionare la casella di controllo per includere il percorso di rete aggiunto all'ambito della scansione.
 - f. Eseguire l'attività Scansione aree critiche.

Scansione su richiesta funziona come previsto se le seguenti condizioni sono soddisfatte:

- Il file eicar.com è stato eliminato dal disco rigido del computer.
- Nella console dell'applicazione al log delle attività è stato assegnato lo stato **Critico**; nel log dell'esecuzione dell'attività Scansione aree critiche è stata aggiunta una riga con le informazioni su una minaccia nel file eicar.com. Per visualizzare il log delle attività, nell'albero della console dell'applicazione espandere il nodo figlio **Scansione su richiesta**, selezionare l'attività Scansione aree critiche e nel riquadro dei dettagli fare clic sul collegamento **Apri log**.

Interfaccia dell'applicazione

È possibile controllare Kaspersky Embedded Systems Security 2.2 tramite la console dell'applicazione locale e il plug-in di amministrazione. Le azioni con la console dell'applicazione locale sono descritte nel *Manuale Utente di Kaspersky Embedded Systems Security 2.2*. L'interfaccia di Kaspersky Security Center Administration Console viene utilizzata per eseguire le operazioni con il plug-in di amministrazione. Informazioni dettagliate sull'interfaccia di Kaspersky Security Center sono disponibili nella *Guida di Kaspersky Security Center*.

Licensing dell'applicazione

Questa sezione fornisce informazioni sui concetti principali correlati alla gestione delle licenze dell'applicazione.

In questo capitolo

Informazioni sul Contratto di licenza con l'utente finale.....	67
Informazioni sulla licenza.....	67
Informazioni sul certificato di licenza.....	68
Informazioni sul codice di attivazione.....	69
Informazioni sulla chiave.....	69
Informazioni sul file chiave.....	69
Informazioni sulla trasmissione dei dati.....	70
Attivazione dell'applicazione con una chiave.....	71
Visualizzazione delle informazioni sulla licenza corrente.....	71
Limitazioni delle funzionalità alla scadenza della licenza.....	73
Rinnovo della licenza.....	74
Eliminazione della chiave.....	74

Informazioni sul Contratto di licenza con l'utente finale

Il *Contratto di licenza con l'utente finale* è un accordo vincolante tra l'utente e AO Kaspersky Lab, in cui sono definite le condizioni di utilizzo dell'applicazione.

Leggere attentamente le condizioni del Contratto di licenza con l'utente finale prima di utilizzare l'applicazione.

È possibile leggere le condizioni del Contratto di licenza con l'utente finale nei seguenti modi:

- Durante l'installazione di Kaspersky Embedded Systems Security 2.2
- Leggendo il file `license.txt`. Questo documento è incluso nel kit di distribuzione dell'applicazione

Confermando l'accettazione del Contratto di licenza con l'utente finale durante l'installazione dell'applicazione, si accettano le condizioni del Contratto di licenza con l'utente finale. Se non si accettano le condizioni del Contratto di licenza con l'utente finale, è necessario interrompere l'installazione dell'applicazione e rinunciare all'utilizzo dell'applicazione.

Informazioni sulla licenza

Una licenza concede per un determinato periodo di tempo il diritto di utilizzare l'applicazione, in conformità con il

Contratto di licenza con l'utente finale.

Una licenza valida consente di ottenere i seguenti servizi:

- Utilizzo dell'applicazione in conformità alle condizioni del Contratto di licenza con l'utente finale
- Assistenza tecnica

L'ambito dei servizi forniti e le condizioni per l'utilizzo dell'applicazione dipendono dal tipo di licenza utilizzata per attivare l'applicazione.

L'applicazione viene attivata tramite un file chiave per una licenza commerciale acquistata.

Una licenza commerciale è una licenza a pagamento fornita con l'acquisto dell'applicazione.

Kaspersky Embedded Systems Security 2.2 offre due tipi di licenze commerciali:

- Licenza standard di Kaspersky Embedded Systems Security
- Licenza estesa di Kaspersky Embedded Systems Security Compliance Edition, che include due componenti aggiuntivi per l'analisi del sistema: Monitoraggio integrità file e Analisi log.

Alla scadenza di una licenza commerciale, l'applicazione continua a funzionare ma alcune delle sue funzionalità diventano non disponibili (ad esempio, i database di Kaspersky Embedded Systems Security 2.2 non possono essere aggiornati). Per continuare a utilizzare tutte le funzionalità di Kaspersky Embedded Systems Security 2.2, è necessario rinnovare la licenza commerciale.

Per garantire la massima protezione del computer dalle minacce per la sicurezza, è consigliabile rinnovare la licenza prima della scadenza.

Verificare che la chiave di riserva aggiunta abbia una data di scadenza successiva a quella della chiave attiva.

Informazioni sul certificato di licenza

Un *certificato di licenza* è un documento ricevuto insieme a un file chiave o a un codice di attivazione (se applicabile).

Un certificato di licenza contiene le seguenti informazioni sulla licenza:

- Numero di ordine
- Informazioni sull'utente a cui è stata concessa la licenza
- Informazioni sull'applicazione che può essere attivata con la licenza
- Limite per il numero di unità concesse in licenza (ad esempio, i dispositivi in cui può essere utilizzata l'applicazione con la licenza)
- Data di inizio del periodo di validità della licenza
- Data di scadenza della licenza o periodo di validità della licenza
- Tipo di licenza

Informazioni sul codice di attivazione

Un *codice di attivazione* è una sequenza univoca di 20 lettere e numeri. È necessario immettere un codice di attivazione per aggiungere una chiave per l'attivazione di Kaspersky Embedded Systems Security 2.2. Il codice di attivazione viene inviato all'indirizzo e-mail specificato al momento dell'acquisto di Kaspersky Embedded Systems Security 2.2.

Per attivare l'applicazione con un codice di attivazione, è necessario l'accesso a Internet per eseguire la connessione ai server di attivazione di Kaspersky Lab.

Se il codice di attivazione è stato smarrito dopo l'installazione dell'applicazione, è possibile eseguirne il ripristino. Il codice di attivazione potrebbe ad esempio essere necessario per eseguire la registrazione a Kaspersky CompanyAccount. Per ripristinare il codice di attivazione, contattare l'Assistenza tecnica di Kaspersky Lab.

Informazioni sulla chiave

Una *chiave* è una sequenza di bit che consente di attivare e quindi utilizzare l'applicazione in conformità alle condizioni del Contratto di licenza con l'utente finale. Una chiave viene generata da Kaspersky Lab.

È possibile aggiungere una chiave all'applicazione utilizzando un file chiave. Dopo avere aggiunto una chiave all'applicazione, la chiave viene visualizzata nell'interfaccia dell'applicazione come una sequenza univoca di caratteri alfanumerici.

Kaspersky Lab può inserire una chiave nella blacklist in seguito a violazioni del Contratto di licenza. Se la chiave viene bloccata, è necessario aggiungere una chiave diversa per consentire il funzionamento dell'applicazione.

Una chiave può essere "attiva" o "di riserva".

Una *chiave attiva* è la chiave che l'applicazione utilizza al momento. È possibile aggiungere come chiave attiva una chiave per una licenza commerciale. L'applicazione non può disporre di più di una chiave attiva.

Una *chiave di riserva* è una chiave che conferma il diritto di utilizzare l'applicazione, pur non essendo attualmente in uso. Una chiave di riserva diventa automaticamente attiva alla scadenza della licenza associata alla chiave attiva corrente. Una chiave di riserva può essere aggiunta solo se è presente una chiave attiva.

Informazioni sul file chiave

Un *file chiave* è un file con estensione .key che si riceve da Kaspersky Lab. I file chiave sono progettati per attivare l'applicazione attraverso l'aggiunta di una chiave.

Il file chiave viene inviato all'indirizzo e-mail specificato al momento dell'acquisto di Kaspersky Embedded Systems Security 2.2.

Non è necessario connettersi ai server di attivazione di Kaspersky Lab per attivare l'applicazione con un file chiave.

È possibile recuperare un file chiave eliminato accidentalmente. Un file chiave potrebbe essere necessario per eseguire la registrazione a Kaspersky CompanyAccount.

Per recuperare un file chiave, eseguire una delle seguenti operazioni:

- Contattare l'Assistenza tecnica <https://support.kaspersky.it/>.
- Ottenere un file chiave sul sito Web di Kaspersky Lab, in base al codice di attivazione esistente.

Informazioni sulla trasmissione dei dati

Il Contratto di licenza per Kaspersky Embedded Systems Security 2.2, soprattutto nella sezione intitolata "Condizioni per l'elaborazione dei dati", specifica le condizioni, la predisposizione e la procedura per l'invio e l'elaborazione dei dati indicati in questa Guida. Prima di accettare il Contratto di licenza, leggere attentamente le relative condizioni, nonché tutti i documenti associati al Contratto di licenza.

I dati che Kaspersky Lab riceve dall'utente durante l'utilizzo dell'applicazione vengono protetti ed elaborati conformemente all'Informativa sulla privacy disponibile all'indirizzo <http://www.kaspersky.com/products-and-services-privacy-policy>.

Accettando le condizioni del Contratto di licenza, si accetta di inviare automaticamente i seguenti dati a Kaspersky Lab:

- Per supportare il meccanismo per la ricezione degli aggiornamenti sono necessarie le informazioni sull'applicazione installata e sulla relativa attivazione: identificatore dell'applicazione installata e il numero di versione completo, tra cui il numero di build, il tipo e l'identificatore di licenza, l'identificatore dell'installazione e l'identificatore univoco dell'attività di aggiornamento.
- Per utilizzare la funzionalità di accesso agli articoli della Knowledge Base quando si verificano errori dell'applicazione (servizio Redirector) sono necessarie informazioni sul tipo di applicazione e collegamento, in particolare: il nome, impostazioni locali e numero di versione completo dell'applicazione, tipo di collegamento di reindirizzamento e identificatore dell'errore.
- Per gestire le conferme relative all'elaborazione dei dati sono necessarie le informazioni sullo stato di accettazione del Contratto di licenza e degli altri documenti in cui vengono stipulate le condizioni per il trasferimento: identificatore e versione del Contratto di licenza o degli altri documenti, nell'ambito di cui vengono accettate o rifiutate le condizioni per l'elaborazione dei dati; un attributo, indicante l'azione dell'utente (conferma o revoca dell'accettazione delle condizioni); data e ora di modifica dello stato dell'accettazione delle condizioni per l'elaborazione dei dati.

È possibile leggere le condizioni del Contratto di licenza con l'utente finale nei seguenti modi:

- Durante l'installazione dell'applicazione, quando l'Installazione guidata di Kaspersky Embedded Systems Security 2.2 visualizza il testo completo del Contratto di licenza e richiede di accettarne le condizioni.
- In qualsiasi momento nel file TXT (license.txt), che contiene il testo completo del Contratto di licenza. Il file è incluso nel kit di distribuzione di Kaspersky Embedded Systems Security 2.2, insieme ai file di installazione dell'applicazione.

Elaborazione locale dei dati

Durante l'esecuzione delle funzioni principali dell'applicazione descritte nella presente Guida, Kaspersky Embedded Systems Security 2.2 elabora e archivia localmente una sequenza di tipi di dati nel computer protetto:

- Informazioni sui file e sugli oggetti esaminati, ad esempio i nomi e attributi dei file elaborati e i relativi percorsi completi nei supporti esaminati, azioni eseguite sui file esaminati, account utente, esecuzione di azioni sulla rete protetta o sul computer protetto, nomi e dati sui dispositivi esaminati, informazioni sui processi in esecuzione nel sistema.
- Informazioni sulle impostazioni e sulle attività del sistema operativo, ad esempio le impostazioni di Windows Firewall, le voci del Registro eventi di Windows, i nomi degli account utente, gli avvii dei file eseguibili, i checksum e gli attributi di tali file.

Kaspersky Embedded Systems Security 2.2 elabora e memorizza i dati nell'ambito delle funzionalità di base dell'applicazione, in particolare per la registrazione degli eventi dell'applicazione e la ricezione dei dati di diagnostica. I dati elaborati in locale vengono protetti secondo le impostazioni dell'applicazione configurate e applicate.

Kaspersky Embedded Systems Security 2.2 consente di configurare il livello di protezione per i dati elaborati in locale: è possibile modificare i privilegi dell'utente per accedere ai dati del processo, modificare i periodi di memorizzazione dei dati per questi ultimi, disabilitare completamente o parzialmente la funzionalità che implica la registrazione dei dati e modificare il percorso e gli attributi della cartella presente nel supporto in cui vengono registrati i dati.

Informazioni dettagliate sulla configurazione delle funzionalità dell'applicazione relative all'elaborazione dei dati e alle impostazioni predefinite per l'archiviazione dei dati elaborati sono disponibili nelle sezioni corrispondenti della Guida.

Per impostazione predefinita, tutti i dati archiviati in un computer locale vengono rimossi dopo la disinstallazione di Kaspersky Embedded Systems Security 2.2, tranne i file con le informazioni di diagnostica (file di traccia e di dump) e i record del log eventi di Windows relativi all'attività dell'applicazione. È necessario rimuovere manualmente questi file. È possibile trovare informazioni dettagliate sulla configurazione dei processi di diagnostica nelle sezioni corrispondenti di questa guida.

Durante la disinstallazione dell'applicazione è possibile salvare il contenuto degli archivi di backup e quarantena.

Attivazione dell'applicazione con una chiave

È possibile attivare Kaspersky Embedded Systems Security 2.2 applicando una chiave.

Se è stata già aggiunta una chiave attiva per Kaspersky Embedded Systems Security 2.2 e si aggiunge un'altra chiave come chiave attiva, la nuova chiave sostituisce la chiave aggiunta precedentemente. La chiave attiva installata in precedenza viene rimossa.

Se è stata già aggiunta una chiave di riserva per Kaspersky Embedded Systems Security 2.2 e si aggiunge un'altra chiave come chiave di riserva, la nuova chiave sostituisce la chiave aggiunta precedentemente. La chiave di riserva installata in precedenza viene rimossa.

Se sono state già aggiunte una chiave attiva e una chiave di riserva per Kaspersky Embedded Systems Security 2.2 e si aggiunge una nuova chiave come chiave attiva, la nuova chiave sostituisce la chiave attiva aggiunta precedentemente e la chiave di riserva non viene eliminata.

► Per attivare Kaspersky Embedded Systems Security 2.2:

1. Nell'albero della console dell'applicazione espandere il nodo **Licenze**.
2. Nel riquadro dei dettagli del nodo **Licenze** fare clic sul collegamento **Aggiungi chiave**.
3. Nella finestra visualizzata fare clic sul pulsante **Sfoglia** e selezionare un file chiave con l'estensione .key.

È anche possibile aggiungere una chiave come di riserva. Per aggiungere una chiave come di riserva, selezionare la casella di controllo **Usa come chiave di riserva**.

4. Fare clic su **OK**.

La chiave selezionata verrà applicata. Le informazioni sulla chiave aggiunta saranno disponibili nel nodo **Licenze**.

Visualizzazione delle informazioni sulla licenza corrente

Visualizzazione delle informazioni sulla licenza

Le informazioni sulla licenza corrente sono visualizzate nel riquadro dei dettagli del nodo **Kaspersky Embedded Systems Security** della console dell'applicazione. Lo stato della chiave può avere i seguenti valori:

- **Controllo dello stato della chiave in corso** - Kaspersky Embedded Systems Security 2.2 sta verificando il file chiave aggiunto o il codice di attivazione applicato ed è in attesa di una risposta sullo stato della chiave corrente.
- **Data di scadenza della licenza** - Kaspersky Embedded Systems Security 2.2 è stato attivato fino alla data e all'ora specificate. Lo stato della chiave è evidenziato in giallo nei seguenti casi:
 - La licenza scadrà entro 14 giorni e non sono stati aggiunti una chiave o un codice di attivazione di riserva.
 - La chiave aggiunta è stata inserita nella blacklist e sta per essere bloccata.

- **Applicazione non attivata** - Kaspersky Embedded Systems Security 2.2 non è attivato perché la chiave non è stata aggiunta o il codice di attivazione non è stato applicato. Lo stato è evidenziato in rosso.
- **La licenza è scaduta** - Kaspersky Embedded Systems Security 2.2 non è attivato perché la licenza è scaduta. Lo stato è evidenziato in rosso.
- **Il Contratto di licenza con l'utente finale è stato violato** - Kaspersky Embedded Systems Security 2.2 non è attivato perché le condizioni del Contratto di licenza con l'utente finale (vedere la sezione "Informazioni sul Contratto di licenza con l'utente finale" a pagina [67](#)) sono state violate. Lo stato è evidenziato in rosso.
- **Chiave presente nella blacklist** - Il file chiave aggiunto è stato bloccato e inserito nella blacklist da Kaspersky Lab, ad esempio se la chiave è stata utilizzata da terze parti per attivare l'applicazione illegalmente. Lo stato è evidenziato in rosso.

Visualizzazione delle informazioni sulla licenza corrente

► Per visualizzare le informazioni sulla licenza corrente:

Nell'albero della console dell'applicazione espandere il nodo **Licenze**.

Le informazioni generali sulla licenza corrente sono visualizzate nel riquadro dei dettagli del nodo **Licenze** (vedere la seguente tabella).

Tabella 15. Informazioni generali sulla licenza nel nodo Licenze

Campo	Descrizione
Codice di attivazione	Numero del codice di attivazione. Questo campo è compilato se si attiva l'applicazione utilizzando un codice di attivazione.
Stato di attivazione	Informazioni sullo stato di attivazione dell'applicazione. Le informazioni nella colonna Stato di attivazione nel pannello di controllo del nodo Licenze possono avere i seguenti valori: <ul style="list-style-type: none"> • Applicato - se l'applicazione è stata attivata utilizzando un codice di attivazione o una chiave. • Attivazione - se è stato applicato un codice di attivazione per attivare l'applicazione, ma il processo di attivazione non è ancora stato finalizzato. Il valore dello stato diventa Applicato dopo che l'attivazione dell'applicazione è stata completata e i contenuti del riquadro dei dettagli del nodo sono stati aggiornati. • Errore di attivazione - se l'attivazione dell'applicazione è non riuscita. È possibile visualizzare la causa per cui l'attivazione non è riuscita nel log delle attività.
Chiave	Numero della chiave utilizzata per attivare l'applicazione.
Tipo di licenza	Tipo di licenza: commerciale.
Data di scadenza	Data e ora di scadenza della licenza associata a una chiave attiva.
Stato del codice di attivazione o della chiave	Stato del codice di attivazione o della chiave: Attiva o Di riserva.

► Per visualizzare le informazioni dettagliate sulla licenza:

Selezionare il nodo **Licenze**, aprire il menu di scelta rapida della stringa con i dati della licenza che si desidera espandere e selezionare **Proprietà**. Nella scheda **Proprietà**: <Stato del codice di attivazione o della

chiave>, nella scheda **Generale** sono visualizzate informazioni dettagliate sulla licenza corrente e nella scheda **Avanzate** sono disponibili le informazioni sul cliente e i dettagli di contatto di Kaspersky Lab o del rivenditore da cui è stato acquistato Kaspersky Embedded Systems Security 2.2 (vedere la seguente tabella).

Tabella 16. Informazioni dettagliate sulla licenza nella finestra *Proprietà*: <stato del codice di attivazione o della chiave>

Campo	Descrizione
Scheda Generale	
Chiave	Numero della chiave utilizzata per attivare l'applicazione.
Data di aggiunta della chiave	Data in cui la chiave è stata aggiunta all'applicazione.
Tipo di licenza	Tipo di licenza: commerciale.
Giorni prima della scadenza	Numero di giorni rimanenti prima della scadenza della licenza associata alla chiave attiva.
Data di scadenza	Data e ora di scadenza della licenza associata a una chiave attiva. Se si attiva l'applicazione con un abbonamento illimitato, il valore del campo è <i>Illimitato</i> . Se Kaspersky Embedded Systems Security 2.2 non riesce a determinare la data di scadenza della licenza, il valore del campo è impostato su <i>Sconosciuto</i> .
Applicazione	Nome dell'applicazione che è stata attivata con la chiave o il codice di attivazione aggiunto.
Limitazione utilizzo chiave	Limitazione per l'utilizzo della chiave (se presente).
Idonea per l'assistenza tecnica	Informazioni che indicano se Kaspersky Lab o uno dei relativi partner fornirà assistenza tecnica per i clienti in base alle condizioni di licenza.
Scheda Avanzate	
Informazioni sulla licenza	Numero e tipo di licenza corrente.
Informazioni sul supporto	Dettagli di contatto di Kaspersky Lab o del relativo partner che fornisce assistenza tecnica. Questo campo può essere vuoto se l'assistenza tecnica non viene fornita.
Informazioni sul proprietario	Informazioni sul cliente della licenza: nome di un cliente e nome di un'organizzazione per cui è stata acquisita la licenza.

Limitazioni delle funzionalità alla scadenza della licenza

Alla scadenza della licenza corrente, vengono applicate le seguenti limitazioni per l'utilizzo dei componenti:

- Tutte le attività vengono arrestate, ad eccezione delle attività Protezione dei file in tempo reale, Scansione su richiesta e Controllo dell'integrità dell'applicazione.
- Viene impedito l'avvio di qualsiasi attività, ad eccezione delle attività Protezione in tempo reale, Scansione su richiesta e Controllo dell'integrità dell'applicazione. Queste attività continuano a essere eseguite utilizzando i database anti-virus precedenti.
- La funzionalità di Prevenzione exploit viene limitata:
 - I processi sono protetti fino al riavvio.

- Non è possibile aggiungere nuovi processi all'ambito della protezione.

Altre funzioni (archivio, log, informazioni diagnostiche) saranno ancora disponibili.

Rinnovo della licenza

Per impostazione predefinita, quando mancano 14 giorni alla scadenza della licenza, Kaspersky Embedded Systems Security 2.2 invia una notifica. In questo caso, lo stato **Data di scadenza della licenza** nel riquadro dei dettagli del nodo **Kaspersky Embedded Systems Security** viene evidenziato in giallo.

È possibile rinnovare anticipatamente la data di scadenza della licenza utilizzando una chiave di riserva o un codice di attivazione. In questo modo è possibile assicurare la protezione del server dopo la scadenza della licenza esistente e prima dell'attivazione dell'applicazione con una nuova licenza.

► *Per rinnovare una licenza, eseguire le seguenti operazioni:*

1. Acquistare un nuovo codice di attivazione o un file chiave.
2. Nell'albero della console dell'applicazione aprire il nodo **Licenze**.
3. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del nodo **Licenze**:
 - Se si desidera rinnovare una licenza utilizzando una chiave di riserva:
 - a. Fare clic sul collegamento **Aggiungi chiave**.
 - b. Nella finestra visualizzata fare clic sul pulsante **Sfoglia** e selezionare un nuovo file chiave con l'estensione .key.
 - c. Selezionare la casella di controllo **Usa come chiave di riserva**.
 - Se si desidera rinnovare una licenza utilizzando un codice di attivazione:
 - a. Fare clic sul collegamento **Aggiungi codice di attivazione**.
 - b. Immettere il codice di attivazione acquistato nella finestra visualizzata.
 - c. Selezionare la casella di controllo **Usa come chiave di riserva**.

È necessaria una connessione Internet per applicare un codice di attivazione.

4. Fare clic su **OK**.

La chiave di riserva o il codice di attivazione sarà aggiunto e applicato automaticamente alla scadenza della licenza corrente di Kaspersky Embedded Systems Security 2.2.

Eliminazione della chiave

È possibile rimuovere la chiave aggiunta.

Se una chiave di riserva è stata aggiunta a Kaspersky Embedded Systems Security 2.2 e si rimuove la chiave attiva, la chiave di riserva diventa automaticamente la chiave attiva.

Se si elimina una chiave aggiunta, è possibile ripristinarla applicando di nuovo il file chiave.

► *Per rimuovere una chiave aggiunta:*

1. Nell'albero della console dell'applicazione selezionare il nodo **Licenze**.
2. Nel riquadro dei dettagli del nodo **Licenze**, nella tabella che contiene le informazioni sulle chiavi aggiunte, selezionare la chiave da rimuovere.
3. Nel menu di scelta rapida della riga che contiene le informazioni sulla chiave selezionata selezionare **Rimuovi**.
4. Fare clic sul pulsante **Sì** nella finestra di conferma per confermare che si desidera eliminare la chiave.

La chiave selezionata verrà rimossa.

Avvio e arresto del plug-in di Kaspersky Embedded Systems Security 2.2

Questa sezione contiene informazioni sull'avvio e l'arresto del plug-in di amministrazione di Kaspersky Embedded Systems Security 2.2 e del Servizio di Kaspersky Security.

In questo capitolo

Avvio del plug-in di amministrazione di Kaspersky Embedded Systems Security 2.2	76
Avvio e arresto del servizio di Kaspersky Security	76

Avvio del plug-in di amministrazione di Kaspersky Embedded Systems Security 2.2

Non sono necessarie ulteriori operazioni per avviare il plug-in di amministrazione di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center. Dopo l'installazione nel computer dell'amministratore, il plug-in viene avviato contemporaneamente a Kaspersky Security Center. Informazioni dettagliate sull'avvio di Kaspersky Security Center sono disponibili nella *Guida di Kaspersky Security Center*.

Avvio e arresto del servizio di Kaspersky Security

Per impostazione predefinita, il servizio di Kaspersky Security viene avviato automaticamente all'avvio del sistema operativo. Il servizio di Kaspersky Security gestisce i processi di lavoro in cui vengono eseguite le attività di Protezione del computer in tempo reale, Controllo attività locali, Scansione su richiesta e le attività di aggiornamento.

Per impostazione predefinita, all'avvio di Kaspersky Embedded Systems Security 2.2 vengono avviate le attività Protezione dei file in tempo reale e Scansione all'avvio del sistema operativo, nonché altre attività di cui è pianificata l'esecuzione **All'avvio dell'applicazione**.

Se il servizio di Kaspersky Security è arrestato, tutte le attività in esecuzione vengono interrotte. Dopo il riavvio del servizio di Kaspersky Security, l'applicazione avvia automaticamente solo le attività la cui pianificazione ha la frequenza di avvio impostata su **All'avvio dell'applicazione**, mentre le altre attività devono essere avviate manualmente.

È possibile avviare e arrestare il servizio di Kaspersky Security utilizzando il menu di scelta rapida del nodo **Kaspersky Embedded Systems Security** o lo snap-in **Servizi** di Microsoft Windows.

È possibile avviare e arrestare l'applicazione se si è membri del gruppo Administrators sul computer protetto.

► Per arrestare o avviare l'applicazione utilizzando la console dell'applicazione, eseguire le seguenti operazioni:

1. Nell'albero della console dell'applicazione aprire il menu di scelta rapida del nodo **Kaspersky Embedded Systems Security**.
2. Selezionare uno degli elementi seguenti:
 - **Arresto servizio**
 - **Avvio servizio**

Il servizio di Kaspersky Security verrà avviato o arrestato.

Autorizzazioni di accesso per le funzioni di Kaspersky Embedded Systems Security 2.2

Questa sezione contiene informazioni sulle autorizzazioni per gestire Kaspersky Embedded Systems Security 2.2 e i servizi di Windows registrati dall'applicazione, nonché istruzioni su come configurare queste autorizzazioni.

In questo capitolo

Informazioni sulle autorizzazioni per la gestione di Kaspersky Embedded Systems Security 2.2.....	77
Informazioni sulle autorizzazioni per la gestione del servizio di Kaspersky Security	79
Informazioni sulle autorizzazioni di accesso per il servizio di gestione di Kaspersky Security	81
Configurazione delle autorizzazioni di accesso per Kaspersky Embedded Systems Security 2.2 e il servizio di Kaspersky Security	81
Accesso protetto tramite password alle funzioni di Kaspersky Embedded Systems Security 2.2	83
Abilitazione delle connessioni di rete per il servizio di gestione di Kaspersky Security	85

Informazioni sulle autorizzazioni per la gestione di Kaspersky Embedded Systems Security 2.2

Per impostazione predefinita, l'accesso a tutte le funzioni di Kaspersky Embedded Systems Security 2.2 viene concesso agli utenti del gruppo Administrators sul computer protetto, agli utenti del gruppo Amministratori ESS creato nel computer protetto durante l'installazione di Kaspersky Embedded Systems Security 2.2 e al gruppo SYSTEM.

Gli utenti che hanno accesso alla funzione **Modifica autorizzazioni** di Kaspersky Embedded Systems Security 2.2 possono concedere l'accesso alle funzioni di Kaspersky Embedded Systems Security 2.2 ad altri utenti registrati nel computer protetto o inclusi nel dominio.

Gli utenti che non sono registrati nell'elenco degli utenti di Kaspersky Embedded Systems Security 2.2 non possono aprire la console dell'applicazione.

È possibile selezionare uno dei seguenti livelli preimpostati di accesso a Kaspersky Embedded Systems Security 2.2 per un utente o un gruppo di utenti:

- **Controllo completo** - accesso a tutte le funzioni dell'applicazione: possibilità di visualizzare e modificare le impostazioni generali di Kaspersky Embedded Systems Security 2.2, le impostazioni dei componenti e le autorizzazioni degli utenti di Kaspersky Embedded Systems Security 2.2, nonché di visualizzare le statistiche di Kaspersky Embedded Systems Security 2.2.
- **Modifica** - accesso a tutte le funzioni dell'applicazione ad eccezione della modifica delle autorizzazioni utente: possibilità di visualizzare e modificare le impostazioni generali di Kaspersky Embedded Systems Security 2.2 e le impostazioni dei componenti di Kaspersky Embedded Systems Security 2.2.
- **Lettura** - possibilità di visualizzare le impostazioni generali di Kaspersky Embedded Systems Security 2.2, le impostazioni dei componenti di Kaspersky Embedded Systems Security 2.2, le statistiche di Kaspersky Embedded Systems Security 2.2 e le autorizzazioni degli utenti di Kaspersky Embedded Systems Security 2.2.

È anche possibile configurare le autorizzazioni di accesso avanzate (vedere la sezione "Configurazione delle autorizzazioni di accesso per Kaspersky Embedded Systems Security 2.2 e il servizio di Kaspersky Security" a pagina [81](#)): consentire o bloccare l'accesso a specifiche funzioni di Kaspersky Embedded Systems Security 2.2.

Se sono state configurate manualmente le autorizzazioni di accesso per un utente o un gruppo, per tale utente o gruppo viene impostato il livello di accesso **Autorizzazioni speciali**.

Tabella 17. Informazioni sulle autorizzazioni di accesso per le funzioni di Kaspersky Embedded Systems Security 2.2

Diritti utente	Descrizione
Gestione attività	Possibilità di avviare, arrestare, sospendere e riprendere attività di Kaspersky Embedded Systems Security 2.2.
Creazione ed eliminazione di attività Scansione su richiesta	Possibilità di creare ed eliminare attività Scansione su richiesta.
Modifica impostazioni	Possibilità di: <ul style="list-style-type: none"> • Importare le impostazioni di Kaspersky Embedded Systems Security 2.2 da un file di configurazione. • Modificare le impostazioni dell'applicazione.
Lettura impostazioni	Possibilità di: <ul style="list-style-type: none"> • Visualizzare le impostazioni generali di Kaspersky Embedded Systems Security 2.2 e le impostazioni delle attività. • Esportare le impostazioni di Kaspersky Embedded Systems Security 2.2 in un file di configurazione. • Visualizzare le impostazioni di log delle attività, log di audit e notifiche.
Gestire gli archivi	Possibilità di: <ul style="list-style-type: none"> • Spostare gli oggetti in Quarantena. • Rimuovere oggetti da Quarantena e Backup. • Ripristinare oggetti da Quarantena e Backup.
Gestire i log	Possibilità di eliminare i log delle attività e di cancellare il log di audit.
Lettura log	Possibilità di visualizzare gli eventi relativi all'anti-virus nei log delle attività e nel log di audit.
Lettura statistiche	Possibilità di visualizzare le statistiche di ogni attività di Kaspersky Embedded Systems Security 2.2.
Licensing dell'applicazione	Kaspersky Embedded Systems Security 2.2 può essere attivato o disattivato.
Disinstallazione dell'applicazione	Possibilità di disinstallare Kaspersky Embedded Systems Security 2.2.
Lettura autorizzazioni	Possibilità di visualizzare l'elenco degli utenti di Kaspersky Embedded Systems Security 2.2 e i privilegi di accesso di ogni utente.
Modifica autorizzazioni	Possibilità di: <ul style="list-style-type: none"> • Modificare l'elenco degli utenti con accesso alla gestione dell'applicazione. • Modificare le autorizzazioni di accesso degli utenti per le funzioni di Kaspersky Embedded Systems Security 2.2.

Informazioni sulle autorizzazioni per la gestione del servizio di Kaspersky Security

Durante l'installazione, Kaspersky Embedded Systems Security 2.2 registra il servizio di Kaspersky Security (KAVFS) in Windows e abilita internamente i componenti funzionali eseguiti all'avvio del sistema operativo. Per ridurre il rischio di accesso di terze parti alle funzioni dell'applicazione e alle impostazioni di sicurezza nel computer protetto tramite la gestione del servizio di Kaspersky Security, è possibile limitare le autorizzazioni per la gestione del servizio di Kaspersky Security dalla console dell'applicazione o dal plug-in di amministrazione.

Per impostazione predefinita, le autorizzazioni di accesso per la gestione del servizio di Kaspersky Security sono concesse agli utenti nel gruppo "Administrators" sul computer protetto, nonché ai gruppi SERVICE e INTERACTIVE con autorizzazioni di lettura e al gruppo SYSTEM con autorizzazioni di lettura ed esecuzione.

Non è possibile eliminare l'account utente SYSTEM o modificare le autorizzazioni per tale account. Se le autorizzazioni dell'account utente SYSTEM sono state modificate, per tale account vengono ripristinati i privilegi massimi al salvataggio delle modifiche.

Gli utenti che hanno accesso alle funzioni (vedere la sezione "Informazioni sulle autorizzazioni per la gestione di Kaspersky Embedded Systems Security 2.2" a pagina [77](#)) del livello Modifica autorizzazioni possono concedere le autorizzazioni di accesso per la gestione del servizio di Kaspersky Security ad altri utenti registrati sul computer protetto o inclusi nel dominio.

È possibile scegliere uno dei seguenti livelli preimpostati di autorizzazioni di accesso per un utente o un gruppo di utenti di Kaspersky Embedded Systems Security 2.2 per la gestione del servizio di Kaspersky Security:

- **Controllo completo:** possibilità di visualizzare e modificare le impostazioni generali e le autorizzazioni degli utenti per il servizio di Kaspersky Security e di avviare e arrestare il servizio di Kaspersky Security.
- **Lettura:** possibilità di visualizzare le impostazioni generali e le autorizzazioni utente del servizio di Kaspersky Security.
- **Modifica:** possibilità di visualizzare e modificare le impostazioni generali e le autorizzazioni utente del servizio di Kaspersky Security.
- **Esecuzione:** possibilità di avviare e arrestare il servizio di Kaspersky Security.

È inoltre possibile configurare le autorizzazioni di accesso avanzate: consentire o negare l'accesso a funzioni specifiche di Kaspersky Embedded Systems Security 2.2 (vedere la seguente tabella).

Se sono state configurate manualmente le autorizzazioni di accesso per un utente o un gruppo, per tale utente o gruppo viene impostato il livello di accesso **Autorizzazioni speciali**.

Tabella 18. Delimitazione delle autorizzazioni di accesso per le funzioni di Kaspersky Embedded Systems Security 2.2

Funzionalità	Descrizione
Visualizzazione delle configurazioni del servizio	Visualizzazione: possibilità di visualizzare le impostazioni generali e le autorizzazioni utente del servizio di Kaspersky Security.
Richiesta stato del servizio da Service Manager	Possibilità di richiedere lo stato di esecuzione del servizio di Kaspersky Security da Gestione controllo servizi di Microsoft Windows.
Richiesta stato dal servizio	Possibilità di richiedere lo stato di esecuzione del servizio dal servizio di Kaspersky Security.

Funzionalità	Descrizione
Lettura elenco di servizi dipendenti	Possibilità di visualizzare un elenco di servizi da cui dipende il servizio di Kaspersky Security e che dipendono dal servizio di Kaspersky Security.
Modifica impostazioni servizio	Possibilità di visualizzare e modificare le impostazioni generali e le autorizzazioni utente del servizio di Kaspersky Security.
Avvio servizio	Possibilità di avviare il servizio di Kaspersky Security.
Arresto servizio	Possibilità di arrestare il servizio di Kaspersky Security.
Sospensione/ripresa servizio	Possibilità di sospendere e riprendere il servizio di Kaspersky Security.
Lettura autorizzazioni	Possibilità di visualizzare l'elenco degli utenti del servizio di Kaspersky Security e i privilegi di accesso di ogni utente.
Modifica autorizzazioni	Possibilità di: <ul style="list-style-type: none"> • Aggiungere e rimuovere utenti del servizio di Kaspersky Security. • Modificare le autorizzazioni di accesso degli utenti per il servizio di Kaspersky Security.
Eliminare il servizio	Possibilità di annullare la registrazione del servizio di Kaspersky Security in Gestione controllo servizi di Microsoft Windows.
Richieste definite dall'utente per il servizio	Possibilità di creare e inviare richieste dell'utente al servizio di Kaspersky Security.

Registrazione del servizio Kaspersky Security come servizio protetto

La tecnologia *Protected Process Light* (anche denominata "PPL") garantisce il caricamento nel sistema operativo solo di processi e servizi attendibili. Per eseguire un servizio come servizio protetto, è necessario installare nel computer protetto un driver *Early Launch AntiMalware*.

Un driver *Early Launch AntiMalware* (anche denominato "ELAM") fornisce la protezione per i computer della rete all'avvio e prima dell'inizializzazione di driver di terze parti.

Il driver ELAM viene installato automaticamente durante l'installazione di Kaspersky Embedded Systems Security 2.2 e viene utilizzato per la registrazione del servizio di Kaspersky Security come PPL all'avvio del sistema operativo. Quando il servizio di Kaspersky Security (kavfs.exe) viene avviato come un processo di sistema protetto, gli altri processi non protetti nel sistema non sono in grado di inserire thread, eseguire operazioni di scrittura nella memoria virtuale del processo protetto o arrestare il servizio.

Quando un processo viene avviato come PPL, non può essere gestito dall'utente ignorando le autorizzazioni utente assegnate. La registrazione del servizio di Kaspersky Security come PPL tramite il driver ELAM è supportata nei sistemi operativi Microsoft Windows 10 e versioni successive. Se si installa Kaspersky Embedded Systems Security 2.2 in un computer con un sistema operativo che supporta PPL, la gestione delle autorizzazioni per il servizio di Kaspersky Security (KAVFS) non sarà disponibile.

Il servizio di Kaspersky Security avvia tutti i processi figli come PPL.

► Per installare Kaspersky Embedded Systems Security 2.2 come PPL, eseguire il seguente comando:

```
msiexec /i ks4ws_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

È possibile utilizzare la riga di comando per configurare l'utilizzo di PPL.

Informazioni sulle autorizzazioni di accesso per il servizio di gestione di Kaspersky Security

È possibile esaminare l'elenco dei servizi di Kaspersky Embedded Systems Security 2.2.

Durante installazione, Kaspersky Embedded Systems Security 2.2 registra il servizio di gestione di Kaspersky Security (KAVFSGT). Per gestire l'applicazione tramite la console dell'applicazione installata in un altro computer, l'account di cui vengono utilizzate le autorizzazioni per connettersi a Kaspersky Embedded Systems Security 2.2 deve avere accesso completo al servizio di gestione di Kaspersky Security nel computer protetto.

Per impostazione predefinita, l'accesso al servizio di gestione di Kaspersky Security viene concesso agli utenti del gruppo Administrators sul computer protetto e agli utenti del gruppo Amministratori ESS creato nel computer protetto durante l'installazione di Kaspersky Embedded Systems Security 2.2.

È possibile gestire il servizio di gestione di Kaspersky Security solo tramite lo snap-in **Servizi** di Microsoft Windows.

Non è possibile consentire o bloccare l'accesso degli utenti al servizio di gestione di Kaspersky Security configurando Kaspersky Embedded Systems Security 2.2.

È possibile connettersi a Kaspersky Embedded Systems Security 2.2 da un account locale se nel computer protetto è registrato un account con lo stesso nome e la stessa password.

Configurazione delle autorizzazioni di accesso per Kaspersky Embedded Systems Security 2.2 e il servizio di Kaspersky Security

È possibile modificare l'elenco di utenti e gruppi di utenti autorizzati ad accedere alle funzioni di Kaspersky Embedded Systems Security 2.2 e gestire il servizio di Kaspersky Security, nonché modificare le autorizzazioni di accesso di tali utenti e gruppi di utenti.

► *Per aggiungere o rimuovere un utente o un gruppo dall'elenco:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Supplementari** eseguire uno dei seguenti passaggi:

- Selezionare **Autorizzazioni di accesso utente per la gestione dell'applicazione** se si desidera modificare l'elenco di utenti che hanno autorizzazioni di accesso per la gestione delle funzioni di Kaspersky Embedded Systems Security 2.2.
- Selezionare **Autorizzazioni di accesso utente per la gestione del servizio Security** se si desidera modificare l'elenco di utenti che hanno autorizzazioni di accesso per la gestione del servizio di Kaspersky Security.

Verrà visualizzata la finestra **Autorizzazioni per il gruppo Kaspersky Embedded Systems Security 2.2**.

4. Nella finestra visualizzata eseguire le seguenti operazioni:

- Per aggiungere un utente o un gruppo all'elenco, fare clic sul pulsante **Aggiungi** e selezionare l'utente o il gruppo a cui concedere i privilegi.
- Per rimuovere un utente o un gruppo dall'elenco, selezionare l'utente o il gruppo di cui si desidera limitare l'accesso e fare clic sul pulsante **Rimuovi**.

5. Fare clic sul pulsante **Applica**.

Gli utenti (o i gruppi) selezionati vengono aggiunti o rimossi.

► *Per modificare le autorizzazioni di un utente o un gruppo per la gestione di Kaspersky Embedded Systems Security 2.2 o del servizio di Kaspersky Security:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Supplementari** eseguire uno dei seguenti passaggi:

- Selezionare **Modifica i diritti utente in ambito di gestione dell'applicazione** se si desidera modificare l'elenco di utenti che hanno autorizzazioni di accesso per la gestione delle funzioni di Kaspersky Embedded Systems Security 2.2.
- Selezionare **Modifica i diritti utente in ambito di gestione del servizio di Kaspersky Security** se si desidera modificare l'elenco di utenti che hanno autorizzazioni di accesso per la gestione

dell'applicazione tramite il servizio di Kaspersky Security.

Verrà visualizzata la finestra **Autorizzazioni per il gruppo Kaspersky Embedded Systems Security**.

4. Nella finestra visualizzata, nell'elenco **Gruppi o utenti**, selezionare l'utente o il gruppo di utenti per cui si desidera modificare le autorizzazioni.
5. Nella sezione **Autorizzazioni per il gruppo "<Utente (Gruppo)>"** selezionare le caselle di controllo **Consenti** o **Blocca** per i seguenti livelli di accesso:
 - **Controllo completo**: set completo di autorizzazioni per la gestione di Kaspersky Embedded Systems Security 2.2 o del servizio di Kaspersky Security.
 - **Lettura**:
 - Le seguenti autorizzazioni per la gestione di Kaspersky Embedded Systems Security 2.2: **Recupero statistiche, Lettura impostazioni, Lettura log e Lettura autorizzazioni**.
 - Le seguenti autorizzazioni per la gestione del servizio di Kaspersky Security: **Lettura impostazioni servizio, Richiesta stato del servizio da Service Control Manager, Richiesta stato dal servizio, Lettura elenco di servizi dipendenti, Lettura autorizzazioni**.
 - **Modifica**:
 - Tutte le autorizzazioni per la gestione di Kaspersky Embedded Systems Security 2.2, tranne **Modifica autorizzazioni**.
 - Le seguenti autorizzazioni per la gestione del servizio di Kaspersky Security: **Modifica impostazioni servizio, Lettura autorizzazioni**.
 - **Esecuzione**: le seguenti autorizzazioni per la gestione del servizio di Kaspersky Security: **Avvio servizio, Arresto servizio, Sospensione/ripresa servizio, Lettura autorizzazioni, Richieste definite dall'utente per il servizio**.
6. Per configurare le impostazioni avanzate delle autorizzazioni per un utente o un gruppo (**Autorizzazioni speciali**), fare clic sul pulsante **Avanzate**.
 - a. Nella finestra **Impostazioni di sicurezza avanzate per Kaspersky Embedded Systems Security 2.2** visualizzata selezionare l'utente o il gruppo desiderato.
 - b. Fare clic sul pulsante **Modifica**.
 - c. Nell'elenco a discesa nella parte superiore della finestra selezionare il tipo di controllo di accesso (**Consenti** o **Blocca**).
 - d. Selezionare le caselle di controllo accanto alle funzioni che si desidera consentire o bloccare per l'utente o il gruppo selezionato.
 - e. Fare clic su **OK**.
 - f. Nella finestra **Impostazioni di sicurezza avanzate per Kaspersky Embedded Systems Security 2.2** fare clic su **OK**.
7. Nella finestra **Autorizzazioni per il gruppo Kaspersky Embedded Systems Security** fare clic sul pulsante **Applica**.

Le autorizzazioni configurate per la gestione di Kaspersky Embedded Systems Security 2.2 o del servizio di Kaspersky Security vengono salvate.

Accesso protetto tramite password alle funzioni di Kaspersky Embedded Systems Security 2.2

È possibile limitare l'accesso alla gestione dell'applicazione e ai servizi registrati configurando autorizzazioni utente

(vedere la sezione "Autorizzazioni di accesso per le funzioni di Kaspersky Embedded Systems Security 2.2" a pagina [76](#)). È inoltre possibile impostare la protezione tramite password nelle impostazioni di Kaspersky Embedded Systems Security 2.2 per un'ulteriore protezione dell'esecuzione di operazioni critiche.

Kaspersky Embedded Systems Security 2.2 richiede una password quando si tenta di accedere alle seguenti funzioni dell'applicazione:

- connessione alla console dell'applicazione;
- disinstallazione di Kaspersky Embedded Systems Security 2.2;
- modifica dei componenti di Kaspersky Embedded Systems Security 2.2;
- esecuzione dei comandi della riga di comando.

L'interfaccia di Kaspersky Embedded Systems Security 2.2 nasconde la password specificata. Kaspersky Embedded Systems Security 2.2 archivia la password come checksum calcolato nel momento in cui viene specificata la password.

È possibile esportare e importare una configurazione dell'applicazione protetta da password. Il file di configurazione, creato in seguito all'esportazione della configurazione dell'applicazione protetta, contiene il checksum della password e il valore del modificatore utilizzato per compilare la stringa della password.

Non modificare il checksum o il modificatore nel file di configurazione. L'importazione di una configurazione protetta tramite password modificata manualmente può determinare il blocco completo dell'accesso all'applicazione.

► *Per proteggere l'accesso alle funzioni di Kaspersky Embedded Systems Security 2.2, eseguire le seguenti operazioni:*

1. Nell'albero di Kaspersky Security Center Administration Console espandere il nodo **Dispositivi gestiti**. Espandere il gruppo di amministrazione con i computer per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni del criterio per un gruppo di computer, selezionare la scheda **Criteri** e aprire **<nome criterio> > Proprietà**.
 - Se si desidera configurare le impostazioni dell'applicazione per un singolo computer, aprire le impostazioni richieste nella finestra **Impostazioni attività** (vedere la sezione "**Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center**" a pagina [100](#)) in Kaspersky Security Center.
3. Nella sezione **Sicurezza** fare clic sul pulsante **Impostazioni**.
Verrà visualizzata la finestra **Impostazioni di sicurezza**.
4. Nella sezione **Impostazioni di protezione tramite password** selezionare la casella di controllo **Applica protezione tramite password**.
I campi **Password** e **Conferma password** diventano attivi.
5. Nel campo **Password** immettere il valore da utilizzare per proteggere l'accesso alle funzioni di Kaspersky Embedded Systems Security 2.2.
6. Nel campo **Conferma password** immettere nuovamente la password.

7. Fare clic su **OK**.

Le impostazioni specificate verranno salvate. Kaspersky Embedded Systems Security 2.2 richiederà la password specificata per accedere alle funzioni protette.

Questa password non può essere ripristinata. Se viene smarrita la password si perde completamente il controllo dell'applicazione. Inoltre non sarà possibile disinstallare l'applicazione dal computer protetto.

È possibile modificare o reimpostare la password specificata nelle impostazioni dell'applicazione in qualsiasi momento.

► *Per ripristinare la password:*

Deselezionare la casella di controllo **Applica protezione tramite password** nelle impostazioni del criterio o dell'applicazione.

La protezione tramite password verrà disabilitata. Kaspersky Embedded Systems Security 2.2 elimina il checksum della password precedente dalle impostazioni dell'applicazione.

Abilitazione delle connessioni di rete per il servizio di gestione di Kaspersky Security

I nomi delle impostazioni possono variare nei diversi sistemi operativi Windows.

► *Per consentire le connessioni di rete per il servizio di gestione di Kaspersky Security nel computer protetto, eseguire le seguenti operazioni:*

1. In un computer protetto con Microsoft Windows selezionare **Start > Pannello di controllo > Sicurezza > Windows Firewall**.
2. Nella finestra **Impostazioni di Windows Firewall** selezionare **Modifica impostazioni**.
3. Nell'elenco delle esclusioni predefinite nella scheda **Esclusioni** selezionare le seguenti caselle di controllo: **Accesso alla rete COM+**, **Strumentazione gestione Windows (WMI)** e **Amministrazione remota**.
4. Fare clic sul pulsante **Aggiungi programma**.
5. Selezionare il file kavfsqt.exe nella finestra **Aggiungi programma**. Questo file è disponibile nella cartella specificata come cartella di destinazione durante l'installazione della console dell'applicazione.
6. Fare clic su **OK**.
7. Fare clic su **OK** nella finestra **Impostazioni di Windows Firewall**.

Le connessioni di rete per il servizio di gestione di Kaspersky Security nel computer protetto verranno consentite.

Creazione e configurazione dei criteri

Questa sezione fornisce informazioni sull'utilizzo dei criteri di Kaspersky Security Center per la gestione di Kaspersky Embedded Systems Security 2.2 in diversi computer.

In questo capitolo

Informazioni sui criteri	86
Configurazione dell'avvio pianificato delle attività locali di sistema	93



Informazioni sui criteri



È possibile creare criteri globali di Kaspersky Security Center per gestire la protezione in diversi computer in cui è installato Kaspersky Embedded Systems Security 2.2.


Un criterio applica le impostazioni, le funzioni e le attività di Kaspersky Embedded Systems Security 2.2 specificate al suo interno a tutti i computer protetti per un gruppo di amministrazione.

È possibile creare diversi criteri per un gruppo di amministrazione e applicarli l'uno dopo l'altro. Il criterio attualmente attivo per un gruppo ha lo stato *attivo* in Administration Console.

Le informazioni sull'applicazione dei criteri vengono registrate nel log di audit di Kaspersky Embedded Systems Security 2.2. Queste informazioni possono essere visualizzate nella console dell'applicazione nel nodo **Log di audit**.

Kaspersky Security Center offre un solo modo per applicare i criteri ai computer locali: *impedire la modifica delle impostazioni*. Dopo l'applicazione di un criterio, Kaspersky Embedded Systems Security 2.2 utilizza i valori per le impostazioni accanto alle quali è stata selezionata l'icona  nelle proprietà del criterio nei computer locali, invece dei valori per tali impostazioni che erano effettivi prima dell'applicazione del criterio. Kaspersky Embedded Systems Security 2.2 non applica i valori delle impostazioni del criterio attivo accanto alle quali è selezionata l'icona  nelle proprietà del criterio.

Se un criterio è attivo, i valori delle impostazioni contrassegnate nel criterio con l'icona  sono visualizzati nella console dell'applicazione, ma non possono essere modificati. I valori delle altre impostazioni (contrassegnate nel criterio con l'icona ) possono essere modificati nella console dell'applicazione.

Le impostazioni configurate nel criterio attivo e contrassegnate con l'icona  impediscono inoltre le modifiche in Kaspersky Security Center per un computer nella finestra **Proprietà: <nome computer>**.

Le impostazioni, specificate e inviate al computer locale tramite un criterio attivo, vengono salvate nelle impostazioni dell'attività locale in seguito alla disattivazione del criterio attivo.

Se il criterio definisce impostazioni per un'attività Protezione in tempo reale e se un'attività di questo tipo è attualmente in esecuzione, le impostazioni definite dal criterio saranno modificate non appena il criterio viene applicato. Se l'attività non è in esecuzione, le impostazioni vengono applicate all'avvio.

Creazione di un criterio

Il processo di creazione di un criterio comprende i seguenti passaggi:



1. Creazione di un criterio tramite la procedura guidata per i criteri. Le impostazioni delle attività Protezione del computer in tempo reale possono essere configurate utilizzando le finestre di dialogo della procedura guidata.
 2. Configurazione delle impostazioni del criterio. Nella finestra **Proprietà: <nome criterio>** del criterio creato è possibile definire le impostazioni delle attività Protezione del computer in tempo reale, le impostazioni generali di Kaspersky Embedded Systems Security 2.2, le impostazioni di Quarantena e Backup, il livello di dettaglio per i log delle attività e le notifiche per utenti e amministratori sugli eventi di Kaspersky Embedded Systems Security 2.2.
- *Per creare un criterio per un gruppo di computer in cui è installato Kaspersky Embedded Systems Security 2.2, eseguire le seguenti operazioni:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console, quindi selezionare il gruppo di amministrazione che contiene i computer per cui creare un criterio.
2. Nel riquadro dei dettagli del gruppo di amministrazione selezionato selezionare la scheda **Criteri** e fare clic sul collegamento **Crea criterio** per avviare la procedura guidata e creare un criterio.

Verrà visualizzata la finestra **Creazione guidata nuovo criterio**.

3. Nella finestra **Selezionare l'applicazione per cui creare un criterio di gruppo** selezionare Kaspersky Embedded Systems Security 2.2 e fare clic su **Avanti**.
4. **Immettere il nome di un criterio di gruppo** nel campo **Nome**.

Il nome del criterio non può contenere i seguenti simboli: " * < : > ? \ | .

5. Per applicare la configurazione del criterio utilizzata per la versione precedente dell'applicazione:
 - a. Selezionare la casella di controllo **Utilizza impostazioni del criterio per la versione precedente dell'applicazione**.
 - b. Fare clic sul pulsante **Sfoggia** e selezionare il criterio da applicare.
 - c. Fare clic su **Avanti**.
6. Nella finestra **Selezione del tipo di operazione** selezionare una delle seguenti opzioni:
 - **Nuovo**, per creare un nuovo criterio con le impostazioni predefinite.
 - **Importa criterio creato con le versioni precedenti di Kaspersky Embedded Systems Security** per utilizzare il criterio di tale versione come modello.
 - Fare clic su **Sfoggia** e selezionare un file di configurazione in cui è archiviato un criterio esistente.
7. Nella finestra **Protezione del computer in tempo reale** configurare le attività Protezione dei file in tempo reale, Utilizzo di KSN e la funzionalità Prevenzione exploit in base alle esigenze. Consentire o impedire l'utilizzo del attività del criterio configurate nei computer locali della rete:
 - Fare clic sul pulsante  per consentire le modifiche alle impostazioni delle attività nei computer della rete e impedire l'applicazione delle impostazioni delle attività configurate nel criterio.
 - Fare clic sul pulsante  per impedire le modifiche alle impostazioni delle attività nei computer della rete e consentire l'applicazione delle impostazioni delle attività configurate nel criterio.

Il nuovo criterio creato utilizza le impostazioni predefinite delle attività di Protezione del computer in tempo reale.

- Per modificare le impostazioni predefinite dell'attività Protezione dei file in tempo reale, fare clic sul pulsante **Impostazioni** nella sezione **Protezione dei file in tempo reale**. Nella finestra visualizzata configurare l'attività in base alle esigenze. Fare clic su **OK**.
- Per modificare le impostazioni predefinite dell'attività Utilizzo di KSN, fare clic sul pulsante **Impostazioni** nella sezione **Utilizzo di KSN**. Nella finestra visualizzata configurare l'attività in base alle esigenze. Fare clic su **OK**.

Per avviare l'attività Utilizzo di KSN, è necessario accettare l'Informativa KSN nella finestra Gestione dei dati (vedere la sezione "Configurazione dell'elaborazione dei dati" a pagina [163](#)).

- Per modificare le impostazioni predefinite del componente Prevenzione exploit, fare clic sul pulsante **Impostazioni** nella sezione **Prevenzione exploit**. Nella finestra visualizzata configurare la funzionalità in base alle esigenze. Fare clic su **OK**.
8. Selezionare uno dei seguenti stati del criterio nella finestra **Creazione di un criterio di gruppo per l'applicazione**:
- **Criterio attivo** se si desidera applicare immediatamente il criterio dopo la creazione. Se è già presente un criterio attivo nel gruppo, questo viene disattivato e viene applicato il nuovo criterio.
 - **Criterio inattivo** se non si desidera applicare immediatamente il criterio creato. In questo caso, il criterio potrebbe essere attivato in seguito.
 - Selezionare la casella di controllo **Apri le proprietà dei criteri subito dopo la relativa creazione** per chiudere automaticamente la **Creazione guidata nuovo criterio** e configurare il criterio creato dopo aver fatto clic sul pulsante **Avanti**.
9. Fare clic sul pulsante **Fine** nella finestra **Complemento della procedura guidata** della procedura guidata.

Il criterio creato verrà visualizzato nell'elenco dei criteri nella scheda **Criteri** del gruppo di amministrazione selezionato. Nella finestra **Proprietà: <nome criterio>** è possibile configurare altre impostazioni, attività e funzioni di Kaspersky Embedded Systems Security 2.2.

Configurazione di un criterio

Nella finestra **Proprietà: <nome criterio>** di un criterio esistente è possibile configurare le impostazioni generali di Kaspersky Embedded Systems Security 2.2, le impostazioni di Quarantena e Backup, le impostazioni dell'area attendibile, le impostazioni di Protezione in tempo reale, le impostazioni di Controllo attività locali, il livello di dettaglio per i log delle attività, nonché le notifiche per utenti e amministratori sugli eventi di Kaspersky Embedded Systems Security 2.2, i privilegi di accesso per la gestione dell'applicazione e del Kaspersky Security e le impostazioni di applicazione del profilo criterio.

► *Per configurare le impostazioni del criterio:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console.
2. Espandere il gruppo di amministrazione per cui si desidera configurare le impostazioni del criterio associato, quindi aprire il nodo figlio **Criteri** nel riquadro dei dettagli.

3. Selezionare il criterio da configurare e aprire la finestra **Proprietà: <nome criterio>** utilizzando uno dei seguenti metodi:
 - Selezionare l'opzione **Proprietà** nel menu di scelta rapida del criterio.
 - Fare clic sul collegamento **Proprietà** nel riquadro dei dettagli a destra del criterio selezionato.
 - Fare doppio clic sul criterio selezionato.
4. Nella scheda **Generale**, nella sezione **Stato criterio**, abilitare o disabilitare il criterio. A tale scopo, selezionare una delle seguenti opzioni:
 - **Criterio attivo**, se si desidera applicare il criterio a tutti i computer nel gruppo di amministrazione selezionato.
 - **Criterio inattivo**, se non si desidera applicare il criterio a tutti i computer nel gruppo selezionato.

L'impostazione **Criterio fuori sede** non è disponibile quando si gestisce Kaspersky Embedded Systems Security 2.2.

5. Nelle sezioni **Notifica eventi**, **Impostazioni applicazione**, **Log e notifiche**, **Supplementari** e **Cronologia revisioni** è possibile modificare la configurazione dell'applicazione (vedere la tabella di seguito).
6. Nelle sezioni **Protezione del computer in tempo reale**, **Controllo attività locali**, **Controllo attività di rete** e **Analisi sistema** configurare le impostazioni dell'applicazione e le impostazioni di avvio dell'applicazione (vedere la seguente tabella).

È possibile abilitare o disabilitare l'esecuzione di qualsiasi attività in tutti i computer nel gruppo di amministrazione tramite un criterio di Kaspersky Security Center.
È possibile configurare l'applicazione delle impostazioni del criterio in tutti i computer della rete per ogni singolo componente software.

7. Fare clic su **OK**.

Le impostazioni configurate verranno applicate nel criterio.

Istruzioni dettagliate su come configurare le impostazioni delle attività e le funzioni dell'applicazione tramite la console dell'applicazione sono disponibili nelle relative sezioni del *Manuale Utente di Kaspersky Embedded Systems Security 2.2*.

Sezioni con le impostazioni dei criteri di Kaspersky Embedded Systems Security 2.2

Generale

Nella sezione **Generale** è possibile configurare le seguenti impostazioni dei criteri:

- Indicare lo stato del criterio.
- Configurare l'ereditarietà delle impostazioni dai criteri padre e per i criteri figlio.

Notifiche degli eventi

Nella sezione **Notifiche degli eventi** è possibile configurare le impostazioni per le seguenti categorie di eventi:

- *Eventi critici*
- *Errore*
- *Avvisi*
- *Evento informativo*

È possibile utilizzare il pulsante **Proprietà** per configurare le seguenti impostazioni per gli eventi selezionati:

- Indicare il percorso di archiviazione e il periodo di conservazione delle informazioni sugli eventi registrati.
- Indicare il metodo di notifica sugli eventi registrati.

Impostazioni dell'applicazione

Tabella 19. Impostazioni della sezione Impostazioni applicazione

Sezione	Opzioni
Scalabilità e interfaccia	Nella sezione Scalabilità e interfaccia è possibile fare clic sul pulsante Impostazioni per configurare le seguenti impostazioni: <ul style="list-style-type: none"> • Scegliere se configurare le impostazioni di scalabilità automaticamente o manualmente. • Configurare le impostazioni per la visualizzazione dell'icona dell'applicazione.
Sicurezza	Nella sezione Sicurezza e affidabilità è possibile fare clic sul pulsante Impostazioni per configurare le seguenti impostazioni: <ul style="list-style-type: none"> • Configurare le impostazioni di esecuzione dell'attività. • Specificare il comportamento dell'applicazione quando il computer passa all'alimentazione tramite UPS. • Abilitare o disabilitare la protezione tramite password delle funzioni dell'applicazione.
Connessioni	Nella sezione Connessioni è possibile utilizzare il pulsante Impostazioni per configurare le seguenti impostazioni del server proxy per la connessione con i server degli aggiornamenti, i server di attivazione e KSN: <ul style="list-style-type: none"> • Configurare le impostazioni del server proxy. • Specificare le impostazioni per l'autenticazione del server proxy.
Eeguire le attività di sistema	Nella sottosezione Eeguire le attività di sistema è possibile utilizzare il pulsante Impostazioni per consentire o impedire l'avvio delle seguenti attività di sistema in base a una pianificazione configurata nei computer locali: <ul style="list-style-type: none"> • Attività Scansione su richiesta. • Attività Aggiornamento e Copia degli aggiornamenti.

Supplementari

Tabella 20. Impostazioni della sezione Supplementari

Sezione	Opzioni
Area attendibile	Fare clic sul pulsante Impostazioni nella sezione Area attendibile per configurare le seguenti impostazioni dell'area attendibile: <ul style="list-style-type: none"> • Creare un elenco di esclusioni dell'area attendibile. • Abilitare o disabilitare la scansione delle operazioni di backup dei file. • Creare un elenco di processi attendibili.
Scansione unità rimovibili	Fare clic sul pulsante Impostazioni per configurare le impostazioni di scansione per le unità USB rimovibili.
Autorizzazioni di accesso utente per la gestione dell'applicazione	In questa sezione è possibile configurare i diritti di utenti e gruppi di utenti per la gestione di Kaspersky Embedded Systems Security 2.2.

Sezione	Opzioni
Autorizzazioni di accesso utente per la gestione del servizio Security	In questa sezione è possibile configurare i diritti di utenti e gruppi di utenti per la gestione del servizio di Kaspersky Security.
Archivi	Nella sottosezione Archivi fare clic sul pulsante Impostazioni per configurare le seguenti impostazioni di Quarantena e Backup: <ul style="list-style-type: none"> • Specificare il percorso della cartella in cui si desidera inserire gli oggetti in Quarantena o in Backup. • Configurare la dimensione massima di Backup e Quarantena e specificare la soglia per lo spazio disponibile. • Specificare il percorso della cartella in cui si desidera posizionare gli oggetti ripristinati da Quarantena o Backup. • Configurare la trasmissione ad Administration Server delle informazioni sugli oggetti in Quarantena e Backup.

Protezione del computer in tempo reale

Tabella 21. Impostazioni della sezione Protezione del computer in tempo reale

Sezione	Opzioni
Protezione dei file in tempo reale	Nella sezione Protezione dei file in tempo reale è possibile fare clic sul pulsante Impostazioni per configurare le seguenti impostazioni dell'attività: <ul style="list-style-type: none"> • Indicare la modalità di protezione. • Configurare l'utilizzo dell'analizzatore euristico. • Configurare l'utilizzo dell'area attendibile. • Indicare l'ambito della protezione. • Impostare il livello di sicurezza per l'ambito della protezione selezionato: è possibile selezionare un livello di sicurezza predefinito o configurare le impostazioni di sicurezza manualmente. • Configurare le impostazioni di avvio dell'attività.
Utilizzo di KSN	Nella sottosezione Utilizzo di KSN è possibile fare clic sul pulsante Impostazioni per configurare le seguenti impostazioni dell'attività: <ul style="list-style-type: none"> • Indicare le azioni da eseguire sugli oggetti non attendibili di KSN. • Configurare il trasferimento dei dati e l'utilizzo di Kaspersky Security Center come server proxy KSN. <p>Fare clic sul pulsante Gestione dei dati per accettare o rifiutare l'Informativa KSN e configurare le impostazioni per lo scambio affidabile dei dati.</p>
Prevenzione exploit	Nella sezione Prevenzione exploit è possibile fare clic sul pulsante Impostazioni per configurare le seguenti impostazioni dell'attività: <ul style="list-style-type: none"> • Selezionare la modalità di protezione della memoria processo. • Indicare le azioni per ridurre i rischi di exploit. • Aggiungere elementi e modificare l'elenco dei processi protetti.

Controllo attività locali

Tabella 22. Impostazioni della sezione Controllo attività locali

Sezione	Opzioni
Controllo dell'avvio delle applicazioni	<p>Nella sezione Controllo dell'avvio delle applicazioni è possibile utilizzare il pulsante Impostazioni per configurare le seguenti impostazioni dell'attività:</p> <ul style="list-style-type: none"> • Selezionare la modalità operativa dell'attività. • Configurare le impostazioni per il controllo dei successivi avvii dell'applicazione. • Indicare l'ambito per l'applicazione delle regole di Controllo dell'avvio delle applicazioni. • Configurare l'utilizzo di KSN. • Configurare le impostazioni di avvio dell'attività.
Controllo dispositivi	<p>Nella sezione Controllo dispositivi è possibile fare clic sul pulsante Impostazioni per configurare le seguenti impostazioni dell'attività:</p> <ul style="list-style-type: none"> • Selezionare la modalità operativa dell'attività. • Configurare le impostazioni di avvio dell'attività.

Controllo attività di rete

Tabella 23. Impostazioni della sezione Controllo attività di rete

Sezione	Opzioni
Gestione firewall	<p>Nella sezione Gestione firewall è possibile fare clic sul pulsante Impostazioni per configurare le seguenti impostazioni dell'attività:</p> <ul style="list-style-type: none"> • Configurare le regole del firewall. • Configurare le impostazioni di avvio dell'attività.

Analisi sistema

Tabella 24. Impostazioni della sezione Analisi sistema

Sezione	Opzioni
Monitoraggio integrità file	<p>Nella sezione Monitoraggio integrità file è possibile configurare il controllo delle modifiche nei file che possono indicare una violazione della sicurezza in un computer protetto.</p>
Analisi log	<p>Nella sezione Analisi log è possibile configurare un controllo dell'integrità di un computer protetto in base ai risultati dell'analisi del Registro eventi di Windows.</p>

Log e notifiche

Tabella 25. Impostazioni della sezione Log e notifiche

Sezione	Opzioni
Log delle attività	<p>Nella sezione Log delle attività è possibile fare clic sul pulsante Impostazioni per configurare le seguenti impostazioni:</p> <ul style="list-style-type: none"> • Specificare il livello di importanza degli eventi registrati per i componenti software selezionati. • Specificare le impostazioni di archiviazione dell'attività. • Specificare l'integrazione SIEM con le impostazioni di Kaspersky Security Center.

Sezione	Opzioni
Notifiche degli eventi	Nella sezione Notifiche degli eventi è possibile fare clic sul pulsante Impostazioni per configurare le seguenti impostazioni: <ul style="list-style-type: none"> • Specificare le impostazioni delle notifiche agli utenti per l'evento <i>Oggetto rilevato</i>. • Specificare le impostazioni delle notifiche agli amministratori per qualsiasi evento selezionato nell'elenco di eventi nella sezione Impostazioni di notifica.
Interazione con Administration Server	Nella sezione Interazione con Administration Server è possibile fare clic sul pulsante Impostazioni per selezionare i tipi di oggetti che Kaspersky Embedded Systems Security 2.2 segnalerà ad Administration Server.

Cronologia revisioni

Nella sezione **Cronologia revisioni** è possibile gestire le revisioni: confrontarle con la revisione corrente o con un altro criterio, aggiungere descrizioni delle revisioni, salvare le revisioni in un file o eseguire un rollback.

Configurazione dell'avvio pianificato delle attività locali di sistema

È possibile utilizzare i criteri per consentire o impedire l'avvio dell'attività locale di sistema Scansione su richiesta e dell'attività Aggiornamento in base alla pianificazione configurata in locale in ogni computer del gruppo di amministrazione:

- Se l'avvio pianificato di un tipo specifico di attività locale di sistema è vietato da un criterio, queste attività non verranno eseguite nel computer locale in base alla pianificazione. È possibile avviare le attività locali di sistema manualmente.
- Se l'avvio pianificato di un tipo specifico di attività locale di sistema è consentito da un criterio, queste attività verranno eseguite in conformità ai parametri pianificati configurati in locale per questa attività.

Per impostazione predefinita, l'avvio delle attività locali di sistema è vietato dal criterio.

È consigliabile non consentire l'avvio delle attività locali di sistema se gli aggiornamenti o le scansioni su richiesta sono gestiti dalle attività di gruppo di Kaspersky Security Center.

Se non si utilizzano attività di aggiornamento di gruppo o di scansione su richiesta, consentire l'avvio delle attività locali di sistema nel criterio: Kaspersky Embedded Systems Security 2.2 eseguirà gli aggiornamenti dei moduli e dei database dell'applicazione e avvierà tutte le attività locali di sistema e le attività di scansione su richiesta in base alla pianificazione predefinita.

È possibile utilizzare i criteri per consentire o impedire l'avvio pianificato delle seguenti attività locali di sistema:

- Attività Scansione su richiesta: Scansione aree critiche, Scansione degli oggetti in quarantena, Scansione all'avvio del sistema operativo, verifica dell'integrità dei moduli software.
- Attività Aggiornamento: Aggiornamento database, Aggiornamento moduli software e Copia degli aggiornamenti.

Se il computer protetto è escluso dal gruppo di amministrazione, la pianificazione delle attività di sistema sarà abilitata automaticamente.

► Per consentire o impedire l'avvio pianificato delle attività di sistema di Kaspersky Embedded Systems Security 2.2 in un criterio, eseguire le seguenti operazioni:

1. Nel nodo **Dispositivi gestiti** nell'albero di Administration Console espandere il gruppo desiderato e selezionare la scheda **Criteri**.
2. Nella scheda **Criteri**, nel menu di scelta rapida del criterio con cui si desidera configurare l'avvio pianificato delle attività di sistema di Kaspersky Embedded Systems Security 2.2 nei computer del gruppo, selezionare il comando **Proprietà**.
3. Nella finestra **Proprietà: <nome criterio>** aprire la sezione **Impostazioni applicazione**. Nella sezione **Eeguire le attività di sistema** fare clic sul pulsante **Impostazioni** e procedere come segue:
 - Selezionare le caselle di controllo **Consenti l'avvio delle attività di scansione su richiesta e Consenti l'avvio delle attività di aggiornamento e dell'attività di copia degli aggiornamenti** per consentire l'avvio pianificato delle attività elencate.
 - Deselezionare le caselle di controllo **Consenti l'avvio delle attività di scansione su richiesta e Consenti l'avvio delle attività di aggiornamento e dell'attività di copia degli aggiornamenti** per impedire l'avvio pianificato delle attività elencate.

La selezione o la deselezione della casella di controllo non influirà sulle impostazioni di avvio delle attività locali personalizzate di questo tipo.

4. Verificare che il criterio (vedere la sezione "Informazioni sui criteri" a pagina [86](#)) da configurare sia attivo e applicato al gruppo di computer selezionato.
5. Fare clic su **OK**.

Le impostazioni di avvio delle attività pianificate configurate verranno applicate per le attività selezionate.

Creazione e configurazione delle attività tramite Kaspersky Security Center

Questa sezione contiene informazioni sulle attività di Kaspersky Embedded Systems Security 2.2, su come crearle, configurarne le impostazioni, nonché su come avviarle e arrestarle.

In questo capitolo

Informazioni sulla creazione di attività in Kaspersky Security Center	95
Creazione di un'attività tramite Kaspersky Security Center.....	96
Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center.....	100
Configurazione di attività di gruppo in Kaspersky Security Center.....	101
Creazione di un'attività Scansione su richiesta	111
Configurazione delle impostazioni di diagnostica degli arresti anomali in Kaspersky Security Center.....	117
Gestione delle pianificazioni delle attività	119

Informazioni sulla creazione di attività in Kaspersky Security Center

È possibile creare attività di gruppo per gruppi di amministrazione e set di computer. È possibile creare i seguenti tipi di attività:

- Attivazione dell'applicazione
- Copia degli aggiornamenti
- Aggiornamento database
- Aggiornamento moduli software
- Rollback dell'aggiornamento database
- Scansione su richiesta
- Controllo dell'integrità dell'applicazione
- Generazione regole per Controllo dell'avvio delle applicazioni
- Generazione regole per Controllo dispositivi

È possibile creare attività locali e di gruppo nei seguenti modi:

- Per un solo computer: nella finestra **Proprietà <nome computer>** nella sezione **Attività**.
- Per un gruppo di amministrazione: nel riquadro dei dettagli del nodo del gruppo di computer selezionato nella scheda **Attività**.
- Per un set di computer: nel riquadro dei dettagli del nodo **Selezioni dispositivi**.

Utilizzando i criteri è possibile disabilitare le pianificazioni per le attività locali di sistema di aggiornamento e Scansione su richiesta (vedere la sezione "Configurazione dell'avvio pianificato delle attività locali di sistema" a pagina 93) in tutti i computer protetti dallo stesso gruppo di amministrazione.

Informazioni generali sulle attività di Kaspersky Security Center sono disponibili nella *Guida di Kaspersky Security Center*.

Creazione di un'attività tramite Kaspersky Security Center

Il processo di configurazione delle impostazioni dei componenti funzionali di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center è simile alla configurazione locale delle impostazioni di questi componenti nella console dell'applicazione. Istruzioni dettagliate su come configurare le impostazioni delle attività e le funzioni dell'applicazione sono disponibili nelle relative sezioni del *Manuale Utente di Kaspersky Embedded Systems Security 2.2*.

► *Per creare una nuova attività in Kaspersky Security Center Administration Console:*

1. Avviare la procedura guidata dell'attività in uno dei seguenti modi:
 - Per creare un'attività locale:
 - a. Espandere il nodo **Dispositivi gestiti** nell'albero di Administration Console e selezionare il gruppo a cui appartiene il computer protetto.
 - b. Nel riquadro dei dettagli, nella scheda **Dispositivi**, aprire il menu di scelta rapida del computer protetto e selezionare **Proprietà**.
 - c. Nella finestra visualizzata fare clic sul pulsante **Aggiungi** nella sezione **Attività**.
 - Per creare un'attività di gruppo:
 - a. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo per cui si desidera creare un'attività.
 - b. Nel riquadro dei dettagli aprire la scheda **Attività** e selezionare **Crea un'attività**.
 - Per creare un'attività per un set personalizzato di computer, nel nodo **Selezioni dispositivi** nell'albero di Kaspersky Security Center Administration Console selezionare **Crea un'attività**.

Verrà visualizzata la finestra della procedura guidata dell'attività.

2. Nella finestra **Selezionare il tipo di attività**, sotto l'intestazione **Kaspersky Embedded Systems Security 2.2**, selezionare il tipo di attività da creare.

3. Se è stato selezionato qualsiasi tipo di attività ad eccezione di Rollback dell'aggiornamento database o Attivazione dell'applicazione, verrà visualizzata la finestra **Impostazioni**. A seconda del tipo di attività creata, eseguire una delle seguenti operazioni:

- *Per creare un'attività Scansione su richiesta:*

a. Creare un ambito della scansione nella finestra **Ambito della scansione**.

Per impostazione predefinita, l'ambito della scansione include le aree critiche del computer. Gli ambiti della scansione sono contrassegnati nella tabella con l'icona .

È possibile modificare l'ambito della scansione: aggiungere specifici ambiti della scansione preimpostati, dischi, cartelle, oggetti di rete e file e assegnare specifiche impostazioni di sicurezza per ogni ambito aggiunto.

- Per escludere tutte le aree critiche dalla scansione, aprire il menu di scelta rapida di ciascuna delle righe e selezionare l'opzione **Rimuovi ambito**.
- Per includere un ambito della scansione predefinito, un disco, una cartella, un oggetto di rete o un file nell'ambito della scansione, fare clic con il pulsante destro del mouse sulla tabella **Ambito della scansione** e selezionare **Aggiungi ambito**. Nella finestra **Aggiungi oggetti all'ambito della scansione** selezionare l'ambito predefinito nell'elenco **Ambito predefinito**, specificare l'unità del computer, la cartella, l'oggetto di rete o il file sul computer o su un altro computer della rete, quindi fare clic sul pulsante **OK**.
- Per escludere sottocartelle o file dalla scansione, selezionare la cartella aggiunta (o il disco) nella finestra **Ambito della scansione** della procedura guidata, aprire il menu di scelta rapida e selezionare l'opzione **Configura**, quindi fare clic sul pulsante **Impostazioni** nella finestra **Livello di sicurezza**. Nella finestra **Impostazioni di scansione su richiesta**, nella scheda **Generale**, deselegionare le caselle di controllo **Sottocartelle** e **File secondari**.
- Per modificare le impostazioni di sicurezza dell'ambito della scansione, aprire il menu di scelta rapida dell'ambito di cui si desidera configurare le impostazioni e selezionare **Configura**. Nella finestra **Impostazioni di scansione su richiesta** selezionare uno dei livelli di sicurezza predefiniti o fare clic sul pulsante **Impostazioni** per configurare manualmente le impostazioni di sicurezza. La configurazione delle impostazioni di sicurezza viene eseguita così come avviene nella console di Kaspersky Embedded Systems Security 2.2.
- Per ignorare gli oggetti incorporati nell'ambito della scansione aggiunto, aprire il menu di scelta rapida nella tabella **Ambito della scansione**, selezionare **Aggiungi esclusione** e specificare gli oggetti da escludere: selezionare l'ambito predefinito nell'elenco **Ambito predefinito**, specificare il disco del computer, la cartella, l'oggetto di rete o il file sul computer protetto o su un altro computer della rete, quindi fare clic sul pulsante **OK**.
- Gli ambiti della scansione esclusi sono contrassegnati con l'icona nella tabella.

b. Eseguire le seguenti operazioni nella finestra **Opzioni**.

Selezionare la casella di controllo **Applica area attendibile** se si desidera escludere gli oggetti descritti nell'area attendibile di Kaspersky Embedded Systems Security 2.2 dall'ambito della scansione dell'attività.

Se si prevede di utilizzare l'attività creata come un'attività Scansione aree critiche, selezionare la casella di controllo **Esegui attività in background** nella finestra **Opzioni**. Kaspersky Security Center valuta la classificazione di sicurezza di uno o più computer in base ai risultati dell'esecuzione delle attività con lo stato *Scansione aree critiche*, non solo in base ai risultati dell'esecuzione delle attività di sistema **Scansione aree critiche**. Durante la creazione di un'attività locale Scansione su richiesta, questa casella di controllo non è disponibile.

Per assegnare la priorità di base **Basso** al processo di lavoro in cui sarà eseguita l'attività,

selezionare la casella di controllo **Esegui attività in background** nella finestra **Opzioni**. Per impostazione predefinita, i processi di lavoro in cui vengono eseguite le attività di Kaspersky Embedded Systems Security 2.2 hanno la priorità **Medio** (Normale). La riduzione della priorità del processo aumenta il tempo necessario per l'esecuzione dell'attività, ma può avere un effetto positivo sulla velocità di esecuzione dei processi di altri programmi attivi.

- *Per creare un'attività di aggiornamento*, configurare le impostazioni dell'attività in base agli specifici requisiti:
 - a. Selezionare la sorgente degli aggiornamenti nella finestra **Sorgente degli aggiornamenti**.
 - b. Fare clic sul pulsante **Impostazioni di connessione**. Verrà visualizzata la finestra **Impostazioni di connessione**.
 - c. Nella finestra **Impostazioni di connessione**:

Specificare la modalità del server FTP per la connessione al computer protetto.

Modificare il timeout della connessione alla sorgente degli aggiornamenti, se necessario.

Configurare le impostazioni di accesso al server proxy per la connessione alla sorgente degli aggiornamenti.

Specificare la posizione dei computer protetti per ottimizzare il download degli aggiornamenti.
- *Per creare l'attività Aggiornamento moduli software*, configurare le impostazioni desiderate per l'aggiornamento dei moduli del programma nella finestra **Impostazioni per gli aggiornamenti dei moduli software dell'applicazione**:
 - a. Scegliere se copiare e installare gli aggiornamenti dei moduli software critici o verificarne solo la disponibilità senza eseguire l'installazione.
 - b. Se è selezionata l'opzione **Copia e installa gli aggiornamenti dei moduli software critici**, può essere necessario il riavvio del computer per l'applicazione dei moduli software installati. Se si desidera che Kaspersky Embedded Systems Security 2.2 riavvii automaticamente il computer dopo il completamento dell'attività, selezionare la casella di controllo **Consenti il riavvio del sistema operativo**. Per disabilitare il riavvio automatico del computer dopo il completamento dell'attività, deselezionare la casella di controllo **Consenti il riavvio del sistema operativo**.
 - c. Per ottenere informazioni sugli aggiornamenti dei moduli di Kaspersky Embedded Systems Security 2.2, selezionare **Ricevi informazioni sugli aggiornamenti dei moduli software pianificati disponibili**.

Kaspersky Lab non pubblica i pacchetti di aggiornamento pianificati nei server di aggiornamento per l'installazione automatica: tali pacchetti possono essere scaricati manualmente dal sito Web di Kaspersky Lab. È possibile configurare una notifica per gli amministratori sull'evento **È disponibile un nuovo aggiornamento pianificato dei moduli software**. Questa notifica conterrà l'URL del sito Web di Kaspersky Lab da cui possono essere scaricati gli aggiornamenti pianificati.
- *Per creare l'attività Copia degli aggiornamenti*, specificare il set di aggiornamenti e la cartella di destinazione nella finestra **Impostazioni di copia degli aggiornamenti**.
- *Per creare l'attività Attivazione dell'applicazione*, nella finestra **Impostazioni di attivazione** applicare il file chiave che si desidera utilizzare per attivare l'applicazione. Selezionare la casella di controllo **Usa come chiave di riserva** se si desidera creare un'attività per rinnovare la licenza.
- *Per creare l'attività Generazione regole per Controllo dell'avvio delle applicazioni o Generazione regole per Controllo dispositivi*, nella finestra **Impostazioni** specificare le impostazioni in base alle quali sarà creato l'elenco delle regole di permesso:
 - a. Specificare un prefisso per i nomi delle regole (solo l'attività Generazione regole per Controllo

- dell'avvio delle applicazioni).
- b. Configurare l'ambito di applicazione delle regole di permesso (solo per l'attività Generazione regole per Controllo dell'avvio delle applicazioni). Fare clic sul pulsante **Avanti**.
 - c. Specificare le azioni che verranno eseguite dall'attività durante la generazione delle regole di permesso (solo per l'attività Generazione regole per Controllo dell'avvio delle applicazioni) e dopo il completamento dell'attività.
4. Configurare la pianificazione dell'attività (è possibile configurare una pianificazione per tutti i tipi di attività tranne l'attività Rollback dell'aggiornamento database). Eseguire le seguenti operazioni nella finestra **Pianificazione**:
- a. Selezionare la casella di controllo **Esegui in base alla pianificazione** per abilitare la pianificazione.
 - b. Specificare la frequenza di avvio dell'attività: selezionare uno dei seguenti valori dall'elenco **Frequenza: Ogni ora, Ogni giorno, Ogni settimana, All'avvio dell'applicazione, Dopo l'aggiornamento del database dell'applicazione** (è anche possibile specificare la frequenza di avvio **Dopo il recupero degli aggiornamenti da parte di Administration Server** nelle seguenti attività di gruppo: Aggiornamento database e Aggiornamento moduli software):
 - Se è selezionata l'opzione **Ogni ora**, specificare il numero di ore in **Ogni <numero> ora/e** nel gruppo di configurazione **Impostazioni avvio attività**.
 - Se è selezionata l'opzione **Ogni giorno**, specificare il numero di giorni in **Ogni <numero> giorno/i** nel gruppo di configurazione **Impostazioni avvio attività**.
 - Se è selezionata l'opzione **Ogni settimana**, specificare il numero di settimane in **Ogni <numero> settimana/e** nel gruppo di configurazione **Impostazioni avvio attività**. Specificare in quali giorni della settimana sarà avviata l'attività (per impostazione predefinita, il lunedì).
 - c. Nel campo **Ora avvio** specificare l'ora di avvio dell'attività. Nel campo **Data avvio** specificare la data in cui diventerà effettiva la pianificazione.
 - d. Specificare le impostazioni di pianificazione rimanenti, se necessario: fare clic sul pulsante **Avanzate** ed eseguire le seguenti operazioni nella finestra **Impostazioni avanzate pianificazione**:
 - Specificare la durata massima dell'esecuzione dell'attività: immettere il numero di ore e minuti nel campo **Durata** del gruppo di configurazione **Impostazioni arresto attività**.
 - Specificare l'intervallo di tempo entro un periodo di 24 ore per cui l'esecuzione di un'attività deve essere sospesa: nel gruppo di configurazione **Impostazioni arresto attività** immettere i valori di inizio e fine dell'intervallo nei campi **Sospendi da e a**.
 - Specificare la data a cui sarà disabilitata la pianificazione: selezionare la casella di controllo **Annulla pianificazione da** e selezionare la data in cui sarà disabilitata la pianificazione utilizzando la finestra **Calendario**.
 - Abilitare l'avvio delle attività perse: selezionare la casella di controllo **Esegui attività ignorate**.
 - Abilitare l'impostazione per la distribuzione dell'ora di avvio: selezionare la casella di controllo **Imposta come casuale l'ora di avvio dell'attività entro un intervallo di** e specificare il valore in minuti.
 - e. Fare clic su **OK**.
5. Se l'attività creata è per dei set di computer, selezionare i computer della rete (il gruppo) in cui sarà eseguita l'attività.
 6. Nella finestra **Selezione di un account per l'esecuzione dell'attività** specificare l'account con cui si desidera eseguire l'attività.
 7. Nella finestra **Definire il nome dell'attività** immettere il nome dell'attività (non più di 100 caratteri) senza

utilizzare i simboli " * < > ? \ | : . È consigliabile aggiungere al nome il tipo di attività (ad esempio, "Scansione su richiesta delle cartelle condivise").

8. Nella finestra **Completamento della creazione dell'attività** selezionare la casella di controllo **Esegui l'attività al termine della procedura guidata** se si desidera avviare l'attività non appena creata. Fare clic sul pulsante **Fine**.

L'attività creata verrà visualizzata nell'elenco **Attività**.

Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center

► *Per configurare le attività locali o le impostazioni generali dell'applicazione nella finestra Impostazioni applicazione per un singolo computer della rete, procedere come segue:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Server e selezionare il gruppo a cui appartiene il computer protetto.
2. Nel riquadro dei dettagli selezionare la scheda **Dispositivi**.
3. Aprire la finestra **Proprietà: <nome computer>** in uno dei seguenti modi:
 - Fare doppio clic sul nome del computer protetto.
 - Aprire il menu di scelta rapida del nome del computer protetto e selezionare **Proprietà**.

Verrà visualizzata la finestra **Proprietà: <nome computer>**.

4. Per configurare le impostazioni dell'attività locale, eseguire le seguenti operazioni:
 - a. Accedere alla sezione **Attività**.
 - Nell'elenco delle attività selezionare un'attività locale da configurare.
 - Fare doppio clic sul nome dell'attività nell'elenco delle attività.
 - Selezionare il nome dell'attività, quindi fare clic sul pulsante **Proprietà**.
 - Selezionare **Proprietà** nel menu di scelta rapida dell'attività selezionata.
5. Per configurare le impostazioni dell'applicazione, eseguire le seguenti operazioni:
 - a. Accedere alla sezione **Applicazioni**.
 - Nell'elenco delle applicazioni installate selezionare un'applicazione da configurare.
 - Fare doppio clic sul nome dell'applicazione nell'elenco delle applicazioni installate.
 - Selezionare il nome dell'applicazione nell'elenco delle applicazioni installate e fare clic sul pulsante **Proprietà**.
 - Aprire il menu di scelta rapida del nome dell'applicazione nell'elenco delle applicazioni installate e selezionare **Proprietà**.

Se all'applicazione è applicato un criterio di Kaspersky Security Center e questo criterio proibisce la modifica delle impostazioni dell'applicazione, queste impostazioni non possono essere modificate tramite la finestra **Impostazioni applicazione**.

Il processo di configurazione delle impostazioni dei componenti funzionali di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center è simile alla configurazione locale delle impostazioni di questi componenti nella console dell'applicazione. Istruzioni dettagliate su come configurare le impostazioni delle attività e le funzioni dell'applicazione sono disponibili nelle relative sezioni del *Manuale Utente di Kaspersky Embedded Systems Security 2.2*.

Configurazione di attività di gruppo in Kaspersky Security Center

Il processo di configurazione delle impostazioni dei componenti funzionali di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center è simile alla configurazione locale delle impostazioni di questi componenti nella console dell'applicazione. Istruzioni dettagliate su come configurare le impostazioni delle attività e le funzioni dell'applicazione sono disponibili nelle relative sezioni del *Manuale Utente di Kaspersky Embedded Systems Security 2.2*.

► Per configurare l'attività di gruppo per più computer:

1. Nell'albero di Kaspersky Security Center Administration Console espandere il nodo **Dispositivi gestiti** e selezionare il gruppo di amministrazione per cui si desidera configurare le attività dell'applicazione.
2. Nel riquadro dei dettagli di un gruppo di amministrazione selezionato aprire la scheda **Attività**.
3. Nell'elenco delle attività di gruppo create in precedenza selezionare un'attività da configurare. Aprire la finestra **Proprietà: <nome attività>** in uno dei seguenti modi:
 - Fare doppio clic sul nome dell'attività nell'elenco delle attività create.
 - Selezionare il nome dell'attività nell'elenco delle attività create e fare clic sul collegamento **Configura attività**.
 - Aprire il menu di scelta rapida del nome dell'attività nell'elenco delle attività create e selezionare **Proprietà**.
4. Nella sezione **Notifica** configurare le impostazioni di notifica degli eventi dell'attività.

Per informazioni dettagliate sulla configurazione delle impostazioni in questa sezione, vedere la *Guida di Kaspersky Security Center*.

5. A seconda del tipo di attività configurata, eseguire una delle seguenti operazioni:
 - Per configurare un'attività Scansione su richiesta:
 - a. Nella sezione **Ambito della scansione** configurare un ambito della scansione.
 - b. Nella sezione **Opzioni** configurare il livello di priorità dell'attività e l'integrazione con altri componenti software.
 - Per configurare un'attività di aggiornamento, definire le impostazioni dell'attività in base agli specifici requisiti:
 - a. Nella sezione **Impostazioni** configurare le impostazioni della sorgente degli aggiornamenti e

l'ottimizzazione dell'utilizzo del sottosistema del disco.

- b. Fare clic sul pulsante **Impostazioni di connessione** per configurare le impostazioni di connessione per la sorgente degli aggiornamenti.
 - Per configurare l'attività Aggiornamento moduli software, nella sezione **Impostazioni per gli aggiornamenti dei moduli software dell'applicazione** scegliere un'azione da eseguire: copiare e installare gli aggiornamenti critici dei moduli software o verificarne solo la disponibilità.
 - Per configurare l'attività Copia degli aggiornamenti, specificare il set di aggiornamenti e la cartella di destinazione nella sezione **Impostazioni di copia degli aggiornamenti**.
 - Per configurare l'attività Attivazione dell'applicazione, nella sezione **Impostazioni di attivazione** applicare il file chiave che si desidera utilizzare per attivare l'applicazione. Selezionare la casella di controllo **Usa come codice di attivazione o chiave di riserva** se si desidera aggiungere un codice di attivazione o una chiave per rinnovare la licenza.
 - Per configurare la generazione automatica delle regole di permesso per il controllo del computer, nella sezione **Impostazioni** specificare le impostazioni in base alle quali sarà creato l'elenco delle regole di permesso.
6. Configurare la pianificazione dell'attività nella sezione **Pianificazione** (è possibile configurare una pianificazione per tutti i tipi di attività tranne Rollback dell'aggiornamento database).
7. Nella sezione **Account** specificare l'account del quale saranno utilizzati i diritti per l'esecuzione dell'attività. Per informazioni dettagliate sulla configurazione delle impostazioni in questa sezione, vedere la *Guida di Kaspersky Security Center*.
8. Se necessario, specificare gli oggetti da escludere dall'ambito dell'attività nella sezione **Esclusioni dall'ambito dell'attività**. Per informazioni dettagliate sulla configurazione delle impostazioni in questa sezione, vedere la *Guida di Kaspersky Security Center*.
9. Nella finestra **Proprietà: <nome attività>** fare clic su **OK**.

Le nuove impostazioni delle attività di gruppo configurate verranno salvate.

Le impostazioni delle attività di gruppo che sono disponibili per la configurazione sono riassunte nella seguente tabella.

Tabella 26. Impostazioni delle attività di gruppo di Kaspersky Embedded Systems Security 2.2

Tipi di attività di Kaspersky Embedded Systems Security 2.2	Sezione nella finestra Proprietà: <nome attività>	Impostazioni delle attività
Generazione regola automatica (vedere la sezione "Attività Generazione regole per Controllo dell'avvio delle applicazioni e Generazione regole per Controllo dispositivi" a pagina 106)	Impostazioni	Durante la configurazione delle impostazioni dell'attività Generazione regole per Controllo dell'avvio delle applicazioni, è possibile: <ul style="list-style-type: none"> • Modificare l'ambito della protezione aggiungendo o rimuovendo i percorsi delle cartelle e specificando i tipi di file per cui l'avvio è consentito dalle regole generate automaticamente. • Tenere conto delle applicazioni attualmente in esecuzione.

Tipi di attività di Kaspersky Embedded Systems Security 2.2	Sezione nella finestra Proprietà: <nome attività>	Impostazioni delle attività
	Opzioni	<p>È possibile specificare le azioni da eseguire durante la creazione delle regole di permesso per il controllo dell'avvio delle applicazioni:</p> <ul style="list-style-type: none"> • Usa certificato digitale • Usa soggetto e identificazione personale del certificato digitale • Se il certificato risulta mancante, usa • Usa hash SHA256 • Genera regole per l'utente o il gruppo di utenti <p>È possibile configurare le impostazioni per i file di configurazione con gli elenchi delle regole di permesso che Kaspersky Embedded Systems Security 2.2 crea dopo il completamento dell'attività.</p>
	Pianificazione	È possibile configurare le impostazioni per l'avvio pianificato dell'attività.
Attivazione dell'applicazione (vedere la sezione "Attività Attivazione dell'applicazione" a pagina 108)	Impostazioni di attivazione	Per attivare l'applicazione o rinnovare la data di scadenza, è possibile aggiungere una chiave.
	Pianificazione	È possibile configurare le impostazioni per l'avvio pianificato dell'attività.
Copia degli aggiornamenti (vedere la sezione "Attività di aggiornamento" a pagina 108)	Sorgente degli aggiornamenti	<p>È possibile specificare Kaspersky Security Center Administration Server o i server di aggiornamento di Kaspersky Lab come sorgente degli aggiornamenti dell'applicazione. È anche possibile creare un elenco personalizzato di sorgenti degli aggiornamenti: aggiungendo manualmente server HTTP e FTP personalizzati o cartelle di rete e impostandoli come sorgenti degli aggiornamenti.</p> <p>È possibile specificare l'utilizzo dei server di aggiornamento di Kaspersky Lab, se i server personalizzati manualmente non sono disponibili.</p>
	Finestra Impostazioni di connessione	Nella casella di gruppo Impostazioni di connessione alla sorgente degli aggiornamenti è possibile specificare se la connessione ai server di aggiornamento di Kaspersky Lab o ad altri server deve essere stabilita tramite un server proxy.
	Impostazioni di copia degli aggiornamenti	È possibile specificare il set di aggiornamenti per la copia. Nel campo Cartella per l'archiviazione locale degli aggiornamenti copiati specificare il percorso di una cartella che verrà utilizzata da Kaspersky Embedded Systems Security 2.2 per l'archiviazione degli aggiornamenti copiati.

Tipi di attività di Kaspersky Embedded Systems Security 2.2	Sezione nella finestra Proprietà: <nome attività>	Impostazioni delle attività
	Pianificazione	È possibile configurare le impostazioni per l'avvio pianificato dell'attività.
Aggiornamento database (vedere la sezione "Attività di aggiornamento" a pagina 108)	Impostazioni	<p>È possibile specificare Kaspersky Security Center Administration Server o i server di aggiornamento di Kaspersky Lab come sorgente degli aggiornamenti nell'applicazione nella casella di gruppo Sorgente degli aggiornamenti. È anche possibile creare un elenco personalizzato di sorgenti degli aggiornamenti: aggiungendo manualmente server HTTP e FTP personalizzati o cartelle di rete e impostandoli come sorgenti degli aggiornamenti.</p> <p>È possibile specificare l'utilizzo dei server di aggiornamento di Kaspersky Lab, se i server personalizzati manualmente non sono disponibili.</p> <p>Nella sezione Ottimizzazione dell'utilizzo dell'I/O del disco è possibile configurare la funzionalità che riduce il carico di lavoro sul sottosistema del disco:</p> <ul style="list-style-type: none"> • Riduci il carico sull'I/O del disco • RAM utilizzata per l'ottimizzazione (MB)
	Finestra Impostazioni di connessione	Nella casella di gruppo Impostazioni di connessione alla sorgente degli aggiornamenti è possibile specificare se la connessione ai server di aggiornamento di Kaspersky Lab o ad altri server deve essere stabilita tramite un server proxy.
	Pianificazione	È possibile configurare le impostazioni per l'avvio pianificato dell'attività.
Aggiornamento moduli software (vedere la sezione "Attività di aggiornamento" a pagina 108)	Sorgente degli aggiornamenti	<p>È possibile specificare Kaspersky Security Center Administration Server o i server di aggiornamento di Kaspersky Lab come sorgente degli aggiornamenti nell'applicazione. È anche possibile creare un elenco personalizzato di sorgenti degli aggiornamenti: aggiungendo manualmente server HTTP e FTP personalizzati o cartelle di rete e impostandoli come sorgenti degli aggiornamenti.</p> <p>È possibile specificare l'utilizzo dei server di aggiornamento di Kaspersky Lab, se i server personalizzati manualmente non sono disponibili.</p>
	Finestra Impostazioni di connessione	Nella casella di gruppo Impostazioni di connessione alla sorgente degli aggiornamenti è possibile specificare se la connessione ai server di aggiornamento di Kaspersky Lab o ad altri server deve essere stabilita tramite un server proxy.

Tipi di attività di Kaspersky Embedded Systems Security 2.2	Sezione nella finestra Proprietà: <nome attività>	Impostazioni delle attività
	Impostazioni per gli aggiornamenti dei moduli software dell'applicazione	È possibile specificare le azioni che devono essere eseguite da Kaspersky Embedded Systems Security 2.2 quando sono disponibili o sono stati già installati aggiornamenti critici dei moduli software e anche se Kaspersky Embedded Systems Security 2.2 deve ricevere informazioni sugli aggiornamenti pianificati.
	Pianificazione	È possibile configurare le impostazioni per l'avvio pianificato dell'attività.
Scansione su richiesta (vedere la sezione "Configurazione dell'attività Scansione su richiesta" a pagina 111).	Ambito della scansione	È possibile specificare un ambito della scansione per l'attività Scansione su richiesta e configurare le impostazioni del livello di sicurezza.
	Finestra Impostazioni di scansione su richiesta	È possibile selezionare uno di livelli di sicurezza predefiniti o personalizzare manualmente il livello di sicurezza.
	Opzioni	<p>È possibile attivare o disattivare l'utilizzo dell'analizzatore euristico per l'attività Scansione su richiesta e impostare il livello di analisi utilizzando un dispositivo di scorrimento nella casella di gruppo Analizzatore euristico.</p> <p>Nella casella di gruppo Integrazione con altri componenti è possibile configurare le seguenti impostazioni:</p> <ul style="list-style-type: none"> • Applicare l'area attendibile per le attività Scansione su richiesta. • Applicare l'utilizzo di KSN per le attività Scansione su richiesta • Impostare una priorità per l'attività Scansione su richiesta: eseguire l'attività in background (priorità bassa) o considerare l'attività una Scansione aree critiche.
	Pianificazione	È possibile configurare le impostazioni per l'avvio pianificato dell'attività.
Verifica dell'integrità dei moduli software (a pagina 110)	Pianificazione	È possibile configurare le impostazioni per l'avvio pianificato dell'attività.

Per attività come Rollback dell'aggiornamento database è possibile configurare solo le impostazioni standard dell'attività nelle sezioni **Notifica** ed **Esclusioni dall'ambito dell'attività**, controllate da Kaspersky Security Center. Per informazioni dettagliate sulla configurazione delle impostazioni in queste sezioni, vedere la *Guida di Kaspersky Security Center*.

In questa sezione

Attività Generazione regole per Controllo dell'avvio delle applicazioni e Generazione regole per Controllo dispositivi	106
Attività Attivazione dell'applicazione	108
Attività Aggiornamento.....	108
Verifica dell'integrità dei moduli software.....	110

Attività Generazione regole per Controllo dell'avvio delle applicazioni e Generazione regole per Controllo dispositivi

► Per configurare l'attività *Generazione regole per Controllo dispositivi* o l'attività *Generazione regole per Controllo dell'avvio delle applicazioni*, procedere come segue:

1. Nell'albero di Kaspersky Security Center Administration Console espandere il nodo **Dispositivi gestiti** e selezionare il gruppo di amministrazione per cui si desidera configurare le attività dell'applicazione.
2. Nel riquadro dei dettagli di un gruppo di amministrazione selezionato aprire la scheda **Attività**.
3. Nell'elenco delle attività di gruppo create in precedenza selezionare un'attività da configurare. Aprire la finestra **Proprietà: <nome attività>** in uno dei seguenti modi:
 - Fare doppio clic sul nome dell'attività nell'elenco delle attività create.
 - Selezionare il nome dell'attività nell'elenco delle attività create e fare clic sul collegamento **Configura attività**.
 - Aprire il menu di scelta rapida del nome dell'attività nell'elenco delle attività create e selezionare **Proprietà**.
4. Nella sezione **Notifica** configurare le impostazioni di notifica degli eventi dell'attività.
5. Per informazioni dettagliate sulla configurazione delle impostazioni in questa sezione, vedere la *Guida di Kaspersky Security Center*.
6. Nella sezione **Impostazioni** è possibile configurare le seguenti impostazioni:
 - Modificare l'ambito della protezione aggiungendo o rimuovendo i percorsi delle cartelle e specificando i tipi di file per cui l'avvio è consentito dalle regole generate automaticamente.
 - Tenere conto delle applicazioni attualmente in esecuzione.
7. Nella sezione **Impostazioni** è possibile specificare le azioni da eseguire durante la creazione delle regole di permesso per il controllo dell'avvio delle applicazioni:
 - **Usa certificato digitale**
 Se questa opzione è selezionata, viene specificata la presenza di un certificato digitale come criterio di attivazione della regola nelle impostazioni delle nuove regole di permesso generate per Controllo dell'avvio delle applicazioni. L'applicazione ora consentirà l'avvio dei programmi avviati utilizzando file con un certificato digitale. Questa opzione è consigliata se si desidera consentire l'avvio di qualsiasi applicazione considerata attendibile nel sistema operativo.
 Questa opzione è selezionata per impostazione predefinita.
 - **Usa soggetto e identificazione personale del certificato digitale**
 Questa casella di controllo consente di abilitare o disabilitare l'utilizzo del soggetto e dell'identificazione personale del certificato digitale del file come criterio per l'attivazione delle

regole di permesso per Controllo dell'avvio delle applicazioni. La selezione di questa casella di controllo consente di specificare condizioni più rigorose per la verifica del certificato digitale.

Se questa casella di controllo è selezionata, i valori del soggetto e dell'identificazione personale del certificato digitale dei file vengono generate le regole sono impostati come criterio per l'attivazione delle regole di permesso per Controllo dell'avvio delle applicazioni. Kaspersky Embedded Systems Security 2.2 consentirà le applicazioni che vengono avviate utilizzando file con un'identificazione personale e un certificato digitale specificati.

La selezione di questa casella di controllo limita notevolmente l'attivazione delle regole di permesso in base a un certificato digitale perché un'identificazione personale è un identificatore univoco di un certificato digitale e non può essere contraffatta.

Se questa casella è deselezionata, l'esistenza di qualsiasi certificato digitale considerato attendibile nel sistema operativo viene impostata come criterio per l'attivazione delle regole di permesso per Controllo dell'avvio delle applicazioni.

Questa casella di controllo è attiva se l'opzione **Usa certificato digitale** è selezionata.

La casella di controllo è selezionata per impostazione predefinita.

- **Se il certificato risulta mancante, usa**

Elenco a discesa che consente di selezionare il criterio per l'attivazione delle regole di permesso per Controllo dell'avvio delle applicazioni se il file utilizzato per generare la regola non ha un certificato digitale.

- **Hash SHA256.** Il valore di checksum del file utilizzato per generare la regola viene impostato come criterio per l'attivazione della regola di permesso per Controllo dell'avvio delle applicazioni. L'applicazione consentirà l'avvio dei programmi avviati utilizzando file con il checksum specificato.
- **Percorso del file.** Il percorso del file utilizzato per generare la regola viene impostato come criterio per l'attivazione della regola di permesso per Controllo dell'avvio delle applicazioni. L'applicazione consentirà l'avvio dei programmi avviati utilizzando i file contenuti nelle cartelle specificate nella scheda della tabella Crea regole di permesso per le applicazioni dalle cartelle.

- **Usa hash SHA256**

Se questa opzione è selezionata, il valore di checksum del file utilizzato per generare la regola viene specificato come criterio di attivazione della regola nelle impostazioni delle nuove regole di permesso generate per Controllo dell'avvio delle applicazioni. L'applicazione consentirà l'avvio dei programmi avviati utilizzando file con il valore di checksum specificato.

Questa opzione è consigliata nei casi in cui le regole generate sono necessarie per soddisfare un livello di sicurezza molto elevato: il checksum SHA256 può essere applicato come un ID univoco del file. L'utilizzo del checksum SHA256 come criterio di attivazione della regola restringe l'ambito di applicazione della regola a un solo file.

- **Genera regole per l'utente o il gruppo di utenti.**

Campo che visualizza un utente e/o un gruppo di utenti. Verrà monitorata qualsiasi applicazione eseguita dall'utente e/o dal gruppo di utenti specificato.

La selezione predefinita è **Everyone**.

È possibile configurare le impostazioni per i file di configurazione con gli elenchi delle regole di permesso che Kaspersky Embedded Systems Security 2.2 crea dopo il completamento dell'attività.

8. Configurare la pianificazione dell'attività nella sezione **Pianificazione** (è possibile configurare una pianificazione per tutti i tipi di attività tranne Rollback dell'aggiornamento database).
9. Nella sezione **Account** specificare l'account del quale saranno utilizzati i diritti per l'esecuzione dell'attività.

10. Se necessario, specificare gli oggetti da escludere dall'ambito dell'attività nella sezione **Esclusioni dall'ambito dell'attività**.

Per informazioni dettagliate sulla configurazione delle impostazioni in queste sezioni, vedere la *Guida di Kaspersky Security Center*.

11. Nella finestra **Proprietà: <nome attività>** fare clic su **OK**.

Le nuove impostazioni delle attività di gruppo configurate verranno salvate.

Attività Attivazione dell'applicazione

► Per configurare un'attività *Attivazione dell'applicazione*, eseguire le seguenti operazioni:

1. Nell'albero di Kaspersky Security Center Administration Console espandere il nodo **Dispositivi gestiti** e selezionare il gruppo di amministrazione per cui si desidera configurare le attività dell'applicazione.
2. Nel riquadro dei dettagli di un gruppo di amministrazione selezionato aprire la scheda **Attività**.
3. Nell'elenco delle attività di gruppo create in precedenza selezionare un'attività da configurare. Aprire la finestra **Proprietà: <nome attività>** in uno dei seguenti modi:
 - Fare doppio clic sul nome dell'attività nell'elenco delle attività create.
 - Selezionare il nome dell'attività nell'elenco delle attività create e fare clic sul collegamento **Configura attività**.
 - Aprire il menu di scelta rapida del nome dell'attività nell'elenco delle attività create e selezionare **Proprietà**.
4. Nella sezione **Notifica** configurare le impostazioni di notifica degli eventi dell'attività.
5. Per informazioni dettagliate sulla configurazione delle impostazioni in questa sezione, vedere la *Guida di Kaspersky Security Center*.
6. Nella sezione **Impostazioni di attivazione**, applicare il file chiave che si desidera utilizzare per attivare l'applicazione. Selezionare la casella di controllo **Usa come chiave di riserva** se si desidera aggiungere una chiave per estendere la licenza.
7. Configurare la pianificazione dell'attività nella sezione **Pianificazione** (è possibile configurare una pianificazione per tutti i tipi di attività tranne Rollback dell'aggiornamento database).
8. Nella sezione **Account** specificare l'account del quale saranno utilizzati i diritti per l'esecuzione dell'attività.
9. Se necessario, specificare gli oggetti da escludere dall'ambito dell'attività nella sezione **Esclusioni dall'ambito dell'attività**.

Per informazioni dettagliate sulla configurazione delle impostazioni in queste sezioni, vedere la *Guida di Kaspersky Security Center*.

10. Nella finestra **Proprietà: <nome attività>** fare clic su **OK**.

Le nuove impostazioni delle attività di gruppo configurate verranno salvate.

Attività Aggiornamento

Per configurare le attività Copia degli aggiornamenti, Aggiornamento database o Aggiornamento moduli software, procedere come segue:

1. Nell'albero di Kaspersky Security Center Administration Console espandere il nodo **Dispositivi gestiti** e

selezionare il gruppo di amministrazione per cui si desidera configurare le attività dell'applicazione.

2. Nel riquadro dei dettagli di un gruppo di amministrazione selezionato aprire la scheda **Attività**.
3. Nell'elenco delle attività di gruppo create in precedenza selezionare un'attività da configurare. Aprire la finestra **Proprietà: <nome attività>** in uno dei seguenti modi:
 - Fare doppio clic sul nome dell'attività nell'elenco delle attività create.
 - Selezionare il nome dell'attività nell'elenco delle attività create e fare clic sul collegamento **Configura attività**.
 - Aprire il menu di scelta rapida del nome dell'attività nell'elenco delle attività create e selezionare **Proprietà**.
4. Nella sezione **Notifica** configurare le impostazioni di notifica degli eventi dell'attività.

Per informazioni dettagliate sulla configurazione delle impostazioni in questa sezione, vedere la *Guida di Kaspersky Security Center*.

5. A seconda del tipo di attività configurata, eseguire una delle seguenti operazioni:
 - Nella sezione **Sorgente degli aggiornamenti** configurare le impostazioni della sorgente degli aggiornamenti e l'ottimizzazione dell'utilizzo del sottosistema del disco.
 - a. È possibile specificare Kaspersky Security Center Administration Server o i server di aggiornamento di Kaspersky Lab come sorgente degli aggiornamenti dell'applicazione nella sezione **Sorgente degli aggiornamenti**. È anche possibile creare un elenco personalizzato di sorgenti degli aggiornamenti: aggiungendo manualmente server HTTP e FTP personalizzati o cartelle di rete e impostandoli come sorgenti degli aggiornamenti.

È possibile specificare l'utilizzo dei server di aggiornamento di Kaspersky Lab, se i server personalizzati manualmente non sono disponibili.
 - b. Nella sezione **Ottimizzazione dell'utilizzo dell'I/O del disco** per l'attività Aggiornamento database, è possibile configurare la funzionalità che riduce il carico di lavoro sul sottosistema del disco:
 - **Riduci il carico sull'I/O del disco**

Questa casella di controllo consente di abilitare o disabilitare la funzionalità di ottimizzazione del sottosistema del disco tramite l'archiviazione dei file degli aggiornamenti in un'unità virtuale nella RAM.

Se la casella di controllo è selezionata, questa funzione è abilitata.

La casella di controllo è deselezionata per impostazione predefinita.
 - **RAM utilizzata per l'ottimizzazione (MB)**

Dimensioni della RAM (in MB) utilizzata dall'applicazione per archiviare i file degli aggiornamenti. La dimensione predefinita della RAM è di 512 MB. La dimensione minima della RAM è di 400 MB.
 - c. Fare clic sul pulsante **Impostazioni di connessione** e, nella finestra **Impostazioni di connessione** visualizzata, configurare l'utilizzo di un server proxy per la connessione al server degli aggiornamenti Kaspersky Lab e ad altri server.
 - Nella sezione **Impostazioni per gli aggiornamenti dei moduli software dell'applicazione** per l'attività Aggiornamento moduli software è possibile specificare quali azioni deve eseguire Kaspersky Embedded Systems Security 2.2 quando sono disponibili aggiornamenti dei moduli software critici o informazioni sugli aggiornamenti pianificati. È inoltre possibile specificare quali azioni deve eseguire Kaspersky Embedded Systems Security 2.2 quando vengono installati aggiornamenti critici.

- Specificare il set di aggiornamenti e la cartella di destinazione nella sezione **Impostazioni di copia degli aggiornamenti** per l'attività **Copia degli aggiornamenti**.
6. Configurare la pianificazione dell'attività nella sezione **Pianificazione** (è possibile configurare una pianificazione per tutti i tipi di attività tranne Rollback dell'aggiornamento database).
 7. Nella sezione **Account** specificare l'account del quale saranno utilizzati i diritti per l'esecuzione dell'attività.

Per informazioni dettagliate sulla configurazione delle impostazioni in queste sezioni, vedere la *Guida di Kaspersky Security Center*.

8. Nella finestra **Proprietà: <nome attività>** fare clic su **OK**.

Le nuove impostazioni delle attività di gruppo configurate verranno salvate.

Per l'attività Rollback dell'aggiornamento database è possibile configurare solo le impostazioni standard dell'attività controllate da Kaspersky Security Center nelle sezioni **Notifiche** ed **Esclusioni dall'ambito dell'attività**. Per informazioni dettagliate sulla configurazione delle impostazioni in queste sezioni, vedere la *Guida di Kaspersky Security Center*.

Verifica dell'integrità dei moduli software

► *Per configurare l'attività di gruppo Aggiornamento moduli software:*

1. Nell'albero di Kaspersky Security Center Administration Console espandere il nodo **Dispositivi gestiti** e selezionare il gruppo di amministrazione per cui si desidera configurare le attività dell'applicazione.
2. Nel riquadro dei dettagli di un gruppo di amministrazione selezionato aprire la scheda **Attività**.
3. Nell'elenco delle attività di gruppo create in precedenza selezionare un'attività da configurare. Aprire la finestra **Proprietà: <nome attività>** in uno dei seguenti modi:
 - Fare doppio clic sul nome dell'attività nell'elenco delle attività create.
 - Selezionare il nome dell'attività nell'elenco delle attività create e fare clic sul collegamento **Configura attività**.
 - Aprire il menu di scelta rapida del nome dell'attività nell'elenco delle attività create e selezionare **Proprietà**.
4. Nella sezione **Notifica** configurare le impostazioni di notifica degli eventi dell'attività.

Per informazioni dettagliate sulla configurazione delle impostazioni in questa sezione, vedere la *Guida di Kaspersky Security Center*.

5. Nella sezione **Dispositivi** selezionare i dispositivi per cui si desidera configurare l'attività di verifica dell'integrità dei moduli software.
6. Configurare la pianificazione dell'attività nella sezione **Pianificazione** (è possibile configurare una pianificazione per tutti i tipi di attività tranne Rollback dell'aggiornamento database).
7. Nella sezione **Account** specificare l'account del quale saranno utilizzati i diritti per l'esecuzione dell'attività.
8. Se necessario, specificare gli oggetti da escludere dall'ambito dell'attività nella sezione **Esclusioni dall'ambito dell'attività**.

Per informazioni dettagliate sulla configurazione delle impostazioni in queste sezioni, vedere la *Guida di Kaspersky Security Center*.

9. Nella finestra **Proprietà: <nome attività>** fare clic su **OK**.

Le nuove impostazioni delle attività di gruppo configurate verranno salvate.

Creazione di un'attività Scansione su richiesta

► Per creare una nuova attività in Administration Console di Kaspersky Security Center:

1. Avviare la procedura guidata dell'attività in uno dei seguenti modi:
 - Per creare un'attività locale:
 - a. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Server e selezionare il gruppo a cui appartiene il computer protetto.
 - b. Nel riquadro dei dettagli, nella scheda **Dispositivi**, aprire il menu di scelta rapida nella riga con le informazioni sul computer protetto e selezionare **Proprietà**.
 - c. Nella finestra visualizzata fare clic sul pulsante **Aggiungi** nella sezione **Attività**.
 - Per creare un'attività di gruppo:
 - a. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo per cui si desidera creare un criterio.
 - b. Nel riquadro dei dettagli aprire il menu di scelta rapida nella scheda **Attività** e selezionare **Nuovo > Attività**.
 - Per creare un'attività per un set personalizzato di computer, nel nodo **Selezioni dispositivi** nell'albero di Kaspersky Security Center Administration Console selezionare **Nuova attività**.

Verrà visualizzata la finestra della procedura guidata dell'attività.

2. Nella finestra **Definire il nome dell'attività** immettere il nome dell'attività (non più di 100 caratteri) senza utilizzare i simboli | * < > ? \ / | :). È consigliabile aggiungere al nome il tipo di attività (ad esempio, "Scansione su richiesta delle cartelle condivise").
3. Nella finestra **Tipo di attività**, sotto l'intestazione **Kaspersky Embedded Systems Security 2.2**, selezionare l'attività **Scansione su richiesta** e fare clic su **Avanti**.
4. Creare un ambito della scansione nella finestra **Ambito della scansione**.

Per impostazione predefinita, l'ambito della scansione include le aree critiche del computer. Gli ambiti della scansione sono contrassegnati nella tabella con l'icona . Gli ambiti della scansione esclusi sono contrassegnati con l'icona nella tabella.

È possibile modificare l'ambito della scansione: aggiungere specifici ambiti della scansione preimpostati, dischi, cartelle, oggetti di rete e file e assegnare specifiche impostazioni di sicurezza per ogni ambito aggiunto.

- Per escludere tutte le aree critiche dalla scansione, aprire il menu di scelta rapida di ciascuna delle righe e selezionare l'opzione **Rimuovi ambito**.

- Per includere un ambito della scansione predefinito, un disco, una cartella, un oggetto di rete o un file nell'ambito della scansione:
 - a. Fare clic con il pulsante destro del mouse sulla tabella **Ambito della scansione** e selezionare **Aggiungi ambito** o fare clic sul pulsante **Aggiungi**.
 - b. Nella finestra **Aggiungi oggetti all'ambito della scansione** selezionare l'ambito predefinito nell'elenco **Ambito predefinito**, specificare l'unità del computer, la cartella, l'oggetto di rete o il file sul computer o su un altro computer della rete, quindi fare clic sul pulsante **OK**.
- Per escludere sottocartelle o file dalla scansione, selezionare la cartella o il disco aggiunto nella finestra **Ambito della scansione** della procedura guidata:
 - a. Aprire il menu di scelta rapida, quindi selezionare l'opzione **Configura**.
 - b. Fare clic sul pulsante **Impostazioni** nella finestra **Livello di sicurezza**.
 - c. Nella scheda **Generale** della finestra **Impostazioni di scansione su richiesta** deselezionare le caselle di controllo **Sottocartelle** e **File secondari**.
- Per modificare le impostazioni di sicurezza dell'ambito della scansione:
 - a. Aprire il menu di scelta rapida dell'ambito di cui si desidera configurare le impostazioni e selezionare **Configura**.
 - b. Nella finestra **Impostazioni di scansione su richiesta** selezionare uno dei livelli di sicurezza predefiniti o fare clic sul pulsante **Impostazioni** per configurare manualmente le impostazioni di sicurezza.

Le impostazioni di sicurezza sono configurate nello stesso modo di quelle dell'attività **Protezione dei file in tempo reale** (vedere la sezione "Configurazione manuale delle impostazioni di sicurezza" a pagina [152](#)).

- Per ignorare gli oggetti incorporati nell'ambito della scansione aggiunto:
 - a. Aprire il menu di scelta rapida della tabella **Ambito della scansione** e selezionare **Aggiungi esclusione**.
 - b. Specificare gli oggetti da escludere: selezionare l'ambito predefinito nell'elenco **Ambito predefinito** e specificare il disco del computer, la cartella, l'oggetto di rete o il file nel computer o in un altro computer della rete.
 - c. Fare clic sul pulsante **OK**.
5. Nella finestra **Opzioni** configurare l'analizzatore euristico e l'integrazione con altri componenti:
- Configurare l'utilizzo dell'analizzatore euristico (vedere la sezione "Utilizzo dell'analizzatore euristico" a pagina [147](#)).
 - Selezionare la casella di controllo **Applica area attendibile** se si desidera escludere gli oggetti descritti nell'area attendibile di Kaspersky Embedded Systems Security 2.2 dall'ambito della scansione dell'attività.

Questa casella di controllo consente di abilitare o disabilitare l'utilizzo dell'area attendibile per un'attività.

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 aggiunge le operazioni sui file dei processi attendibili alle esclusioni della scansione configurate nelle impostazioni dell'attività.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 ignora le operazioni sui file dei processi attendibili al momento della creazione dell'ambito della protezione per l'attività **Protezione dei file in tempo reale**.

La casella di controllo è selezionata per impostazione predefinita.

- Selezionare la casella di controllo **Utilizzo di KSN per la scansione** se si desidera utilizzare i servizi cloud di Kaspersky Security Network per l'attività.

Questa casella di controllo consente di abilitare o disabilitare l'utilizzo dei servizi cloud di Kaspersky Security Network (KSN) nell'attività.

Se la casella di controllo è selezionata, l'applicazione utilizza i dati ricevuti dai servizi KSN per garantire un tempo di risposta inferiore alle nuove minacce e ridurre la probabilità di falsi positivi.

Se la casella di controllo è deselezionata, l'attività Scansione su richiesta non utilizza il servizio KSN.

La casella di controllo è selezionata per impostazione predefinita.

- Per assegnare la priorità di base **Basso** al processo di lavoro in cui sarà eseguita l'attività, selezionare la casella di controllo **Esegui attività in background** nella finestra **Opzioni**.

La casella di controllo modifica la priorità dell'attività.

Se la casella di controllo è selezionata, la priorità dell'attività nel sistema operativo viene ridotta. Il sistema operativo fornisce le risorse per l'esecuzione dell'attività a seconda del carico sulla CPU e sul file system del computer da parte di altre attività di Kaspersky Embedded Systems Security 2.2 e applicazioni. Di conseguenza, le prestazioni dell'attività rallentano con carichi superiori e accelerano con carichi inferiori.

Se la casella di controllo è deselezionata, l'attività verrà avviata ed eseguita con la stessa priorità di altre attività di Kaspersky Embedded Systems Security 2.2 e altre applicazioni. In questo caso, la velocità di esecuzione dell'attività aumenta.

La casella di controllo è deselezionata per impostazione predefinita.

Per impostazione predefinita, i processi di lavoro in cui vengono eseguite le attività di Kaspersky Embedded Systems Security 2.2 hanno la priorità **Medio** (Normale).

- Per utilizzare l'attività creata come un'attività Scansione aree critiche, selezionare la casella di controllo **Considera l'attività come scansione aree critiche** nella finestra **Opzioni**.

La casella di controllo modifica la priorità dell'attività: abilita o disabilita la registrazione dell'evento *Scansione aree critiche* e l'aggiornamento dello stato della protezione del computer. Kaspersky Security Center valuta la classificazione di protezione del computer in base ai risultati delle prestazioni delle attività con lo stato *Scansione aree critiche*. La casella di controllo non è disponibile nelle proprietà delle attività locali di sistema e personalizzate di Kaspersky Embedded Systems Security 2.2. È possibile modificare questa impostazione solo tramite Kaspersky Security Center.

Se questa casella di controllo è selezionata, Administration Server registra l'evento Scansione aree critiche completata e aggiorna lo stato della protezione del computer in base ai risultati dell'esecuzione dell'attività. L'attività di scansione ha una priorità alta.

Se la casella di controllo è deselezionata, l'attività viene eseguita con una priorità bassa.

Per impostazione predefinita, la casella di controllo è selezionata per l'attività Scansione aree critiche.

6. Fare clic su **Avanti**.

7. Nella finestra **Pianificazione** configurare una pianificazione (vedere la sezione "Configurazione delle impostazioni della pianificazione dell'avvio delle attività" a pagina [119](#)) per l'attività.

8. Specificare un account utente con cui eseguire l'attività e definire il nome dell'attività.
9. Fare clic su **Fine**.

La nuova attività Scansione su richiesta verrà creata per un computer selezionato o un gruppo di computer.

Configurazione dell'attività Scansione su richiesta

► Per configurare un'attività Scansione su richiesta esistente, eseguire le seguenti operazioni:

1. Nell'albero di Kaspersky Security Center Administration Console espandere il nodo **Dispositivi gestiti** e selezionare il gruppo di amministrazione per cui si desidera configurare le attività dell'applicazione.
2. Nel riquadro dei dettagli di un gruppo di amministrazione selezionato aprire la scheda **Attività**.
3. Nell'elenco delle attività di gruppo create in precedenza selezionare un'attività da configurare. Aprire la finestra **Proprietà: <nome attività>** in uno dei seguenti modi:
 - Fare doppio clic sul nome dell'attività nell'elenco delle attività create.
 - Selezionare il nome dell'attività nell'elenco delle attività create e fare clic sul collegamento **Configura attività**.
 - Aprire il menu di scelta rapida del nome dell'attività nell'elenco delle attività create e selezionare **Proprietà**.
4. Nella sezione **Notifica** configurare le impostazioni di notifica degli eventi dell'attività.

Per informazioni dettagliate sulla configurazione delle impostazioni in questa sezione, vedere la *Guida di Kaspersky Security Center*.

5. Nella sezione **Impostazioni** è possibile eseguire le seguenti azioni:
 - a. Nella sezione **Ambito della scansione** selezionare le caselle di controllo accanto alle risorse file che si desidera includere nell'ambito della scansione.
 - b. Fare clic sul pulsante **Configura** e selezionare il livello di sicurezza.
È possibile selezionare uno di livelli di sicurezza predefiniti o personalizzare manualmente il livello di sicurezza.
 - c. Per configurare manualmente il livello di sicurezza, nella finestra **Impostazioni di scansione su richiesta** fare clic sul pulsante **Impostazioni**.
6. Nella sezione **Opzioni** è possibile eseguire le seguenti azioni:
 - a. Abilitare o disabilitare l'utilizzo dell'**analizzatore euristico** e impostare il livello di analisi utilizzando il dispositivo di scorrimento nel gruppo **Analizzatore euristico**.
 - b. Configurare le impostazioni avanzate (vedere la sezione "Creazione di un'attività Scansione su richiesta" a pagina [111](#)).
7. Configurare la pianificazione dell'attività nella sezione **Pianificazione** (è possibile configurare una pianificazione per tutti i tipi di attività tranne Rollback dell'aggiornamento database).
8. Nella sezione **Account** specificare l'account del quale saranno utilizzati i diritti per l'esecuzione dell'attività.
9. Se necessario, specificare gli oggetti da escludere dall'ambito dell'attività nella sezione **Esclusioni dall'ambito dell'attività**.

Per informazioni dettagliate sulla configurazione delle impostazioni in queste sezioni, vedere la *Guida di Kaspersky Security Center*.

10. Nella finestra **Proprietà: <nome attività>** fare clic su **OK**.

Le nuove impostazioni delle attività di gruppo configurate verranno salvate.

Assegnazione dello stato Scansione aree critiche all'attività Scansione su richiesta

Per impostazione predefinita, Kaspersky Security Center assegna lo stato *Avviso* al computer se l'attività Scansione aree critiche viene eseguita con una frequenza inferiore rispetto all'impostazione della soglia di generazione dell'evento **La scansione aree critiche non viene eseguita da molto tempo** di Kaspersky Embedded Systems Security 2.2.

► Per configurare la scansione di tutti i computer in un singolo gruppo di amministrazione, eseguire le seguenti operazioni:

1. Creare un'attività di gruppo Scansione su richiesta.
2. Nella finestra **Opzioni** della procedura guidata dell'attività selezionare la casella di controllo **Considera l'attività come scansione aree critiche**. Le impostazioni dell'attività specificate (ambito della scansione e impostazioni di sicurezza) saranno applicate a tutti i computer nel gruppo. Configurare la pianificazione dell'attività.

È possibile selezionare la casella di controllo **Considera l'attività come scansione aree critiche** sia al momento della creazione dell'attività Scansione su richiesta per un gruppo di computer o un set di computer che in seguito, nella finestra **Proprietà: <nome attività>**.

3. Utilizzando un criterio nuovo o esistente, disabilitare l'avvio pianificato delle attività di scansione del sistema (vedere la sezione "Configurazione dell'avvio pianificato delle attività locali di sistema" a pagina [93](#)) nei computer del gruppo.

Kaspersky Security Center Administration Server valuterà quindi lo stato di sicurezza del computer protetto e invierà una notifica in proposito in base ai risultati dell'ultima esecuzione dell'attività con lo stato Attività Scansione aree critiche, invece che in base ai risultati dell'attività di sistema *Scansione aree critiche*.

È possibile assegnare lo stato dell'attività *Scansione aree critiche* sia alle attività di gruppo Scansione su richiesta che alle attività per set di computer.

La console dell'applicazione può essere utilizzata per determinare se l'attività Scansione su richiesta è un'attività Scansione aree critiche.

Nella console dell'applicazione la casella di controllo **Considera l'attività come scansione aree critiche** è visualizzata nella proprietà dell'attività, ma non può essere modificata.

Scansione dei file in un archivio cloud

Informazioni sui file cloud





Kaspersky Embedded Systems Security 2.2 può interagire con i file cloud di Microsoft OneDrive. L'applicazione

supporta la nuova funzionalità File di OneDrive su richiesta.




Kaspersky Embedded Systems Security 2.2 non supporta altri archivi cloud.


La funzionalità File di OneDrive su richiesta consente di accedere a tutti i file in OneDrive senza doverli scaricare e utilizzare spazio di archiviazione nel dispositivo. È possibile scaricare i file sul disco rigido quando è necessario.

Quando la funzionalità File di OneDrive su richiesta è attivata, vengono visualizzate icone di stato accanto a ogni file nella colonna **Stato** in Esplora file. Ogni file può avere uno dei seguenti stati:








-  Questa icona di stato indica che il file è *disponibile solo online*. I file solo online non sono archiviati fisicamente sul disco rigido. Non è possibile aprire i file solo online quando il dispositivo non è connesso a Internet.
-  Questa icona di stato indica che un file è *disponibile in locale*. Questo accade quando si apre un file solo online, che viene scaricato nel dispositivo. È possibile aprire un file disponibile in locale in qualsiasi momento, anche senza accesso a Internet. Per liberare spazio, è possibile impostare di nuovo il file come  solo online.
-  Questa icona di stato indica che un file è *archiviato sul disco rigido ed è sempre disponibile*.


Scansione dei file cloud

Kaspersky Embedded Systems Security 2.2 è in grado di esaminare solo i file cloud archiviati in locale in un computer protetto. Tali file OneDrive hanno gli stati  e . I file  vengono ignorati durante la scansione, dal momento che non sono presenti fisicamente nel computer protetto.

Kaspersky Embedded Systems Security 2.2 non scarica automaticamente i file  dal cloud durante la scansione, anche se sono inclusi nell'ambito della scansione.

I file cloud vengono elaborati da più attività di Kaspersky Embedded Systems Security 2.2 in vari scenari, a seconda del tipo di attività:

- Scansione in tempo reale dei file cloud: è possibile aggiungere le cartelle che contengono i file cloud all'ambito della protezione dell'attività Protezione dei file in tempo reale. Il file viene analizzato quando l'utente vi accede. Se l'utente accede a un file , questo viene scaricato, diventa disponibile in locale e il relativo stato diventa . Questo consente l'elaborazione del file da parte dell'attività Protezione dei file in tempo reale.
- Scansione dei file cloud su richiesta: è possibile aggiungere le cartelle che contengono i file cloud all'ambito della scansione dell'attività Scansione su richiesta. L'attività esamina i file con gli stati  e . Se nell'ambito vengono rilevati file , questi sono ignorati durante la scansione e viene registrato un evento informativo nel log delle attività, che indica che il file da esaminare è solo un segnaposto per un file cloud e non è presente in un'unità locale.
- Generazione e utilizzo di regole di Controllo Applicazioni: è possibile creare regole di permesso e di negazione per i file  e  utilizzando l'attività Generazione regole per Controllo dell'avvio delle applicazioni. L'attività Controllo dell'avvio delle applicazioni applica il principio Default deny e le regole create per l'elaborazione e il blocco dei file cloud.

L'attività Controllo dell'avvio delle applicazioni blocca l'avvio di tutti i file cloud, indipendentemente dal relativo stato. I file  non sono inclusi dall'applicazione nell'ambito di generazione della regola, perché non sono archiviati fisicamente su un disco rigido. Dal momento che non è possibile creare regole di permesso per tali file, questi sono soggetti al principio Default deny.

Quando viene rilevata una minaccia in un file cloud di OneDrive, viene applicata l'azione specificata nelle impostazioni dell'attività che esegue la scansione. In questo modo, il file può essere rimosso, disinfettato, spostato in Quarantena o in Backup.

Le modifiche apportate ai file locali vengono sincronizzate con le copie memorizzate in OneDrive in conformità con i principi descritti nella documentazione di Microsoft OneDrive.

Configurazione delle impostazioni di diagnostica degli arresti anomali in Kaspersky Security Center

Se si verifica un problema durante l'esecuzione di Kaspersky Embedded Systems Security 2.2 (ad esempio, un arresto anomalo di Kaspersky Embedded Systems Security 2.2) e si desidera eseguirne la diagnostica, è possibile abilitare la creazione dei file di traccia e del file di dump del processo di Kaspersky Embedded Systems Security 2.2 e inviare questi file per l'analisi all'Assistenza tecnica di Kaspersky Lab.

Kaspersky Embedded Systems Security 2.2 non invia automaticamente i file di traccia o di dump. I dati di diagnostica possono essere inviati solo dall'utente con le autorizzazioni corrispondenti.

Kaspersky Embedded Systems Security 2.2 scrive le informazioni nei file di traccia e nel file di dump in formato non criptato. La cartella in cui vengono salvati i file viene selezionata dall'utente ed è gestita in base alla configurazione del sistema operativo e alle impostazioni di Kaspersky Embedded Systems Security 2.2. È possibile configurare le autorizzazioni di accesso (vedere la sezione "Autorizzazioni di accesso per le funzioni di Kaspersky Embedded Systems Security 2.2" a pagina [76](#)) e consentire l'accesso ai log, ai file di traccia e di dump solo agli utenti necessari.

► Per configurare le impostazioni di diagnostica degli arresti anomali in Kaspersky Security Center:

1. In Kaspersky Security Center Administration Console aprire la finestra **Impostazioni applicazione** (vedere la sezione "**Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center**" a pagina [100](#)).
2. Aprire la sezione **Diagnostica malfunzionamento** ed eseguire le seguenti operazioni:
 - Se si desidera che l'applicazione scriva le informazioni di debug in un file, selezionare la casella di controllo **Scrivi informazioni di debug nel file di traccia**.
 - Nel campo sottostante specificare la cartella in cui Kaspersky Embedded Systems Security 2.2 deve salvare i file di traccia.
 - Configurare il livello di dettaglio delle informazioni di debug.

Questo elenco a discesa consente di selezionare il livello di dettaglio delle informazioni di debug che Kaspersky Embedded Systems Security 2.2 salva nel file di traccia.

È possibile selezionare uno dei seguenti livelli di dettaglio:

- **Eventi critici** - Kaspersky Embedded Systems Security 2.2 salva nel file di traccia solo le informazioni sugli eventi critici.
- **Errori** - Kaspersky Embedded Systems Security 2.2 salva nel file di traccia le informazioni sugli eventi critici e sugli errori.
- **Eventi importanti** - Kaspersky Embedded Systems Security 2.2 salva nel file di traccia le informazioni su eventi critici, errori ed eventi importanti.
- **Eventi informativi** - Kaspersky Embedded Systems Security 2.2 salva nel file di traccia le informazioni su eventi critici, errori, eventi importanti ed eventi Informativi.
- **Tutte le informazioni di debug** - Kaspersky Embedded Systems Security 2.2 salva nel file di traccia tutte le informazioni di debug.

Un addetto del servizio di Assistenza tecnica determina il livello di dettaglio che è necessario impostare per risolvere il problema che si è verificato.

Il livello di dettaglio predefinito è impostato su **Tutte le informazioni di debug**.

L'elenco a discesa è disponibile se è selezionata la casella di controllo **Scrivi informazioni di debug nel file di traccia**.

- Specificare la dimensione massima del file di traccia.
- Specificare i componenti di cui eseguire il debug. I codici dei componenti devono essere separati con un punto e virgola. Per i codici viene applicata la distinzione tra maiuscole e minuscole (vedere la seguente tabella).

Tabella 27. Codici dei sottosistemi di Kaspersky Embedded Systems Security 2.2

Codice del componente	Nome del componente
*	Tutti i componenti.
gui	Sottosistema dell'interfaccia utente, snap-in di Kaspersky Embedded Systems Security 2.2 in Microsoft Management Console.
ak_conn	Sottosistema per l'integrazione di Network Agent e Kaspersky Security Center.
bl	Processo di controllo, implementa le attività di controllo di Kaspersky Embedded Systems Security 2.2.
wp	Processo di lavoro, gestisce le attività di protezione anti-virus.
blgate	Processo di gestione remota di Kaspersky Embedded Systems Security 2.2.
ods	Sottosistema di Scansione su richiesta.
oas	Sottosistema di Protezione dei file in tempo reale.
qb	Sottosistema di Quarantena e Backup.
scandll	Modulo ausiliario per la scansione anti-virus.
core	Sottosistema per la funzionalità anti-virus di base.
avscan	Sottosistema di elaborazione anti-virus.
avserv	Sottosistema per il controllo del kernel anti-virus.
prague	Sottosistema per la funzionalità di base.
updater	Sottosistema per l'aggiornamento di database e moduli software.

Codice del componente	Nome del componente
snmp	Sottosistema di supporto del protocollo SNMP.
perfcount	Sottosistema per i contatori delle prestazioni.

Le impostazioni di traccia dello snap-in di Kaspersky Embedded Systems Security 2.2 (gui) e del plug-in di amministrazione per Kaspersky Security Center (ak_conn) vengono applicate in seguito al riavvio di questi componenti. Le impostazioni di traccia del sottosistema di supporto del protocollo SNMP (snmp) sono applicate dopo il riavvio del servizio SNMP. Le impostazioni di traccia del sottosistema per i contatori delle prestazioni (perfcount) sono applicate dopo il riavvio di tutti i processi che utilizzano i contatori delle prestazioni. Le impostazioni di traccia per gli altri sottosistemi di Kaspersky Embedded Systems Security 2.2 sono applicate al momento del salvataggio delle impostazioni di diagnostica degli arresti anomali.

Per impostazione predefinita, vengono registrate le informazioni di debug per tutti i componenti di Kaspersky Embedded Systems Security 2.2.

Il campo di immissione è disponibile se è selezionata la casella di controllo **Scrivi informazioni di debug nel file di traccia**.

- Se si desidera che l'applicazione crei un file di dump, selezionare la casella di controllo **Crea file di dump**.
 - Nel campo sottostante specificare la cartella in cui Kaspersky Embedded Systems Security 2.2 deve salvare i file di dump della memoria.

3. Fare clic su **OK**.

Le impostazioni dell'applicazione configurate verranno applicate al computer protetto.

Gestione delle pianificazioni delle attività

È possibile configurare la pianificazione di avvio per le attività di Kaspersky Embedded Systems Security 2.2 e configurare le impostazioni per l'esecuzione delle attività in base a una pianificazione.

In questa sezione

Configurazione delle impostazioni della pianificazione di avvio delle attività	119
Abilitazione e disabilitazione delle attività pianificate	121

Configurazione delle impostazioni della pianificazione di avvio delle attività

È possibile configurare la pianificazione di avvio per le attività locali di sistema e personalizzate nella console dell'applicazione. Non è possibile configurare la pianificazione di avvio per le attività di gruppo.

► Per configurare le impostazioni della pianificazione di avvio delle attività, eseguire le seguenti operazioni:

1. Nell'albero di Kaspersky Security Center Administration Console espandere il nodo **Dispositivi gestiti** e procedere come segue:
 - Se si desidera configurare le impostazioni del criterio, nel gruppo di computer selezionare **Criterio > <Nome criterio> > <Sezione> > Configura > Gestione attività**.
 - Se si desidera configurare le impostazioni dell'applicazione per un singolo computer utilizzando Kaspersky Security Center, aprire la finestra **Impostazioni attività** (vedere la sezione "**Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center**" a pagina [100](#)) in Kaspersky Security Center.

Verrà visualizzata la finestra **Impostazioni**.

2. Nella finestra visualizzata, nella scheda **Pianificazione**, selezionare la casella di controllo **Esegui in base alla pianificazione**.

I campi con le impostazioni di pianificazione per le attività Scansione su richiesta e Aggiornamento non sono disponibili se il relativo avvio pianificato è bloccato da un criterio di Kaspersky Security Center.

3. Configurare le impostazioni della pianificazione in base agli specifici requisiti. A tale scopo, eseguire le seguenti operazioni:
 - a. Nell'elenco **Frequenza** selezionare uno dei seguenti valori:
 - **Ogni ora**, se si desidera che l'attività venga eseguita a intervalli di un numero specificato di ore. Specificare il numero di ore nel campo **Ogni <numero> ora/e**.
 - **Ogni giorno**, se si desidera che l'attività venga eseguita a intervalli di un numero specificato di giorni. Specificare il numero di giorni nel campo **Ogni <numero> giorno/i**.
 - **Ogni settimana**, se si desidera che l'attività venga eseguita a intervalli di un numero specificato di settimane. Specificare il numero di settimane nel campo **Ogni <numero> settimana/e**. Specificare i giorni della settimana in cui verrà avviata l'attività (per impostazione predefinita, l'attività viene eseguita ogni lunedì).
 - **All'avvio dell'applicazione**, se si desidera che l'attività venga eseguita ogni volta che si avvia Kaspersky Embedded Systems Security 2.2.
 - **Dopo l'aggiornamento del database dell'applicazione**, se si desidera che l'attività venga eseguita dopo ogni aggiornamento dei database dell'applicazione.
 - b. Specificare l'ora per il primo avvio dell'attività nel campo **Ora avvio**.
 - c. Nel campo **Data avvio** specificare la data da cui si applica la pianificazione.

Dopo avere specificato la frequenza di avvio dell'attività, l'ora del primo avvio dell'attività e la data da cui si applica la pianificazione, le informazioni sul tempo stimato per il successivo avvio dell'attività sono visualizzate nella parte superiore della finestra nel campo **Prossimo avvio**. Le informazioni aggiornate sull'orario stimato del prossimo avvio dell'attività saranno visualizzate ogni volta che si apre la scheda **Pianificazione** della finestra **Impostazioni attività**.

Nel campo **Prossimo avvio** è visualizzato il valore **Bloccato dal criterio** se le impostazioni del criterio attivo di Kaspersky Security Center impediscono l'avvio delle attività di sistema pianificate (vedere la sezione "**Configurazione dell'avvio pianificato delle attività locali di sistema**" a pagina [93](#)).

4. Utilizzare la scheda **Avanzate** per configurare le seguenti impostazioni di pianificazione in base agli

specifici requisiti.

- Nella sezione **Impostazioni arresto attività**:
 - a. Selezionare la casella di controllo **Durata** e immettere il numero richiesto di ore e minuti nei campi a destra per specificare la durata massima dell'esecuzione dell'attività.
 - b. Selezionare la casella di controllo **Sospendi da** e immettere il valore iniziale e finale dell'intervallo di tempo nei campi a destra per specificare un intervallo di tempo inferiore alle 24 ore durante il quale l'esecuzione dell'attività sarà sospesa.
 - Nella sezione **Impostazioni avanzate**:
 - a. Selezionare la casella di controllo **Annulla pianificazione da** e specificare la data da cui la pianificazione cesserà di funzionare.
 - b. Selezionare la casella di controllo **Esegui attività ignorate** per abilitare l'avvio delle attività ignorate.
 - c. Selezionare la casella di controllo **Imposta come casuale l'avvio dell'attività entro un intervallo di** e specificare un valore in minuti.
5. Fare clic sul pulsante **Applica** per salvare le impostazioni di avvio dell'attività.

Abilitazione e disabilitazione delle attività pianificate

È possibile abilitare e disabilitare le attività pianificate prima o dopo avere configurato le impostazioni di pianificazione.

► *Per abilitare o disabilitare la pianificazione dell'avvio dell'attività, eseguire le seguenti operazioni:*

1. Nell'albero della console dell'applicazione aprire il menu di scelta rapida del nome dell'attività per cui si desidera configurare la pianificazione di avvio.
2. Selezionare **Proprietà**.
Verrà visualizzata la finestra **Impostazioni attività**.
3. Nella finestra visualizzata, nella scheda **Pianificazione**, eseguire una delle seguenti operazioni:
 - Selezionare la casella di controllo **Esegui in base alla pianificazione** se si desidera abilitare l'avvio dell'attività pianificata.
 - Deselezionare la casella di controllo **Esegui in base alla pianificazione** se si desidera disabilitare l'avvio dell'attività pianificata.

Le impostazioni configurate per la pianificazione dell'avvio dell'attività non vengono eliminate e saranno applicate al successivo avvio pianificato dell'attività.

4. Fare clic sul pulsante **Applica**.

Le impostazioni configurate per la pianificazione dell'avvio dell'attività verranno salvate.

Gestione delle impostazioni dell'applicazione

Questa sezione contiene informazioni sulla configurazione delle impostazioni generali di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center.

In questo capitolo

Gestione di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center	122
Configurazione delle impostazioni generali dell'applicazione in Kaspersky Security Center	123
Configurazione delle funzionalità avanzate	128
Configurazione di log e notifiche.....	137

Gestione di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center

È possibile gestire a livello centralizzato diversi computer in cui è installato Kaspersky Embedded Systems Security 2.2 e inclusi in un gruppo di amministrazione tramite il plug-in di amministrazione di Kaspersky Embedded Systems Security 2.2. Kaspersky Security Center consente inoltre di configurare separatamente le impostazioni di esecuzione di ciascun computer incluso nel gruppo di amministrazione.

Il *gruppo di amministrazione* viene creato manualmente in Kaspersky Security Center e include diversi computer in cui è installato Kaspersky Embedded Systems Security 2.2, per cui si desidera configurare le stesse impostazioni di protezione e controllo. Per informazioni dettagliate sull'utilizzo dei gruppi di amministrazione, vedere la *Guida di Kaspersky Security Center*.

Le impostazioni dell'applicazione per un computer non sono disponibili se l'esecuzione di Kaspersky Embedded Systems Security 2.2 in tale computer è controllata da un criterio di Kaspersky Security Center attivo.

Kaspersky Embedded Systems Security 2.2 può essere gestito da Kaspersky Security Center nei seguenti modi:

- **Utilizzando i criteri di Kaspersky Security Center.** I criteri di Kaspersky Security Center possono essere utilizzati per configurare in remoto le stesse impostazioni di protezione per un gruppo di computer. Le impostazioni delle attività specificate nel criterio attivo hanno la priorità rispetto alle impostazioni delle attività configurate in locale nella console dell'applicazione o in remoto nella finestra **Proprietà: <nome computer>** di Kaspersky Security Center.

È possibile utilizzare i criteri per configurare le impostazioni generali dell'applicazione, le impostazioni dell'attività Protezione in tempo reale, le impostazioni delle attività Controllo attività locali, le impostazioni di avvio delle attività di sistema pianificate e le impostazioni di utilizzo dei profili.

- **Utilizzando le attività di gruppo di Kaspersky Security Center.** Le attività di gruppo di Kaspersky Security Center consentono la configurazione remota delle impostazioni comuni delle attività con un periodo di scadenza per un gruppo di computer.
- È possibile utilizzare le attività di gruppo per attivare l'applicazione e configurare le impostazioni dell'attività

Scansione su richiesta, le impostazioni delle attività di aggiornamento e le impostazioni dell'attività Generazione regole per Controllo dell'avvio delle applicazioni.

- **Utilizzando le attività per un set di dispositivi.** Le attività per un set di dispositivi consentono la configurazione remota delle impostazioni delle attività comuni con un periodo di esecuzione limitato per i computer che non appartengono ad alcun gruppo di amministrazione.
- **Utilizzando la finestra delle proprietà di un singolo computer.** Nella finestra **Proprietà: <nome computer>** è possibile configurare in remoto le impostazioni delle attività per un singolo computer incluso nel gruppo di amministrazione.
È possibile configurare sia le impostazioni generali dell'applicazione che le impostazioni di tutte le attività di Kaspersky Embedded Systems Security 2.2 se il computer selezionato non è controllato da un criterio di Kaspersky Security Center attivo.

Kaspersky Security Center consente di configurare le impostazioni dell'applicazione, le funzionalità avanzate, nonché di utilizzare log e notifiche. È possibile configurare queste impostazioni per un gruppo di computer e per un singolo computer.

Configurazione delle impostazioni generali dell'applicazione in Kaspersky Security Center

È possibile configurare le impostazioni generali di Kaspersky Embedded Systems Security 2.2 da Kaspersky Security Center per un gruppo di computer o per un solo computer.

In questa sezione

Configurazione della scalabilità e dell'interfaccia in Kaspersky Security Center	123
Configurazione delle impostazioni di sicurezza in Kaspersky Security Center	125
Configurazione delle impostazioni di connessione tramite Kaspersky Security Center	127

Configurazione della scalabilità e dell'interfaccia in Kaspersky Security Center

Il processo di configurazione delle impostazioni dei componenti funzionali di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center è simile alla configurazione locale delle impostazioni di questi componenti nella console dell'applicazione. Istruzioni dettagliate su come configurare le impostazioni delle attività e le funzioni dell'applicazione sono disponibili nelle relative sezioni del *Manuale Utente di Kaspersky Embedded Systems Security 2.2*.

- ▶ *Per configurare le impostazioni di scalabilità e l'interfaccia dell'applicazione, eseguire le seguenti operazioni:*
 1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
 2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e

aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).

- Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Impostazioni applicazione**, in **Scalabilità e interfaccia**, fare clic su **Impostazioni**.
4. Nella finestra **Scalabilità e interfaccia** nella scheda **Generale**, configurare le seguenti impostazioni:
 - Nella sezione **Impostazioni scalabilità** configurare le impostazioni che definiscono il numero di processi utilizzati da Kaspersky Embedded Systems Security 2.2:
 - **Rileva automaticamente le impostazioni di scalabilità.**
Kaspersky Embedded Systems Security 2.2 regola automaticamente il numero di processi utilizzati.
 - **Imposta manualmente il numero di processi di lavoro.**
Kaspersky Embedded Systems Security 2.2 regola il numero di processi di lavoro attivi in base ai valori specificati.
Questo è il valore predefinito.
 - **Numero massimo di processi attivi.**
Numero massimo di processi utilizzati da Kaspersky Embedded Systems Security 2.2. Il campo di immissione è disponibile se l'opzione **Imposta manualmente il numero di processi di lavoro** è selezionata.
 - **Numero di processi per la protezione in tempo reale.**
Numero massimo di processi utilizzati dai componenti dell'attività Protezione in tempo reale. Il campo di immissione è disponibile se l'opzione **Imposta manualmente il numero di processi di lavoro** è selezionata.
 - **Numero di processi per le attività di scansione su richiesta in background.**
Numero massimo di processi utilizzati dal componente Scansione su richiesta durante l'esecuzione delle attività Scansione su richiesta in background. Il campo di immissione è disponibile se l'opzione **Imposta manualmente il numero di processi di lavoro** è selezionata.

Nella sezione **Interazione con l'utente** configurare la visualizzazione dell'icona dell'applicazione nell'area di notifica della barra delle applicazioni: deselezionare o selezionare la casella di controllo **Visualizza l'icona nell'area di notifica della barra delle applicazioni**.

5. Fare clic su **OK**.

Le impostazioni dell'applicazione configurate verranno salvate.

Configurazione delle impostazioni di sicurezza in Kaspersky Security Center

Il processo di configurazione delle impostazioni dei componenti funzionali di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center è simile alla configurazione locale delle impostazioni di questi componenti nella console dell'applicazione. Istruzioni dettagliate su come configurare le impostazioni delle attività e le funzioni dell'applicazione sono disponibili nelle relative sezioni del *Manuale Utente di Kaspersky Embedded Systems Security 2.2*.

► Per configurare manualmente le impostazioni di sicurezza, eseguire le seguenti operazioni:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Impostazioni applicazione**, fare clic sul pulsante **Impostazioni** sotto le impostazioni **Sicurezza e affidabilità**.
4. Nella finestra **Impostazioni di sicurezza** configurare le seguenti impostazioni:
 - Nella sezione **Impostazioni affidabilità** configurare le impostazioni per il ripristino delle attività di Kaspersky Embedded Systems Security 2.2 quando l'applicazione restituisce un errore o viene arrestata.
 - **Esegui ripristino attività**
Questa casella di controllo consente di abilitare o disabilitare il ripristino delle attività di Kaspersky Embedded Systems Security 2.2 quando l'applicazione restituisce un errore o viene arrestata.
Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 ripristina automaticamente le attività di Kaspersky Embedded Systems Security 2.2 quando l'applicazione restituisce un errore o viene arrestata.
Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 non ripristina le attività di Kaspersky Embedded Systems Security 2.2 quando l'applicazione restituisce un errore o viene arrestata.
La casella di controllo è selezionata per impostazione predefinita.
 - **Ripristina le attività di scansione su richiesta non più di (volte)**
Numero di tentativi di ripristinare un'attività Scansione su richiesta dopo che Kaspersky Embedded Systems Security 2.2 restituisce un errore. Il campo di immissione è

disponibile se la casella di controllo **Esegui ripristino attività** è selezionata.

- Nella sezione **Azioni in caso di passaggio all'alimentazione di backup UPS** specificare le limitazioni sul carico del computer create da Kaspersky Embedded Systems Security 2.2 dopo il passaggio all'alimentazione UPS:

- **Non avviare le attività di scansione pianificate**

Questa casella di controllo consente di abilitare o disabilitare l'avvio di un'attività di scansione pianificata dopo il passaggio del computer a una fonte di alimentazione UPS finché non viene ripristinata la modalità di alimentazione standard.

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 non avvia le attività di scansione pianificate dopo il passaggio del computer a una fonte di alimentazione UPS finché non viene ripristinata la modalità di alimentazione standard.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 avvia le attività di scansione pianificate indipendentemente dalla modalità di alimentazione.

La casella di controllo è selezionata per impostazione predefinita.

- **Arresta le attività di scansione correnti**

La casella di controllo consente di abilitare o disabilitare l'esecuzione delle attività di scansione in corso dopo il passaggio del computer a una fonte di alimentazione UPS.

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 sospende le attività di scansione in corso dopo il passaggio del computer a una fonte di alimentazione UPS.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 prosegue le attività di scansione in corso dopo il passaggio del computer a una fonte di alimentazione UPS.

La casella di controllo è selezionata per impostazione predefinita.

Il computer passa all'alimentazione UPS solo se il livello di carica della batteria scende al di sotto del 90%.

- Nella sezione **Impostazioni di protezione tramite password** impostare una password per proteggere l'accesso alle funzioni di Kaspersky Embedded Systems Security 2.2.

5. Fare clic su **OK**.

Le impostazioni di scalabilità e affidabilità verranno salvate.

Configurazione delle impostazioni di connessione tramite Kaspersky Security Center

Il processo di configurazione delle impostazioni dei componenti funzionali di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center è simile alla configurazione locale delle impostazioni di questi componenti nella console dell'applicazione. Istruzioni dettagliate su come configurare le impostazioni delle attività e le funzioni dell'applicazione sono disponibili nelle relative sezioni del *Manuale Utente di Kaspersky Embedded Systems Security 2.2*.

Le impostazioni di connessione configurate vengono utilizzate per la connessione di Kaspersky Embedded Systems Security 2.2 ai server di aggiornamento e di attivazione e durante l'integrazione delle applicazioni con i servizi KSN.

► Per configurare le impostazioni di connessione, eseguire le seguenti operazioni:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Impostazioni applicazione** fare clic sul pulsante **Impostazioni** nel gruppo **Server proxy**. Verrà visualizzata la finestra **Impostazioni di connessione**.
4. Nella finestra **Impostazioni di connessione** configurare le seguenti impostazioni:
 - Nella sezione **Impostazioni del server proxy** selezionare le impostazioni di utilizzo del server proxy:
 - **Non utilizzare un server proxy.**
Se questa opzione è selezionata, Kaspersky Embedded Systems Security 2.2 si connette direttamente ai servizi KSN, senza utilizzare un server proxy.
 - **Rileva automaticamente le impostazioni del server proxy.**
Se questa opzione è selezionata, Kaspersky Embedded Systems Security 2.2 definisce automaticamente le impostazioni per la connessione ai servizi KSN utilizzando il protocollo WPAD (Web Proxy Auto-Discovery).
Questa opzione è selezionata per impostazione predefinita.

- **Usa le impostazioni del server proxy specificate.**

Se questa opzione è selezionata, Kaspersky Embedded Systems Security 2.2 si connette a KSN utilizzando le impostazioni del server proxy specificate manualmente.

- Indirizzo IP o nome simbolico del server proxy e numero di porta.

- **Non utilizzare un server proxy per gli indirizzi locali.**

La casella di controllo consente di abilitare o disabilitare l'utilizzo di un server proxy durante l'accesso ai computer contenuti nella stessa rete del computer in cui è installato Kaspersky Embedded Systems Security 2.2.

Se questa casella di controllo è selezionata, l'accesso ai computer viene eseguito direttamente dalla rete che ospita il computer in cui è installato Kaspersky Embedded Systems Security 2.2. Non viene utilizzato alcun server proxy.

Se la casella di controllo è deselezionata, viene utilizzato il server proxy per la connessione ai computer locali.

La casella di controllo è selezionata per impostazione predefinita.

- Nella sezione **Impostazioni di autenticazione del server proxy** specificare le impostazioni di autenticazione:

- Selezionare le impostazioni di autenticazione nell'elenco a discesa.

- **Non usare l'autenticazione** - l'autenticazione non viene eseguita. Questa modalità è selezionata per impostazione predefinita.

- **Usa l'autenticazione NTLM** - l'autenticazione viene eseguita tramite il protocollo di autenticazione di rete NTLM sviluppato da Microsoft.

- **Usa l'autenticazione NTLM con nome utente e password** - l'autenticazione viene eseguita utilizzando il nome utente e la password tramite il protocollo di autenticazione di rete NTLM sviluppato da Microsoft.

- **Applica nome utente e password** - l'autenticazione viene eseguita utilizzando il nome utente e la password.

- Immettere il nome utente e la password, se necessario.

- Nella sezione **Licenze** deselezionare o selezionare l'opzione **Usa Kaspersky Security Center come server proxy durante l'attivazione dell'applicazione**.

5. Fare clic su **OK**.

Le impostazioni di connessione configurate verranno salvate.

Configurazione delle funzionalità avanzate

È possibile configurare le funzionalità avanzate di Kaspersky Embedded Systems Security 2.2 da Kaspersky Security Center per un gruppo di computer o per un singolo computer.

In questa sezione

Configurazione delle impostazioni dell'area attendibile in Kaspersky Security Center	129
Scansione unità rimovibili	133
Configurazione delle autorizzazioni di accesso in Kaspersky Security Center	135
Configurazione delle impostazioni di Quarantena e Backup in Kaspersky Security Center	136

Configurazione delle impostazioni dell'area attendibile in Kaspersky Security Center

Per impostazione predefinita, l'area attendibile viene applicata ai nuovi criteri e attività creati.

► *Per configurare le impostazioni dell'area attendibile:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Supplementari** fare clic sul pulsante **Impostazioni** nel gruppo **Area attendibile**.
Verrà visualizzata la finestra **Area attendibile**.
4. Nella scheda **Esclusioni** specificare gli oggetti che devono essere ignorati da Kaspersky Embedded Systems Security 2.2 durante la scansione:
 - Per creare le esclusioni consigliate, fare clic sul pulsante **Aggiungi esclusioni consigliate**.
Questo pulsante consente di estendere l'elenco delle esclusioni aggiungendo le esclusioni raccomandate da Microsoft e le esclusioni raccomandate da Kaspersky Lab.
 - Per importare le esclusioni, fare clic sul pulsante **Importa** e nella finestra visualizzata selezionare i file che devono essere ritenuti attendibili da Kaspersky Embedded Systems Security 2.2.
 - Per specificare manualmente le condizioni per cui un file sarà ritenuto attendibile, fare clic sul pulsante **Aggiungi**. Nella finestra visualizzata specificare le seguenti impostazioni:
 - **Oggetto da analizzare**
Aggiungere un file, una cartella, un'unità o un file di script a un'esclusione.
Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 ignora l'ambito predefinito, il file, la cartella, l'unità o il file di script specificato durante l'esecuzione della scansione tramite il componente di Kaspersky Embedded Systems Security 2.2 selezionato nella sezione **Ambito di utilizzo dell'esclusione**.
La casella di controllo è selezionata per impostazione predefinita.
 - **Oggetti da rilevare**
Gli oggetti vengono esclusi dalla scansione in base al nome o alla maschera per il nome dell'oggetto rilevabile. L'elenco di nomi degli oggetti rilevabili è disponibile sul sito Web dell'Enciclopedia dei Virus (<http://www.securelist.com>).
Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 ignora gli oggetti rilevabili specificati durante la scansione.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 rileva tutti gli oggetti specificati nell'applicazione per impostazione predefinita.

La casella di controllo è deselezionata per impostazione predefinita.

- **Ambito di utilizzo dell'esclusione**

Nome dell'attività di Kaspersky Embedded Systems Security 2.2 in cui viene utilizzata la regola.

- Se necessario, specificare informazioni aggiuntive per descrivere l'esclusione nel campo **Commento**.

5. Nella finestra **Area attendibile**, nella scheda **Processi attendibili**, specificare i processi che devono essere ignorati da Kaspersky Embedded Systems Security 2.2 durante la scansione:

- **Non controllare le operazioni di backup dei file**

La casella di controllo consente di abilitare o disabilitare la scansione delle operazioni di lettura dei file se tali operazioni sono eseguite da strumenti di backup installati nel computer.

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 ignora le operazioni di lettura dei file eseguite da strumenti di backup installati nel computer.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 esamina le operazioni di lettura dei file eseguite da strumenti di backup installati nel computer.

La casella di controllo è selezionata per impostazione predefinita.

- **Non controllare le attività sui file dei processi specificati**

La casella di controllo consente di abilitare o disabilitare la scansione delle attività sui file dei processi attendibili.

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 ignora le operazioni dei processi attendibili durante la scansione.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 esamina le operazioni sui file dei processi attendibili.

La casella di controllo è deselezionata per impostazione predefinita.

6. Se necessario, aggiungere i processi di cui non si desidera esaminare le attività sui file (vedere la sezione "Aggiunta di processi attendibili" a pagina [130](#)) facendo clic sul pulsante **Aggiungi**.

7. Fare clic su **OK** nella finestra **Area attendibile** per salvare le modifiche.

Aggiunta di processi attendibili

► *Per aggiungere uno o più processi all'elenco dei processi attendibili:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Supplementari** fare clic sul pulsante **Impostazioni** nel gruppo **Area attendibile**.
Verrà visualizzata la finestra **Area attendibile**.
4. Nella scheda **Processi attendibili** selezionare la casella di controllo **Non controllare le attività sui file dei processi specificati**.
5. Fare clic sul pulsante **Aggiungi**.
6. Dal menu di scelta rapida del pulsante selezionare una delle opzioni:

- **Più processi.**

Nella finestra **Aggiunta di processi attendibili** visualizzata configurare le seguenti impostazioni:

- a. **Utilizza il percorso completo del processo sul disco per considerarlo attendibile.**

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 utilizzerà il percorso completo del file per determinare lo stato di attendibilità del processo.

Se la casella di controllo è deselezionata, il percorso del file non viene considerato come criterio per determinare lo stato di attendibilità del processo.

La casella di controllo è selezionata per impostazione predefinita.

- b. **Utilizza l'hash del file del processo per considerarlo attendibile.**

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 utilizza l'hash del file selezionato per determinare lo stato di attendibilità del processo.

Se la casella di controllo è deselezionata, l'hash del file non verrà considerato come criterio per determinare lo stato di attendibilità del processo.

La casella di controllo è selezionata per impostazione predefinita.

- c. Fare clic sul pulsante **Sfoglia** per aggiungere i dati in base ai processi dei file eseguibili.

- d. Selezionare un file eseguibile nella finestra visualizzata.

È possibile aggiungere un solo file eseguibile alla volta. Ripetere i passaggi c-d per aggiungere altri file eseguibili.

- e. Fare clic sul pulsante **Processi** per aggiungere i dati in base ai processi in esecuzione.

- f. Selezionare i processi nella finestra visualizzata. Per selezionare più processi, tenere premuto **CTRL** durante la selezione.

- g. Fare clic su **OK**.

È necessario che l'account con cui viene eseguita l'attività Protezione dei file in tempo reale disponga dei diritti di amministratore sul computer in cui è installato Kaspersky Embedded Systems Security 2.2 per consentire di visualizzare l'elenco dei processi attivi. È possibile ordinare i processi nell'elenco dei processi attivi in base al nome del file, al PID o al percorso al file eseguibile del processo nel computer locale. È possibile selezionare i processi in esecuzione facendo clic sul pulsante **Processi** solo utilizzando la console dell'applicazione in un computer locale o nelle impostazioni dell'host specificate tramite Kaspersky Security Center.

- **Un processo in base al nome e al percorso.**

Nella finestra **Aggiungi processo attendibile manualmente** visualizzata configurare le seguenti impostazioni:

- a. Immettere il percorso di un file eseguibile (incluso il nome del file).
- b. Fare clic su **OK**.

- **Un processo in base alle proprietà dell'oggetto.**

Nella finestra **Aggiungi processo attendibile** visualizzata configurare le seguenti impostazioni:

- a. Fare clic sul pulsante **Sfoggia** e selezionare un processo.
- b. **Utilizza il percorso completo del processo sul disco per considerarlo attendibile.**

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 utilizzerà il percorso completo del file per determinare lo stato di attendibilità del processo.

Se la casella di controllo è deselezionata, il percorso del file non viene considerato come criterio per determinare lo stato di attendibilità del processo.

La casella di controllo è selezionata per impostazione predefinita.
- c. **Utilizza l'hash del file del processo per considerarlo attendibile.**

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 utilizza l'hash del file selezionato per determinare lo stato di attendibilità del processo.

Se la casella di controllo è deselezionata, l'hash del file non verrà considerato come criterio per determinare lo stato di attendibilità del processo.

La casella di controllo è selezionata per impostazione predefinita.
- d. Fare clic su **OK**.

Per aggiungere il processo selezionato all'elenco dei processi attendibili, deve essere selezionato almeno un criterio di attendibilità.

7. Nella finestra **Aggiungi processo attendibile** fare clic sul pulsante **OK**.

Il file o il processo selezionato verrà aggiunto all'elenco dei processi attendibili nella finestra **Area attendibile**.

Applicazione della maschera not-a-virus

La maschera not-a-virus consente di ignorare i file del software e le risorse Web legittimi, che possono essere considerati dannosi, durante la scansione. La maschera influisce sulle seguenti attività:

- Protezione dei file in tempo reale.
- Scansione su richiesta.

Se la maschera non viene aggiunta all'elenco delle esclusioni, Kaspersky Embedded Systems Security 2.2 applicherà le azioni specificate nelle impostazioni dell'attività per il software o le risorse Web che appartengono a questa categoria.

► *Per applicare la maschera not-a-virus:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Supplementari** fare clic sul pulsante **Impostazioni** nel gruppo **Area attendibile**.
Verrà visualizzata la finestra **Area attendibile**.
4. Nella scheda **Esclusioni** scorrere l'elenco, quindi selezionare la riga con il valore **not-a-virus:***, se la casella di controllo è deselezionata.
5. Fare clic su **OK**.

La nuova configurazione verrà applicata.

Scansione unità rimovibili

È possibile configurare la scansione delle unità rimovibili connesse al computer protetto tramite la porta USB.

Kaspersky Embedded Systems Security 2.2 esamina un'unità rimovibile utilizzando l'attività Scansione su richiesta. L'applicazione crea automaticamente una nuova attività Scansione su richiesta quando l'unità rimovibile è connessa ed elimina l'attività al termine della scansione. L'attività creata viene eseguita con il livello di sicurezza predefinito per la scansione delle unità rimovibili. Non è possibile configurare le impostazioni dell'attività Scansione su richiesta temporanea.

Kaspersky Embedded Systems Security 2.2 esamina le unità USB rimovibili connesse quando sono registrate come dispositivi di archiviazione di massa USB nel sistema operativo. L'applicazione non esamina un'unità rimovibile se la connessione è bloccata dall'attività Controllo dispositivi. L'applicazione non esamina i dispositivi mobili connessi tramite MTP.

Kaspersky Embedded Systems Security 2.2 consente l'accesso alle unità rimovibili durante la scansione.

I risultati della scansione per ogni unità rimovibile sono disponibili nel log per l'attività Scansione su richiesta creata al momento della connessione dell'unità rimovibile.

È possibile modificare le impostazioni del componente Scansione unità rimovibili (vedere la seguente tabella).

Tabella 28. Impostazioni di Scansione unità rimovibili

Impostazione	Valore predefinito	Descrizione
Esamina unità rimovibili al momento della connessione tramite USB	La casella di controllo è deselezionata	È possibile attivare o disattivare la scansione dell'unità rimovibile al momento della connessione al computer protetto tramite USB.
Esamina unità rimovibili se il volume dei dati archiviati non supera (MB):	1024 MB	È possibile ridurre l'ambito del componente impostando il volume massimo di dati sull'unità sottoposta a scansione. Kaspersky Embedded Systems Security 2.2 non esegue la scansione delle unità rimovibili se il volume dei dati archiviati supera il valore specificato.
Esamina con il livello di sicurezza	Massima protezione	È possibile configurare le attività Scansione su richiesta create selezionando uno dei tre livelli di sicurezza: <ul style="list-style-type: none"> • Massima protezione • Raccomandato • Massima performance L'algoritmo utilizzato quando vengono rilevati oggetti infetti, potenzialmente infetti e di altro tipo e le altre impostazioni di scansione per ciascun livello di sicurezza corrispondono ai livelli di sicurezza predefiniti nelle attività Scansione su richiesta.

► Per configurare la scansione delle unità rimovibili al momento della connessione, eseguire le seguenti azioni:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Supplementari** fare clic su **Impostazioni** nel gruppo **Scansione unità rimovibili**.
Verrà visualizzata la finestra **Scansione unità rimovibili**.
4. Nella sezione **Esamina alla connessione** procedere come segue:
 - Selezionare la casella di controllo **Esamina unità rimovibili al momento della connessione tramite USB** se si desidera che Kaspersky Embedded Systems Security 2.2 esamini automaticamente le unità

rimovibili quando sono connesse.

- Se richiesto, selezionare **Esamina unità rimovibili se il volume dei dati archiviati non supera (MB)** e specificare il valore massimo nel campo a destra.
- Nell'elenco a discesa **Esamina con il livello di sicurezza** specificare il livello di sicurezza con le impostazioni richieste per la scansione delle unità rimovibili.

5. Fare clic su **OK**.

Le impostazioni specificate vengono salvate e applicate.

Configurazione delle autorizzazioni di accesso in Kaspersky Security Center

È possibile configurare le autorizzazioni di accesso per gestire l'applicazione e il servizio di Kaspersky Security in Kaspersky Security Center per un gruppo di computer o per un computer distinto.

Il processo di configurazione delle impostazioni dei componenti funzionali di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center è simile alla configurazione locale delle impostazioni di questi componenti nella console dell'applicazione. Istruzioni dettagliate su come configurare le impostazioni delle attività e le funzioni dell'applicazione sono disponibili nelle relative sezioni del *Manuale Utente di Kaspersky Embedded Systems Security 2.2*.

► *Per configurare le autorizzazioni di accesso per la gestione dell'applicazione e del servizio di Kaspersky Security:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Aprire la sezione **Supplementari** ed eseguire le seguenti operazioni:
 - Per configurare le autorizzazioni di accesso per la gestione di Kaspersky Embedded Systems Security 2.2 per un utente o un gruppo di utenti, nella sezione **Autorizzazioni di accesso utente per la gestione dell'applicazione** fare clic sul pulsante **Impostazioni**.
 - Per configurare le autorizzazioni di accesso per la gestione del servizio di Kaspersky Security per un utente o un gruppo di utenti, nella sezione **Autorizzazioni di accesso utente per la gestione del servizio Security** fare clic sul pulsante **Impostazioni**.

4. Nella finestra visualizzata configurare i privilegi di accesso (vedere la sezione "Autorizzazioni di accesso per le funzioni di Kaspersky Embedded Systems Security 2.2" a pagina [76](#)) in base alle esigenze.

Le impostazioni specificate verranno salvate.

Configurazione delle impostazioni di quarantena e backup in Kaspersky Security Center

Il processo di configurazione delle impostazioni dei componenti funzionali di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center è simile alla configurazione locale delle impostazioni di questi componenti nella console dell'applicazione. Istruzioni dettagliate su come configurare le impostazioni delle attività e le funzioni dell'applicazione sono disponibili nelle relative sezioni del *Manuale Utente di Kaspersky Embedded Systems Security 2.2*.

► Per configurare le impostazioni generali di Backup in Kaspersky Security Center:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Supplementari** fare clic sul pulsante **Impostazioni** nel gruppo **Archivi**.
4. Utilizzare la scheda **Backup** della finestra **Impostazioni archivi** per configurare le seguenti impostazioni di **Backup**:
 - Per specificare la **cartella Backup**, utilizzare il campo **Cartella Backup** per selezionare la cartella desiderata nell'unità locale del computer protetto o immettere il relativo percorso completo.
 - Per impostare la dimensione massima della cartella **Backup**, selezionare la casella di controllo **Dimensione massima backup (MB)** e specificare il valore appropriato (in megabyte) nel campo di immissione.
 - Per impostare la soglia dello spazio disponibile in Backup, definire il valore dell'impostazione **Dimensione massima backup (MB)**, selezionare la casella di controllo **Valore di soglia dello spazio disponibile (MB)** e specificare il valore minimo dello spazio disponibile nella cartella **Backup** (in megabyte).
 - Per specificare una cartella per gli oggetti ripristinati, selezionare la cartella appropriata in un'unità locale del computer protetto nella sezione Impostazioni ripristino o immettere il nome e il percorso completo della cartella nel campo **Cartella di destinazione per il ripristino degli oggetti**.

5. Nella finestra **Impostazioni archivi**, nella scheda **Quarantena**, configurare le seguenti impostazioni della **Quarantena**:
 - Per modificare la cartella **Quarantena**, nel campo di immissione **Cartella Quarantena** specificare il percorso completo della cartella nell'unità locale del computer protetto.
 - Per impostare la dimensione massima della cartella **Quarantena**, selezionare la casella di controllo **Dimensione massima quarantena (MB)** e specificare il valore di questo parametro (in megabyte) nel campo di immissione.
 - Per impostare la quantità minima di spazio disponibile in **Quarantena**, selezionare la casella di controllo **Dimensione massima quarantena (MB)** e la casella di controllo **Valore di soglia dello spazio disponibile (MB)**, quindi specificare il valore di questo parametro (in megabyte) nel campo di immissione.
 - Per modificare la cartella in cui devono essere ripristinati gli oggetti dalla Quarantena, nel campo di immissione **Cartella di destinazione per il ripristino degli oggetti** specificare il percorso completo della cartella nell'unità locale del computer protetto.
6. Fare clic su **OK**.

Le impostazioni configurate per Quarantena e Backup verranno salvate.

Configurazione di log e notifiche

È possibile utilizzare Kaspersky Security Center Administration Console per configurare le notifiche per gli amministratori e gli utenti sui seguenti eventi relativi a Kaspersky Embedded Systems Security 2.2 e allo stato della protezione anti-virus nel computer protetto:

- L'amministratore può ricevere informazioni sugli eventi dei tipi selezionati.
- Gli utenti della rete LAN che accedono al computer protetto e gli utenti di computer terminali possono ricevere informazioni sugli eventi di tipo *Oggetto rilevato*.

Le notifiche sugli eventi di Kaspersky Embedded Systems Security 2.2 possono essere configurate per un singolo computer utilizzando la finestra **Proprietà: <nome computer>** del computer selezionato o per un gruppo di computer nella finestra **Proprietà: <nome criterio>** del gruppo di amministrazione selezionato.

Nella scheda **Eventi** o nella finestra **Impostazioni di notifica** è possibile configurare i seguenti tipi di notifiche:

- Le notifiche per gli amministratori sugli eventi dei tipi selezionati possono essere configurate utilizzando la scheda **Eventi** (la scheda standard dell'applicazione Kaspersky Security Center). Per informazioni dettagliate sui metodi di notifica, vedere la *Guida di Kaspersky Security Center*.
- Le notifiche per gli amministratori e gli utenti possono essere configurate nella finestra **Impostazioni di notifica**.

Il processo di configurazione delle impostazioni dei componenti funzionali di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center è simile alla configurazione locale delle impostazioni di questi componenti nella console dell'applicazione. Istruzioni dettagliate su come configurare le impostazioni delle attività e le funzioni dell'applicazione sono disponibili nelle relative sezioni del *Manuale Utente di Kaspersky Embedded Systems Security 2.2*.

È possibile configurare le notifiche per alcuni tipi di eventi solo nella finestra o nella scheda. Possono essere utilizzate sia la finestra che la scheda per configurare le notifiche per gli altri tipi di eventi.

Se si configurano notifiche sugli eventi dello stesso tipo utilizzando la stessa modalità nella scheda **Eventi** e nella finestra **Impostazioni di notifica**, l'amministratore di sistema riceverà le notifiche di tali eventi due volte, ma nella stessa modalità.

In questa sezione

Configurazione delle impostazioni dei log	138
Log di sicurezza	139
Configurazione delle impostazioni di integrazione SIEM	139
Configurazione delle impostazioni di notifica	142
Configurazione dell'interazione con Administration Server	143

Configurazione delle impostazioni dei log

Il processo di configurazione delle impostazioni dei componenti funzionali di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center è simile alla configurazione locale delle impostazioni di questi componenti nella console dell'applicazione. Istruzioni dettagliate su come configurare le impostazioni delle attività e le funzioni dell'applicazione sono disponibili nelle relative sezioni del *Manuale Utente di Kaspersky Embedded Systems Security 2.2*.

► Per configurare i log di Kaspersky Embedded Systems Security 2.2, eseguire le seguenti operazioni:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Log e notifiche** fare clic sul pulsante **Impostazioni** nel gruppo **Log delle attività**.
4. Nella finestra **Impostazioni log** definire le seguenti impostazioni di Kaspersky Embedded Systems Security 2.2 in base ai requisiti:
 - Configurare il livello di dettaglio degli eventi nei log. A tale scopo, eseguire le seguenti operazioni:
 - a. Nell'elenco **Componente** selezionare il componente di Kaspersky Embedded Systems Security 2.2 per cui si desidera impostare il livello di dettaglio.
 - b. Per definire il livello di dettaglio nei log delle attività e nel log di audit di sistema per il componente

selezionato, selezionare il livello desiderato da **Livello di importanza**.

- Per modificare il percorso predefinito per i log, specificare il percorso completo della cartella o fare clic sul pulsante **Sfoggia** per selezionarlo.
- Specificare il numero di giorni per cui archiviare i log delle attività.
- Specificare il numero di giorni per cui archiviare le informazioni visualizzate nel nodo **Log di audit**.

5. Fare clic su **OK**.

Le impostazioni dei log configurate verranno salvate.

Log di sicurezza

Kaspersky Embedded Systems Security 2.2 mantiene un log degli eventi associati alle violazioni di sicurezza o ai tentativi di violazioni di sicurezza nel computer protetto. In questo log vengono registrati i seguenti eventi:

- Eventi di Prevenzione exploit.
- Eventi critici di Analisi log.
- Eventi critici che indicano un tentativo di violazione di sicurezza (per le attività Protezione del computer in tempo reale, Scansione su richiesta, Monitoraggio integrità file, Controllo dell'avvio delle applicazioni e Controllo dispositivi).

È possibile cancellare il log di sicurezza seguendo la stessa procedura per il log di audit. Kaspersky Embedded Systems Security 2.2 registra inoltre gli eventi di audit relativi alla cancellazione del log di sicurezza.

Configurazione delle impostazioni di integrazione SIEM

Per ridurre il carico sui dispositivi con prestazioni ridotte e ridurre il rischio di compromissione del sistema in seguito all'aumento dei volumi dei log dell'applicazione, è possibile configurare la pubblicazione degli eventi di audit e degli eventi relativi alle prestazioni dell'attività nel *server syslog* tramite il protocollo Syslog.

Un server syslog è un server esterno per l'aggregazione degli eventi (SIEM). Raccoglie e analizza gli eventi ricevuti ed esegue anche altre azioni per la gestione dei log.

È possibile utilizzare l'integrazione SIEM in due modalità:

- **Duplicazione degli eventi nel server syslog:** questa modalità prevede che tutti gli eventi relativi alle prestazioni dell'attività la cui pubblicazione è configurata nelle impostazioni dei log e tutti gli eventi di audit di sistema continuo a essere archiviati nel computer locale anche dopo l'invio a SIEM.

È consigliabile utilizzare questa modalità per ridurre il più possibile il carico sul computer protetto.

- **Eliminazione delle copie locali degli eventi:** questa modalità prevede che tutti gli eventi registrati durante il funzionamento dell'applicazione e pubblicati in SIEM vengano eliminati dal computer locale.

L'applicazione non elimina mai le versioni locali del log di sicurezza.

Kaspersky Embedded Systems Security 2.2 può convertire gli eventi in log dell'applicazione in formati supportati dal server syslog in modo che tali eventi possano essere trasmessi e riconosciuti correttamente da SIEM. L'applicazione supporta la conversione in formato dati strutturati e in formato JSON.

Per ridurre il rischio di errata trasmissione degli eventi a SIEM, è possibile definire le impostazioni per la

connessione al server syslog mirror.

Un server syslog mirror è un server syslog aggiuntivo a cui l'applicazione passa automaticamente se la connessione al server syslog principale non è disponibile o se il server principale non può essere utilizzato.

Per impostazione predefinita, l'integrazione SIEM non è utilizzata. È possibile abilitare e disabilitare l'integrazione SIEM e configurare le impostazioni della funzionalità (vedere la seguente tabella).

Tabella 29. Impostazioni di integrazione SIEM

Impostazione	Valore predefinito	Descrizione
Invia eventi a un server syslog remoto tramite un protocollo syslog	Non applicato	È possibile abilitare o disabilitare l'integrazione SIEM selezionando o deselezionando la casella di controllo a seconda dei casi.
Rimuovi copie locali per gli eventi che sono stati inviati a un server syslog remoto	Non applicato	È possibile configurare le impostazioni per l'archiviazione delle copie locali dei log dopo l'invio a SIEM selezionando o deselezionando la casella di controllo.
Formato eventi	Dati strutturati	È possibile selezionare uno dei due formati in cui l'applicazione converte gli eventi prima di inviarli al server syslog per un migliore riconoscimento di questi eventi da parte di SIEM.
Protocollo di connessione	TCP	È possibile utilizzare l'elenco a discesa per configurare la connessione al server syslog principale tramite i protocolli TCP o UDP e al server syslog mirror tramite il protocollo TCP.
Impostazioni di connessione al server syslog principale	Indirizzo IP: 127.0.0.1 Porta: 514	È possibile utilizzare i campi appropriati per configurare l'indirizzo IP e la porta utilizzati per la connessione al server syslog principale. È possibile specificare l'indirizzo IP solo in formato IPv4.
Usa server syslog mirror se il server principale non è accessibile	Non applicato	È possibile utilizzare la casella di controllo per abilitare o disabilitare l'utilizzo di un server syslog mirror.
Impostazioni di connessione al server syslog mirror	Indirizzo IP: 127.0.0.1 Porta: 514	È possibile utilizzare i campi appropriati per configurare l'indirizzo IP e la porta utilizzati per la connessione al server syslog principale. È possibile specificare l'indirizzo IP solo in formato IPv4.

► *Per configurare le impostazioni di integrazione SIEM:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.

2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Log e notifiche** fare clic sul pulsante **Impostazioni** nel gruppo **Log delle attività**.
Verrà visualizzata la finestra **Impostazioni log e notifiche**.
4. Selezionare la scheda **Integrazione SIEM**.
5. Nella sezione **Impostazioni di integrazione** selezionare la casella di controllo **Invia eventi a un server syslog remoto tramite un protocollo syslog**.

La casella di controllo consente di abilitare o disabilitare la funzionalità per l'invio degli eventi pubblicati a un server syslog esterno.

Se la casella di controllo è selezionata, l'applicazione invia gli eventi pubblicati in SIEM in base alle impostazioni di integrazione SIEM configurate.

Se la casella di controllo è deselezionata, l'applicazione non esegue l'integrazione SIEM. Non è possibile configurare le impostazioni di integrazione SIEM se la casella di controllo è deselezionata.

La casella di controllo è deselezionata per impostazione predefinita.

6. Se necessario, nella sezione **Impostazioni di integrazione** selezionare la casella di controllo **Rimuovi copie locali per gli eventi che sono stati inviati a un server syslog remoto**.

La casella di controllo consente di abilitare o disabilitare l'eliminazione delle copie locali dei log quando questi vengono inviati a SIEM.

Se la casella di controllo è selezionata, l'applicazione elimina le copie locali degli eventi dopo l'avvenuta pubblicazione in SIEM. Questa modalità è consigliata nei computer con prestazioni ridotte.

Se la casella di controllo è deselezionata, l'applicazione invia soltanto gli eventi a SIEM. Le copie dei log continuano a essere archiviate in locale.

La casella di controllo è deselezionata per impostazione predefinita.

Lo stato della casella di controllo **Rimuovi copie locali per gli eventi che sono stati inviati a un server syslog remoto** non influisce sulle impostazioni per l'archiviazione degli eventi del log di sicurezza: l'applicazione non elimina mai automaticamente gli eventi dei log di sicurezza.

7. Nella sezione **Formato eventi** specificare il formato in cui si desidera convertire gli eventi sull'esecuzione dell'applicazione in modo che possano essere inviati a SIEM.
Per impostazione predefinita, l'applicazione li converte nel formato dati strutturati.
8. Nella sezione **Impostazioni di connessione**:
 - Specificare il protocollo di connessione SIEM.

- Specificare le impostazioni per la connessione al server syslog principale.

È possibile specificare un indirizzo IP solo in formato IPv4.

- Se necessario, selezionare la casella di controllo **Usa server syslog mirror se il server principale non è accessibile** se si desidera che l'applicazione utilizzi altre impostazioni di connessione quando non è in grado di inviare gli eventi al server syslog principale.
 - Specificare le seguenti impostazioni per la connessione al server syslog mirror: **Porta** e **Indirizzo IP**.

I campi **Indirizzo IP** e **Porta** per il server syslog mirror non possono essere modificati se la casella di controllo **Usa server syslog mirror se il server principale non è accessibile** è deselezionata.

È possibile specificare un indirizzo IP solo in formato IPv4.

9. Fare clic su **OK**.

Verranno applicate le impostazioni di integrazione SIEM configurate.

Configurazione delle impostazioni di notifica

► Per configurare le notifiche di Kaspersky Embedded Systems Security 2.2, eseguire le seguenti operazioni:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Log e notifiche** fare clic sul pulsante **Impostazioni** nel gruppo **Notifiche degli eventi**.
4. Nella finestra **Impostazioni di notifica** definire le seguenti impostazioni di Kaspersky Embedded Systems Security 2.2 in base ai requisiti:
 - Nell'elenco **Impostazioni di notifica** selezionare il tipo di notifica di cui si desidera configurare le impostazioni.
 - Nella sezione **Notifica per gli utenti** configurare il metodo di notifica per gli utenti. Se necessario, immettere il testo del messaggio di notifica.
 - Nella sezione **Notifica per gli amministratori** configurare il metodo di notifica per gli amministratori. Se necessario, immettere il testo del messaggio di notifica. Se necessario, configurare le impostazioni di notifica aggiuntive facendo clic sul pulsante **Impostazioni**.
 - Nella sezione **Soglie di generazione degli eventi** specificare gli intervalli di tempo al termine dei quali Kaspersky Embedded Systems Security 2.2 registra gli eventi *Il database dell'applicazione non è aggiornato, Il database dell'applicazione non è aggiornato da molto tempo* e *La scansione aree critiche*

non viene eseguita da molto tempo.

- **Il database dell'applicazione non è aggiornato (giorni)**

Numero di giorni che sono trascorsi dall'ultimo aggiornamento dei database.

Il valore predefinito è 7 giorni.

- **Il database dell'applicazione non è aggiornato da molto tempo (giorni)**

Numero di giorni che sono trascorsi dall'ultimo aggiornamento dei database.

Il valore predefinito è 14 giorni.

- **La scansione aree critiche non viene eseguita da molto tempo (giorni)**

Numero di giorni dopo il completamento dell'ultima Scansione aree critiche.

Il valore predefinito è 30 giorni.

5. Fare clic su **OK**.

Le impostazioni di notifica configurate verranno salvate.

Configurazione dell'interazione con Administration Server

► Per selezionare i tipi di oggetti su cui Kaspersky Embedded Systems Security 2.2 invia le informazioni a Kaspersky Security Center Administration Server:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Log e notifiche** fare clic sul pulsante **Impostazioni** nel gruppo **Interazione con Administration Server**.
Verrà visualizzata la finestra **Elenchi delle reti di Administration Server**.
4. Nella finestra **Elenchi delle reti di Administration Server** selezionare i tipi di oggetti su cui Kaspersky Embedded Systems Security 2.2 invierà le informazioni a Kaspersky Security Center Administration Server:
 - Oggetti in quarantena.
 - Oggetti sottoposti a backup.
5. Fare clic su **OK**.
Kaspersky Embedded Systems Security 2.2 invierà le informazioni sui tipi di oggetti selezionati ad Administration Server.

Protezione del computer in tempo reale

Questa sezione fornisce informazioni sui componenti di Protezione del computer in tempo reale: Protezione dei file in tempo reale, Utilizzo di KSN e Prevenzione exploit. Vengono inoltre fornite istruzioni su come configurare le attività di Protezione in tempo reale e gestire le impostazioni di sicurezza di un computer protetto.

In questo capitolo

Protezione dei file in tempo reale	144
Utilizzo di KSN	159
Prevenzione exploit	166

Protezione dei file in tempo reale

Questa sezione contiene informazioni sull'attività Protezione dei file in tempo reale e su come configurarla.

In questa sezione

Informazioni sull'attività Protezione dei file in tempo reale	144
Configurazione delle impostazioni dell'attività Protezione dei file in tempo reale	145
Utilizzo dell'analizzatore euristico	147
Selezione della modalità di protezione	147
Ambito della protezione nell'attività Protezione dei file in tempo reale	149
Configurazione manuale delle impostazioni di sicurezza	152

Informazioni sull'attività Protezione dei file in tempo reale

Quando l'attività Protezione dei file in tempo reale è in esecuzione, Kaspersky Embedded Systems Security 2.2 esamina i seguenti oggetti del computer protetto al momento dell'accesso:

- File.
- Flussi alternativi del file system (flussi NTFS).
- Record di avvio principale e settori di avvio nelle unità disco rigido locali e nei dispositivi esterni.
- File contenitore di Windows Server® 2016 e Windows Server 2019.

Quando un'applicazione scrive un file in un computer o ne esegue la lettura, Kaspersky Embedded Systems Security 2.2 intercetta il file, lo esamina alla ricerca di minacce, e, se viene rilevata una minaccia, esegue un'azione predefinita o un'azione specificata dall'utente: tenta di disinfettarlo, lo mette in Quarantena o lo elimina. Kaspersky Embedded Systems Security 2.2 restituisce il file all'applicazione se non è infetto o se è stato disinfettato.

Kaspersky Embedded Systems Security 2.2 intercetta le operazioni sui file eseguite nei contenitori di Windows

Server 2016 e Windows Server 2019.

Un *contenitore* è un ambiente isolato, che consente l'esecuzione delle applicazioni senza un'interazione diretta con il sistema operativo. Se un contenitore è incluso nell'ambito di protezione dell'attività, Kaspersky Embedded Systems Security 2.2 esamina i file contenitore a cui accedono gli utenti, alla ricerca di eventuali minacce. Quando viene rilevata una minaccia, l'applicazione tenta di disinfettare il contenitore. Se il tentativo ha esito positivo, il contenitore continua a funzionare. Se la disinfezione non riesce, il contenitore viene disattivato.

Kaspersky Embedded Systems Security 2.2 rileva anche il malware per i processi in esecuzione in Windows Subsystem for Linux®. Per tali processi, l'attività Protezione dei file in tempo reale applica l'azione definita dalla configurazione corrente.

Configurazione delle impostazioni dell'attività Protezione dei file in tempo reale

Per impostazione predefinita, l'attività di sistema Protezione dei file in tempo reale utilizza le impostazioni descritte nella seguente tabella. È possibile modificare i valori di queste impostazioni.

Tabella 30. Impostazioni predefinite dell'attività Protezione dei file in tempo reale

Impostazione	Valore predefinito	Descrizione
Ambito della protezione	Intero computer, escluse le unità virtuali.	È possibile limitare l'ambito della protezione.
Livello di sicurezza	Impostazioni comuni per l'intero ambito della protezione; corrisponde al livello di sicurezza Raccomandato .	Per i nodi selezionati nell'albero delle risorse di file del computer, è possibile: <ul style="list-style-type: none"> • Applicare un altro livello di sicurezza predefinito. • Modificare il livello di sicurezza manualmente. • Salvare le impostazioni di sicurezza del nodo selezionato come un modello per utilizzarle successivamente.
Modalità di protezione degli oggetti	In fase di accesso e modifica.	È possibile selezionare la modalità di protezione, ovvero definire il tipo di accesso con cui Kaspersky Embedded Systems Security 2.2 esaminerà gli oggetti.
Analizzatore euristico	Viene applicato il livello di protezione Medio .	È possibile abilitare o disabilitare l'analizzatore euristico e configurare il livello di analisi.
Applica area attendibile	Applicato.	Elenco generale di esclusioni che possono essere utilizzate nelle attività selezionate.
Utilizzo di KSN per la protezione	Applicato.	È possibile migliorare la protezione del computer utilizzando l'infrastruttura di servizi cloud di Kaspersky Security Network (disponibile se è stata accettata l'Informativa KSN).
Pianificazione dell'avvio dell'attività	All'avvio dell'applicazione.	È possibile configurare l'avvio pianificato dell'attività.

► Per configurare le impostazioni dell'attività *Protezione dei file in tempo reale*, eseguire le seguenti operazioni:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Protezione dei file in tempo reale** fare clic sul pulsante **Impostazioni** nel gruppo **Protezione dei file in tempo reale**.
Verrà visualizzata la finestra **Protezione dei file in tempo reale**.
4. Configurare le seguenti impostazioni dell'attività:
 - Nella scheda **Generale**:
 - Modalità di protezione (vedere la sezione "Selezione della modalità di protezione" a pagina [147](#))
 - Utilizzo dell'analizzatore euristico (vedere pagina [147](#))
 - Impostazioni dell'integrazione con gli altri componenti di Kaspersky Embedded Systems Security 2.2.
 - Nella scheda **Gestione attività**:
 - Impostazioni di avvio delle attività pianificate (vedere la sezione "Configurazione delle impostazioni della pianificazione dell'avvio delle attività" a pagina [119](#)).
5. Selezionare la scheda **Ambito della protezione** e procedere come segue:
 - Fare clic sul pulsante **Aggiungi** o **Modifica** per modificare l'ambito della protezione (vedere la sezione "Ambito della protezione nell'attività Protezione dei file in tempo reale" a pagina [149](#)).
 - Nella finestra visualizzata selezionare gli elementi da includere nell'ambito della protezione dell'attività:
 - **Ambito predefinito**
 - **Disco, cartella o percorso di rete**
 - **File**
 - Selezionare uno dei livelli di sicurezza predefiniti (vedere la sezione "Selezione dei livelli di sicurezza predefiniti" a pagina [150](#)) o configurare manualmente le impostazioni di protezione (vedere la sezione "Configurazione manuale delle impostazioni di sicurezza" a pagina [152](#)).
6. Fare clic su **OK** nella finestra **Protezione dei file in tempo reale**.

Kaspersky Embedded Systems Security 2.2 applica immediatamente le nuove impostazioni all'attività in esecuzione. Le informazioni sulla data e l'ora in cui le impostazioni sono state modificate e i valori delle impostazioni dell'attività prima e dopo la modifica vengono salvati nel log dell'attività.

Utilizzo dell'analizzatore euristico

È possibile utilizzare l'analizzatore euristico e configurare il livello di analisi per le attività di Kaspersky Embedded Systems Security 2.2.

► *Per configurare l'analizzatore euristico:*

1. Aprire le impostazioni dell'applicazione (vedere la sezione "Gestione di Kaspersky Embedded Systems Security 2.2 da Kaspersky Security Center" a pagina [122](#)) o le impostazioni del criterio (vedere la sezione "Configurazione del criterio" a pagina [88](#)) per cui si desidera configurare l'analizzatore euristico.

2. Deselezionare o selezionare la casella di controllo **Usa l'analizzatore euristico**.

Questa casella di controllo consente di abilitare o disabilitare l'analizzatore euristico durante la scansione degli oggetti.

Se la casella di controllo è selezionata, l'analizzatore euristico è abilitato.

Se la casella di controllo è deselezionata, l'analizzatore euristico è disabilitato.

La casella di controllo è selezionata per impostazione predefinita.

3. Se necessario, modificare il livello di analisi utilizzando il dispositivo di scorrimento.

Il dispositivo di scorrimento consente di regolare il livello dell'analisi euristica. Il livello di intensità della scansione definisce un equilibrio tra il livello di dettaglio delle ricerche delle minacce, il carico sulle risorse del sistema operativo e il tempo richiesto per la scansione.

Sono disponibili i seguenti livelli di intensità della scansione:

- **Leggero.** L'analizzatore euristico esegue meno operazioni nei file eseguibili. La probabilità di rilevamento delle minacce è leggermente inferiore. La scansione è più rapida e richiede meno risorse.
- **Medio.** L'analizzatore euristico esegue il numero di istruzioni nei file eseguibili consigliato dagli esperti di Kaspersky Lab.
Questo livello è selezionato per impostazione predefinita.
- **Approfondito.** L'analizzatore euristico esegue più operazioni nei file eseguibili. La probabilità di rilevamento delle minacce è superiore. La scansione utilizza più risorse di sistema, richiede più tempo e può causare un numero più elevato di falsi allarmi.
Il dispositivo di scorrimento è disponibile se la casella di controllo **Usa l'analizzatore euristico** è selezionata.

4. Fare clic su **OK**.

Le impostazioni dell'attività configurate vengono applicate immediatamente all'attività in esecuzione. Se l'attività non è in esecuzione, le impostazioni modificate vengono applicate al successivo avvio.

Selezione della modalità di protezione

Nell'attività Protezione dei file in tempo reale è possibile selezionare la modalità di protezione. La sezione **Modalità di protezione degli oggetti** consente di specificare il tipo di accesso agli oggetti con cui Kaspersky Embedded Systems Security 2.2 deve esaminare gli oggetti.

L'impostazione **Modalità di protezione degli oggetti** ha il valore comune per l'intero ambito della protezione specificato nell'attività. Non è possibile specificare diversi valori per l'impostazione per i singoli nodi nell'ambito della protezione.

► Per selezionare la modalità di protezione, eseguire le seguenti operazioni:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Protezione del computer in tempo reale** fare clic sul pulsante **Impostazioni** nel gruppo **Protezione dei file in tempo reale**.

Verrà visualizzata la finestra **Protezione dei file in tempo reale**.

4. Nella finestra visualizzata aprire la scheda **Generale** e selezionare la modalità di protezione che si desidera impostare:

- **Modalità smart**

Kaspersky Embedded Systems Security 2.2 seleziona autonomamente gli oggetti da esaminare. L'oggetto viene esaminato all'apertura e di nuovo dopo essere stato salvato se è stato modificato. Se sono state eseguite più chiamate all'oggetto dal processo mentre era in esecuzione e se il processo lo ha modificato, Kaspersky Embedded Systems Security 2.2 esamina di nuovo l'oggetto solo dopo che è stato salvato dal processo per l'ultima volta.

- **In fase di accesso e modifica**

Kaspersky Embedded Systems Security 2.2 esamina l'oggetto quando viene aperto e lo esamina di nuovo dopo che è salvato se l'oggetto è stato modificato.

Questa opzione è selezionata per impostazione predefinita.

- **In fase di accesso**

Kaspersky Embedded Systems Security 2.2 esamina tutti gli oggetti quando vengono aperti per la lettura, per l'esecuzione o per la modifica.

- **Durante l'esecuzione**

Kaspersky Embedded Systems Security 2.2 esamina il file solo al momento dell'accesso per l'esecuzione.

5. Fare clic su **OK**.

La modalità di protezione selezionata verrà applicata.

Ambito della protezione nell'attività Protezione dei file in tempo reale

Questa sezione fornisce istruzioni sulla creazione e la gestione di un ambito della protezione nell'attività Protezione dei file in tempo reale.

In questa sezione

Ambiti della protezione predefiniti.....	149
Selezione dei livelli di sicurezza predefiniti.....	150

Ambiti della protezione predefiniti

Le risorse file del computer protetto sono visualizzate nelle impostazioni dell'attività **Protezione dei file in tempo reale** nella scheda **Ambito della protezione**.

L'albero o l'elenco delle risorse dei file visualizza i nodi a cui si dispone di accesso in lettura in base alle impostazioni di sicurezza di Microsoft Windows configurate.

Kaspersky Embedded Systems Security 2.2 copre i seguenti ambiti di protezione predefiniti:

- **Unità disco rigido locali.** Kaspersky Embedded Systems Security 2.2 protegge i file nelle unità disco rigido del computer.
- **Unità rimovibili.** Kaspersky Embedded Systems Security 2.2 protegge i file nei dispositivi esterni, ad esempio CD o unità USB. Tutti i dischi rimovibili o singoli dischi, cartelle o file possono essere inclusi o esclusi dall'ambito della protezione.
- **Rete.** Kaspersky Embedded Systems Security 2.2 protegge i file che vengono scritti in cartelle di rete o letti da queste cartelle dalle applicazioni in esecuzione nel computer. Kaspersky Embedded Systems Security 2.2 non protegge i file quando viene eseguito l'accesso a tali file da applicazioni in altri computer.
- **Unità virtuali.** È possibile includere nell'ambito della protezione le cartelle dinamiche e i file e le unità che sono temporaneamente connessi al computer, ad esempio le unità cluster comuni.

Per impostazione predefinita, è possibile visualizzare e configurare gli ambiti della protezione predefiniti nell'elenco degli ambiti. È anche possibile aggiungere ambiti predefiniti all'elenco durante la sua creazione nelle impostazioni dell'ambito della protezione.

Per impostazione predefinita, l'ambito della protezione include tutte le aree predefinite tranne le unità virtuali.

Le unità virtuali create tramite un comando SUBST non sono visualizzate nell'albero delle risorse dei file del computer nella console dell'applicazione. Per includere gli oggetti nell'unità virtuale nell'ambito della protezione, includere la cartella del computer a cui è associata questa unità virtuale nell'ambito della protezione. Anche le unità di rete connesse non saranno visualizzate nell'elenco delle risorse dei file del computer. Per includere gli oggetti nelle unità di rete nell'ambito della protezione, specificare il percorso della cartella che corrisponde a questa unità di rete nel formato UNC.

Selezione dei livelli di sicurezza predefiniti

È possibile applicare uno dei seguenti livelli di sicurezza predefiniti per i nodi selezionati nell'elenco delle risorse file del computer: **Massima performance**, **Raccomandato** e **Massima protezione**. Ciascuno di questi livelli contiene uno specifico set predefinito di impostazioni di sicurezza (vedere la seguente tabella).

Massima performance

Il livello di sicurezza **Massima performance** è consigliato se, in aggiunta all'utilizzo di Kaspersky Embedded Systems Security 2.2 nei computer, sono previste ulteriori misure di sicurezza per i computer all'interno della rete, ad esempio firewall e criteri di sicurezza esistenti.

Raccomandato

Il livello di sicurezza **Raccomandato** garantisce una combinazione ottimale tra protezione e impatto sulle prestazioni dei computer protetti. Questo livello è consigliato dagli esperti di Kaspersky Lab come sufficiente per la protezione dei computer nella maggior parte delle reti aziendali. Il livello di sicurezza **Raccomandato** è selezionato per impostazione predefinita.

Massima protezione

Il livello di sicurezza **Massima protezione** è consigliato se la rete dell'organizzazione prevede requisiti elevati per la sicurezza dei computer.

Tabella 31. Livelli di sicurezza preimpostati e valori delle impostazioni corrispondenti

Opzioni	Livello di sicurezza		
	Massima performance	Raccomandato	Massima protezione
Protezione degli oggetti	Per estensione	Per formato	Per formato
Proteggi solo i file nuovi e modificati	Abilitata	Abilitata	Disabilitata
Azione da eseguire sugli oggetti infetti e di altro tipo	Blocca l'accesso e disinfetta. Rimuovi se la disinfezione fallisce	Blocca l'accesso ed esegui l'azione consigliata	Blocca l'accesso e disinfetta. Rimuovi se la disinfezione fallisce
Azione da eseguire sugli oggetti potenzialmente infetti	Blocca l'accesso e sposta in quarantena	Blocca l'accesso ed esegui l'azione consigliata	Blocca l'accesso e sposta in quarantena
Escludi file	No	No	No
Non rilevare	No	No	No
Interrompi la scansione se richiede più di (sec.)	60 sec.	60 sec.	60 sec.
Non esaminare gli oggetti composti di dimensioni superiori a (MB)	8 MB	8 MB	Non impostato
Esamina flussi NTFS alternativi	Sì	Sì	Sì
Esamina settori di avvio del disco e MBR	Sì	Sì	Sì

Opzioni	Livello di sicurezza		
Protezione degli oggetti compositi	<ul style="list-style-type: none"> Oggetti compressi* *Solo oggetti nuovi e modificati	<ul style="list-style-type: none"> Archivi SFX* Oggetti compressi* Oggetti OLE incorporati* *Solo oggetti nuovi e modificati	<ul style="list-style-type: none"> Archivi SFX* Oggetti compressi* Oggetti OLE incorporati* *Tutti gli oggetti
Rimuovi interamente i file compositi che non possono essere modificati dall'applicazione in caso di oggetti incorporati	No	No	Sì

Le impostazioni **Protezione degli oggetti**, **Usa la tecnologia iChecker**, **Usa la tecnologia iSwift** e **Usa l'analizzatore euristico** non sono incluse nelle impostazioni dei livelli di sicurezza predefiniti. Se si modificano le impostazioni di sicurezza **Protezione degli oggetti**, **Usa la tecnologia iChecker**, **Usa la tecnologia iSwift** o **Usa l'analizzatore euristico** dopo avere selezionato uno dei livelli di sicurezza predefiniti, il livello di sicurezza selezionato non cambierà.

► Per selezionare uno dei livelli di sicurezza predefiniti, eseguire le seguenti operazioni:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Protezione del computer in tempo reale** fare clic sul pulsante **Impostazioni** nel gruppo **Protezione dei file in tempo reale**.
Verrà visualizzata la finestra **Protezione dei file in tempo reale**.
4. Nella scheda **Ambito della protezione** selezionare il nodo per cui configurare le impostazioni di sicurezza e fare clic su **Configura**.
Verrà visualizzata la finestra **Impostazioni protezione dei file in tempo reale**.

5. Selezionare il livello di sicurezza desiderato nell'elenco a discesa:

- **Massima protezione**
- **Raccomandato**
- **Massima performance**

6. Fare clic su **OK**.

Le nuove impostazioni configurate sono state salvate.

Kaspersky Embedded Systems Security 2.2 applica immediatamente le nuove impostazioni all'attività in esecuzione. Le informazioni sulla data e l'ora in cui le impostazioni sono state modificate e i valori delle impostazioni dell'attività prima e dopo la modifica vengono salvati nel log dell'attività.

Configurazione manuale delle impostazioni di sicurezza

Per impostazione predefinita, l'attività Protezione dei file in tempo reale utilizza impostazioni di sicurezza comuni per l'intero ambito della protezione. Queste impostazioni corrispondono a quelle del livello di sicurezza predefinito **Raccomandato** (vedere la sezione "Selezione dei livelli di sicurezza predefiniti" a pagina [150](#)).

I valori predefiniti delle impostazioni di sicurezza possono essere modificati configurandoli come impostazioni comuni per l'intero ambito della protezione oppure come impostazioni differenti per i diversi nodi nell'elenco o nell'albero delle risorse dei file del computer.

Quando si lavora con l'albero delle risorse dei file del computer, le impostazioni di sicurezza configurate per il nodo padre selezionato vengono applicate automaticamente a tutti i nodi figlio. Le impostazioni di sicurezza del nodo padre non vengono applicate ai nodi figlio configurati separatamente.

► *Per configurare manualmente le impostazioni di sicurezza del nodo selezionato:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Protezione del computer in tempo reale** fare clic sul pulsante **Impostazioni** nel gruppo **Protezione dei file in tempo reale**.

Verrà visualizzata la finestra **Protezione dei file in tempo reale**.

4. Nella scheda **Ambito della protezione** selezionare il nodo per cui configurare le impostazioni di sicurezza e fare clic su **Configura**.

Verrà visualizzata la finestra **Impostazioni protezione dei file in tempo reale**.

5. Nella scheda **Livello di sicurezza** è possibile selezionare un livello esistente o fare clic sul pulsante **Impostazioni** per impostare una configurazione personalizzata.
6. È possibile configurare le impostazioni di sicurezza personalizzate del nodo selezionato in base agli specifici requisiti:
 - Impostazioni generali (vedere la sezione "Configurazione delle impostazioni generali dell'attività" a pagina [153](#))
 - Azioni (vedere la sezione "Configurazione delle azioni" a pagina [156](#))
 - Prestazioni (vedere la sezione "Configurazione delle prestazioni" a pagina [158](#))
7. Fare clic su **Salva** nella finestra **Impostazioni dell'ambito della protezione**.

Le nuove impostazioni dell'ambito della protezione verranno salvate.

Configurazione delle impostazioni generali dell'attività

► *Per configurare le impostazioni generali di sicurezza dell'attività Protezione dei file in tempo reale:*

1. Aprire la finestra **Impostazioni protezione dei file in tempo reale** (vedere la sezione "Configurazione manuale delle impostazioni di sicurezza" a pagina [152](#)).
2. Selezionare la scheda **Generale**.
3. Nella sezione **Protezione degli oggetti** specificare i tipi di oggetti da includere nell'ambito della protezione:
 - **Tutti gli oggetti**
Kaspersky Embedded Systems Security 2.2 esamina tutti gli oggetti.
 - **Oggetti analizzati in base al formato**
Kaspersky Embedded Systems Security 2.2 esamina solo gli oggetti infettabili in base al formato del file.
Kaspersky Lab compila l'elenco dei formati. È incluso nei database di Kaspersky Embedded Systems Security 2.2.
 - **Oggetti analizzati in base all'elenco di estensioni specificate nel database anti-virus**
Kaspersky Embedded Systems Security 2.2 esamina solo gli oggetti infettabili in base all'estensione del file.
Kaspersky Lab compila l'elenco delle estensioni. È incluso nei database di Kaspersky Embedded Systems Security 2.2.
 - **Oggetti analizzati in base all'elenco di estensioni specificato**
Kaspersky Embedded Systems Security 2.2 esamina i file in base all'estensione. L'elenco delle estensioni dei file può essere personalizzato manualmente nella finestra **Elenco di estensioni**, che può essere aperta facendo clic sul pulsante **Modifica**.
 - **Esamina settori di avvio del disco e MBR**
Abilita la protezione di settori di avvio e record di avvio principali.
Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2

esamina i settori di avvio e i record di avvio principali nei dischi rigidi e nelle unità rimovibili del computer.

La casella di controllo è selezionata per impostazione predefinita.

- **Esamina flussi NTFS alternativi**

Scansione dei flussi alternativi di file e cartelle nelle unità con file system NTFS.

Se la casella di controllo è selezionata, l'applicazione esamina un oggetto potenzialmente infetto e tutti i flussi NTFS associati a tale oggetto.

Se la casella di controllo è deselezionata, l'applicazione esamina solo l'oggetto che è stato rilevato e considerato potenzialmente infetto.

La casella di controllo è selezionata per impostazione predefinita.

4. Nella sezione **Prestazioni** selezionare o deselezionare la casella di controllo **Proteggi solo i file nuovi e modificati**.

Questa casella di controllo consente di abilitare o disabilitare la scansione e la protezione dei file che sono stati riconosciuti da Kaspersky Embedded Systems Security 2.2 come nuovi o modificati dall'ultima scansione.

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 esamina e protegge solo i file che ha riconosciuto come nuovi o modificati dall'ultima scansione.

Se la casella di controllo è deselezionata, è possibile scegliere se esaminare e proteggere solo i nuovi file o tutti i file, indipendentemente dal relativo stato di modifica.

Per impostazione predefinita, la casella di controllo è selezionata per i livelli di sicurezza **Massima performance** e **Raccomandato**. Se è impostato il livello di sicurezza **Massima protezione**, la casella di controllo è deselezionata.

Per passare da una all'altra delle opzioni disponibili quando la casella di controllo è deselezionata, fare clic sul collegamento **Tutti / Solo i nuovi** per ognuno dei tipi di oggetti composti.

5. Nella sezione **Protezione degli oggetti composti** specificare gli oggetti composti da includere nell'ambito della protezione:

- **Tutto / Solo i nuovi archivi**

Scansione degli archivi ZIP, CAB, RAR, ARJ e di altri formati di archivio.

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 esamina gli archivi.

Se questa casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 ignora gli archivi durante la scansione.

Il valore predefinito dipende dal livello di sicurezza selezionato.

- **Tutto / Solo i nuovi archivi SFX**

Scansione degli archivi autoestraenti.

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 esamina gli archivi SFX.

Se questa casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 ignora gli archivi SFX durante la scansione.

Il valore predefinito dipende dal livello di sicurezza selezionato.

Questa opzione è attiva quando la casella di controllo **Archivi** è deselezionata.

- **Tutti / Solo i nuovi database e-mail**

Scansione dei file di database di posta Microsoft Outlook® e Microsoft Outlook Express.

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 esamina i file di database di posta.

Se questa casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 ignora i file di database di posta durante la scansione.

Il valore predefinito dipende dal livello di sicurezza selezionato.

- **Tutti / Solo i nuovi oggetti compressi**

Scansione dei file eseguibili compressi da utilità di compressione del codice binario, come UPX o ASPack.

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 esamina i file eseguibili compressi da utilità di compressione.

Se questa casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 ignora i file eseguibili compressi da utilità di compressione durante la scansione.

Il valore predefinito dipende dal livello di sicurezza selezionato.

- **Tutti / Solo la nuova posta semplice**

Scansione dei file di formati di posta, ad esempio i messaggi di Microsoft Outlook Express e Microsoft Outlook.

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 esamina i file dei formati di posta.

Se questa casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 ignora i file dei formati di posta durante la scansione.

Il valore predefinito dipende dal livello di sicurezza selezionato.

- **Tutti / Solo i nuovi oggetti OLE incorporati**

Scansione degli oggetti incorporati nei file (ad esempio, macro di Microsoft Word o allegati dei messaggi e-mail).

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 esamina gli oggetti incorporati nei file.

Se questa casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 ignora gli oggetti incorporati nei file durante la scansione.

Il valore predefinito dipende dal livello di sicurezza selezionato.

6. Fare clic su **Salva**.

La nuova configurazione dell'attività verrà salvata.

Configurazione delle azioni

► Per configurare le azioni sugli oggetti infetti e gli altri oggetti rilevati per l'attività *Protezione dei file in tempo reale*:

1. Aprire la finestra **Impostazioni protezione dei file in tempo reale** (vedere la sezione "Configurazione manuale delle impostazioni di sicurezza" a pagina [152](#)).
2. Selezionare la scheda **Azioni**.
3. Selezionare l'azione da eseguire sugli oggetti infetti e gli altri oggetti rilevati:

- **Solo notifica.**

Quando questa modalità è selezionata, Kaspersky Embedded Systems Security 2.2 non blocca l'accesso agli oggetti infetti e agli altri oggetti rilevati, né esegue un'azione su di essi. Il seguente evento viene registrato nel log delle attività: *Oggetto non disinfettato. Motivo: non è stata eseguita alcuna azione per la neutralizzazione dell'oggetto rilevato a causa delle impostazioni definite dall'utente.* L'evento specifica tutte le informazioni disponibili sull'oggetto rilevato.

La modalità **Solo notifica** deve essere configurata per ogni area di protezione separatamente. Questa modalità non viene utilizzata per impostazione predefinita in alcuno dei livelli di sicurezza. Se si seleziona questa modalità, Kaspersky Embedded Systems Security 2.2 cambia automaticamente il livello di sicurezza in **Personalizzato**.

- **Blocca l'accesso.**

Quando questa opzione è selezionata, Kaspersky Embedded Systems Security 2.2 blocca l'accesso all'oggetto rilevato o potenzialmente infetto. È possibile selezionare un'azione aggiuntiva sugli oggetti bloccati nell'elenco a discesa.

- **Esegui azione aggiuntiva.**

Selezionare l'azione dall'elenco a discesa:

- **Disinfetta.**
- **Disinfetta. Rimuovi se la disinfezione fallisce.**
- **Rimuovi.**
- **Raccomandato.**

4. Selezionare l'azione da eseguire sugli oggetti potenzialmente infetti:

- **Solo notifica.**

Quando questa modalità è selezionata, Kaspersky Embedded Systems Security 2.2 non blocca l'accesso agli oggetti infetti e agli altri oggetti rilevati, né esegue un'azione su di essi. Il seguente evento viene registrato nel log delle attività: *Oggetto non disinfettato. Motivo: non è stata eseguita alcuna azione per la neutralizzazione dell'oggetto rilevato a causa delle impostazioni definite dall'utente.* L'evento specifica tutte le informazioni disponibili sull'oggetto rilevato.

La modalità **Solo notifica** deve essere configurata per ogni area di protezione separatamente. Questa modalità non viene utilizzata per impostazione predefinita in alcuno dei livelli di sicurezza. Se si seleziona questa modalità, Kaspersky Embedded Systems Security 2.2 cambia automaticamente il livello di sicurezza in **Personalizzato**.

- **Blocca l'accesso.**

Quando questa opzione è selezionata, Kaspersky Embedded Systems Security 2.2 blocca l'accesso all'oggetto rilevato o potenzialmente infetto. È possibile selezionare un'azione

aggiuntiva sugli oggetti bloccati nell'elenco a discesa.

- **Esegui azione aggiuntiva.**

Selezionare l'azione dall'elenco a discesa:

- **Quarantena.**
- **Rimuovi.**
- **Raccomandato.**

5. Configurare le azioni da eseguire sugli oggetti a seconda del tipo di oggetto rilevato:

a. Selezionare o deselezionare la casella di controllo **Esegui le azioni a seconda del tipo di oggetto rilevato**.

Se la casella di controllo è selezionata, è possibile impostare l'azione principale e secondaria per ogni tipo di oggetto rilevato facendo clic sul pulsante **Impostazioni** accanto alla casella di controllo.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 esegue le azioni selezionate nelle sezioni **Azione da eseguire sugli oggetti infetti e di altro tipo** e **Azione da eseguire sugli oggetti potenzialmente infetti** per i rispettivi tipi di oggetti.

La casella di controllo è deselezionata per impostazione predefinita.

b. Fare clic sul pulsante **Impostazioni**.

c. Nella finestra visualizzata selezionare l'azione principale e secondaria (eseguita se l'azione principale ha esito negativo) per ogni tipo di oggetto rilevato.

d. Fare clic su **OK**.

6. Selezionare l'azione da eseguire sui file composti non modificabili: selezionare o deselezionare la casella di controllo **Rimuovi interamente i file composti che non possono essere modificati dall'applicazione in caso di oggetti incorporati**.

Questa casella di controllo consente abilitare o disabilitare la rimozione forzata del file composito padre quando viene rilevato un oggetto figlio incorporato dannoso, potenzialmente infetto o di altro tipo.

Se la casella di controllo è selezionata e l'attività è configurata per la rimozione degli oggetti infetti e potenzialmente infetti, Kaspersky Embedded Systems Security 2.2 rimuove in modo forzato l'intero oggetto composito padre quando viene rilevato un oggetto incorporato dannoso o di altro tipo. La rimozione forzata di un file padre insieme a tutto il relativo contenuto viene eseguita se l'applicazione non può rimuovere solo l'oggetto figlio rilevato (ad esempio, se l'oggetto padre non è modificabile).

Se questa casella di controllo è deselezionata e l'attività è configurata per la rimozione degli oggetti infetti e potenzialmente infetti, Kaspersky Embedded Systems Security 2.2 non esegue l'azione selezionata se l'oggetto padre non è modificabile.

Per impostazione predefinita, la casella di controllo è selezionata per il livello di sicurezza **Massima protezione** e deselezionata per i livelli di sicurezza **Raccomandato** e **Massima performance**.

7. Fare clic su **Salva**.

La nuova configurazione dell'attività verrà salvata.

Configurazione delle prestazioni

► Per configurare le prestazioni per l'attività *Protezione dei file in tempo reale*:

1. Aprire la finestra **Impostazioni protezione dei file in tempo reale** (vedere la sezione "Configurazione manuale delle impostazioni di sicurezza" a pagina [152](#)).

2. Selezionare la scheda **Prestazioni**.

3. Nella sezione **Esclusioni**:

- Deselezionare o selezionare la casella di controllo **Escludi file**.

Esclusione di file dalla scansione in base al nome del file o a una maschera per il nome del file.

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 ignora gli oggetti specificati durante la scansione.

Se questa casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 esamina tutti gli oggetti.

La casella di controllo è deselezionata per impostazione predefinita.

- Deselezionare o selezionare la casella di controllo **Non rilevare**.

Gli oggetti vengono esclusi dalla scansione in base al nome o alla maschera per il nome dell'oggetto rilevabile. L'elenco di nomi degli oggetti rilevabili è disponibile sul sito Web dell'Enciclopedia dei Virus <http://www.securelist.com>.

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 ignora gli oggetti rilevabili specificati durante la scansione.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 rileva tutti gli oggetti specificati nell'applicazione per impostazione predefinita.

La casella di controllo è deselezionata per impostazione predefinita.

- Fare clic sul pulsante **Modifica** per ogni impostazione per cui aggiungere esclusioni.

4. Nella sezione **Impostazioni avanzate**:

- **Interrompi la scansione se richiede più di (sec.)**

Limita la durata della scansione degli oggetti. Il valore predefinito è 60 secondi.

Se la casella di controllo è deselezionata, la durata della scansione è limitata al valore specificato.

Se la casella di controllo è deselezionata, la durata della scansione è illimitata.

La casella di controllo è selezionata per impostazione predefinita.

- **Non esaminare gli oggetti composti di dimensioni superiori a (MB)**

Esclude dalla scansione gli oggetti più grandi della dimensione specificata.

Se la casella di controllo è selezionata, durante la scansione anti-virus Kaspersky Embedded Systems Security 2.2 ignora gli oggetti composti le cui dimensioni superano il limite specificato.

Se questa casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 esamina gli oggetti composti di qualsiasi dimensione.

Per impostazione predefinita, la casella di controllo è selezionata per i livelli di sicurezza **Raccomandato** e **Massima performance**.

- **Usa la tecnologia iSwift**

iSwift confronta l'identificatore NTFS del file, archiviato in un database, con un identificatore corrente. La scansione viene eseguita solo per i file i cui identificatori sono stati modificati (nuovi file e file modificati dall'ultima scansione degli oggetti di sistema NTFS).

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 esamina i soli file nuovi o modificati dall'ultima scansione di oggetti di sistema NTFS.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 esamina i file di sistema NTFS senza tenere conto della data di creazione o di modifica del file.

La casella di controllo è selezionata per impostazione predefinita.

- **Usa la tecnologia iChecker**

iChecker calcola e memorizza i checksum dei file esaminati. Se un oggetto viene modificato, il checksum cambia. L'applicazione confronta tutti i checksum durante l'attività di scansione ed esamina solo i nuovi file e quelli modificati dall'ultima scansione.

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 esamina solo i file nuovi e modificati.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 esamina i file senza tenere conto della data di creazione o di modifica del file.

La casella di controllo è selezionata per impostazione predefinita.

5. Fare clic su **Salva**.

La nuova configurazione dell'attività verrà salvata.

Utilizzo di KSN

Questa sezione contiene informazioni sull'attività Utilizzo di KSN e su come configurarla.

In questa sezione

Informazioni sull'attività Utilizzo di KSN.....	159
Configurazione dell'attività Utilizzo di KSN	161
Configurazione dell'elaborazione dei dati	163
Configurazione del trasferimento di dati aggiuntivi.....	165

Informazioni sull'attività Utilizzo di KSN

Kaspersky Security Network (anche denominato "KSN") è un'infrastruttura di servizi online che consente di accedere alla Knowledge Base operativa di Kaspersky Lab, in cui sono disponibili informazioni sulla reputazione di file, risorse Web e programmi. Kaspersky Security Network consente a Kaspersky Embedded Systems Security 2.2 di reagire tempestivamente alle nuove minacce, migliora le prestazioni di diversi componenti di protezione e riduce la probabilità di falsi positivi.

Per avviare l'attività Utilizzo di KSN, è necessario accettare l'Informativa su Kaspersky Security Network.

Le informazioni che Kaspersky Embedded Systems Security 2.2 riceve da Kaspersky Security Network sono relative solo alla reputazione dei programmi.

La partecipazione a KSN consente a Kaspersky Lab di ricevere informazioni in tempo reale sui tipi e le origini delle nuove minacce, sviluppare modi per neutralizzarle e ridurre il numero di falsi positivi nei componenti dell'applicazione.

Informazioni più dettagliate su trasferimento, elaborazione, archiviazione ed eliminazione delle informazioni sull'utilizzo dell'applicazione sono disponibili nella finestra Gestione dei dati dell'attività Utilizzo di KSN e nell'Informativa sulla privacy disponibile nel sito Web di Kaspersky Lab.

La partecipazione al programma Kaspersky Security Network è facoltativa. La decisione relativa alla partecipazione a Kaspersky Security Network avviene dopo l'installazione di Kaspersky Embedded Systems Security 2.2. È possibile cambiare idea in merito alla partecipazione a Kaspersky Security Network in qualsiasi momento.

Kaspersky Security Network può essere utilizzato nelle seguenti attività di Kaspersky Embedded Systems Security 2.2:

- Protezione dei file in tempo reale.
- Scansione su richiesta.
- Controllo dell'avvio delle applicazioni.

Kaspersky Private Security Network

Visualizzare i dettagli su come configurare Kaspersky Private Security Network (di seguito denominato "KSN privato") nella *Guida di Kaspersky Security Center*.

Se si utilizza KSN privato nel computer protetto, nella finestra **Gestione dei dati** (vedere la sezione "Configurazione dell'elaborazione dei dati" a pagina [163](#)) dell'attività Utilizzo di KSN è possibile leggere l'Informativa KSN e abilitare l'attività selezionando la casella di controllo **Accetto i termini dell'Informativa su Kaspersky Private Security Network**. Accettando le condizioni, si accetta di inviare tutti i tipi di dati menzionati nell'Informativa KSN (richieste di protezione, dati statistici) ai servizi KSN.

Dopo l'accettazione delle condizioni di KSN privato, le caselle di controllo che regolano l'utilizzo di KSN globale non sono disponibili.

Se si disabilita KSN privato durante l'esecuzione dell'attività Utilizzo di KSN, si verifica l'errore *Violazione della licenza* e l'attività viene interrotta. Per mantenere la protezione del computer, è necessario accettare l'Informativa KSN nella scheda **Gestione dei dati** e riavviare l'attività.

Revoca dell'accettazione dell'Informativa KSN

È possibile revocare l'accettazione e interrompere qualsiasi scambio di dati con Kaspersky Security Network in qualsiasi momento. Le seguenti azioni consentono di revocare parzialmente o completamente l'accettazione dell'Informativa KSN:

- Deselezione della casella di controllo **Invia i dati sui file esaminati**: l'applicazione interrompe l'invio dei

checksum del file esaminati al servizio KSN per l'analisi.

- Deselezione della casella di controllo **Invia le statistiche di Kaspersky Security Network**: l'applicazione interrompe l'elaborazione dei dati con le statistiche aggiuntive di KSN.
- Deselezione della casella di controllo **Accetto i termini dell'Informativa su Kaspersky Security Network**: l'applicazione interrompe completamente l'elaborazione dei dati relativi a KSN e l'attività Utilizzo di KSN viene arrestata.
- Disinstallazione del componente Utilizzo di KSN: tutta l'elaborazione dei dati relativi a KSN viene interrotta.
- Disinstallazione di Kaspersky Embedded Systems Security 2.2: tutta l'elaborazione dei dati relativi a KSN viene interrotta.

Configurazione dell'attività Utilizzo di KSN

È possibile modificare le impostazioni predefinite dell'attività Utilizzo di KSN (vedere la seguente tabella).

Tabella 32. Impostazioni predefinite dell'attività Utilizzo di KSN

Impostazione	Valore predefinito	Descrizione
Azione da eseguire sugli oggetti non attendibili di KSN	Rimuovi	È possibile specificare le azioni che Kaspersky Embedded Systems Security 2.2 deve eseguire sugli oggetti identificati da KSN come non attendibili.
Trasferimento dei dati	Il checksum del file (hash MD5) viene calcolato per i file di dimensioni non superiori a 2 MB.	È possibile specificare la dimensione massima dei file per cui viene calcolato un checksum utilizzando l'algoritmo MD5 per l'invio a KSN. Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 calcola l'hash MD5 per i file di qualsiasi dimensione.
Informativa KSN	La casella di controllo Accetto i termini dell'Informativa su Kaspersky Security Network è deselezionata.	Se si desidera partecipare a KSN dopo l'installazione. È possibile modificare la decisione in qualsiasi momento.
Invia le statistiche di Kaspersky Security Network	Selezionata (applicata solo se l'Informativa KSN è stata accettata)	Se viene accettata l'Informativa KSN, le statistiche KSN verranno inviate automaticamente, a meno che non si deselezioni la casella di controllo.
Invia i dati sui file esaminati	Selezionata (applicata solo se l'Informativa KSN è stata accettata)	Se l'Informativa KSN è stata accettata, i dati sui file esaminati e analizzati dall'avvio dell'attività vengono inviati. È possibile deselezionare la casella di controllo in qualsiasi momento.
Accetto i termini dell'Informativa su Kaspersky Managed Protection	Deselezionata	È possibile abilitare o disabilitare il servizio KMP. Il servizio è disponibile solo se è stato sottoscritto il contratto aggiuntivo durante il processo di acquisto dell'applicazione.
Pianificazione dell'avvio dell'attività	La prima esecuzione non è pianificata.	È possibile avviare l'attività manualmente o configurare un avvio pianificato.

Impostazione	Valore predefinito	Descrizione
Usa Kaspersky Security Center come proxy KSN	Selezionato	Per impostazione predefinita i dati vengono inviati a KSN tramite Kaspersky Security Center.

► Per configurare l'attività *Utilizzo di KSN*, eseguire le seguenti operazioni:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Protezione del computer in tempo reale** fare clic sul pulsante **Impostazioni** nel gruppo **Utilizzo di KSN**.

Verrà visualizzata la finestra **Utilizzo di KSN**.

4. Nella scheda **Generale** configurare le seguenti impostazioni dell'attività:
 - Nella sezione **Azione da eseguire sugli oggetti non attendibili di KSN** specificare l'azione che Kaspersky Embedded Systems Security 2.2 deve eseguire se rileva un oggetto identificato da KSN come non attendibile:
 - **Rimuovi**
Kaspersky Embedded Systems Security 2.2 elimina l'oggetto con lo stato non attendibile di KSN e ne crea una copia in Backup.
Questa opzione è selezionata per impostazione predefinita.
 - **Informazioni log**
Kaspersky Embedded Systems Security 2.2 registra le informazioni sull'oggetto con lo stato non attendibile di KSN nel log delle attività. Kaspersky Embedded Systems Security 2.2 non elimina l'oggetto non attendibile.
 - Nella sezione **Trasferimento dei dati** limitare la dimensione dei file per cui viene calcolato il checksum:
 - Deselezionare o selezionare la casella di controllo **Non calcolare il checksum prima dell'invio a KSN se la dimensione del file è superiore a (MB)**.
Questa casella di controllo consente di abilitare o disabilitare il calcolo del checksum per i file della dimensione specificata per l'invio di queste informazioni al servizio KSN.
La durata del calcolo del checksum dipende dalle dimensioni del file.
Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2

non calcola il checksum per i file che superano la dimensione specificata (in MB).

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 calcola il checksum per i file di qualsiasi dimensione.

La casella di controllo è selezionata per impostazione predefinita.

- Se necessario, nel campo a destra modificare la dimensione massima dei file per cui Kaspersky Embedded Systems Security 2.2 calcola il checksum.
- Selezionare o deselezionare la casella di controllo **Usa Kaspersky Security Center come proxy KSN**.

La casella di controllo consente di gestire il trasferimento dei dati tra i computer protetti e KSN.

Se la casella di controllo è deselezionata, i dati dall'Administration Server e i computer protetti vengono inviati direttamente a KSN (non tramite Kaspersky Security Center). Il criterio attivo definisce il tipo di dati che può essere inviato direttamente a KSN.

Se la casella di controllo è selezionata, tutti i dati vengono inviati a KSN tramite Kaspersky Security Center.

La casella di controllo è selezionata per impostazione predefinita.

Per abilitare il proxy KSN è necessario accettare l'informativa KSN e configurare correttamente Kaspersky Security Center. Per informazioni dettagliate, vedere la [Guida di Kaspersky Security Center](#).

5. Se necessario, configurare la pianificazione dell'avvio dell'attività nella scheda **Gestione attività**. È ad esempio possibile avviare l'attività in base alla pianificazione e specificare la frequenza **All'avvio dell'applicazione** se si desidera eseguire automaticamente l'attività al riavvio del computer.

L'applicazione avvierà automaticamente l'attività Utilizzo di KSN in base alla pianificazione.

6. Configurare la gestione dei dati (vedere la sezione "Configurazione dell'elaborazione dei dati" a pagina [163](#)) prima dell'avvio dell'attività.
7. Fare clic su **OK**.

Le impostazioni modificate verranno applicate. La data e l'ora di modifica delle impostazioni, nonché le informazioni sulle impostazioni dell'attività prima e dopo la modifica, vengono salvate nel log delle attività.

Configurazione dell'elaborazione dei dati

► Per configurare i dati che verranno elaborati dai servizi KSN e accettare l'Informativa KSN:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra

Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Protezione del computer in tempo reale** fare clic sul pulsante **Gestione dei dati** nel gruppo **Utilizzo di KSN**.

Verrà visualizzata la finestra **Gestione dei dati**.

4. Nella scheda **Statistiche e servizi** leggere l'informativa e selezionare la casella di controllo **Accetto i termini dell'Informativa su Kaspersky Security Network**.
5. Per aumentare il livello di protezione, le seguenti caselle di controllo sono selezionate automaticamente:

- **Invia i dati sui file esaminati.**

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 invia il checksum dei file esaminati a Kaspersky Lab. La conclusione sulla sicurezza di ogni file si basa sulla reputazione ricevuta da KSN.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 non invia il checksum dei file a KSN.

Si noti che le richieste di reputazione di file potrebbero essere inviate in una modalità limitata. Le limitazioni vengono utilizzate per la protezione dei server di reputazione di Kaspersky Lab dagli attacchi DDoS. In questo scenario, i parametri delle richieste di reputazione dei file inviate sono definiti dalle regole e dai metodi stabiliti dagli specialisti di Kaspersky Lab e non possono essere configurati dall'utente in un computer protetto. Gli aggiornamenti di tali regole e metodi vengono ricevuti insieme agli aggiornamenti dei database dell'applicazione. Se sono applicate limitazioni, viene visualizzato lo stato *Abilitato da Kaspersky Lab per la protezione dei server KSN dagli attacchi DDoS* nelle statistiche dell'attività Utilizzo di KSN.

La casella di controllo è selezionata per impostazione predefinita.

- **Inviare le statistiche di Kaspersky Security Network.**

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 invia statistiche aggiuntive, che possono contenere dati personali. L'elenco di tutti i dati inviati come statistiche KSN è specificato nell'Informativa KSN. I dati ricevuti da Kaspersky Lab vengono utilizzati per migliorare la qualità delle applicazioni e i tassi di rilevamento delle minacce.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 non invia ulteriori statistiche. La casella di controllo è selezionata per impostazione predefinita.

È possibile deselezionare queste caselle di controllo e interrompere l'invio di dati aggiuntivi in qualsiasi momento.

6. Nella scheda **Kaspersky Managed Protection** leggere l'informativa e selezionare la casella di controllo **Accetto i termini dell'Informativa su Kaspersky Managed Protection**.

Se la casella di controllo è selezionata, l'utente accetta di inviare le statistiche sull'attività del computer protetto agli specialisti di Kaspersky Lab. I dati ricevuti vengono utilizzati per attività di analisi e generazione di rapporti, necessarie per prevenire incidenti associati a violazioni della sicurezza.

La casella di controllo è deselezionata per impostazione predefinita.

Le modifiche dello stato della casella di controllo **Accetto i termini dell'Informativa su Kaspersky Managed Protection** non determinano immediatamente l'avvio o l'interruzione dell'elaborazione dei dati. Per applicare le modifiche, è necessario riavviare Kaspersky Embedded Systems Security 2.2.

Per utilizzare il servizio KMP, è necessario sottoscrivere il contratto corrispondente ed eseguire i file di configurazione in un computer protetto.

Per utilizzare il servizio KMP, è necessario accettare le condizioni di elaborazione dei dati dell'Informativa KSN nella scheda **Statistiche e servizi**.

7. Fare clic su **OK**.

La configurazione dell'elaborazione dei dati verrà salvata.

Configurazione del trasferimento di dati aggiuntivi

Kaspersky Embedded Systems Security 2.2 può essere configurato per l'invio dei seguenti dati a Kaspersky Lab:

- Checksum dei file esaminati (casella di controllo **Invia i dati sui file esaminati**).
- Statistiche aggiuntive, inclusi dati personali (casella di controllo **Invia le statistiche di Kaspersky Security Network**).

Vedere la sezione "Gestione dei dati locali" di questa guida per informazioni dettagliate sui dati inviati a Kaspersky Lab.

Le caselle di controllo corrispondenti possono essere selezionate o deselezionate solo se la casella di controllo **Accetto i termini dell'Informativa su Kaspersky Security Network** è selezionata.

Per impostazione predefinita, Kaspersky Embedded Systems Security 2.2 invia i checksum dei file e le statistiche aggiuntive una volta accettata l'Informativa KSN.

Tabella 33. Possibili stati della casella di controllo e relative condizioni

Stato della casella di controllo	Condizioni per lo stato della casella di controllo Invia i dati sui file esaminati	Condizioni per lo stato della casella di controllo Invia le statistiche di Kaspersky Security Network
<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> • le richieste di reputazione vengono inviate • la casella di controllo è modificabile 	<ul style="list-style-type: none"> • le statistiche aggiuntive vengono inviate • la casella di controllo è modificabile
<input type="checkbox"/>	<ul style="list-style-type: none"> • le richieste di reputazione non vengono inviate • la casella di controllo non è modificabile 	<ul style="list-style-type: none"> • le statistiche aggiuntive non vengono inviate • la casella di controllo non è modificabile

Stato della casella di controllo	Condizioni per lo stato della casella di controllo Invia i dati sui file esaminati	Condizioni per lo stato della casella di controllo Invia le statistiche di Kaspersky Security Network
<input type="checkbox"/>	<ul style="list-style-type: none"> • le richieste di reputazione non vengono inviate • la casella di controllo è modificabile 	<ul style="list-style-type: none"> • le statistiche aggiuntive non vengono inviate • la casella di controllo è modificabile
<input type="checkbox"/>	<ul style="list-style-type: none"> • le richieste di reputazione non vengono inviate • la casella di controllo non è modificabile 	<ul style="list-style-type: none"> • le statistiche aggiuntive non vengono inviate • la casella di controllo non è modificabile

Prevenzione exploit

Questa sezione contiene istruzioni su come configurare le impostazioni di protezione della memoria processo.

In questo capitolo

Informazioni su Prevenzione exploit	166
Configurazione delle impostazioni di protezione della memoria processo	167
Aggiunta di un processo per la protezione	169
Tecniche di prevenzione exploit	170

Informazioni su Prevenzione exploit

Kaspersky Embedded Systems Security 2.2 consente di proteggere la memoria processo dagli exploit. Questa funzionalità è implementata nel componente Prevenzione exploit. È possibile modificare lo stato dell'attività del componente e configurare le impostazioni di protezione della memoria processo.

Il componente protegge la memoria processo dagli exploit inserendo un agente di protezione dei processi esterno ("agente") nel processo protetto.

Un agente di protezione dei processi è un modulo di Kaspersky Embedded Systems Security 2.2 caricato in modo dinamico inserito nei processi protetti per monitorarne l'integrità e ridurre il rischio di exploit.

L'esecuzione dell'agente nel processo protetto richiede di avviare e arrestare il processo: il caricamento iniziale dell'agente in un processo aggiunto all'elenco dei processi protetti è possibile solo se il processo viene riavviato. Inoltre, dopo la rimozione di un processo dall'elenco dei processi protetti, l'agente può essere scaricato solo dopo il riavvio del processo.

È necessario arrestare l'agente per poterlo scaricare dai processi protetti: se il componente Prevenzione exploit è disinstallato, l'applicazione blocca l'ambiente e forza lo scaricamento dell'agente dai processi protetti. Se durante la disinstallazione del componente, l'agente è inserito in uno dei processi protetti, è necessario terminare il processo in questione. Potrebbe essere richiesto il riavvio del computer (ad esempio, se il processo di sistema è protetto).

Se viene rilevato un indicatore di attacco exploit in un processo protetto, Kaspersky Embedded Systems Security

2.2 esegue una delle azioni seguenti:

- Termina il processo se viene effettuato un tentativo di exploit.
- Segnala la compromissione del processo.

È possibile arrestare la protezione del processo utilizzando uno dei seguenti metodi:

- Disinstallazione del componente.
- Rimozione del processo dall'elenco dei processi protetti e riavvio del processo.

Servizio Prevenzione exploit di Kaspersky Security

Per garantire la massima efficienza del componente Prevenzione exploit, è richiesto il servizio Prevenzione exploit di Kaspersky Security nel computer protetto. Questo servizio e il componente Prevenzione exploit fanno parte dell'installazione consigliata. Durante l'installazione del servizio nel computer protetto, viene creato e avviato il processo kavfsw. Il processo comunica le informazioni sui processi protetti dal componente all'agente di sicurezza.

Dopo l'arresto del servizio Prevenzione exploit di Kaspersky Security, Kaspersky Embedded Systems Security 2.2 continua a proteggere i processi aggiunti all'elenco dei processi protetti, viene caricato nei nuovi processi aggiunti e applica tutte le tecniche di riduzione dell'impatto disponibili per proteggere la memoria processo.

Se il servizio Prevenzione exploit di Kaspersky Security viene arrestato, l'applicazione non riceverà informazioni sugli eventi che si verificano in relazione ai processi protetti (comprese le informazioni sugli attacchi exploit e sull'arresto dei processi). Inoltre, l'agente non sarà in grado di ricevere informazioni sulle nuove impostazioni di protezione e sull'aggiunta di nuovi processi all'elenco dei processi protetti.

Modalità Prevenzione exploit

È possibile selezionare una delle seguenti modalità per configurare le azioni mirate a ridurre il rischio di exploit delle vulnerabilità nei processi protetti:

- **Termina in caso di exploit:** applicare questa modalità per terminare un processo quando viene effettuato un tentativo di exploit.

Al rilevamento di un tentativo di exploit di una vulnerabilità in un processo del sistema operativo critico protetto, Kaspersky Embedded Systems Security 2.2 non termina il processo, indipendentemente dalla modalità indicata nelle impostazioni del componente Prevenzione exploit.

- **Notifica solo il processo compromesso:** applicare questa modalità per ricevere informazioni sui casi di exploit nei processi protetti utilizzando gli eventi nell'audit di sicurezza filtrato.

Se questa modalità è selezionata, Kaspersky Embedded Systems Security 2.2 registra tutti i tentativi di exploit delle vulnerabilità attraverso la creazione di eventi.

Configurazione delle impostazioni di protezione della memoria processo

► Per configurare le impostazioni di protezione della memoria dei processi aggiunti all'elenco dei processi protetti, eseguire le azioni seguenti:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.

2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Protezione del computer in tempo reale** fare clic sul pulsante **Impostazioni** nel gruppo **Prevenzione exploit**.

Verrà visualizzata la finestra **Prevenzione exploit**.

4. Nella sezione **Modalità di prevenzione exploit** configurare le seguenti impostazioni:

- **Impedisci gli exploit dei processi vulnerabili.**

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 riduce il rischio di exploit delle vulnerabilità nei processi nell'elenco dei processi protetti.

Se questa casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 non protegge i processi del computer dagli exploit.

La casella di controllo è deselezionata per impostazione predefinita.

- **Termina in caso di exploit.**

Se questa modalità è selezionata, Kaspersky Embedded Systems Security 2.2 termina un processo protetto al rilevamento di un tentativo di exploit se al processo è stata applicata una tecnica di riduzione dell'impatto.

- **Notifica solo il processo compromesso.**

Se questa modalità è selezionata, Kaspersky Embedded Systems Security 2.2 segnala gli exploit tramite una finestra terminale. Il processo compromesso rimane in esecuzione.

Se Kaspersky Embedded Systems Security 2.2 rileva un exploit in un processo critico mentre l'applicazione è in esecuzione in modalità **Termina in caso di exploit**, il componente passa obbligatoriamente alla modalità **Notifica solo il processo compromesso**.

5. Nella sezione **Azioni di prevenzione** configurare le seguenti impostazioni:

- **Notifica i processi compromessi tramite servizio terminal.**

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 visualizza una finestra terminale con una descrizione del motivo dell'attivazione della protezione e un indicatore del processo in cui è stato rilevato un tentativo di exploit.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 visualizza una finestra terminale quando viene rilevato un tentativo di exploit o l'arresto di un processo compromesso. Viene visualizzata una finestra terminale indipendentemente dallo stato del servizio Prevenzione exploit di Kaspersky Security. La casella di controllo è selezionata per impostazione predefinita.

- **Impedisci gli exploit dei processi vulnerabili anche se il servizio di Kaspersky Security è disabilitato.**

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 ridurrà il rischio di exploit delle vulnerabilità nei processi già avviati, indipendentemente dal fatto che il servizio di Kaspersky Security sia o meno in esecuzione. Kaspersky Embedded Systems Security 2.2 non proteggerà i processi aggiunti dopo l'arresto del servizio di Kaspersky Security. Dopo l'avvio del servizio, la riduzione dell'impatto degli exploit verrà arrestata per tutti i processi.

Se questa casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 non protegge i processi dagli exploit quando il servizio di Kaspersky Security viene arrestato.

La casella di controllo è selezionata per impostazione predefinita.

6. Fare clic su **OK**.

Le impostazioni di protezione della memoria processo configurate verranno salvate e applicate da Kaspersky Embedded Systems Security 2.2.

Aggiunta di un processo per la protezione

Per impostazione predefinita, il componente Prevenzione exploit protegge numerosi processi. È possibile escludere i processi dall'ambito della protezione deselezionando le caselle di controllo corrispondenti nell'elenco.

► *Per aggiungere un processo all'elenco dei processi protetti:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Protezione del computer in tempo reale** fare clic sul pulsante **Impostazioni** nel gruppo **Prevenzione exploit**.
Verrà visualizzata la finestra **Prevenzione exploit**.
4. Nella scheda **Processi protetti** fare clic sul pulsante **Sfoggia**.
Verrà visualizzata la finestra Esplora risorse di Microsoft Windows.
5. Selezionare il processo che si desidera aggiungere all'elenco.
6. Fare clic sul pulsante **Apri**.

Il nome del processo viene visualizzato nella riga.

7. Fare clic sul pulsante **Aggiungi**.

Il processo verrà aggiunto all'elenco dei processi protetti.

8. Selezionare il processo aggiunto e fare clic su **Imposta tecniche di prevenzione exploit**.

Verrà visualizzata la finestra **Tecniche di prevenzione exploit**.

9. Selezionare una delle opzioni per l'applicazione delle tecniche di riduzione dell'impatto:

- **Applica tutte le tecniche di prevenzione exploit disponibili.**

Se questa opzione è selezionata, l'elenco non può essere modificato. Per impostazione predefinita, vengono applicate tutte le tecniche disponibili per un processo.

- **Applica le tecniche di prevenzione exploit elencate per il processo.**

Se questa opzione è selezionata, è possibile modificare l'elenco delle tecniche di riduzione dell'impatto applicate:

- a. Selezionare le caselle di controllo relative alle tecniche che si desidera applicare per proteggere il processo selezionato.
- b. Selezionare o deselezionare la casella di controllo **Applica tecnica di riduzione della superficie di attacco**.

10. Configurare le impostazioni per la tecnica di riduzione della superficie di attacco:

- Immettere i nomi dei moduli per cui l'avvio verrà bloccato dal processo protetto nel campo **Nega i moduli**.
- Nel campo **Non negare i moduli se avviati nell'area Internet** selezionare le caselle di controllo relative alle opzioni con cui consentire l'avvio dei moduli:
 - Internet
 - Intranet locale
 - Siti Web attendibili
 - Siti con limitazioni
 - Computer

Queste impostazioni sono applicabili solo a Internet Explorer®.

11. Fare clic su **OK**.

Il processo viene aggiunto all'ambito della protezione dell'attività.

Tecniche di prevenzione exploit

Tabella 34. Tecniche di prevenzione exploit

Tecnica di prevenzione exploit	Descrizione
DEP (Data Execution Prevention)	Data Execution Prevention blocca l'esecuzione di codice arbitrario nelle aree protette della memoria.

Tecnica di prevenzione exploit	Descrizione
ASLR (Address Space Layout Randomization)	Modifiche del layout delle strutture dati nello spazio di indirizzi del processo.
SEHOP (Structured Exception Handler Overwrite Protection)	Sostituzione dei record delle eccezioni o sostituzione del gestore eccezione.
Null Page Allocation	Prevenzione del reindirizzamento del puntatore NULL.
LoadLibrary Network Call Check (Anti ROP)	Protezione dal caricamento dei moduli DLL dai percorsi di rete.
Executable Stack (Anti ROP)	Blocco dell'esecuzione non autorizzata di aree dello stack.
Anti RET Check (Anti ROP)	Verifica che l'istruzione CALL sia chiamata in modo sicuro.
Anti Stack Pivoting (Anti ROP)	Protezione dal riposizionamento del puntatore dello stack ESP in un indirizzo eseguibile.
Simple Export Address Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register)	Protezione dell'accesso in lettura alla tabella degli indirizzi di esportazione per kernel32.dll, kernelbase.dll e ntdll.dll
Heap Spray Allocation (Heapspray)	Protezione dall'allocazione della memoria per l'esecuzione di codice dannoso.
Execution Flow Simulation (Anti Return Oriented Programming)	Rilevamento di catene di istruzioni sospette (potenziale gadget ROP) nel componente API Windows.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Protezione dall'escalation dei privilegi tramite una vulnerabilità nel driver AFD (esecuzione di codice arbitrario nel circuito 0 tramite una chiamata QueryIntervalProfile).
ASR (Attack Surface Reduction)	Blocco dell'avvio dei componenti aggiuntivi vulnerabili tramite il processo protetto.
Anti Process Hollowing (Hollowing)	Protezione contro la creazione e l'esecuzione di copie dannose di processi attendibili.
Anti AtomBombing (APC)	Exploit della tabella Atom globale tramite chiamate APC (Asynchronous Procedure Call).
Anti CreateRemoteThread (RThreadLocal)	Un altro processo ha creato un thread in un processo protetto.
Anti CreateRemoteThread (RThreadRemote)	Un processo protetto ha creato un thread in un altro processo.

Controllo attività locali

Questa sezione fornisce informazioni sulla funzionalità di Kaspersky Embedded Systems Security 2.2 che controlla gli avvii delle applicazioni, le connessioni dei dispositivi esterni tramite USB e Windows Firewall.

In questo capitolo

Gestione dell'avvio delle applicazioni da Kaspersky Security Center	172
Gestione delle connessioni dei dispositivi tramite Kaspersky Security Center	190

Gestione dell'avvio delle applicazioni da Kaspersky Security Center

È possibile consentire o impedire l'avvio delle applicazioni in tutti i computer della rete aziendale creando elenchi comuni di regole di Controllo dell'avvio delle applicazioni in Kaspersky Security Center per gruppi di computer.

In questa sezione

Utilizzo di un profilo per configurare le attività Controllo dell'avvio delle applicazioni in un criterio di Kaspersky Security Center	172
Configurazione delle impostazioni dell'attività Controllo dell'avvio delle applicazioni	173
Informazioni su Controllo distribuzione software	178
Configurazione di Controllo distribuzione software	180
Abilitazione della modalità Default allow	183
Informazioni sulla generazione delle regole di Controllo dell'avvio delle applicazioni per tutti i computer in Kaspersky Security Center	184

Utilizzo di un profilo per configurare le attività Controllo dell'avvio delle applicazioni in un criterio di Kaspersky Security Center

Le regole di Controllo dell'avvio delle applicazioni configurate nel criterio vengono applicate a tutti i computer nel gruppo di amministrazione. Se un gruppo di amministrazione include computer di vari tipi, possono essere necessari elenchi personalizzati di regole per Controllo dell'avvio delle applicazioni in ogni computer. È possibile utilizzare *profili criterio* per applicare differenti criteri ai computer in un singolo gruppo di amministrazione.

È consigliabile applicare i profili criterio per impostare le regole di Controllo dell'avvio delle applicazioni per diversi tipi di computer in un singolo gruppo di amministrazione gestito tramite un criterio unificato. Questo consente di ottimizzare la protezione di un computer, nella misura in cui le regole specificate coprono solo gli avvii delle applicazioni tipiche per questo specifico tipo di computer.

I profili criterio sono applicati ai computer del gruppo di amministrazione in base ai *tag* assegnati loro. È possibile configurare un profilo criterio per tutti i computer del gruppo che hanno un singolo tag.

Informazioni dettagliate sui tag e i profili criterio e istruzioni per il relativo utilizzo sono disponibili nella *Guida di Kaspersky Security Center*.

► *Per applicare un profilo criterio nell'attività Controllo dell'avvio delle applicazioni:*

1. Nell'albero di Kaspersky Security Center Administration Console espandere il nodo **Dispositivi gestiti**. Espandere il gruppo di amministrazione per cui si desidera configurare l'applicazione dei profili criterio.
2. Assegnare tag a ogni computer nel gruppo di amministrazione in base al tipo di computer. A tale scopo, eseguire le seguenti operazioni:
 - Nel riquadro dei dettagli del gruppo di amministrazione selezionato aprire la scheda **Dispositivi** e selezionare il computer a cui si desidera assegnare tag. Nella finestra **Proprietà: <nome computer>** del computer selezionato selezionare la sezione **Tag** e creare un elenco di tag. Fare clic su **OK**.
3. Creare un profilo criterio e configurare la relativa applicazione per la protezione dei computer nel gruppo di amministrazione. A tale scopo, eseguire le seguenti operazioni:
 - Nel riquadro dei dettagli del gruppo di amministrazione selezionato aprire la scheda **Criteri** e selezionare il criterio per cui si desidera configurare l'applicazione dei profili. Nella finestra **Proprietà: <nome criterio>** del criterio selezionato aprire la sezione **Profili criterio** e fare clic sul pulsante **Aggiungi** per creare un nuovo profilo. Verrà visualizzata la finestra **Proprietà: <nome profilo>**. Eseguire le seguenti operazioni:
 - a. Nella sezione **Regole di attivazione** configurare l'ambito di applicazione del profilo e specificare le condizioni di attivazione del profilo.
 - b. Nella sezione **Controllo dell'avvio delle applicazioni** configurare gli elenchi di regole di Controllo dell'avvio delle applicazioni per il profilo che si sta modificando.
 - c. Fare clic su **OK**.
4. Nella finestra **Proprietà: <nome criterio>** fare clic su **OK**.

Il profilo configurato sarà applicato nel criterio correlato all'attività Controllo dell'avvio delle applicazioni.

Configurazione delle impostazioni dell'attività Controllo dell'avvio delle applicazioni

È possibile modificare le impostazioni predefinite dell'attività Controllo dell'avvio delle applicazioni (vedere la seguente tabella).

Tabella 35. Impostazioni predefinite dell'attività Controllo dell'avvio delle applicazioni

Impostazione	Valore predefinito	Descrizione
Modalità attività	Solo statistiche. L'attività registra gli eventi di avvio e di blocco delle applicazioni in base alle regole impostate. L'avvio delle applicazioni non viene impedito effettivamente.	È possibile selezionare Attivo per la protezione del computer dopo la generazione dell'elenco finale delle regole.
Gestione delle regole	Sostituisci regole locali con le regole criterio	È possibile selezionare una modalità per l'applicazione delle regole specificate in un criterio contestualmente alle regole nel computer locale.
Ambito di applicazione delle regole	L'attività controlla l'avvio di file eseguibili, script e pacchetti MSI.	È possibile specificare i tipi di file per cui viene controllato l'avvio in base alle regole.

Impostazione	Valore predefinito	Descrizione
Utilizzo di KSN	I dati sulla reputazione delle applicazioni in KSN non vengono utilizzati.	È possibile utilizzare i dati sulla reputazione delle applicazioni di KSN durante l'esecuzione dell'attività Controllo dell'avvio delle applicazioni.
Consenti automaticamente la distribuzione software per le applicazioni e i pacchetti elencati	Non applicato.	È possibile consentire la distribuzione software tramite i programmi di installazione e le applicazioni specificati nelle impostazioni. Per impostazione predefinita, la distribuzione software è consentita solo tramite il servizio Windows Installer.
Consenti sempre la distribuzione software tramite Windows Installer	Applicato.	È possibile consentire qualsiasi installazione o aggiornamento di software, se le operazioni vengono eseguite tramite Windows Installer.
Nega l'avvio di interpreti della riga di comando senza comandi da eseguire	Non applicato.	È possibile impedire l'avvio degli interpreti dei comandi senza alcun comando per l'esecuzione.
Avvio attività	La prima esecuzione non è pianificata.	L'attività Controllo dell'avvio delle applicazioni non viene eseguita automaticamente all'avvio di Kaspersky Embedded Systems Security 2.2. È possibile avviare l'attività manualmente o configurare un avvio pianificato.

► Per configurare le impostazioni generali dell'attività Controllo dell'avvio delle applicazioni, eseguire le seguenti operazioni:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Controllo attività locali** fare clic sul pulsante **Impostazioni** nella sezione **Controllo dell'avvio delle applicazioni**.

Verrà visualizzata la finestra **Controllo dell'avvio delle applicazioni**.

4. Nella scheda **Generale** selezionare le seguenti impostazioni nella sezione **Modalità**:

Nell'elenco a discesa **Modalità attività** specificare la modalità di esecuzione dell'attività.

In questo elenco a discesa è possibile selezionare una modalità per l'attività Controllo dell'avvio delle applicazioni:

- **Attivo.** Kaspersky Embedded Systems Security 2.2 utilizza le regole specificate per monitorare qualsiasi applicazione eseguita.
- **Solo statistiche.** Kaspersky Embedded Systems Security 2.2 non utilizza le regole specificate per monitorare gli avvii delle applicazioni, ma registra soltanto le informazioni sugli avvii nel log delle attività. L'avvio di tutti i programmi è consentito. È possibile utilizzare questa modalità per generare un elenco di regole di Controllo dell'avvio delle applicazioni sulla base delle informazioni registrate nel log delle attività.

Per impostazione predefinita, l'attività Controllo dell'avvio delle applicazioni viene eseguita nella modalità **Solo statistiche**.

- Selezionare o deselezionare la casella di controllo **Ripeti l'azione eseguita per il primo avvio del file in tutti i successivi avvii del file**.

La casella di controllo consente di abilitare o disabilitare il controllo dell'avvio per il secondo tentativo di avviare le applicazioni e quelli successivi, in base alle informazioni memorizzate nella cache.

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 consente o meno di riavviare un'applicazione in base alla conclusione determinata al primo avvio dell'applicazione. Ad esempio, se il primo avvio dell'applicazione è stato consentito dalle regole, le informazioni su questa azione saranno memorizzate nella cache e anche il secondo tentativo e quelli successivi saranno consentiti, senza eseguire controlli aggiuntivi.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 analizza un'applicazione a ogni tentativo di avvio.

La casella di controllo è selezionata per impostazione predefinita.

- Deselezionare o selezionare la casella di controllo **Nega l'avvio di interpreti della riga di comando senza comandi da eseguire**.

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 impedisce l'avvio dell'interprete della riga di comando anche se l'avvio dell'interprete è consentito. La riga di comando senza alcun comando può essere avviata solo se sono soddisfatte entrambe le seguenti condizioni:

- È consentito l'avvio dell'interprete della riga di comando.
- Il comando eseguito è consentito.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 considera solo le regole di permesso per l'avvio della riga di comando. L'avvio viene impedito se non è applicata alcuna regola di permesso o se il processo eseguibile non ha lo stato attendibile in KSN. Se è applicata una regola di permesso o se il processo ha lo stato attendibile in KSN, la riga di comando può essere avviata con o senza un comando per l'esecuzione.

Kaspersky Embedded Systems Security 2.2 riconosce i seguenti interpreti della riga di comando:

- cmd.exe
- powershell.exe
- python.exe
- perl.exe

5. Nella sezione **Regole** configurare le impostazioni per l'applicazione delle regole:

- a. Fare clic sul pulsante **Elenco di regole** per aggiungere regole di permesso per il controllo dell'avvio dell'attività.

Kaspersky Embedded Systems Security 2.2 non riconosce i percorsi contenenti barre "/". Utilizzare la barra rovesciata "\" per immettere correttamente il percorso.

- b. Selezionare la modalità per l'applicazione delle regole:

- **Sostituisci regole locali con le regole criterio.**

L'applicazione applica l'elenco di regole specificato nel criterio per il controllo dell'avvio delle applicazioni centralizzato a un gruppo di computer. Gli elenchi di regole locali non possono essere create, modificate o applicate.

- **Aggiungi regole criterio alle regole locali.**

L'applicazione applica l'elenco di regole specificato in un criterio contestualmente agli elenchi di regole locali. È possibile modificare gli elenchi di regole locali utilizzando l'attività Generazione regole per Controllo dell'avvio delle applicazioni.

Per impostazione predefinita, Kaspersky Embedded Systems Security 2.2 applica due regole preimpostate che consentono un elenco di script, pacchetti MSI e file di avvio basati su un certificato.

6. Nella sezione **Ambito di applicazione delle regole** specificare le seguenti impostazioni:

- **Applica le regole ai file eseguibili.**

La casella di controllo consente di abilitare o disabilitare il controllo dell'avvio dei file eseguibili dei programmi.

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 consente o blocca l'avvio dei file eseguibili dei programmi utilizzando le regole specificate le cui impostazioni specificano i file eseguibili come ambito.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 non controlla l'avvio dei file eseguibili dei programmi utilizzando le regole specificate. L'avvio dei file eseguibili dei programmi è consentito.

La casella di controllo è selezionata per impostazione predefinita.

- **Monitora il caricamento dei moduli DLL.**

La casella di controllo consente di abilitare o disabilitare il monitoraggio del caricamento dei moduli DLL

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 consente o blocca i download dei moduli DLL utilizzando le regole specificate le cui

impostazioni specificano i file eseguibili come ambito.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 non controlla i download dei moduli DLL utilizzando le regole specificate. Il download dei moduli DLL è consentito.

La casella di controllo è attiva se la casella di controllo Applica le regole ai file eseguibili è selezionata.

La casella di controllo è deselezionata per impostazione predefinita.

Il monitoraggio del download dei moduli DLL può influire sulle prestazioni del sistema operativo.

- **Applica le regole a script e pacchetti MSI.**

La casella di controllo consente di abilitare o disabilitare l'avvio di script e pacchetti MSI.

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 consente o blocca l'esecuzione di script e pacchetti MSI utilizzando le regole specificate le cui impostazioni specificano gli script e i pacchetti MSI come ambito.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 non controlla l'avvio degli script e dei pacchetti MSI utilizzando le regole specificate. L'avvio degli script e dei pacchetti MSI è consentito.

La casella di controllo è selezionata per impostazione predefinita.

7. Nella sezione **Utilizzo di KSN** configurare le seguenti impostazioni di avvio delle applicazioni:

- **Nega le applicazioni non considerate attendibili da KSN.**

La casella di controllo consente di abilitare o disabilitare Controllo dell'avvio delle applicazioni in base alla reputazione delle applicazioni in KSN.

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 blocca l'esecuzione di qualsiasi applicazione con uno stato non attendibile in KSN. Le regole di permesso di Controllo dell'avvio delle applicazioni che si applicano alle applicazioni non classificate come attendibili da KSN non verranno attivate. La selezione della casella di controllo fornisce una protezione aggiuntiva dal malware.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 non tiene conto della reputazione dei programmi classificati come non attendibili da KSN e consente o blocca l'avvio in base alle regole che si applicano a tali programmi.

La casella di controllo è deselezionata per impostazione predefinita.

- **Consenti le applicazioni considerate attendibili da KSN.**

La casella di controllo consente di abilitare o disabilitare Controllo dell'avvio delle applicazioni in base alla reputazione delle applicazioni in KSN.

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 consente l'esecuzione delle applicazioni se hanno uno stato attendibile in KSN. Le regole di negazione di Controllo dell'avvio delle applicazioni che vengono applicate alle applicazioni considerate attendibili da KSN hanno una priorità più elevata: se l'applicazione è considerata attendibile dai servizi KSN, l'avvio di questa applicazione sarà vietato.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 non tiene conto della reputazione dei programmi classificati come attendibili da KSN e consente o blocca l'avvio in base alle regole che si applicano a tali programmi.

La casella di controllo è deselezionata per impostazione predefinita.

- Utenti e/o gruppi di utenti autorizzati all'avvio delle applicazioni attendibili in KSN.
8. Nella scheda **Controllo distribuzione Software** configurare le impostazioni per il controllo della distribuzione del software (vedere la sezione "Configurazione di Controllo distribuzione software" a pagina [180](#)).
 9. Nelle scheda **Gestione attività** configurare le impostazioni di avvio dell'attività pianificata (vedere la sezione "Configurazione delle impostazioni della pianificazione dell'avvio delle attività" a pagina [119](#)).
 10. Fare clic su **OK** nella finestra **Impostazioni attività**.

Kaspersky Embedded Systems Security 2.2 applica immediatamente le nuove impostazioni all'attività in esecuzione. Le informazioni sulla data e l'ora in cui le impostazioni sono state modificate e i valori delle impostazioni dell'attività prima e dopo la modifica vengono salvati nel log dell'attività.

Informazioni su Controllo distribuzione software

La generazione delle regole per il controllo dell'avvio delle applicazioni può essere complessa, se bisogna tenere conto anche del controllo della distribuzione del software in un computer protetto. Ad esempio per i computer in cui vengono regolarmente eseguiti aggiornamenti automatici del software installato. In questo caso è necessario aggiornare l'elenco delle regole di permesso dopo ogni aggiornamento software affinché le impostazioni dell'attività Controllo dell'avvio delle applicazioni tengano conto dei nuovi file creati. Per semplificare il controllo dell'avvio negli scenari di distribuzione del software è possibile utilizzare il sottosistema Controllo dell'avvio delle applicazioni.

Un *pacchetto di distribuzione software* (anche denominato semplicemente "pacchetto") rappresenta un'applicazione software da installare in un computer. Ogni pacchetto contiene almeno un'applicazione e può anche includere singoli file, aggiornamenti o perfino un singolo comando, oltre alle applicazioni, in particolare per l'installazione di un'applicazione software o un aggiornamento.

Il sottosistema Controllo distribuzione software viene implementato come elenco aggiuntivo di esclusioni. Quando si aggiunge un pacchetto di distribuzione software all'elenco, l'applicazione consentirà la decompressione di questi pacchetti attendibili e l'avvio automatico del software creato o modificato da parte di un pacchetto attendibile. I file estratti possono ereditare l'attributo attendibile di un pacchetto di distribuzione principale. Un *pacchetto di distribuzione principale* è un pacchetto che è stato aggiunto all'elenco delle esclusioni di Controllo distribuzione software dall'utente ed è quindi impostato come pacchetto attendibile.

Kaspersky Embedded Systems Security 2.2 controlla solo i cicli completi di distribuzione del software. L'applicazione non può elaborare correttamente l'avvio dei file modificati da un pacchetto attendibile se, durante il primo avvio del pacchetto Controllo distribuzione software è disattivato o non è installato il componente Controllo dell'avvio delle applicazioni.

Controllo distribuzione software non è disponibile se la casella di controllo **Applica le regole ai file eseguibili** è deselezionata nelle impostazioni dell'attività Controllo dell'avvio delle applicazioni.

Cache di distribuzione software

Kaspersky Embedded Systems Security 2.2 stabilisce una connessione tra i pacchetti attendibili e i file creati durante la procedura di distribuzione del software tramite la *cache di distribuzione del software* generata in modo dinamico (denominata anche "cache di distribuzione"). All'avvio del primo pacchetto Kaspersky Embedded Systems Security 2.2 rileva tutti i file creati durante il processo di distribuzione del software da questo pacchetto e archivia i checksum e i percorsi dei file nella cache di distribuzione. Successivamente, l'avvio di tutti i file memorizzati nella cache di distribuzione è consentito per impostazione predefinita.

Non è possibile esaminare, deselezionare o modificare manualmente la cache di distribuzione tramite l'interfaccia

utente. La cache viene popolata e controllata da Kaspersky Embedded Systems Security 2.2.

È possibile esportare la cache di distribuzione nel file di configurazione (in formato XML) e svuotare la cache utilizzando le opzioni della riga di comando.

- *Per esportare la cache di distribuzione in un file di configurazione, eseguire il seguente comando:*

```
kavshell appcontrol /config /savetofile:<percorso completo> /sdc
```

- *Per svuotare la cache di distribuzione eseguire il seguente comando:*

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security 2.2 aggiorna la cache di distribuzione ogni 24 ore. Se viene modificato il percorso completo o il checksum di un file precedentemente consentito, l'applicazione elimina il record del file dalla cache di distribuzione. Se l'attività Controllo dell'avvio delle applicazioni viene eseguita in modalità attiva, i successivi avvii del file verranno bloccati.

Elaborazione dei file estratti

L'attributo attendibile per tutti i file estratti del pacchetto attendibile vengono ereditati al primo avvio del pacchetto. Se si diseleziona la casella di controllo dopo il primo avvio, l'ereditarietà per tutti i file estratti dal pacchetto verrà mantenuta. Per ripristinare l'ereditarietà applicata inizialmente per tutti i file estratti, è necessario svuotare la cache di distribuzione e diselezionare la casella di controllo **Consenti l'avvio per tutti i file da questa catena di estrazione dei pacchetti di distribuzione** prima di avviare di nuovo il pacchetto di distribuzione attendibile.

I file estratti e i pacchetti che vengono creati da un pacchetto di distribuzione principale attendibile acquisiscono l'attributo attendibile, perché i relativi checksum vengono aggiunti alla cache di distribuzione quando si apre per la prima volta il pacchetto di distribuzione del software nell'elenco delle esclusioni. Di conseguenza, saranno considerati attendibili il pacchetto di distribuzione stesso e tutti i file estratti da questo pacchetto. Per impostazione predefinita, il numero di livelli per l'ereditarietà dell'attributo attendibile è illimitato.

L'attributo attendibile verrà mantenuto dai file estratti dopo il riavvio del sistema operativo.

L'elaborazione dei file è configurata nelle impostazioni di Controllo distribuzione software (vedere la sezione "Configurazione di Controllo distribuzione software" a pagina [180](#)) selezionando o diselezionando la casella di controllo **Consenti l'avvio per tutti i file da questa catena di estrazione dei pacchetti di distribuzione**.

Ad esempio, aggiungere un pacchetto test.msi contenente diversi altri pacchetti e applicazioni all'elenco delle esclusioni e selezionare la casella di controllo. In questo caso, è consentita l'esecuzione o l'estrazione di tutti i pacchetti e le applicazioni che sono contenuti nel pacchetto test.msi, se contengono altri file. Questo scenario funziona per i file estratti in tutti i livelli nidificati.

Se si aggiunge un pacchetto test.msi all'elenco delle esclusioni e si diseleziona la casella di controllo **Consenti l'avvio per tutti i file da questa catena di estrazione dei pacchetti di distribuzione**, l'applicazione assegnerà l'attributo attendibile solo ai pacchetti e ai file eseguibili estratti direttamente da un pacchetto attendibile principale (nidificato al primo livello). I checksum di tali file sono archiviati nella cache di distribuzione. Tutti i file nidificati nel secondo livello e in quelli successivi verranno bloccati in base al principio Default deny.

Interazione con l'elenco delle regole per il controllo all'avvio delle applicazioni

L'elenco dei pacchetti attendibili del sottosistema Controllo distribuzione software è un elenco di esclusioni che

estende, ma non sostituisce, l'elenco generale delle regole per il controllo dell'avvio delle applicazioni.

Le regole di negazione del controllo dell'avvio delle applicazioni hanno la massima priorità: la decompressione dei pacchetti attendibili e l'avvio dei file nuovi o modificati verranno bloccati se questi pacchetti e file sono interessati dalle regole di negazione del controllo dell'avvio delle applicazioni.

Le esclusioni di Controllo distribuzione software vengono applicate sia per i pacchetti attendibili che per i file creati o modificati da questi pacchetti, se a questi pacchetti e file non si applicano le regole di negazione nell'elenco di controllo dell'avvio delle applicazioni.

Utilizzo delle conclusioni KSN

Le conclusioni KSN hanno una priorità superiore rispetto alle esclusioni di Controllo distribuzione software: la decompressione di un pacchetto attendibile o l'avvio dei file creati e modificati da questo pacchetto verranno bloccati se si riceve una conclusione non attendibile per tali file da KSN.

Configurazione di Controllo distribuzione software

► *Per aggiungere un pacchetto di distribuzione attendibile, procedere come segue:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Controllo attività locali** fare clic sul pulsante **Impostazioni** nella sezione **Controllo dell'avvio delle applicazioni**.
Verrà visualizzata la finestra **Controllo dell'avvio delle applicazioni**.
4. Nella scheda selezionata spuntare la casella di controllo **Consenti automaticamente la distribuzione software per le applicazioni e i pacchetti elencati**.

La casella di controllo consente di abilitare e disabilitare la creazione automatica delle esclusioni per tutti i file avviati utilizzando i pacchetti di distribuzione specificati nell'elenco.

Se la casella di controllo è selezionata, l'applicazione consente automaticamente l'avvio dei file nei pacchetti di distribuzione attendibili. L'elenco di applicazioni e pacchetti di distribuzione per cui è consentito l'avvio può essere modificato.

Se la casella di controllo è deselezionata, l'applicazione non applica le esclusioni specificate nell'elenco.

La casella di controllo è deselezionata per impostazione predefinita.

È possibile selezionare **Consenti automaticamente la distribuzione software per le applicazioni e i pacchetti elencati** se la casella di controllo **Applica le regole ai file eseguibili** è selezionata nelle impostazioni dell'attività **Controllo dell'avvio delle applicazioni**.

5. Se necessario, deseleggiare la casella di controllo **Consenti sempre la distribuzione software tramite Windows Installer**.

La casella di controllo consente di abilitare e disabilitare la creazione automatica delle esclusioni per tutti i file eseguiti tramite Windows Installer.

Se la casella di controllo è selezionata, l'applicazione consentirà sempre l'avvio dei file installati tramite Windows Installer.

Se la casella di controllo è deseleggiata, l'applicazione non sarà consentita in qualsiasi caso, anche se avviata tramite Windows Installer.

La casella di controllo è selezionata per impostazione predefinita.

La casella di controllo non è modificabile se la casella di controllo **Consenti automaticamente la distribuzione software per i pacchetti elencati** non è selezionata.

È consigliabile deseleggiare la casella di controllo **Consenti sempre la distribuzione software tramite Windows Installer** solo se assolutamente necessario. La disattivazione di questa funzione può causare problemi di aggiornamento dei file del sistema operativo, oltre a impedire l'avvio dei file estratti da un pacchetto di distribuzione.

6. Se richiesto, selezionare la casella di controllo **Consenti sempre la distribuzione software tramite SCCM utilizzando Servizio trasferimento intelligente in background**.

La casella di controllo attiva o disattiva la distribuzione software automatica utilizzando System Center Configuration Manager.

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 consente automaticamente la distribuzione di Microsoft Windows tramite System Center Configuration Manager. L'applicazione consente la distribuzione software solo tramite Servizio trasferimento intelligente in background.

L'applicazione controlla l'avvio degli oggetti con le seguenti estensioni:

- .exe
- .msi

La casella di controllo è deseleggiata per impostazione predefinita.

L'applicazione controlla il ciclo di distribuzione software nel computer dalla distribuzione del pacchetto all'installazione o all'aggiornamento. L'applicazione non controlla i processi se una delle fasi di distribuzione è stata eseguita prima dell'installazione dell'applicazione nel computer.

7. Per modificare l'elenco dei pacchetti di distribuzione attendibili, fare clic su **Modifica elenco dei pacchetti** e selezionare uno dei metodi seguenti nella finestra visualizzata:

- **Aggiungi un pacchetto di distribuzione.**

- a. Fare clic sul pulsante **Sfoggia** e selezionare il file eseguibile o il pacchetto di distribuzione.

La sezione **Criteri di attendibilità** viene automaticamente popolata con i dati relativi al file selezionato.

- b. Deselezionare o selezionare la casella di controllo **Consenti l'avvio per tutti i file da questa catena di estrazione dei pacchetti di distribuzione**.
- c. Selezionare una delle due opzioni disponibili per i criteri da utilizzare per determinare se un file o un pacchetto di distribuzione è attendibile:

- **Usa certificato digitale**

Se questa opzione è selezionata, viene specificata la presenza di un certificato digitale come criterio di attivazione della regola nelle impostazioni delle nuove regole di permesso generate per Controllo dell'avvio delle applicazioni. L'applicazione ora consentirà l'avvio dei programmi avviati utilizzando file con un certificato digitale. Questa opzione è consigliata se si desidera consentire l'avvio di qualsiasi applicazione considerata attendibile nel sistema operativo.

- **Usa hash SHA256**

Se questa opzione è selezionata, il valore di checksum del file utilizzato per generare la regola viene specificato come criterio di attivazione della regola nelle impostazioni delle nuove regole di permesso generate per Controllo dell'avvio delle applicazioni. L'applicazione consentirà l'avvio dei programmi avviati utilizzando file con il valore di checksum specificato.

Questa opzione è consigliata nei casi in cui le regole generate sono necessarie per soddisfare un livello di sicurezza molto elevato: il checksum SHA256 può essere applicato come un ID univoco del file. L'utilizzo del checksum SHA256 come criterio di attivazione della regola restringe l'ambito di applicazione della regola a un solo file.

Questa opzione è selezionata per impostazione predefinita.

- **Aggiungi diversi pacchetti in base all'hash.**

È possibile selezionare un numero illimitato di file eseguibili e pacchetti di distribuzione e aggiungerli tutti all'elenco contemporaneamente. Kaspersky Embedded Systems Security 2.2 esamina l'hash e consente al sistema operativo di avviare i file specificati.

- **Modifica pacchetto selezionato.**

Utilizzare questa opzione per selezionare un file eseguibile o un pacchetto di distribuzione diverso oppure per modificare i criteri di attendibilità.

- **Importa elenco dei pacchetti di distribuzione da file.**

È possibile importare l'elenco dei pacchetti di distribuzione attendibili dal file di configurazione. Il file riconosciuto da Kaspersky Embedded Systems Security 2.2 deve soddisfare i seguenti parametri:

- Il file ha un'estensione di testo.
- Il file contiene informazioni strutturate come un elenco di righe, dove ogni riga include i dati relativi a uno dei file attendibili.
- Il file deve contenere un elenco in uno dei seguenti formati:
 - <nome file>:<hash SHA256>.
 - <hash SHA256>*<nome file>.

Nella finestra **Apri** specificare il file di configurazione contenente un elenco di pacchetti di distribuzione attendibili.

8. Se si desidera rimuovere un'applicazione o un pacchetto di distribuzione aggiunto precedentemente all'elenco attendibile, fare clic sul pulsante **Elimina pacchetti di distribuzione**. L'esecuzione dei file estratti

sarà consentita.

Per impedire l'avvio dei file estratti, disinstallare l'applicazione nel computer protetto o creare una regola di negazione nelle impostazioni dell'attività Controllo dell'avvio delle applicazioni.

9. Fare clic su **OK**.

Le nuove impostazioni configurate sono state salvate.

Abilitazione della modalità Default allow

La modalità Default allow consente l'avvio di tutte le applicazioni, se non sono bloccate in base alle regole o ritenute non attendibili da KSN. La modalità Default allow può essere abilitata aggiungendo specifiche regole di permesso. È possibile abilitare la modalità Default allow solo per gli script o per tutti i file eseguibili.

► *Per aggiungere una regola Default allow:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Controllo attività locali** fare clic sul pulsante **Impostazioni** nel gruppo **Controllo dell'avvio delle applicazioni**.
4. Nella scheda **Generale** fare clic sul pulsante **Elenco di regole**.
Verrà visualizzata la finestra **Regole di Controllo dell'avvio delle applicazioni**.
5. Fare clic sul pulsante **Aggiungi** e nel menu di scelta rapida del pulsante selezionare l'opzione **Aggiungi una regola**.
Verrà visualizzata la finestra **Impostazioni regola**.
6. Nel campo **Nome** immettere il nome della regola.
7. Nell'elenco a discesa **Tipo** selezionare il tipo di regola **Permesso**.
8. Nell'elenco a discesa **Ambito** selezionare il tipo di file la cui esecuzione sarà controllata dalla regola:
 - **File eseguibili** se si desidera che la regola controlli l'avvio dei file eseguibili delle applicazioni.
 - **Script e pacchetti MSI** se si desidera che la regola controlli l'avvio di script e pacchetti MSI.
9. Nella sezione **Criterio di attivazione della regola** selezionare un'opzione **Percorso del file**.

10. Immettere la seguente maschera: ?:\

11. Fare clic su **OK** nella finestra **Impostazioni regola**.

Kaspersky Embedded Systems Security 2.2 applica la modalità Default allow.

Informazioni sulla generazione delle regole di Controllo dell'avvio delle applicazioni per tutti i computer in Kaspersky Security Center

È possibile creare elenchi di regole di Controllo dell'avvio delle applicazioni utilizzando le attività e i criteri di Kaspersky Security Center per tutti i computer e i gruppi di computer della rete aziendale contemporaneamente. Questo scenario è consigliato se la rete aziendale non dispone di un computer di riferimento e l'utente non è in grado di creare un elenco comune delle regole utilizzando un'attività di generazione automatica delle regole di permesso in base alle applicazioni installate nel computer di riferimento.

Il componente Controllo dell'avvio delle applicazioni viene installato con due regole di permesso predefinite:

- Regola di permesso per gli script e i pacchetti MSI con un certificato attendibile del sistema operativo.
- Regola di permesso per i file eseguibili con un certificato attendibile del sistema operativo.

È possibile creare elenchi di regole di Controllo dell'avvio delle applicazioni in Kaspersky Security Center in due modi:

- Utilizzando un'attività di gruppo Generazione regole per Controllo dell'avvio delle applicazioni per Controllo dell'avvio delle applicazioni.

Quando si utilizza questo scenario, un'attività di gruppo genera il proprio elenco di regole di Controllo dell'avvio delle applicazioni per ogni computer nella rete e salva tali elenchi in un file XML nella cartella di rete condivisa specificata. È possibile quindi importare manualmente l'elenco di regole creato nell'attività Controllo dell'avvio delle applicazioni del criterio di Kaspersky Security Center. È possibile configurare un criterio di Kaspersky Security Center per l'aggiunta automatica delle regole create all'elenco di regole di Controllo dell'avvio delle applicazioni quando l'attività di gruppo Generazione regole per Controllo dell'avvio delle applicazioni viene completata.

Questo scenario è consigliato quando è necessario creare elenchi di regole di Controllo dell'avvio delle applicazioni con un breve preavviso. È consigliabile configurare l'avvio pianificato dell'attività Generazione regole per Controllo dell'avvio delle applicazioni solo se l'ambito di applicazione delle regole di permesso include cartelle che contengono file che sono senza dubbio sicuri.

Prima di utilizzare il criterio di Controllo dell'avvio delle applicazioni, assicurarsi che tutti i computer protetti abbiano accesso a una cartella di rete condivisa. Se il criterio dell'organizzazione non prevede l'utilizzo di una cartella di rete condivisa nella rete, è consigliabile avviare le attività di generazione automatica delle regole per le regole di controllo del computer nel gruppo di computer di prova o in un computer di riferimento.

- In base a un rapporto sugli eventi dell'attività generati in Kaspersky Security Center per l'esecuzione dell'attività Controllo dell'avvio delle applicazioni in modalità **Solo statistiche**.

Quando si utilizza questo scenario, Kaspersky Embedded Systems Security 2.2 non impedisce l'avvio delle applicazioni, ma durante l'esecuzione di Controllo dell'avvio delle applicazioni in modalità **Solo statistiche** segnala tutti gli avvii delle applicazioni consentiti e negati in tutti computer della rete nella sezione **Eventi** di Kaspersky Security Center. Kaspersky Security Center genera l'elenco unificato degli eventi di avvio non consentito delle applicazioni, in base al log dell'attività.

È necessario configurare il periodo di esecuzione dell'attività in modo che durante il periodo di tempo specificato vengano eseguiti tutti i possibili scenari di esecuzione dei computer protetti e dei gruppi di computer e almeno un riavvio. Quando vengono aggiunte le regole all'attività Controllo dell'avvio delle

applicazioni, è quindi possibile importare i dati sugli avvii delle applicazioni dal file del rapporto sugli eventi di Kaspersky Security Center salvato (in formato TXT) e generare le regole di permesso di Controllo dell'avvio delle applicazioni per tali applicazioni in base a questi dati.

Questo scenario è consigliato se una rete aziendale include una grande quantità di computer di tipo diverso (vedere la sezione "Utilizzo di un profilo per configurare le attività Controllo dell'avvio delle applicazioni in un criterio di Kaspersky Security Center" a pagina [172](#)) (computer con differenti set di software installati).

- In base agli eventi di avvio non consentito delle applicazioni ricevuti tramite Kaspersky Security Center, senza creare e importare un file di configurazione.

Per utilizzare questa funzionalità, l'attività Controllo dell'avvio delle applicazioni nel computer locale deve essere eseguita con un criterio di Kaspersky Security Center attivo. In questo caso, tutti gli eventi nel computer locale vengono inviati ad Administration Server.

È consigliabile aggiornare l'elenco di regole quando cambia il set di applicazioni installate nei computer della rete (ad esempio, quando vengono installati aggiornamenti o reinstallati i sistemi operativi). Per generare un elenco aggiornato di regole è consigliabile utilizzare l'attività Generazione regole per Controllo dell'avvio delle applicazioni o il criterio Controllo dell'avvio delle applicazioni in modalità **Solo statistiche**, in esecuzione nei computer del gruppo di amministrazione di prova. Il gruppo di amministrazione di test include i computer richiesti per l'avvio di test delle nuove applicazioni prima che vengano installate nei computer della rete.

Prima di aggiungere regole di permesso, selezionare una delle modalità di applicazione delle regole disponibili (vedere la sezione "Configurazione delle impostazioni dell'attività Controllo dell'avvio delle applicazioni" a pagina [173](#)). L'elenco delle regole del criterio di Kaspersky Security Center visualizza solo le regole specificate dal criterio, indipendentemente dalla modalità di applicazione della regola. L'elenco delle regole locali visualizza tutte le regole applicate: sia quelle locali sia quelle aggiunte tramite un criterio.

In questa sezione

Creazione di regole di permesso dagli eventi di Kaspersky Security Center	185
Importazione delle regole di Controllo dell'avvio delle applicazioni da un file XML.....	186
Importazione delle regole dal file di un rapporto sulle applicazioni bloccate di Kaspersky Security Center	188

Creazione di regole di permesso dagli eventi di Kaspersky Security Center

- *Per generare regole di permesso utilizzando l'opzione "Crea regole di permesso per le applicazioni dagli eventi Kaspersky Security Center" in Controllo dell'avvio delle applicazioni, procedere come segue:*

1. In Kaspersky Security Center Administration Console espandere il nodo **Dispositivi gestiti**.
2. Espandere il gruppo di amministrazione per cui si desidera configurare le impostazioni del criterio e selezionare la scheda **Criteri** nel riquadro dei dettagli.
3. Selezionare **Proprietà** nel menu di scelta rapida del criterio da configurare.
Verrà visualizzata la finestra **Proprietà: <nome criterio>**.
4. Nella sezione **Controllo attività locali** fare clic sul pulsante **Impostazioni** nel gruppo **Controllo dell'avvio delle applicazioni**.
5. Nella scheda **Generale** fare clic sul pulsante **Elenco di regole**.

Verrà visualizzata la finestra **Regole di Controllo dell'avvio delle applicazioni**.

6. Fare clic sul pulsante **Aggiungi** e nel menu di scelta rapida del pulsante selezionare **Crea regole di permesso per le applicazioni dagli eventi Kaspersky Security Center**.
7. Selezionare il principio per l'aggiunta delle regole all'elenco delle regole di Controllo dell'avvio delle applicazioni create in precedenza:
 - **Aggiungi alle regole esistenti** se si desidera aggiungere le regole importate all'elenco di quelle esistenti. Le regole con impostazioni identiche vengono duplicate.
 - **Sostituisci le regole esistenti** se si desidera sostituire le regole esistenti con quelle importate.
 - **Unisci con le regole esistenti** se si desidera aggiungere le regole importate all'elenco di quelle esistenti. Le regole con impostazioni identiche non vengono aggiunte: la regola viene aggiunta se almeno un parametro della regola è univoco.

Verrà visualizzata la finestra **Generazione delle regole di Controllo dell'avvio delle applicazioni**.

8. Configurare le seguenti impostazioni per le richieste:
 - **Indirizzo di Administration Server**
 - **Porta**
 - **Utente**
 - **Password**
9. Selezionare i tipi di eventi su cui si desidera basare la generazione dell'attività:
 - **Modalità Solo statistiche: avvio dell'applicazione non consentito.**
 - **Avvio dell'applicazione non consentito.**
10. Selezionare il periodo di tempo dall'elenco a discesa **Eventi richiesta generati entro il periodo**.
11. Fare clic sul pulsante **Genera regole**.
12. Fare clic sul pulsante **Salva** nella finestra **Regole di Controllo dell'avvio delle applicazioni**.

L'elenco di regole nel criterio di Controllo dell'avvio delle applicazioni verrà compilato con le nuove regole generate in base ai dati di sistema del computer in cui è installata Kaspersky Security Center Administration Console.

Se l'elenco delle regole di Controllo dell'avvio delle applicazioni è già specificato nel criterio, Kaspersky Embedded Systems Security 2.2 aggiunge le regole selezionate dagli eventi di blocco alle regole già specificate. Le regole con lo stesso hash non vengono aggiunte, perché tutte le regole in un elenco devono essere univoche.

Importazione delle regole di Controllo dell'avvio delle applicazioni da un file XML

È possibile importare i rapporti generati al completamento dell'attività di gruppo Generazione regole per Controllo dell'avvio delle applicazioni e applicarli come un elenco di regole di permesso nel criterio che si sta configurando.

Al termine dell'attività di gruppo Generazione regole per Controllo dell'avvio delle applicazioni, l'applicazione esporta le regole di permesso create in file XML salvati nella cartella di rete condivisa specificata. Ogni file con l'elenco di regole viene creato in base all'analisi dei file eseguiti e alle applicazioni avviate in ogni computer nella rete aziendale. Gli elenchi contengono regole di permesso per i file e le applicazioni il cui tipo corrisponde al tipo specificato nell'attività di gruppo Generazione regole per Controllo dell'avvio delle applicazioni.

Il processo di configurazione delle impostazioni dei componenti funzionali di Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center è simile alla configurazione locale delle impostazioni di questi componenti nella console dell'applicazione. Istruzioni dettagliate su come configurare le impostazioni delle attività e le funzioni dell'applicazione sono disponibili nelle relative sezioni del *Manuale Utente di Kaspersky Embedded Systems Security 2.2*.

► Per specificare le regole di permesso per l'avvio delle applicazioni per un gruppo di computer in base a un elenco generato automaticamente di regole di permesso, eseguire le seguenti operazioni.

1. Nella scheda **Attività**, nel pannello di controllo del gruppo di computer che si sta configurando, creare un'attività di gruppo Generazione regole per Controllo dell'avvio delle applicazioni o selezionare un'attività esistente.
2. Nelle proprietà dell'attività di gruppo Generazione regole per Controllo dell'avvio delle applicazioni creata o nella procedura guidata dell'attività specificare le seguenti impostazioni:
 - Nella sezione **Notifica** configurare le impostazioni per il salvataggio del rapporto sull'esecuzione dell'attività.

Per istruzioni dettagliate sulla configurazione delle impostazioni in questa sezione, vedere la *Guida di Kaspersky Security Center*.

- Nella sezione **Impostazioni** specificare i tipi di applicazioni per cui sarà consentito l'avvio dalle regole create. È possibile modificare il contenuto delle cartelle che contengono le applicazioni consentite: escludere le cartelle predefinite dall'ambito dell'attività o aggiungere manualmente nuove cartelle.
- Nella sezione **Opzioni** specificare le operazioni dell'attività mentre è in esecuzione e dopo il completamento. Specificare il criterio in base al quale saranno generate le regole e il nome del file in cui saranno esportate queste regole.
- Nella sezione **Pianificazione** configurare le impostazioni di pianificazione dell'avvio dell'attività.
- Nella sezione **Account** specificare l'account utente con cui sarà eseguita l'attività.
- Nella sezione **Esclusioni dall'ambito dell'attività** specificare i gruppi di computer da escludere dall'ambito dell'attività.

Kaspersky Embedded Systems Security 2.2 non crea regole di permesso per le applicazioni avviate nei computer esclusi.

3. Nella scheda **Attività**, nel pannello di controllo del gruppo di computer configurati, selezionare nell'elenco delle attività di gruppo l'attività Generazione regole per Controllo dell'avvio delle applicazioni creata e fare clic sul pulsante **Avvia** per avviare l'attività.

Una volta completata l'attività, gli elenchi di regole di permesso generati automaticamente verranno salvati in file XML in una cartella di rete condivisa.

Prima di utilizzare il criterio di Controllo dell'avvio delle applicazioni, assicurarsi che tutti i computer protetti abbiano accesso a una cartella di rete condivisa. Se il criterio dell'organizzazione non prevede l'utilizzo di una cartella di rete condivisa nella rete, è consigliabile avviare le attività di generazione automatica delle regole per le regole di controllo del computer nel gruppo di computer di prova o in un computer di riferimento.

4. Aggiungere gli elenchi di regole di permesso generati all'attività Controllo dell'avvio delle applicazioni. A tale scopo, nelle proprietà del criterio configurato, nelle impostazioni dell'attività Controllo dell'avvio delle applicazioni:
 - a. Nella scheda **Generale** fare clic sul pulsante **Elenco di regole**.
Verrà visualizzata la finestra **Regole di Controllo dell'avvio delle applicazioni**.
 - b. Fare clic sul pulsante **Aggiungi** e nell'elenco visualizzato selezionare **Importa regole da file XML**.
 - c. Selezionare il principio per l'aggiunta delle regole di permesso generate automaticamente all'elenco delle regole di Controllo dell'avvio delle applicazioni create in precedenza:
 - **Aggiungi alle regole esistenti** se si desidera aggiungere le regole importate all'elenco di quelle esistenti. Le regole con impostazioni identiche vengono duplicate.
 - **Sostituisci le regole esistenti** se si desidera sostituire le regole esistenti con quelle importate.
 - **Unisci con le regole esistenti** se si desidera aggiungere le regole importate all'elenco di quelle esistenti. Le regole con impostazioni identiche non vengono aggiunte: la regola viene aggiunta se almeno un parametro della regola è univoco.
 - d. Nella finestra standard di Microsoft Windows visualizzata selezionare i file XML creati dopo il completamento dell'attività di gruppo Generazione regole per Controllo dell'avvio delle applicazioni.
 - e. Fare clic su **OK** nelle finestre **Regole di Controllo dell'avvio delle applicazioni** e **Impostazioni attività**.
5. Se si desidera applicare le regole create per controllare l'avvio delle applicazioni, nelle proprietà dell'attività Controllo dell'avvio delle applicazioni del criterio selezionare la modalità di esecuzione dell'attività **Attivo**.

Le regole di permesso generate automaticamente in base alle esecuzioni dell'attività in ogni computer verranno applicate a tutti i computer della rete a cui si applica il criterio configurato. In questi computer sarà consentito avviare solo quelle applicazioni per cui sono state create regole di permesso.

Importazione delle regole dal file di un rapporto sulle applicazioni bloccate di Kaspersky Security Center

È possibile importare i dati sugli avvii delle applicazioni bloccati dal rapporto generato in Kaspersky Security Center dopo il completamento dell'attività Controllo dell'avvio delle applicazioni nella modalità **Solo statistiche** e utilizzare questi dati per generare un elenco di regole di permesso di Controllo dell'avvio delle applicazioni nel criterio configurato.

Quando si genera il rapporto sugli eventi che si verificano durante un'attività Controllo dell'avvio delle applicazioni, è possibile tenere traccia delle applicazioni di cui viene bloccato l'avvio.

Al momento dell'importazione dei dati dal rapporto sulle applicazioni bloccate nelle impostazioni del criterio, verificare che l'elenco in uso contenga solo le applicazioni di cui si desidera consentire l'avvio.

► Per specificare le regole di permesso per l'avvio delle applicazioni per un gruppo di computer in base al rapporto sulle applicazioni bloccate di Kaspersky Security Center, eseguire le seguenti operazioni:

1. Nelle proprietà del criterio, nelle impostazioni dell'attività Controllo dell'avvio delle applicazioni, selezionare la modalità operativa **Solo statistiche**.
2. Nelle proprietà del criterio, nella sezione **Eventi**, verificare che:
 - La scheda **Eventi critici** dell'evento Avvio dell'applicazione non consentito mostri un tempo di archiviazione degli eventi superiore al tempo pianificato di esecuzione dell'attività nella modalità **Solo statistiche** (il valore predefinito è 30 giorni).
 - La scheda **Avviso** dell'evento *Solo statistiche: avvio delle applicazioni non consentito* mostri un tempo di archiviazione degli eventi superiore al tempo pianificato di esecuzione dell'attività nella modalità **Solo statistiche** (il valore predefinito è 30 giorni).

Al termine del periodo specificato nella colonna **Tempo di archiviazione**, le informazioni sugli eventi registrati vengono eliminate e non sono riportate nel file del rapporto. Prima di eseguire l'attività Controllo dell'avvio delle applicazioni nella modalità **Solo statistiche**, verificare che il tempo di esecuzione dell'attività non superi il tempo di archiviazione configurato per gli eventi specificati.

3. Una volta completata l'attività, esportare gli eventi registrati in un file TXT:
 - a. A tale scopo, nelle proprietà dell'attività Controllo dell'avvio delle applicazioni espandere il nodo **Log e notifiche**.
 - b. Nel nodo figlio **Eventi** creare una selezione di eventi in base al criterio *Bloccato* per visualizzare le applicazioni di cui verrà bloccato l'avvio dall'attività Controllo dell'avvio delle applicazioni.
 - c. Nel riquadro dei dettagli della selezione fare clic sull'elenco **Esporta eventi in un file** per salvare il rapporto sugli avvii delle applicazioni bloccati in un file TXT.

Prima di importare e applicare il rapporto generato in un criterio, verificare che il rapporto contenga dati solo sulle applicazioni di cui si desidera consentire l'avvio.

4. Importare i dati sugli avvii delle applicazioni bloccati nell'attività Controllo dell'avvio delle applicazioni. A tale scopo, nelle proprietà del criterio, nelle impostazioni dell'attività Controllo dell'avvio delle applicazioni:
 - a. Nella scheda **Generale** fare clic sul pulsante **Elenco di regole**.
Verrà visualizzata la finestra **Regole di Controllo dell'avvio delle applicazioni**.
 - b. Fare clic sul pulsante **Aggiungi** e nel menu di scelta rapida del pulsante selezionare **Importa i dati delle applicazioni bloccate dal report di Kaspersky Security Center**.
 - c. Selezionare il principio per l'aggiunta delle regole dall'elenco creato in base al rapporto di Kaspersky Security Center all'elenco delle regole di Controllo dell'avvio delle applicazioni configurate in precedenza:
 - **Aggiungi alle regole esistenti** se si desidera aggiungere le regole importate all'elenco di quelle esistenti. Le regole con impostazioni identiche vengono duplicate.
 - **Sostituisci le regole esistenti** se si desidera sostituire le regole esistenti con quelle importate.
 - **Unisci con le regole esistenti** se si desidera aggiungere le regole importate all'elenco di quelle esistenti. Le regole con impostazioni identiche non vengono aggiunte: la regola viene aggiunta se almeno un parametro della regola è univoco.
 - d. Nella finestra standard di Microsoft Windows visualizzata selezionare il file TXT in cui sono stati

esportati gli eventi dal rapporto sugli avvii delle applicazioni bloccati.

- e. Fare clic su **OK** nelle finestre Regole di Controllo dell'avvio delle applicazioni e **Impostazioni attività**.

Le regole create in base al rapporto di Kaspersky Security Center sulle applicazioni bloccate verranno aggiunte all'elenco delle regole di Controllo dell'avvio delle applicazioni.

Gestione delle connessioni dei dispositivi tramite Kaspersky Security Center

È possibile consentire o limitare le connessioni di unità flash e altri dispositivi di archiviazione di massa a tutti i computer della rete generando elenchi di controllo dei computer unificati tramite Kaspersky Security Center per i gruppi di computer.

In questa sezione

Informazioni sull'attività Controllo dispositivi.....	190
Informazioni sulla generazione delle regole di Controllo dispositivi per tutti i computer in Kaspersky Security Center	191
Generazione delle regole in base ai dati di sistema sui dispositivi esterni connessi ai computer della rete.....	193
Importazione delle regole dal file di un rapporto sui dispositivi bloccati di Kaspersky Security Center	196

Informazioni sull'attività Controllo dispositivi

Kaspersky Embedded Systems Security 2.2 controlla la registrazione e l'utilizzo dei dispositivi di archiviazione di massa e delle unità CD/DVD per proteggere il computer dalle minacce per la sicurezza che possono verificarsi durante lo scambio di file con unità flash o altri tipi di dispositivi esterni connessi tramite USB. Un dispositivo di archiviazione di massa è un dispositivo esterno che può essere connesso a un computer per copiare o archiviare file.

Kaspersky Embedded Systems Security 2.2 controlla le connessioni dei seguenti dispositivi esterni USB:

- Unità flash connesse tramite USB
- Unità CD/DVD-ROM
- Unità floppy connesse tramite USB
- Dispositivi mobili MTP connessi tramite USB

Kaspersky Embedded Systems Security 2.2 segnala all'utente tutti i dispositivi connessi tramite USB con l'evento corrispondente nei log eventi e delle attività. I dettagli degli eventi includono il tipo di dispositivo e il percorso di connessione. All'avvio dell'attività Controllo dispositivi, Kaspersky Embedded Systems Security 2.2 verifica ed elenca tutti i dispositivi connessi tramite USB. È possibile configurare le notifiche nella sezione Impostazioni di notifica di Kaspersky Security Center.

L'attività Controllo dispositivi monitora tutti i tentativi di connessione di dispositivi esterni a un computer protetto tramite USB e blocca la connessione, se non sono presenti regole di permesso per tali dispositivi. Una volta che la

connessione è bloccata, il dispositivo non è disponibile.

L'applicazione prescrive uno dei seguenti stati per ogni dispositivo di archiviazione di massa connesso:

- **Attendibile.** Dispositivo per cui si desidera consentire lo scambio di file. Dopo la generazione dell'elenco di regole, il valore del percorso dell'istanza del dispositivo è incluso nell'ambito di applicazione per almeno una regola.
- **Non attendibile.** Dispositivo per cui si desidera limitare lo scambio di file. Il percorso dell'istanza del dispositivo non è incluso in alcun ambito di applicazione delle regole di permesso.

È possibile creare regole di permesso per i dispositivi esterni per consentire lo scambio di dati tramite Generazione regole per Controllo dispositivi. È anche possibile espandere l'ambito di applicazione per le regole già specificate. Non è possibile creare le regole di permesso manualmente.

Kaspersky Embedded Systems Security 2.2 identifica i dispositivi di archiviazione di massa registrati nel sistema utilizzando il valore *Percorso dell'istanza del dispositivo*. Percorso dell'istanza del dispositivo è una funzionalità predefinita specificata in modo univoco per ogni dispositivo esterno. Il valore di Percorso dell'istanza del dispositivo è specificato per ogni dispositivo esterno nelle relative proprietà di Windows ed è determinato automaticamente da Kaspersky Embedded Systems Security 2.2 durante la generazione della regola.

L'attività Controllo dispositivi può operare in due modalità:

- **Attivo.** Kaspersky Embedded Systems Security 2.2 applica le regole per controllare la connessione di unità flash e altri dispositivi esterni, quindi consente o blocca l'utilizzo di tutti i dispositivi in base al principio Default deny e alle regole di permesso specificate. L'utilizzo di dispositivi esterni attendibili è consentito. L'utilizzo di dispositivi esterni non attendibili è bloccato per impostazione predefinita.

Se un dispositivo esterno considerato non attendibile viene connesso a un computer protetto prima che l'attività Controllo dispositivi venga eseguita in modalità Attivo, il dispositivo non viene bloccato dall'applicazione. È consigliabile disconnettere manualmente il dispositivo non attendibile o riavviare il computer. In caso contrario, il principio Default deny non sarà applicato al dispositivo.

- **Solo statistiche.** Kaspersky Embedded Systems Security 2.2 non controlla la connessione di unità flash e altri dispositivi esterni, ma registra solo le informazioni sulla connessione e la registrazione dei dispositivi esterni in un computer protetto e sulle regole di permesso di Controllo dispositivi attivate dai dispositivi connessi. L'utilizzo di tutti i dispositivi esterni è consentito. Questa modalità è utilizzata per impostazione predefinita.

È possibile applicare questa modalità per la generazione delle regole in base alle informazioni registrate durante l'esecuzione dell'attività.

Informazioni sulla generazione delle regole di Controllo dispositivi per tutti i computer in Kaspersky Security Center

È possibile creare elenchi di regole di Controllo dispositivi utilizzando le attività di Kaspersky Security Center per tutti i computer e i gruppi di computer della rete aziendale contemporaneamente.

È possibile creare elenchi di regole di Controllo dispositivi in Kaspersky Security Center in due modi:

- Utilizzando l'attività di gruppo Generazione regole per Controllo dispositivi.

In questo scenario, l'attività di gruppo genera elenchi di regole in base ai dati di ogni computer su tutti i dispositivi di archiviazione di massa che sono stati connessi in precedenza ai computer protetti. L'attività

consente inoltre di rilevare tutti i dispositivi di archiviazione di massa che sono connessi al momento dell'esecuzione dell'attività. Dopo il completamento dell'attività di gruppo, Kaspersky Embedded Systems Security 2.2 genera elenchi di regole di permesso per tutti i dispositivi di archiviazione di massa registrati nella rete e salva questi elenchi in un file XML in una cartella specificata. È quindi possibile importare manualmente le regole generate nelle impostazioni del criterio di Controllo dispositivi. A differenza di un'attività in un computer locale, il criterio non consente di configurare l'aggiunta automatica delle regole create all'elenco di regole di Controllo dispositivi quando l'attività di gruppo Generazione regole per Controllo dispositivi viene completata.

Questo scenario è consigliato per generare l'elenco delle regole di permesso prima del primo avvio del criterio di Controllo dispositivi nella modalità di applicazione delle regole attiva.

Prima di utilizzare il criterio Controllo dispositivi, assicurarsi che tutti i computer protetti abbiano accesso a una cartella di rete condivisa. Se il criterio dell'organizzazione non prevede l'utilizzo di una cartella di rete condivisa nella rete, è consigliabile avviare le attività di generazione automatica delle regole per le regole di controllo del computer nel gruppo di computer di prova o in un computer di riferimento.

- In base a un rapporto sugli eventi dell'attività generati in Kaspersky Security Center per l'attività Controllo dispositivi in modalità **Solo statistiche**.

In questo scenario, Kaspersky Embedded Systems Security 2.2 non limita le connessioni dei dispositivi di archiviazione di massa, ma registra le informazioni su tutte le connessioni dei dispositivi di archiviazione di massa in tutti i computer della rete durante l'attività Controllo dispositivi in esecuzione nella modalità **Solo statistiche**. Le informazioni registrate sono disponibili nella sezione **Eventi** di Kaspersky Security Center. Kaspersky Security Center genera l'elenco unificato degli eventi di blocco e di permesso dei dispositivi di archiviazione di massa, in base al log dell'attività.

È necessario configurare il periodo di esecuzione dell'attività in modo che tutte le connessioni dei dispositivi di archiviazione di massa vengano eseguite durante il periodo impostato. Quando vengono aggiunte le regole all'attività Controllo dispositivi, è quindi possibile importare i dati sulle connessioni dei dispositivi dal file del rapporto sugli eventi di Kaspersky Security Center salvato (in formato TXT) e generare le regole di permesso di Controllo dispositivi per tali dispositivi in base a questi dati. Il tipo di eventi su cui è basato un log importato non influisce sul tipo di regole generato: vengono generate solo le regole di permesso.

Questo scenario è consigliato per aggiungere le regole di permesso per numerosi nuovi dispositivi di archiviazione di massa, nonché per generare le regole per i dispositivi mobili attendibili connessi tramite MTP.

- In base ai dati di sistema sui dispositivi di archiviazione di massa connessi (utilizzando l'opzione Genera regole in base ai dati del sistema nelle impostazioni del criterio Controllo dispositivi).

In questo scenario, Kaspersky Embedded Systems Security 2.2 genera le regole di permesso per i dispositivi di archiviazione di massa che sono stati connessi in precedenza o che sono connessi al momento a un computer in cui è installato Kaspersky Security Center.

Questo scenario è consigliato per generare le regole per un numero limitato di nuovi dispositivi di archiviazione di massa da impostare come attendibili in tutti i computer della rete.

- In base ai dati sui dispositivi connessi attualmente (tramite **Genera regole in base ai dispositivi connessi**).

In questo contesto, Kaspersky Embedded Systems Security 2.2 genera regole di permesso solo per i dispositivi connessi attualmente. È possibile selezionare uno o più dispositivi per cui si desidera generare regole di permesso.

Kaspersky Embedded Systems Security 2.2 non ottiene l'accesso ai dati di sistema sui dispositivi mobili connessi tramite MTP. Non è possibile generare le regole di permesso per i dispositivi mobili attendibili connessi tramite MTP utilizzando gli scenari per la compilazione dell'elenco di regole in base ai dati di sistema su tutti i dispositivi connessi.

Generazione delle regole in base ai dati di sistema sui dispositivi esterni connessi ai computer della rete

È possibile generare le regole (vedere la sezione "Informazioni sulla generazione delle regole di Controllo dispositivi per tutti i computer in Kaspersky Security Center" a pagina [191](#)) in base ai dati di Windows su tutti gli archivi di massa che sono stati connessi in precedenza o che sono connessi al momento tramite tre scenari:

- Utilizzando l'attività di gruppo **Generazione regole per Controllo dispositivi**. Utilizzare questo scenario durante il processo di generazione delle regole per tenere conto di tutti i dispositivi di archiviazione di massa connessi in precedenza che sono registrati dai sistemi in tutti i computer della rete.
- Utilizzando l'opzione **Genera regole in base ai dati del sistema** nelle impostazioni del criterio di Controllo dispositivi. Utilizzare questo scenario durante il processo di generazione delle regole per tenere conto di tutti i dispositivi di archiviazione di massa connessi in precedenza che sono registrati dal sistema del computer in cui è installata Kaspersky Security Center Administration Console.
- Utilizzando le impostazioni dell'attività **Genera regole in base ai dispositivi connessi** nel criterio Controllo dispositivi e le impostazioni dell'attività **Generazione regole per Controllo dispositivi**. Utilizzare questo metodo se si desidera tenere in considerazione soltanto i dati sui dispositivi attualmente connessi al computer protetto durante la generazione di regole di permesso.

Kaspersky Embedded Systems Security 2.2 non ottiene l'accesso ai dati di sistema sui dispositivi mobili connessi tramite MTP. Non è possibile generare le regole di permesso per i dispositivi mobili attendibili connessi tramite MTP utilizzando gli scenari per la compilazione dell'elenco di regole in base ai dati di sistema su tutti i dispositivi connessi.

In questa sezione

Creazione delle regole utilizzando l'attività Generazione regole per Controllo dispositivi	193
Creazione delle regole di permesso in base ai dati del sistema in un criterio di Kaspersky Security Center	195
Generazione delle regole per i dispositivi connessi	195

Creazione delle regole utilizzando l'attività **Generazione regole per Controllo dispositivi**

► *Per specificare le regole di permesso per Controllo dispositivi relativamente a un gruppo di computer tramite l'attività **Generazione regole per Controllo dispositivi**, eseguire le seguenti operazioni.*

1. Nella scheda **Attività**, nel pannello di controllo del gruppo di computer che si sta configurando, creare un'attività di gruppo **Generazione regole per Controllo dispositivi** o selezionare un'attività esistente.

2. Nelle proprietà dell'attività di gruppo Generazione regole per Controllo dell'avvio delle applicazioni creata o nella procedura guidata dell'attività specificare le seguenti impostazioni:
 - Nella sezione **Notifiche** configurare le impostazioni per il salvataggio del rapporto sull'esecuzione dell'attività.
 - Nella sezione **Impostazioni** specificare le operazioni dell'attività dopo il completamento. Specificare il nome del file in cui saranno esportate le regole generate.
 - Nella sezione **Pianificazione** configurare le impostazioni di pianificazione dell'avvio dell'attività.
3. Nella scheda **Attività**, nel pannello di controllo del gruppo di computer configurati, selezionare nell'elenco delle attività di gruppo l'attività Generazione regole per Controllo dispositivi creata e fare clic sul pulsante **Avvia** per avviare l'attività.

Una volta completata l'attività, gli elenchi di regole di permesso generati automaticamente verranno salvati in file XML in una cartella di rete condivisa.

Prima di utilizzare il criterio Controllo dispositivi, assicurarsi che tutti i computer protetti abbiano accesso a una cartella di rete condivisa. Se il criterio dell'organizzazione non prevede l'utilizzo di una cartella di rete condivisa nella rete, è consigliabile avviare le attività di generazione automatica delle regole per le regole di controllo del computer nel gruppo di computer di prova o in un computer di riferimento.

4. Aggiungere gli elenchi di regole di permesso generati all'attività Controllo dispositivi. A tale scopo, nelle proprietà del criterio configurato, nelle impostazioni dell'attività Controllo dispositivi:
 - a. Nella scheda **Generale** fare clic sul pulsante **Elenco di regole**.
Verrà visualizzata la finestra **Regole di Controllo dispositivi**.
 - b. Fare clic sul pulsante **Aggiungi** e nell'elenco visualizzato selezionare **Importa regole da file XML**.
 - c. Selezionare il principio per l'aggiunta delle regole di permesso generate automaticamente all'elenco delle regole di Controllo dispositivi create in precedenza:
 - **Aggiungi alle regole esistenti** se si desidera aggiungere le regole importate all'elenco di quelle esistenti. Le regole con impostazioni identiche vengono duplicate.
 - **Sostituisci le regole esistenti** se si desidera sostituire le regole esistenti con quelle importate.
 - **Unisci con le regole esistenti** se si desidera aggiungere le regole importate all'elenco di quelle esistenti. Le regole con impostazioni identiche non vengono aggiunte: la regola viene aggiunta se almeno un parametro della regola è univoco.
 - d. Nella finestra standard di Microsoft Windows visualizzata selezionare i file XML creati dopo il completamento dell'attività di gruppo Generazione regole per Controllo dispositivi.
 - e. Fare clic su **OK** nelle finestre Regole di Controllo dispositivi e **Impostazioni attività**.
5. Se si desidera applicare le regole di Controllo dispositivi generate, selezionare la modalità dell'attività **Attivo** nelle impostazioni del criterio di **Controllo dispositivi**.

Le regole di permesso generate automaticamente in base ai dati di sistema in ogni computer verranno applicate a tutti i computer della rete a cui si applica il criterio configurato. In questi computer sarà consentito connettere solo quei dispositivi per cui sono state create regole di permesso.

Creazione delle regole di permesso in base ai dati del sistema in un criterio di Kaspersky Security Center

► Per specificare le regole di permesso utilizzando l'opzione **Genera regole in base ai dati del sistema** nel criterio di **Controllo dispositivi**, eseguire le seguenti operazioni:

1. Se necessario, connettere un nuovo dispositivo di archiviazione di massa da impostare come attendibile a un computer in cui è installata Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console espandere il nodo **Dispositivi gestiti**.
3. Espandere il gruppo di amministrazione per cui si desidera configurare le impostazioni del criterio e selezionare la scheda **Criteri** nel riquadro dei dettagli.
4. Selezionare **Proprietà** nel menu di scelta rapida del criterio da configurare.
5. Verrà visualizzata la finestra **Proprietà: <nome criterio>**.
6. Nelle impostazioni del criterio aprire le impostazioni dell'attività **Controllo dispositivi** ed eseguire le seguenti operazioni:
 - a. Nella scheda **Generale** fare clic sul pulsante **Elenco di regole**.
Verrà visualizzata la finestra **Regole di Controllo dispositivi**.
 - b. Fare clic sul pulsante **Aggiungi** e nel menu di scelta rapida visualizzato selezionare l'opzione **Genera regole in base ai dati del sistema**.
 - c. Selezionare il principio per l'aggiunta delle regole di permesso all'elenco delle regole di **Controllo dispositivi** create in precedenza:
 - **Aggiungi alle regole esistenti** se si desidera aggiungere le regole importate all'elenco di quelle esistenti. Le regole con impostazioni identiche vengono duplicate.
 - **Sostituisci le regole esistenti** se si desidera sostituire le regole esistenti con quelle importate.
 - **Unisci con le regole esistenti** se si desidera aggiungere le regole importate all'elenco di quelle esistenti. Le regole con impostazioni identiche non vengono aggiunte: la regola viene aggiunta se almeno un parametro della regola è univoco.
7. Fare clic su **OK** nelle finestre **Regole di Controllo dispositivi** e **Impostazioni attività**.

L'elenco di regole nel criterio di **Controllo dispositivi** verrà compilato con le nuove regole generate in base ai dati di sistema del computer in cui è installata Kaspersky Security Center Administration Console.

Generazione delle regole per i dispositivi connessi

► Per specificare le regole di permesso utilizzando l'opzione **Genera regole in base ai dati del sistema** nel criterio di **Controllo dispositivi**, eseguire le seguenti operazioni:

1. In Kaspersky Security Center Administration Console espandere il nodo **Dispositivi gestiti**.
2. Espandere il gruppo di amministrazione per cui si desidera configurare le impostazioni del criterio e selezionare la scheda **Criteri** nel riquadro dei dettagli.
3. Selezionare **Proprietà** nel menu di scelta rapida del criterio da configurare.
4. Verrà visualizzata la finestra **Proprietà: <nome criterio>**.
5. Nella sezione **Controllo attività locali** fare clic sul pulsante **Impostazioni** nella sezione

Controllo dispositivi.

6. Nella scheda **Generale** fare clic sul pulsante **Elenco di regole**.
Verrà visualizzata la finestra **Regole di Controllo dispositivi**.
7. Fare clic sul pulsante **Aggiungi** e nel menu di scelta rapida selezionare **Genera regole in base ai dispositivi connessi**.
Verrà visualizzata la finestra **Genera regole in base ai dati del sistema**.
8. Nell'elenco dei dispositivi rilevati connessi al computer protetto, selezionare i dispositivi per cui si desidera generare regole di permesso.
9. Fare clic sul pulsante **Aggiungi regole per i dispositivi selezionati**.
10. Fare clic sul pulsante **Salva** nella finestra **Controllo dispositivi**.

L'elenco di regole nel criterio di Controllo dispositivi verrà compilato con le nuove regole generate in base ai dati di sistema del computer in cui è installata Kaspersky Security Center Administration Console.

Importazione delle regole dal file di un rapporto sui dispositivi bloccati di Kaspersky Security Center

È possibile importare i dati sulle connessioni dei dispositivi limitate dal rapporto generato in Kaspersky Security Center dopo il completamento dell'attività Controllo dispositivi nella modalità **Solo statistiche** e utilizzare questi dati per generare un elenco di regole di permesso di Controllo dispositivi nel criterio configurato.

Quando si genera il rapporto sugli eventi che si verificano durante un'attività Controllo dispositivi, è possibile tenere traccia dei dispositivi di cui viene limitata la connessione.

Al momento dell'importazione dei dati dal rapporto sui dispositivi con limitazioni nelle impostazioni del criterio, verificare che l'elenco in uso contenga solo i dispositivi per cui si desidera consentire la connessione.

- *Per specificare le regole di permesso per la connessione dei dispositivi per un gruppo di computer in base al rapporto di Kaspersky Security Center sui dispositivi limitati, eseguire le seguenti operazioni:*
 1. Nelle proprietà del criterio, nelle impostazioni dell'attività Controllo dispositivi, selezionare la modalità **Solo statistiche**.
 2. Nelle proprietà del criterio, nella sezione **Eventi**, verificare che:
 - La scheda **Eventi critici** dell'evento *Archiviazione di massa limitata* mostri un tempo di archiviazione degli eventi superiore al tempo pianificato di esecuzione dell'attività nella modalità **Solo statistiche** (il valore predefinito è 30 giorni).

- La scheda **Avviso** dell'evento *Solo statistiche: archiviazione di massa non attendibile rilevata* mostri un tempo di archiviazione degli eventi superiore al tempo pianificato di esecuzione dell'attività nella modalità **Solo statistiche** (il valore predefinito è 30 giorni).

Al termine del periodo specificato nella colonna **Tempo di archiviazione**, le informazioni sugli eventi registrati vengono eliminate e non sono riportate nel file del rapporto. Prima di eseguire l'attività **Controllo dispositivi** nella modalità **Solo statistiche**, verificare che il tempo di esecuzione dell'attività non superi il tempo di archiviazione configurato per gli eventi specificati.

3. Una volta completata l'attività, esportare gli eventi registrati in un file TXT. A tale scopo, espandere il nodo **Log e notifiche** e nel nodo figlio **Eventi** creare una selezione di eventi in base al criterio *Negato* per visualizzare i dispositivi di cui sarà limitata la connessione dall'attività **Controllo dispositivi**. Nel riquadro dei dettagli della selezione fare clic sull'elenco **Esporta eventi in un file** per salvare il rapporto sugli avvii delle applicazioni bloccati in un file TXT.

Prima di importare e applicare il rapporto generato in un criterio, verificare che il rapporto contenga dati solo sui dispositivi di cui si desidera consentire la connessione.

4. Importare i dati sulle connessioni dei dispositivi limitate nel criterio di **Controllo dispositivi**. A tale scopo, nelle proprietà del criterio configurato, nelle impostazioni dell'attività **Controllo dispositivi**, eseguire le seguenti operazioni:
 - a. Nella scheda **Generale** fare clic sul pulsante **Elenco di regole**.
Verrà visualizzata la finestra **Regole di Controllo dispositivi**.
 - b. Fare clic sul pulsante **Aggiungi** e nel menu di scelta rapida del pulsante selezionare **Importa i dati dei dispositivi bloccati dal report di Kaspersky Security Center**.
 - c. Selezionare il principio per l'aggiunta delle regole dall'elenco creato in base al rapporto di Kaspersky Security Center all'elenco delle regole di **Controllo dispositivi** configurate in precedenza:
 - **Aggiungi alle regole esistenti** se si desidera aggiungere le regole importate all'elenco di quelle esistenti. Le regole con impostazioni identiche vengono duplicate.
 - **Sostituisci le regole esistenti** se si desidera sostituire le regole esistenti con quelle importate.
 - **Unisci con le regole esistenti** se si desidera aggiungere le regole importate all'elenco di quelle esistenti. Le regole con impostazioni identiche non vengono aggiunte: la regola viene aggiunta se almeno un parametro della regola è univoco.
 - d. Nella finestra standard di Microsoft Windows visualizzata selezionare il file TXT in cui sono stati esportati gli eventi dal rapporto sui dispositivi limitati.
 - e. Fare clic su **OK** nelle finestre **Regole di Controllo dispositivi** e **Impostazioni attività**.

Le regole create in base al rapporto di Kaspersky Security Center sui dispositivi limitati verranno aggiunte all'elenco delle regole di **Controllo dispositivi**.

Controllo attività di rete

Questa sezione contiene informazioni sull'attività Gestione firewall.

Gestione firewall

Questa sezione contiene informazioni sull'attività Gestione firewall e su come configurarla.

In questa sezione

Informazioni sull'attività Gestione firewall	198
Informazioni sulle regole del firewall	199
Attivazione e disattivazione delle regole del firewall	200
Aggiunta manuale delle regole del firewall	201
Eliminazione delle regole del firewall	203

Informazioni sull'attività Gestione firewall

Kaspersky Embedded Systems Security 2.2 offre una soluzione affidabile ed ergonomica per la protezione delle connessioni di rete tramite l'attività Gestione firewall.

L'attività Gestione firewall non esegue il filtro del traffico di rete indipendente, ma consente di gestire Windows Firewall tramite l'interfaccia grafica di Kaspersky Embedded Systems Security 2.2. Durante l'attività Gestione firewall, Kaspersky Embedded Systems Security 2.2 assume il controllo della gestione delle impostazioni e dei criteri del firewall del sistema operativo e blocca tutte le possibilità di configurazione di un firewall esterno.

Durante l'installazione dell'applicazione, il componente Gestione firewall legge e copia lo stato di Windows Firewall e tutte le regole specificate. Successivamente, il set di regole e i parametri delle regole possono solo essere modificati, mentre il firewall può solo essere attivato o disattivato in Kaspersky Embedded Systems Security 2.2.

Se Windows Firewall è disattivato durante l'installazione di Kaspersky Embedded Systems Security 2.2, l'attività Gestione firewall non sarà eseguita dopo il completamento dell'installazione. Se Windows Firewall è attivato durante l'installazione dell'applicazione, l'attività Gestione firewall verrà eseguita dopo il completamento dell'installazione, bloccando tutte le connessioni di rete che non sono consentite dalle regole specificate.

Il componente Gestione firewall non è installato per impostazione predefinita, poiché non è incluso nel set di componenti per l'installazione consigliata.

L'attività Gestione firewall impone il blocco di tutte le connessioni in entrata e in uscita non consentite dalle regole specificate dell'attività.

L'attività esegue regolarmente il polling di Windows Firewall e ne monitora lo stato. Per impostazione predefinita, l'intervallo di polling è impostato su 1 minuto e non può essere modificato. Se durante il polling Kaspersky

Embedded Systems Security 2.2 rileva una mancata corrispondenza tra le impostazioni di Windows Firewall e le impostazioni dell'attività Gestione firewall, l'applicazione applica forzatamente le impostazioni dell'attività nel firewall del sistema operativo.

Con il polling in tempo reale di Windows Firewall, Kaspersky Embedded Systems Security 2.2 monitora quanto segue:

- Stato operativo di Windows Firewall.
- Stato delle regole aggiunte dopo l'installazione di Kaspersky Embedded Systems Security 2.2 da parte di altri strumenti o applicazioni (ad esempio, l'aggiunta di una nuova regola dell'applicazione per una porta o applicazione con wf.msc).

Durante l'applicazione delle nuove regole a Windows Firewall, Kaspersky Embedded Systems Security 2.2 crea un set di regole di gruppo Kaspersky Security nello snap-in **Windows Firewall**. Questo set di regole unisce tutte le regole create da Kaspersky Embedded Systems Security 2.2 tramite l'attività Gestione firewall. Le regole di gruppo Kaspersky Security non sono monitorate dall'applicazione durante il polling in tempo reale e non vengono automaticamente sincronizzate con l'elenco di regole specificate nelle impostazioni dell'attività Gestione firewall.

► *Per aggiornare le regole di gruppo Kaspersky Security manualmente:*

Riavviare l'attività Gestione firewall di Kaspersky Embedded Systems Security 2.2.

È inoltre possibile modificare le regole di gruppo Kaspersky Security manualmente tramite lo snap-in **Gestione firewall**.

Se Windows Firewall è gestito dal criterio di gruppo di Kaspersky Security Center, l'attività Gestione firewall non può essere avviata.

Informazioni sulle regole del firewall

L'attività Gestione firewall controlla il filtro del traffico di rete in entrata e in uscita tramite le regole di permesso applicate forzatamente a Windows Firewall durante l'esecuzione dell'attività.

Al primo avvio dell'attività, Kaspersky Embedded Systems Security 2.2 legge e copia tutte le regole del traffico di rete in entrata specificate nelle impostazioni di Windows Firewall nelle impostazioni dell'attività Gestione firewall. A questo punto l'applicazione viene seguita in base alle regole seguenti:

- Se viene creata una nuova regola nelle impostazioni di Windows Firewall (manualmente o automaticamente durante l'installazione di una nuova applicazione), Kaspersky Embedded Systems Security 2.2 elimina la regola.
- Se una regola esistente viene eliminata dalle impostazioni di Windows Firewall, Kaspersky Embedded Systems Security 2.2 ripristina la regola.
- Se i parametri di una regola esistente vengono modificati nelle impostazioni di Windows Firewall, Kaspersky Embedded Systems Security 2.2 esegue il rollback delle modifiche.
- Se viene creata una nuova regola nelle impostazioni di Gestione firewall, Kaspersky Embedded Systems Security 2.2 applica forzatamente la regola a Windows Firewall.
- Se una regola esistente viene eliminata dalle impostazioni di Gestione firewall, Kaspersky Embedded Systems Security 2.2 elimina forzatamente la regola delle impostazioni di Windows Firewall.

Kaspersky Embedded Systems Security 2.2 non funziona con le regole di blocco o con le regole che controllano il traffico di rete in uscita. All'avvio dell'attività Gestione firewall, Kaspersky Embedded Systems Security 2.2 elimina tutte le regole simili dalle impostazioni di Windows Firewall.

È possibile impostare, eliminare e modificare le regole di filtro per il traffico di rete in entrata.

Non è possibile specificare una nuova regola per controllare il traffico di rete in uscita nelle impostazioni dell'attività Gestione firewall. Tutte le regole del firewall specificate in Kaspersky Embedded Systems Security 2.2 controllano solo il traffico di rete in entrata.

È possibile gestire i seguenti tipi di regole del firewall:

- Regole delle applicazioni.
- Regole delle porte.

Regole delle applicazioni

Questo tipo di regola consente le connessioni di rete mirate per applicazioni specifiche. Il criterio di attivazione per queste regole si basa sul percorso di un file eseguibile.

È possibile gestire le regole delle applicazioni in modo da:

- Aggiungere nuove regole.
- Rimuovere regole esistenti.
- Abilitare o disabilitare regole specificate.
- Modificare i parametri delle regole specificate: specificare il nome della regola, il percorso del file eseguibile e l'area di applicazione delle regole.

Regole delle porte

Questo tipo di regola consente le connessioni di rete per determinate porte e protocolli (TCP/UDP). I criteri di attivazione per queste regole si basano sul numero di porta e sul tipo di protocollo.

È possibile gestire le regole delle porte in modo da:

- Aggiungere nuove regole.
- Rimuovere regole esistenti.
- Abilitare o disabilitare regole specificate.
- Modificare i parametri delle regole specificate: impostare il nome della regola, il numero di porta, il tipo di protocollo e l'ambito per l'applicazione della regola.

Le regole delle porte hanno un ambito più ampio rispetto alle regole delle applicazioni. Consentendo le connessioni in base alle regole delle porte, si riduce il livello di sicurezza del computer protetto.

Attivazione e disattivazione delle regole del firewall

- Per attivare o disattivare una regola esistente per il filtro del traffico di rete in entrata, procedere

come segue:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Controllo attività di rete** fare clic sul pulsante **Impostazioni** nel gruppo **Gestione firewall**.
4. Fare clic sul pulsante **Elenco di regole** nella finestra visualizzata.
Verrà visualizzata la finestra **Elenco di regole**.
5. In base al tipo della regola per cui si desidera modificare lo stato, selezionare **Applicazioni** o **Porte**.
6. Nell'elenco di regole selezionare la regola per cui si desidera modificare lo stato e procedere come segue:
 - Se si desidera abilitare una regola disabilitata, selezionare la casella di controllo a sinistra del nome della regola.
La regola selezionata viene abilitata.
 - Se si desidera disabilitare una regola abilitata, deselegionare la casella di controllo a sinistra del nome della regola.
La regola selezionata viene disabilitata.
7. Fare clic su **Salva** nella finestra **Elenco di regole**.
Le impostazioni dell'attività specificate vengono salvate. I nuovi parametri della regola verranno inviati a Windows Firewall.

Aggiunta manuale delle regole del firewall

È possibile soltanto aggiungere e modificare le regole per applicazioni e porte. Non è possibile aggiungere nuove regole di gruppo o modificare regole di gruppo esistenti.

- *Per aggiungere una nuova regola o modificare una regola esistente per il filtro del traffico di rete in entrata, procedere come segue:*
1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
 2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda

Criteri e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).

- Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Controllo attività di rete** fare clic sul pulsante **Impostazioni** nel gruppo **Gestione firewall**.
4. Fare clic sul pulsante **Elenco di regole** nella finestra visualizzata.
Verrà visualizzata la finestra **Elenco di regole**.

5. A seconda del tipo di regola che si desidera aggiungere, selezionare la scheda **Applicazioni** o **Porte** e procedere come segue:
 - Per modificare una regola esistente, selezionare la regola che si desidera modificare nell'elenco di regole e fare clic su **Modifica**.

- Per aggiungere una nuova regola, fare clic su **Aggiungi**.

A seconda del tipo di regola configurata, verrà visualizzata la finestra **Regola porta** o **Regola applicazione**.

6. Nella finestra visualizzata eseguire le seguenti operazioni:
 - Se si utilizza una regola dell'applicazione, procedere come segue:
 - a. Immettere il **Nome regola** della regola modificata.
 - b. Specificare il **Percorso applicazione** del file eseguibile dell'applicazione per cui si consente una connessione modificando questa regola.
È possibile impostare il percorso manualmente o utilizzando il pulsante **Sfoggia**.
 - c. Nel campo **Ambito di applicazione della regola** specificare gli indirizzi di rete per cui verrà applicata la regola modificata.

È possibile utilizzare solo indirizzi IP IPv4.

- Se si utilizza una regola della porta, procedere come segue:
 - a. Immettere il **Nome regola** della regola modificata.
 - b. Specificare il **Numero di porta** per cui l'applicazione consentirà le connessioni.
 - c. Selezionare il tipo di protocollo (TCP/UDP) per cui l'applicazione consentirà le connessioni.
 - d. Nel campo **Ambito di applicazione della regola** specificare gli indirizzi di rete per cui verrà applicata la regola modificata.

È possibile utilizzare solo indirizzi IP IPv4.

7. Fare clic su **OK** nella finestra **Regola applicazione** o **Regola porta**.

8. Fare clic su **Salva** nella finestra **Regole firewall**.

Le impostazioni dell'attività specificate vengono salvate. I nuovi parametri della regola verranno inviati a Windows Firewall.

Eliminazione delle regole del firewall

È possibile eliminare soltanto le regole delle applicazioni e le regole delle porte. Non è possibile eliminare le regole di gruppo esistenti.

► Per eliminare una regola esistente per il filtro del traffico di rete in entrata, procedere come segue:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Controllo attività di rete** fare clic sul pulsante **Impostazioni** nel gruppo **Gestione firewall**.
4. Fare clic sul pulsante **Elenco di regole** nella finestra visualizzata.
Verrà visualizzata la finestra **Elenco di regole**.
5. In base al tipo della regola per cui si desidera modificare lo stato, selezionare la scheda **Applicazioni** o **Porte**.
6. Nell'elenco di regole selezionare la regola che si desidera eliminare.
7. Fare clic sul pulsante **Rimuovi**.
La regola selezionata viene eliminata.
8. Fare clic su **Salva** nella finestra **Regole firewall**.

Le impostazioni dell'attività Gestione firewall specificate vengono salvate. I nuovi parametri della regola verranno inviati a Windows Firewall.

Analisi sistema

Questa sezione contiene informazioni sull'attività Monitoraggio integrità file e sulle funzionalità per l'analisi del log del sistema operativo.

In questo capitolo

Monitoraggio integrità file.....	204
Analisi log.....	212

Monitoraggio integrità file

Questa sezione contiene informazioni sull'avvio e la configurazione dell'attività Monitoraggio integrità file.

In questa sezione

Informazioni sull'attività Monitoraggio integrità file	204
Informazioni sulle regole di monitoraggio operazioni file.....	205
Configurazione dell'attività Monitoraggio integrità file	207
Configurazione delle regole di monitoraggio	209

Informazioni sull'attività Monitoraggio integrità file

L'attività Monitoraggio integrità file consente di tenere traccia delle azioni eseguite con i file e le cartelle specificati negli ambiti del monitoraggio definiti nelle impostazioni dell'attività. È possibile utilizzare l'attività per rilevare modifiche nei file che possono indicare una violazione di sicurezza nel computer protetto. È inoltre possibile configurare il tracciamento delle modifiche nei file durante i periodi in cui il monitoraggio è interrotto.

Un'*interruzione del monitoraggio* si verifica quando l'ambito del monitoraggio si discosta temporaneamente dall'ambito dell'attività, ad esempio se l'attività viene arrestata o se un dispositivo protetto non è fisicamente presente in un computer protetto. Kaspersky Embedded Systems Security 2.2 segnala le operazioni file rilevate nell'ambito del monitoraggio non appena viene riconnesso un dispositivo di archiviazione di massa.

Se l'esecuzione dell'attività si interrompe nell'ambito del monitoraggio specificato a causa di una reinstallazione del componente di Monitoraggio integrità file, non si tratta di interruzione del monitoraggio. In questo caso, l'attività Monitoraggio integrità file non viene eseguita.

Requisiti relativi all'ambiente

Per avviare l'attività Monitoraggio integrità file, devono essere soddisfatte le seguenti condizioni:

- Nel computer protetto deve essere installato un dispositivo di archiviazione che supporti i file system ReFS e NTFS.
- Deve essere abilitato il journal USN di Windows. Il componente esegue query nel journal per ricevere informazioni sulle operazioni file.

Se il journal USN viene abilitato in seguito alla creazione di una regola per un volume e all'avvio dell'attività Monitoraggio integrità file, l'attività deve essere riavviata. In caso contrario, la regola non verrà applicata durante il monitoraggio.

Ambiti del monitoraggio esclusi

È possibile creare esclusioni per l'ambito del monitoraggio (vedere la sezione "Configurazione delle regole di monitoraggio" a pagina [209](#)). Le esclusioni vengono specificate per ogni singola regola e si applicano solo all'ambito del monitoraggio indicato. È possibile specificare un numero illimitato di esclusioni per ogni regola.

Le esclusioni hanno una priorità più elevata rispetto all'ambito del monitoraggio e non sono monitorate dall'attività, anche se una cartella indicata o un file indicato rientra nell'ambito del monitoraggio. Se le impostazioni per una delle regole specificano un ambito del monitoraggio a un livello inferiore rispetto a una cartella specificata nelle esclusioni, l'ambito del monitoraggio non viene preso in considerazione durante l'esecuzione delle attività.

Per specificare le esclusioni, è possibile utilizzare le stesse maschere utilizzate per specificare gli ambiti del monitoraggio.

Informazioni sulle regole di monitoraggio operazioni file

L'attività Monitoraggio integrità file viene eseguita in base alle regole di monitoraggio operazioni file. È possibile utilizzare i criteri di attivazione della regola per configurare le condizioni che fungono da trigger per l'attività e modificare il livello di importanza degli eventi per le operazioni file rilevate e registrate nel log delle attività.

È specificata una regola di monitoraggio operazioni file per ciascun ambito del monitoraggio.

È possibile configurare i seguenti criteri di attivazione della regola:

- Utenti attendibili.
- Indicatori operazioni file.

Utenti attendibili

Per impostazione predefinita, l'applicazione considera tutte le azioni dell'utente potenziali violazioni della sicurezza. L'elenco degli utenti attendibili è vuoto. È possibile configurare il livello di importanza degli eventi creando un elenco di utenti attendibili nelle impostazioni della regola di monitoraggio operazioni file.

Utente non attendibile: qualsiasi utente non indicato nell'elenco degli utenti attendibili nelle impostazioni delle regole dell'ambito del monitoraggio. Se Kaspersky Embedded Systems Security 2.2 rileva un'operazione file eseguita da un utente non attendibile, l'attività Monitoraggio integrità file registra un Evento critico nel log delle attività.

Utente attendibile: un utente o un gruppo di utenti hanno autorizzato a eseguire operazioni file nell'ambito del monitoraggio specificato. Se Kaspersky Embedded Systems Security 2.2 rileva operazioni file eseguite da un utente attendibile, l'attività Monitoraggio integrità file registra un Evento informativo nel log delle attività.

Kaspersky Embedded Systems Security 2.2 non è in grado di determinare gli utenti che avviano operazioni durante i periodi di interruzione monitoraggio. In questo caso, lo stato dell'utente viene considerato sconosciuto.

Utente sconosciuto: questo stato viene assegnato a un utente se Kaspersky Embedded Systems Security 2.2 non è in grado di ricevere informazioni su un utente a causa di un'interruzione dell'attività o di un errore del driver di sincronizzazione dei dati o del journal USN. Se Kaspersky Embedded Systems Security 2.2 rileva un'operazione file eseguita da un utente sconosciuto, l'attività Monitoraggio integrità file registra un Avviso nel log delle attività.

Indicatori operazioni file

Durante l'esecuzione dell'attività Monitoraggio integrità file, Kaspersky Embedded Systems Security 2.2 utilizza gli indicatori operazioni file per stabilire se un'azione è stata eseguita su un file.

Un indicatore operazioni file è un descrittore univoco che può caratterizzare un'operazione file.

Ogni operazione file può essere un'azione singola o una catena di azioni relative ai file. A ogni azione di questo tipo corrisponde un indicatore operazioni file. Se l'indicatore specificato come criterio di attivazione della regola viene rilevato in una catena di operazioni file, l'applicazione registra un evento che indica che l'operazione file in questione è stata eseguita.

Il livello di importanza degli eventi registrati non dipende dagli indicatori operazioni file selezionati o dal numero di eventi.

Per impostazione predefinita, Kaspersky Embedded Systems Security 2.2 prende in considerazione tutti gli indicatori operazioni file disponibili. È possibile selezionare gli indicatori operazioni file manualmente nelle impostazioni della regola dell'attività.

Tabella 36. Indicatori operazioni file

ID operazione file	Indicatore operazioni file	File system supportati
BASIC_INFO_CHANGE	Attributi o indicatori temporali di un file o di una cartella modificati	NTFS, ReFS
COMPRESSION_CHANGE	Compressione di un file o di una cartella modificata	NTFS, ReFS
DATA_EXTEND	Dimensioni del file o della cartella incrementate	NTFS, ReFS
DATA_OVERWRITE	I dati in un file o in una cartella sono stati sovrascritti	NTFS, ReFS
DATA_TRUNCATION	File o cartella troncato	NTFS, ReFS
EA_CHANGE	Attributi file o cartella estesi modificati	Solo NTFS
ENCRYPTION_CHANGE	Stato criptaggio di un file o di una cartella modificato	NTFS, ReFS
FILE_CREATE	File o cartella creato per la prima volta	NTFS, ReFS

ID operazione file	Indicatore operazioni file	File system supportati
FILE_DELETE	File o cartella eliminato definitivamente tramite la combinazione MAIUSC+CANC	NTFS, ReFS
HARD_LINK_CHANGE	Collegamento reale creato o eliminato per un file o una cartella	Solo NTFS
INDEXABLE_CHANGE	Stato di indicizzazione di un file o di una cartella modificato	NTFS, ReFS
INTEGRITY_CHANGE	Attributo di integrità modificato per un flusso di file denominato	Solo ReFS
NAMED_DATA_EXTEND	Dimensioni di un flusso di file denominato incrementate	NTFS, ReFS
NAMED_DATA_OVERWRITE	Flusso di file denominato sovrascritto	NTFS, ReFS
NAMED_DATA_TRUNCATION	Flusso di file denominato troncato	NTFS, ReFS
OBJECT_ID_CHANGE	Identificatore file o cartella modificato	NTFS, ReFS
RENAME_NEW_NAME	Nuovo nome assegnato a un file o a una cartella	NTFS, ReFS
REPARSE_POINT_CHANGE	Nuovo reparse point creato o reparse point esistente modificato per un file o una cartella	NTFS, ReFS
SECURITY_CHANGE	Diritti di accesso per un file o una cartella modificati	NTFS, ReFS
STREAM_CHANGE	Nuovo flusso di file denominato creato o flusso di file denominato esistente modificato	NTFS, ReFS
TRANSACTION_CHANGE	Flusso di file denominato modificato tramite transazione TxF	Solo ReFS

Configurazione dell'attività Monitoraggio integrità file

È possibile modificare le impostazioni predefinite dell'attività Monitoraggio integrità file (vedere la seguente tabella).

Tabella 37. Impostazioni predefinite dell'attività Monitoraggio integrità file

Impostazione	Valore predefinito	Descrizione
Ambito del monitoraggio	Non configurata	È possibile specificare le cartelle e i file per cui verranno monitorate le azioni. Verranno generati eventi di monitoraggio per le cartelle e i file nell'ambito del monitoraggio specificato.
Elenco Utenti attendibili	Non configurata	È possibile specificare utenti e/o gruppi di utenti le cui azioni nelle directory specificate saranno considerate sicure dal componente.

Impostazione	Valore predefinito	Descrizione
Monitora operazioni file quando l'attività non è in esecuzione	Utilizzati	È possibile abilitare o disabilitare la registrazione delle operazioni file eseguite negli ambiti del monitoraggio indicati durante i periodi in cui l'attività non è in esecuzione.
Tieni conto dell'ambito del monitoraggio escluso	Non applicato	È possibile controllare l'utilizzo delle esclusioni per le cartelle in cui non è necessario monitorare le operazioni file. Durante l'esecuzione dell'attività Monitoraggio integrità file, Kaspersky Embedded Systems Security 2.2 ignorerà gli ambiti del monitoraggio specificati come esclusioni.
Calcolo checksum	Non applicato	È possibile configurare il calcolo del checksum del file dopo avere apportato le modifiche nel file.
Tieni conto degli indicatori operazioni file	Vengono tenuti in considerazione tutti gli indicatori operazioni file disponibili	È possibile specificare il set di indicatori operazioni file. Se un'operazione file eseguita in un ambito del monitoraggio è caratterizzata da uno o più indicatori specificati, Kaspersky Embedded Systems Security 2.2 genera un evento di audit.
Pianificazione dell'avvio dell'attività	La prima esecuzione non è pianificata	È possibile configurare le impostazioni per l'avvio pianificato dell'attività.

► Per configurare le impostazioni generali dell'attività Monitoraggio integrità file, eseguire le seguenti operazioni:

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nel gruppo **Monitoraggio integrità file** della sezione **Analisi sistema** fare clic sul pulsante **Impostazioni**. Verrà visualizzata la finestra **Monitoraggio integrità file**.

4. Nella scheda **Impostazioni di monitoraggio delle operazioni file** della finestra visualizzata configurare le impostazioni dell'ambito del monitoraggio:
 - a. Selezionare o deselezionare la casella di controllo **Registra informazioni sulle operazioni file visualizzate durante il periodo di interruzione del monitoraggio**.

La casella di controllo consente di abilitare o disabilitare il monitoraggio delle operazioni file specificate nelle impostazioni dell'attività Monitoraggio integrità file quando l'attività non viene eseguita per qualche motivo (rimozione di un disco rigido, attività interrotta dall'utente, errore software).

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 registrerà gli eventi in tutti gli ambiti del monitoraggio quando l'attività Monitoraggio integrità file non è in esecuzione.

Se la casella di controllo è deselezionata, l'applicazione non registrerà le operazioni file negli ambiti del monitoraggio quando l'attività non è in esecuzione.

La casella di controllo è selezionata per impostazione predefinita.
 - b. Aggiungere gli ambiti del monitoraggio (vedere la sezione "Configurazione delle regole di monitoraggio" a pagina [209](#)) che devono essere monitorati dall'attività.
5. Nella scheda **Gestione attività** avviare l'attività in base a una pianificazione (vedere la sezione "Gestione delle pianificazioni delle attività" a pagina [119](#)).
6. Fare clic su **OK** per salvare le modifiche.

Configurazione delle regole di monitoraggio

Per impostazione predefinita non è specificato alcun ambito del monitoraggio e l'attività non monitora le operazioni file in alcuna directory.

► *Per aggiungere un ambito del monitoraggio, eseguire le seguenti operazioni:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina 88).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nel gruppo **Monitoraggio integrità file** della sezione **Analisi sistema** fare clic sul pulsante **Impostazioni**. Verrà visualizzata la finestra **Proprietà: Monitoraggio integrità file**.
4. Nella sezione **Ambito del monitoraggio** fare clic sul pulsante **Aggiungi**. Verrà visualizzata la finestra **Ambito del monitoraggio**.

5. Aggiungere un ambito del monitoraggio in uno dei seguenti modi:
 - Se si desidera selezionare cartelle tramite la finestra di dialogo standard di Microsoft Windows:
 - a. Fare clic sul pulsante **Sfoglia**.
Verrà visualizzata la finestra standard di Microsoft Windows Cerca cartella.
 - b. Nella finestra visualizzata selezionare la cartella per cui si desidera monitorare le operazioni e fare clic sul pulsante **OK**.
 - Se si desidera specificare un ambito del monitoraggio manualmente, aggiungere un percorso utilizzando una maschera supportata:
 - `<*.ext>` - tutti i file con estensione `<ext>`, indipendentemente dalla posizione;
 - `<*\name.ext>` - tutti i file con nome `<name>` ed estensione `<ext>`, indipendentemente dalla posizione;
 - `<\dir*>` - tutti i file nella directory `<\dir>`;
 - `<\dir*\name.ext>` - tutti i file con nome `<name>` ed estensione `<ext>` nella directory `<\dir>` e in tutte le sottodirectory.

Quando viene specificato un ambito del monitoraggio manualmente, accertarsi che il percorso sia nel formato seguente: `<lettera di unità>:\<mask>`. Se la lettera di unità non è presente, Kaspersky Embedded Systems Security 2.2 non aggiungerà l'ambito del monitoraggio specificato.

6. Nella scheda **Utenti attendibili** fare clic sul pulsante **Aggiungi**.
Verrà visualizzata la finestra standard **Seleziona utenti o gruppi** di Microsoft Windows.
7. Selezionare gli utenti o i gruppi di utenti per cui le operazioni file sono consentite nell'ambito del monitoraggio selezionato e fare clic sul pulsante **OK**.

Per impostazione predefinita, Kaspersky Embedded Systems Security 2.2 considera non attendibili tutti gli utenti non presenti nell'elenco degli utenti attendibili (vedere la sezione "Informazioni sulle regole di monitoraggio operazioni file" a pagina [205](#)) e genera Eventi critici per tali utenti.

8. Selezionare la scheda **Indicatori operazioni file**.
9. Se richiesto, eseguire le azioni seguenti per selezionare una serie di indicatori:
 - a. Selezionare l'opzione **Individua operazioni file che si basano sui seguenti indicatori**.
 - b. Nell'elenco delle operazioni file disponibili (vedere la sezione "Informazioni sulle regole di monitoraggio operazioni file" a pagina [205](#)) selezionare le caselle di controllo relative alle operazioni che si desidera monitorare.

Per impostazione predefinita, Kaspersky Embedded Systems Security 2.2 rileva tutti gli indicatori operazioni file se l'opzione **Individua operazioni file che si basano su tutti gli indicatori riconoscibili** è selezionata.

10. Se si desidera che Kaspersky Embedded Systems Security 2.2 calcoli il checksum dei file dopo l'esecuzione dell'operazione, procedere come segue:
 - a. Nella sezione **Calcolo checksum** selezionare la casella di controllo **Calcola checksum per la**

versione finale di un file in seguito alla modifica del file, se possibile.

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 calcola il checksum del file modificato, in cui è stata rilevata l'operazione file con almeno un indicatore selezionato.

Se l'operazione file viene rilevata da una serie di indicatori, viene calcolato solo il checksum del file finale successivamente a tutte le modifiche.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 non calcola il checksum per i file modificati.

Non viene eseguito alcun calcolo del checksum nei casi seguenti:

- Se il file è diventato non disponibile (ad esempio a causa della modifica delle autorizzazioni di accesso).
- Se l'operazione file viene rilevata nel file che è stato successivamente rimosso.

La casella di controllo è deselezionata per impostazione predefinita.

- b. Nell'elenco a discesa **Calcolare il checksum utilizzando l'algoritmo** selezionare una delle opzioni:

- **Hash MD5**
- **Hash SHA256**

11. Se non si desidera monitorare tutte le operazioni file nell'elenco delle operazioni file disponibili (vedere la sezione "Informazioni sulle regole di monitoraggio operazioni file" a pagina [205](#)), selezionare le caselle di controllo relative alle operazioni da monitorare.

12. Se necessario, aggiungere gli ambiti del monitoraggio esclusi tramite i seguenti passaggi:

- a. Selezionare la scheda **Esclusioni**.
- b. Selezionare la casella di controllo **Tieni conto dell'ambito del monitoraggio escluso**.

La casella di controllo consente di disabilitare l'utilizzo delle esclusioni per le cartelle in cui non è necessario monitorare le operazioni file.

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 ignora gli ambiti del monitoraggio specificati nell'elenco delle esclusioni quando viene eseguita l'attività Monitoraggio integrità file.

Se la casella di controllo è deselezionata, Kaspersky Embedded Systems Security 2.2 registra gli eventi per tutti gli ambiti del monitoraggio specificati.

Per impostazione predefinita, la casella di controllo è deselezionata e l'elenco delle esclusioni è vuoto.

- c. Fare clic sul pulsante **Aggiungi**.
- Verrà visualizzata la finestra **Seleziona la cartella da aggiungere**.
- d. Nella finestra visualizzata specificare la cartella da escludere dall'ambito del monitoraggio.
- e. Fare clic su **OK**.

La cartella specificata viene aggiunta all'elenco degli ambiti esclusi.

13. Fare clic su **OK** nella finestra **Ambito del monitoraggio**.

Le impostazioni delle regole specificate verranno applicate all'ambito del monitoraggio selezionato dell'attività Monitoraggio integrità file.

Analisi log

Questa sezione contiene informazioni sull'attività Analisi log e sulle impostazioni dell'attività.

In questa sezione

Informazioni sull'attività Analisi log	212
Configurazione delle regole predefinite dell'attività	213
Configurazione delle regole di analisi log	215

Informazioni sull'attività Analisi log

Durante l'esecuzione dell'attività Analisi log, Kaspersky Embedded Systems Security 2.2 monitora l'integrità dell'ambiente protetto in base ai risultati di un'analisi dei log degli eventi di Windows. L'applicazione informa l'amministratore quando rileva un comportamento anomalo nel sistema che può indicare un tentativo di attacchi informatici.

Kaspersky Embedded Systems Security 2.2 valuta i log degli eventi di Windows e identifica le violazioni in base alle regole specificate da un utente o dalle impostazioni dell'analizzatore euristico, utilizzato dall'attività per analizzare i log.

Regole predefinite e analisi euristica

È possibile utilizzare l'attività Analisi log per monitorare lo stato del sistema protetto applicando le regole predefinite, che sono basate sull'analizzatore euristico. L'analizzatore euristico identifica l'attività anomala nel computer protetto, che può indicare un tentativo di attacco. I modelli per identificare un comportamento anomalo sono inclusi nelle regole disponibili nelle impostazioni delle regole predefinite.

Nell'elenco delle regole per l'attività Analisi log sono incluse sette regole. È possibile abilitare o disabilitare l'utilizzo di ciascuna regola. Non è possibile eliminare le regole esistenti o crearne di nuove.

È possibile configurare i criteri di attivazione per le regole di monitoraggio degli eventi per le seguenti operazioni:

- Rilevamento password di forza bruta
- Rilevamento accesso di rete

È inoltre possibile configurare le esclusioni nelle impostazioni dell'attività. L'analizzatore euristico non è attivato quando viene eseguito l'accesso da parte di un utente attendibile o da un indirizzo IP attendibile.

Kaspersky Embedded Systems Security 2.2 non utilizza l'analizzatore euristico per analizzare i log di Windows se l'analizzatore euristico non viene utilizzato dall'attività. Per impostazione predefinita, l'analizzatore euristico è abilitato.

Quando le regole vengono applicate, l'applicazione registra un *Evento critico* nel log delle attività di Analisi log.

Regole personalizzate per l'attività Analisi log

È possibile utilizzare le impostazioni delle regole delle attività per specificare e modificare i criteri per l'attivazione delle regole al rilevamento degli eventi selezionati nel log di Windows specificato. Per impostazione predefinita, l'elenco delle regole dell'attività Analisi log contiene quattro regole. È possibile abilitare e disabilitare l'utilizzo di

queste regole, rimuovere le regole e modificare le impostazioni delle regole.

Per ogni regola è possibile configurare i seguenti criteri di attivazione della regola:

- Elenco di identificatori record nel Registro eventi di Windows.

La regola viene attivata quando viene creato un nuovo record nel Registro eventi di Windows, se le proprietà dell'evento includono un identificatore evento specificato per la regola. È inoltre possibile aggiungere e rimuovere gli identificatori per ogni regola specificata.

- Origine evento.

Per ogni regola è possibile definire un log secondario del Registro eventi di Windows. L'applicazione cerca i record con gli identificatori evento specificati solo nel log secondario. È possibile selezionare uno dei log secondari standard (Applicazione, Sicurezza o Sistema) oppure specificare un log secondario personalizzato immettendo il nome nel campo di selezione dell'origine.

L'applicazione non verifica l'effettiva esistenza del log secondario specificato nel Registro eventi di Windows.

Quando la regola viene attivata, Kaspersky Embedded Systems Security 2.2 registra un Evento critico nel log delle attività di Analisi log.

Per impostazione predefinita, l'attività Analisi log non applica le regole personalizzate.

Prima di avviare l'attività Analisi log, verificare che il criterio di audit del sistema sia impostato correttamente. Per informazioni dettagliate, fare riferimento all'articolo Microsoft <https://technet.microsoft.com/en-us/library/cc952128.aspx>.

Configurazione delle regole predefinite dell'attività

► *Procedere come segue per configurare le regole predefinite per l'attività Analisi log:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Analisi sistema** fare clic sul pulsante **Impostazioni** nel gruppo **Analisi log**.
Verrà visualizzata la finestra **Impostazioni analisi log**.
4. Selezionare la scheda **Regole predefinite**.

5. Selezionare o deselezionare la casella di controllo **Applica regole predefinite per l'analisi log**.

Se questa casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 applica l'analizzatore euristico per rilevare attività anomale nel computer protetto.

Se questa casella di controllo è deselezionata, l'analizzatore euristico non è in esecuzione e Kaspersky Embedded Systems Security 2.2 applica regole preimpostate o personalizzate per rilevare attività anomale.

La casella di controllo è selezionata per impostazione predefinita.

Affinché l'attività venga eseguita, deve essere selezionata almeno una regola di analisi log.

6. Selezionare le regole che si desidera applicare dall'elenco delle regole predefinite:
 - Sono presenti pattern di un possibile attacco di forza bruta nel sistema.
 - Sono presenti pattern di una possibile compromissione del Registro eventi di Windows.
 - Rilevate azioni atipiche per conto di un nuovo servizio installato.
 - Rilevato accesso atipico che utilizza credenziali esplicite.
 - Sono presenti pattern di un possibile attacco PAC basato su Kerberos PAC (MS14-068) nel sistema.
 - Sono state rilevate azioni atipiche dirette a un gruppo di amministratori predefinito.
 - È stata rilevata un'attività atipica durante una sessione di accesso alla rete.
7. Per configurare le regole selezionate, fare clic sul pulsante **Impostazioni avanzate**.
Verrà visualizzata la finestra **Analisi log**.
8. Nella sezione **Rilevamento attacco di forza bruta** impostare il numero di tentativi e un intervallo di tempo in cui si sono verificati questi tentativi, che opereranno come trigger per l'analizzatore euristico.
9. Nella sezione **Rilevamento accesso alla rete** indicare l'inizio e la fine dell'intervallo di tempo durante il quale Kaspersky Embedded Systems Security 2.2 considera i tentativi di accesso attività anomale.
10. Selezionare la scheda **Esclusioni**.
11. Eseguire le azioni seguenti per aggiungere utenti attendibili:
 - a. Fare clic sul pulsante **Sfoglia**.
 - b. Selezionare un utente.
 - c. Fare clic su **OK**.Un utente selezionato viene aggiunto all'elenco degli utenti attendibili.
12. Eseguire le azioni seguenti per aggiungere indirizzi IP attendibili:
 - a. Immettere l'indirizzo IP.
 - b. Fare clic sul pulsante **Aggiungi**.
13. Un indirizzo IP immesso viene aggiunto all'elenco di indirizzi IP attendibili.
14. Nella scheda **Gestione attività** configurare la pianificazione di avvio dell'attività (vedere la sezione "Configurazione delle impostazioni della pianificazione dell'avvio delle attività" a pagina [119](#)).
15. Fare clic su **OK**.

La configurazione dell'attività Analisi log viene salvata.

Configurazione delle regole di analisi log

► *Procedere come segue per aggiungere e configurare una nuova regola di analisi log personalizzata:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Eseguire una delle seguenti operazioni nel riquadro dei dettagli del gruppo di amministrazione selezionato:
 - Per configurare le impostazioni dell'applicazione per un gruppo di computer, selezionare la scheda **Criteri** e aprire la finestra **Proprietà: <nome criterio>** (vedere la sezione "Configurazione del criterio" a pagina [88](#)).
 - Per configurare un'applicazione per un singolo computer, selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).

Se un dispositivo è gestito da un criterio di Kaspersky Security Center attivo e questo criterio impedisce le modifiche nelle impostazioni dell'applicazione, queste impostazioni non possono essere modificate nella finestra **Impostazioni applicazione**.

3. Nella sezione **Analisi sistema** fare clic sul pulsante **Impostazioni** nel gruppo **Analisi log**.
Verrà visualizzata la finestra **Analisi log**.
4. Nella scheda **Regole di analisi log** selezionare o deselezionare la casella di controllo **Applica regole personalizzate per l'analisi log**.

Se la casella di controllo è selezionata, Kaspersky Embedded Systems Security 2.2 applica le regole personalizzate per Analisi log in base alle impostazioni di ogni regola. È possibile aggiungere, rimuovere e configurare le regole di analisi log.

Se la casella di controllo è deselezionata, non è possibile aggiungere o modificare le regole personalizzate. Kaspersky Embedded Systems Security 2.2 applica le impostazioni delle regole predefinite.

La casella di controllo è selezionata per impostazione predefinita. Solo la regola Rilevamento popup dell'applicazione è attiva.

È possibile controllare se le regole preimpostate vengono applicate per Analisi log. Selezionare le caselle di controllo corrispondenti alle regole che si desidera applicare per Analisi log.

5. Per aggiungere una nuova regola personalizzata, fare clic sul pulsante **Aggiungi**.
Verrà visualizzata la finestra **Regole di analisi log**.
6. Nella sezione **Generale** immettere le informazioni seguenti sulla nuova regola:
 - **Nome**
 - **Sorgente**

Selezionare un log di origine per utilizzare gli eventi registrati per l'analisi. Sono disponibili i seguenti tipi di log degli eventi di Windows:

- Applicazione
- Sicurezza
- Sistema

È possibile aggiungere un nuovo log personalizzato immettendo il nome del log nel campo **Sorgente**.

7. Nella sezione **ID eventi attivati** specificare gli ID che attiveranno la regola al momento del rilevamento:
 - a. Immettere il valore numerico di un ID.
 - b. Fare clic sul pulsante **Aggiungi**.
Un ID regola selezionato viene aggiunto all'elenco. È possibile aggiungere un numero illimitato di identificatori per ogni regola.
 - c. Fare clic su **OK**.

La regola di analisi log viene aggiunta all'elenco di regole.

Generazione dei rapporti in Kaspersky Security Center

I rapporti in Kaspersky Security Center contengono informazioni sullo stato dei dispositivi gestiti. I rapporti sono basati sulle informazioni memorizzate in Administration Server.

A partire da Kaspersky Security Center 11, sono disponibili i seguenti tipi di rapporti per Kaspersky Embedded Systems Security 2.2:

- Rapporto sullo stato dei componenti dell'applicazione
- Rapporto sulle applicazioni non consentite
- Rapporto sulle applicazioni non consentite in modalità di test

Per informazioni dettagliate su tutti i rapporti di Kaspersky Security Center e su come configurarli, vedere la [Guida di Kaspersky Security Center](#).

Rapporto sullo stato dei componenti dell'applicazione

È possibile monitorare lo stato della protezione di tutti i dispositivi di rete e ottenere una panoramica strutturata del set di componenti su ogni dispositivo.

Il rapporto visualizza uno dei seguenti stati per ogni componente: *In esecuzione*, *Sospeso*, *Arrestato*, *Malfunzionamento*, *Non installato*, *Avvio in corso*.

Lo stato *Non installato* si riferisce al componente, non all'applicazione stessa. Se l'applicazione non è installata, Kaspersky Security Center assegna lo stato N/D (Non disponibile).

È possibile creare selezioni di componenti e utilizzare i filtri per visualizzare i dispositivi di rete con il set di componenti specificato e il relativo stato.

Per informazioni dettagliate sulla creazione e l'utilizzo delle selezioni, vedere la [Guida di Kaspersky Security Center](#).

► *Per esaminare gli stati di componenti nelle impostazioni dell'applicazione:*

1. Espandere il nodo **Dispositivi gestiti** nell'albero di Kaspersky Security Center Administration Console e selezionare il gruppo di amministrazione per cui si desidera configurare le impostazioni dell'applicazione.
2. Selezionare la scheda **Dispositivi** e aprire la finestra **Impostazioni applicazione** (vedere la sezione "Configurazione delle attività locali nella finestra Impostazioni applicazione di Kaspersky Security Center" a pagina [100](#)).
3. Selezionare la sezione **Componenti**.
4. Controllare la tabella dello stato.

► *Per esaminare un rapporto standard di Kaspersky Security Center:*

1. Selezionare il nodo **Administration Server <nome computer>** nell'albero di Administration Console.
2. Aprire la scheda **Rapporti**.
3. Fare doppio clic sull'elemento dell'elenco **Rapporto sullo stato dei componenti dell'applicazione**.
Verrà generato un rapporto.
4. Esaminare i seguenti dettagli del rapporto:
 - Un diagramma.
 - Una tabella riepilogativa dei componenti, con i dati aggregati sui dispositivi di rete in cui è installato ogni componente e i gruppi a cui appartengono.
 - Una tabella dettagliata che specifica stato, versione, dispositivo e gruppo dei componenti.

Rapporti sulle applicazioni bloccate in modalità Attivo e Solo statistiche

In base ai risultati dell'esecuzione dell'attività Controllo dell'avvio delle applicazioni (vedere la sezione "Gestione dell'avvio delle applicazioni da Kaspersky Security Center" a pagina [172](#)), possono essere generati due tipi di rapporti: il rapporto sulle applicazioni non consentite (se l'attività viene avviata in modalità **Attivo**) e il rapporto sulle applicazioni non consentite in modalità di test (se l'attività viene avviata in modalità **Solo statistiche**). Questi rapporti visualizzano le informazioni sulle applicazioni bloccate nei server protetti della rete. Ogni rapporto viene generato per tutti i gruppi di amministrazione e raccoglie dati da tutte le applicazioni Kaspersky Lab installate nei dispositivi protetti.

► *Per esaminare un rapporto sulle applicazioni non consentite in modalità di test:*

1. Avviare l'attività Controllo Applicazioni in modalità Solo statistiche (vedere la sezione "Configurazione delle impostazioni dell'attività Controllo dell'avvio delle applicazioni" a pagina [173](#)).
2. Selezionare il nodo **Administration Server <nome computer>** nell'albero di Administration Console.
3. Aprire la scheda **Rapporti**.
4. Fare doppio clic sull'elemento dell'elenco **Rapporto sulle applicazioni non consentite in modalità di test**.
Verrà generato un rapporto.
5. Esaminare i seguenti dettagli del rapporto:
 - Un diagramma che visualizza le dieci applicazioni con il maggior numero di avvii bloccati.
 - Una tabella riepilogativa dei blocchi delle applicazioni, che specifica il nome del file eseguibile, il motivo, l'ora del blocco e il numero di dispositivi in cui si è verificato.
 - Una tabella dettagliata che specifica i dati sul dispositivo, il percorso del file e i criteri per il blocco.

► *Per esaminare un rapporto sulle applicazioni non consentite in modalità Attivo:*

1. Avviare l'attività Controllo Applicazioni in modalità Attivo (vedere la sezione "Configurazione delle impostazioni dell'attività Controllo dell'avvio delle applicazioni" a pagina [173](#)).
2. Selezionare il nodo **Administration Server <nome computer>** nell'albero di Administration Console.
3. Aprire la scheda **Rapporti**.
4. Fare doppio clic su un elemento dell'elenco **Rapporto sulle applicazioni non consentite**.
Verrà generato un rapporto.

Questo rapporto contiene le stesse sezioni di dati del rapporto sulle applicazioni non consentite in modalità di test.

Utilizzo di Kaspersky Embedded Systems Security 2.2 dalla riga di comando

Questa sezione illustra l'utilizzo di Kaspersky Embedded Systems Security 2.2 dalla riga di comando.

In questo capitolo

Comandi della riga di comando	219
Codici restituiti dalla riga di comando	244

Comandi della riga di comando

È possibile eseguire comandi di base per la gestione di Kaspersky Embedded Systems Security 2.2 dalla riga di comando del computer protetto se è stato incluso il componente Utilità della riga di comando nell'elenco delle funzionalità installate durante l'installazione di Kaspersky Embedded Systems Security 2.2.

Utilizzando i comandi della riga di comando, è possibile gestire solo quelle funzioni che sono accessibili in base alle autorizzazioni assegnate all'utente in Kaspersky Embedded Systems Security 2.2.

Determinati comandi di Kaspersky Embedded Systems Security 2.2 sono eseguiti nelle seguenti modalità:

- Modalità sincrona: la gestione torna alla console solo una volta che l'esecuzione del comando è stata completata.
- Modalità asincrona: la gestione torna alla console subito dopo che il comando è stato eseguito.

► *Per interrompere l'esecuzione del comando in modalità sincrona*

Premere la combinazione di tasti **CTRL+C**.

Attenersi alle seguenti regole per l'immissione dei comandi di Kaspersky Embedded Systems Security 2.2:

- Immettere modificatori e comandi utilizzando lettere maiuscole e minuscole.
- Delimitare i modificatori con uno spazio.
- Se il nome del file o della cartella di cui si specifica il percorso come valore della chiave contiene uno spazio, specificare il percorso del file o della cartella tra virgolette, ad esempio: "C:\TEST\test cpp.exe"
- Se necessario, utilizzare i segnaposto nel nome del file o nelle maschere per il percorso, ad esempio: "C:\Temp\Temp*\", "C:\Temp\Temp???.doc", "C:\Temp\Temp*.doc"

È possibile utilizzare la riga di comando per tutte le operazioni richieste per la gestione e l'amministrazione di Kaspersky Embedded Systems Security 2.2 (vedere la seguente tabella).

Tabella 38. Comandi di Kaspersky Embedded Systems Security 2.2

Comando	Descrizione
KAVSHELL APPCONTROL (vedere la sezione "Compilazione dell'elenco delle regole di Controllo dell'avvio delle applicazioni. KAVSHELL APPCONTROL" a pagina 232)	Rinnova l'elenco delle regole specificato in base al principio di aggiunta selezionato.
KAVSHELL APPCONTROL /CONFIG (vedere la sezione "Gestione dell'attività Controllo dell'avvio delle applicazioni. KAVSHELL APPCONTROL /CONFIG" a pagina 229)	Controlla la modalità operativa dell'attività Controllo dell'avvio delle applicazioni
KAVSHELL APPCONTROL /GENERATE (vedere la sezione "Generazione regole per Controllo dell'avvio delle applicazioni. KAVSHELL APPCONTROL /GENERATE" a pagina 230)	Avvia l'attività Generazione regole per Controllo dell'avvio delle applicazioni.
KAVSHELL VACUUM (vedere la sezione "Deframmentazione dei file di log di Kaspersky Embedded Systems Security 2.2.KAVSHELL VACUUM" a pagina 240)	Deframmenta i file di log di Kaspersky Embedded Systems Security 2.2.
KAVSHELL PASSWORD	Gestisce le impostazioni di protezione della password.
KAVSHELL HELP (vedere la sezione "Visualizzazione della Guida per i comandi di Kaspersky Embedded Systems Security 2.2. KAVSHELL HELP" a pagina 221)	Visualizza la Guida per i comandi di Kaspersky Embedded Systems Security 2.2.
KAVSHELL START (vedere la sezione "Avvio e arresto del servizio di Kaspersky Security. KAVSHELL START, KAVSHELL STOP" a pagina 222)	Avvia il servizio di Kaspersky Embedded Systems Security 2.2.
KAVSHELL STOP (vedere la sezione "Avvio e arresto del servizio di Kaspersky Security. KAVSHELL START, KAVSHELL STOP" a pagina 222)	Arresta il servizio di Kaspersky Embedded Systems Security 2.2.
KAVSHELL SCAN (vedere la sezione "Scansione dell'area selezionata. KAVSHELL SCAN" a pagina 222)	Crea e avvia un'attività Scansione su richiesta temporanea con l'ambito della scansione e le impostazioni di sicurezza impostati dai modificatori del comando.
KAVSHELL SCANCritical (vedere la sezione "Avvio dell'attività Scansione aree critiche. KAVSHELL SCANCritical" a pagina 226)	Avvia l'attività di sistema Scansione aree critiche.
KAVSHELL TASK (vedere la sezione "Gestione dell'attività specificata in modo asincrono. KAVSHELL TASK" a pagina 227)	Avvia, sospende, riprende o interrompe l'attività selezionata in modo asincrono / restituisce lo stato o le statistiche dell'attività corrente.
KAVSHELL RTP (vedere la sezione "Avvio e arresto delle attività Protezione in tempo reale. KAVSHELL RTP" a pagina 228)	Avvia o interrompe tutte le attività Protezione in tempo reale.

Comando	Descrizione
KAVSHELL UPDATE (vedere la sezione "Avvio dell'attività di aggiornamento dei database di Kaspersky Embedded Systems Security 2.2. KAVSHELL UPDATE" a pagina 233)	Avvia l'attività di aggiornamento dei database di Kaspersky Embedded Systems Security 2.2 con le impostazioni specificate utilizzando i modificatori del comando.
KAVSHELL ROLLBACK (vedere la sezione "Rollback degli aggiornamenti dei database di Kaspersky Embedded Systems Security 2.2. KAVSHELL ROLLBACK" a pagina 236)	Esegue il rollback dei database alla versione precedente.
KAVSHELL LICENSE (vedere la sezione "Attivazione dell'applicazione. KAVSHELL LICENSE" a pagina 237)	Gestisce le chiavi.
KAVSHELL TRACE (vedere la sezione "Abilitazione, configurazione e disabilitazione del log di traccia. KAVSHELL TRACE" a pagina 238)	Abilita o disabilita il log di traccia e gestisce le impostazioni del log di traccia.
KAVSHELL DUMP (vedere la sezione "Abilitazione e disabilitazione della creazione del file di dump. KAVSHELL DUMP" a pagina 241)	Abilita o disabilita i file di dump del processo di Kaspersky Embedded Systems Security 2.2 in caso di un arresto anomalo dei processi.
KAVSHELL IMPORT (vedere la sezione "Importazione delle impostazioni. KAVSHELL IMPORT" a pagina 243)	Importa le impostazioni generali, le funzioni e le attività di Kaspersky Embedded Systems Security 2.2 da un file di configurazione creato in precedenza.
KAVSHELL EXPORT (vedere la sezione "Esportazione delle impostazioni. KAVSHELL EXPORT" a pagina 243)	Esporta tutte le impostazioni e le attività esistenti di Kaspersky Embedded Systems Security 2.2 in un file di configurazione.
KAVSHELL DEVCONTROL (vedere la sezione "Compilazione dell'elenco delle regole di Controllo dispositivi. KAVSHELL DEVCONTROL" a pagina 233)	Esegue l'aggiunta nell'elenco delle regole di controllo dei dispositivi generate in base al metodo selezionato.

Visualizzazione della Guida per i comandi di Kaspersky Embedded Systems Security 2.2. KAVSHELL HELP

Per ottenere l'elenco di tutti i comandi di Kaspersky Embedded Systems Security 2.2, eseguire uno dei seguenti comandi:

```
KAVSHELL
```

```
KAVSHELL HELP
```

```
KAVSHELL /?
```

Per ottenere una descrizione di un comando e la relativa sintassi, eseguire uno dei seguenti comandi:

```
KAVSHELL HELP <comando>
```

```
KAVSHELL <comando> /?
```

Esempi di comandi KAVSHELL HELP

Per visualizzare informazioni dettagliate sul comando KAVSHELL SCAN, eseguire il seguente comando:

```
KAVSHELL HELP SCAN
```

Avvio e arresto del servizio di Kaspersky Security. KAVSHELL START, KAVSHELL STOP

Per eseguire il servizio di Kaspersky Security, eseguire il comando

```
KAVSHELL START
```

Per impostazione predefinita, all'avvio del servizio di Kaspersky Security, verranno avviate le attività Protezione dei file in tempo reale e Scansione all'avvio del sistema operativo, nonché altre attività pianificate per l'esecuzione **All'avvio dell'applicazione**.

Per arrestare il servizio di Kaspersky Security, eseguire il comando

```
KAVSHELL STOP
```

Potrebbe essere richiesta la password per eseguire il comando. Immettere la chiave di utilizzo [/pwd:<password>] della password corrente.

Scansione dell'area selezionata. KAVSHELL SCAN

Per avviare un'attività per la scansione di aree specifiche del computer protetto, utilizzare il comando KAVSHELL SCAN. I modificatori del comando specificano l'ambito della scansione e le impostazioni di sicurezza del nodo selezionato.

L'attività Scansione su richiesta avviata tramite il comando KAVSHELL SCAN è un'attività temporanea. Viene visualizzata nella console dell'applicazione solo durante l'esecuzione (non è possibile visualizzare le impostazioni dell'attività nella console dell'applicazione). Il log dell'esecuzione dell'attività viene generato contemporaneamente. È visualizzato in **Log delle attività** nella console dell'applicazione.

Quando si specificano i percorsi nelle attività di scansione per aree specifiche, è possibile utilizzare variabili di ambiente. Se si utilizza la variabile di ambiente specificata per l'utente, eseguire il comando KAVSHELL SCAN con le autorizzazioni per questo utente.

Il comando KAVSHELL SCAN viene eseguito in modalità sincrona.

Per avviare un'attività Scansione su richiesta esistente dalla riga di comando, utilizzare il comando KAVSHELL TASK (vedere la sezione "Gestione dell'attività specificata in modo asincrono. KAVSHELL TASK" a pagina [227](#)).

Sintassi del comando KAVSHELL SCAN

```
KAVSHELL SCAN <ambito della scansione>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<percorso del file
con l'elenco degli ambiti della scansione>] [/F<A|C|E>] [/NEWONLY]
```

```
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>]
[/EM:<"maschere">] [/ES:<dimensione>] [/ET:<numero di secondi>] [/TZOFF]
[/OF:<SKIP|RESIDENT|SCAN[=<giorni>] [NORECALL]>]
[/NOICHECKER] [/NOISWIFT] [/ANALYZERLEVEL] [/NOCHECKMSSIGN] [/W:<percorso del file
di log dell'attività>] [/ANSI] [/ALIAS:<alias dell'attività>]
```

Il comando KAVSHELL SCAN ha sia chiavi obbligatorie che facoltative (vedere la seguente tabella).

Esempi di comandi KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe
"\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA
/E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1
/NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Tabella 39. Modificatori di comando KAVSHELL SCAN

Chiave	Descrizione
Ambito della scansione. Modificatore obbligatorio.	
<file>	Specifica l'ambito della scansione: l'elenco di file, cartelle, percorsi di rete e aree predefinite.
<cartelle>	Specificare i percorsi di rete nel formato UNC (Universal Naming Convention).
<percorso di rete>	Nel seguente esempio la cartella Folder4 viene specificata senza un percorso. È contenuta nella cartella da cui viene eseguito il comando KAVSHELL: KAVSHELL SCAN Folder4 Se il nome dell'oggetto da controllare contiene spazi, deve essere racchiuso tra virgolette. Quando si seleziona una cartella, Kaspersky Embedded Systems Security 2.2 verifica anche tutte le sottocartelle della cartella in questione. I simboli * o ? possono essere utilizzati per esaminare un gruppo di file.
/MEMORY	Scansione degli oggetti nella RAM
/SHARED	Scansione delle cartelle condivise sul computer
/STARTUP	Scansione degli oggetti di avvio
/REMDRIVES	Scansione delle unità rimovibili
/FIXDRIVES	Scansione delle unità disco rigido
/MYCOMP	Scansione di tutte le aree del computer protetto

Chiave	Descrizione
/L:<percorso del file con l'elenco degli ambiti della scansione>	<p>Nome del file con l'elenco degli ambiti della scansione, incluso il percorso completo del file.</p> <p>Delimitare gli ambiti della scansione nei file utilizzando interruzioni di riga. È possibile specificare aree di scansione predefinite, come mostrato di seguito in questo esempio di un file con un elenco di ambiti della scansione:</p> <p>C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED</p>
Oggetti esaminati (tipi di file). Se non si specificano valori per questo modificatore, Kaspersky Embedded Systems Security 2.2 esaminerà gli oggetti in base al formato.	
/FA	Scansione di tutti gli oggetti
/FC	Scansione degli oggetti in base al formato (per impostazione predefinita). Kaspersky Embedded Systems Security 2.2 esamina solo gli oggetti il cui formato è incluso nell'elenco dei formati degli oggetti infettabili.
/FE	Scansione degli oggetti in base all'estensione. Kaspersky Embedded Systems Security 2.2 esamina solo gli oggetti con estensioni incluse nell'elenco delle estensioni degli oggetti infettabili.
/NEWONLY	<p>Esamina solo i file nuovi e modificati.</p> <p>Se non si specifica questo modificatore, Kaspersky Embedded Systems Security 2.2 esaminerà tutti gli oggetti.</p>
Azione da eseguire sugli oggetti infetti e di altro tipo. Se non si specificano valori per questo modificatore, Kaspersky Embedded Systems Security 2.2 eseguirà l'azione Ignora .	
DISINFECT	Disinfetta, ignora se la disinfezione è impossibile
DISINFDEL	Disinfetta, elimina se la disinfezione è impossibile
DELETE	<p>Elimina</p> <p>Le impostazioni DISINFECT e DELETE sono salvate nella versione corrente di Kaspersky Embedded Systems Security 2.2 per garantire la compatibilità con le versioni precedenti. Queste impostazioni possono essere utilizzate invece dei comandi chiave /AI: e /AS: In questo caso, Kaspersky Embedded Systems Security 2.2 non elaborerà gli oggetti potenzialmente infetti.</p>
REPORT	Invia il rapporto (impostazione predefinita)
AUTO	Esegui l'azione consigliata
/AS: Azione da eseguire sugli oggetti potenzialmente infetti. Se non si specificano valori per questo modificatore, Kaspersky Embedded Systems Security 2.2 eseguirà l'azione Ignora .	
QUARANTINE	Quarantena
DELETE	Elimina
REPORT	Invia il rapporto (impostazione predefinita)
AUTO	Esegui l'azione consigliata

Chiave	Descrizione
Esclusioni	
/E:ABMSPO	Esclude gli oggetti composti dei seguenti tipi: A - archivi (esamina solo gli archivi SFX) B - database e-mail M - posta semplice S - archivi e archivi SFX P - oggetti compressi O - oggetti OLE incorporati
/EM:<"maschere">	Escludi i file in base alla maschera È possibile specificare diverse maschere, ad esempio: EM:"*.txt; *.png; C:\Videos*.avi".
/ET:<numero di secondi>	Interrompi l'elaborazione dell'oggetto se continua più a lungo del numero di secondi specificati dal valore <numero di secondi>. Per impostazione predefinita, non è prevista alcuna restrizione per il tempo.
/ES:<dimensione>	Non esaminare gli oggetti composti più grandi della dimensione (in MB) specificata dal valore <dimensione>. Per impostazione predefinita, Kaspersky Embedded Systems Security 2.2 esamina gli oggetti di qualsiasi dimensione:
/TZOFF	Disabilita le esclusioni dell'area attendibile
Impostazioni avanzate (opzioni)	
/NOICHECKER	Disabilita l'utilizzo di iChecker (abilitato per impostazione predefinita)
/NOISWIFT	Disabilita l'utilizzo di iSwift (abilitato per impostazione predefinita)
/ANALYZERLEVEL: <intensità dell'analisi>	Abilita l'analizzatore euristico e configura il livello di analisi. Sono disponibili i seguenti livelli di analisi euristica: 1 - leggero 2 - medio 3 - approfondito Se si omette il modificatore, Kaspersky Embedded Systems Security 2.2 non utilizzerà l'analizzatore euristico.
/ALIAS:<alias dell'attività>	Consente di assegnare all'attività Scansione su richiesta un nome temporaneo con cui è possibile accedere all'attività durante la sua esecuzione, ad esempio per visualizzare le relative statistiche utilizzando il comando TASK. L'alias dell'attività deve essere univoco tra gli alias di attività di tutti i componenti funzionali di Kaspersky Embedded Systems Security 2.2. Se non si specifica questo modificatore, viene utilizzato il nome temporaneo scan_<pid_kavshell>, ad esempio scan_1234. Nella console dell'applicazione all'attività viene assegnato il nome Esamina gli oggetti (<data e ora>), ad esempio Esamina gli oggetti 16/8/2007 17:13:14.
Impostazioni dei log delle attività (impostazioni dei rapporti)	

Chiave	Descrizione
/W:<percorso del file di log dell'attività>	<p>Se si specifica questa chiave, Kaspersky Embedded Systems Security 2.2 salverà il file di log dell'attività con il nome definito dal valore della chiave.</p> <p>Il file di log contiene le statistiche sull'esecuzione dell'attività, l'ora di avvio e completamento (interruzione) e le informazioni sugli eventi relativi all'attività.</p> <p>Il log viene utilizzato per registrare gli eventi definiti dalle impostazioni dei log dell'attività e del log eventi di Kaspersky Embedded Systems Security 2.2 nel "Visualizzatore eventi".</p> <p>È possibile specificare il percorso assoluto o relativo del file di log. Se si specifica solo il nome di un file senza specificare il relativo percorso, il file di log sarà creato nella cartella corrente.</p> <p>Riavviando il comando con le stesse impostazioni per il log, verrà sovrascritto il file di log esistente.</p> <p>Il file di log può essere visualizzato mentre un'attività è in esecuzione.</p> <p>Il log è visualizzato nel nodo Log delle attività della console dell'applicazione.</p> <p>Se Kaspersky Embedded Systems Security 2.2 non riesce a creare il file di log, non interrompe l'esecuzione del comando ma visualizza un messaggio di errore.</p>
/ANSI	<p>L'opzione abilita la registrazione degli eventi nel file di log con la codifica ANSI.</p> <p>L'opzione ANSI non sarà applicata se l'opzione W non è definita.</p> <p>Se non si specifica l'opzione ANSI, il log dell'attività viene generato utilizzando la codifica UNICODE.</p>

Avvio dell'attività Scansione aree critiche. KAVSHELL SCANCRITICAL

Utilizzare il comando `KAVSHELL SCANCRITICAL` per avviare l'attività Scansione aree critiche con le impostazioni definite nella console dell'applicazione.

Sintassi del comando KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<percorso del file di log dell'attività>]
```

Esempi di comandi KAVSHELL SCANCRITICAL

Per eseguire l'attività Scansione aree critiche e salvare il log dell'attività `scancritical.log` nella cartella corrente, eseguire il seguente comando:

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

A seconda della sintassi del modificatore `/W`, è possibile configurare il percorso del log dell'attività (vedere la seguente tabella).

Tabella 40. Sintassi del modificatore /W per il comando `KAVSHELL SCANCritical`

Chiave	Descrizione
/W:<percorso del file di log dell'attività>	<p>Se si specifica questa chiave, Kaspersky Embedded Systems Security 2.2 salverà il file di log dell'attività con il nome definito dal valore della chiave.</p> <p>Il file di log contiene le statistiche sull'esecuzione dell'attività, l'ora di avvio e completamento (interruzione) e le informazioni sugli eventi relativi all'attività.</p> <p>Il log viene utilizzato per registrare gli eventi definiti dalle impostazioni dei log dell'attività e del log eventi dell'applicazione nel Visualizzatore eventi.</p> <p>È possibile specificare il percorso assoluto o relativo del file di log. Se si specifica solo il nome di un file senza specificare il relativo percorso, il file di log sarà creato nella cartella corrente.</p> <p>Riavviando il comando con le stesse impostazioni per il log, verrà sovrascritto il file di log esistente.</p> <p>Il file di log può essere visualizzato mentre un'attività è in esecuzione.</p> <p>Il log è visualizzato nel nodo Log delle attività della console dell'applicazione.</p> <p>Se Kaspersky Embedded Systems Security 2.2 non riesce a creare il file di log, non interrompe l'esecuzione del comando ma visualizza un messaggio di errore.</p>

Gestione dell'attività specificata in modo asincrono. `KAVSHELL TASK`

Utilizzando il comando `KAVSHELL TASK` è possibile gestire l'attività specificata: eseguire, sospendere, riprendere e arrestare l'attività specificata, nonché visualizzare lo stato e le statistiche dell'attività corrente. Il comando viene eseguito in modalità asincrona.

Potrebbe essere richiesta la password per eseguire il comando. Immettere la chiave di utilizzo `[/pwd:<password>]` della password corrente.

Sintassi del comando `KAVSHELL TASK`

```
KAVSHELL TASK [<alias del nome delle attività> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Esempi di comandi `KAVSHELL TASK`

```
KAVSHELL TASK
```

```
KAVSHELL TASK on-access /START
```

```
KAVSHELL TASK user-task_1 /STOP
```

```
KAVSHELL TASK scan-computer /STATE
```

Il comando `KAVSHELL TASK` può essere eseguito senza modificatori oppure con uno o più modificatori (vedere la seguente tabella).

Tabella 41. Modificatori di comando KAVSHELL TASK

Chiave	Descrizione
Senza chiavi	Restituisce l'elenco di tutte le attività Kaspersky Embedded Systems Security 2.2 esistenti. L'elenco contiene i campi: nome alternativo dell'attività, categoria dell'attività (di sistema o personalizzata) e stato dell'attività corrente.
<alias dell'attività>	Invece del nome dell'attività, nel comando SCAN TASK utilizzare l'alias dell'attività, un nome aggiuntivo in formato breve che Kaspersky Embedded Systems Security 2.2 assegna alle attività. Per visualizzare gli alias delle attività di Kaspersky Embedded Systems Security 2.2, immettere il comando KAVSHELL TASK senza modificatori.
/START	Avvia l'attività specificata in modalità asincrona.
/STOP	Interrompe l'attività specificata.
/PAUSE	Sospende l'attività specificata.
/RESUME	Riprende l'attività specificata in modalità asincrona.
/STATE	Restituisce lo stato dell'attività corrente (ad esempio In esecuzione , Completata , Sospesa , Arrestata , Non riuscita , Avvio in corso , Ripristino in corso).
/STATISTICS	Recupera le statistiche dell'attività - informazioni sul numero di oggetti elaborati dall'avvio dell'attività fino al momento corrente.

Codici restituiti per il comando KAVSHELL TASK (vedere la sezione "Codici restituiti per il comando KAVSHELL TASK" a pagina [246](#)).

Avvio e arresto delle attività Protezione in tempo reale. KAVSHELL RTP

Utilizzando il comando `KAVSHELL RTP`, è possibile avviare o interrompere le attività Protezione in tempo reale.

Potrebbe essere richiesta la password per eseguire il comando. Immettere la chiave di utilizzo `[/pwd:<password>]` della password corrente.

Sintassi del comando KAVSHELL RTP

```
KAVSHELL RTP {/START | /STOP}
```

Esempi di comandi KAVSHELL RTP

Per avviare tutte le attività Protezione in tempo reale, eseguire il seguente comando:

```
KAVSHELL RTP /START
```

Il comando `KAVSHELL RTP` può includere due modificatori obbligatori (vedere la seguente tabella).

Tabella 42. Modificatori di comando KAVSHELL RTP

Chiave	Descrizione
/START	Avvia tutte le attività Protezione in tempo reale: Protezione dei file in tempo reale e Utilizzo di KSN.
/STOP	Interrompe tutte le attività Protezione in tempo reale.

Gestione dell'attività Controllo dell'avvio delle applicazioni KAVSHELL APPCONTROL /CONFIG

È possibile utilizzare il comando `KAVSHELL APPCONTROL/CONFIG` per configurare la modalità in cui l'attività Controllo dell'avvio delle applicazioni viene eseguita e monitora il caricamento dei moduli DLL.

Sintassi del comando KAVSHELL APPCONTROL /CONFIG

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config
/savetofile:<percorso completo del file XML>
```

Esempi del comando KAVSHELL APPCONTROL /CONFIG

- Per eseguire l'attività Controllo dell'avvio delle applicazioni in modalità **Attivo** senza caricare un modulo DLL e quindi salvare le impostazioni dell'attività al completamento, eseguire il seguente comando:

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

È possibile configurare le impostazioni dell'attività Controllo dell'avvio delle applicazioni utilizzando i parametri della riga di comando (vedere la seguente tabella).

Tabella 43. Opzioni comando `KAVSHELL APPCONTROL /GENERATE`

Chiave	Descrizione
<code>/mode:<applyrules statistics></code>	Modalità operativa dell'attività Controllo dell'avvio delle applicazioni. È possibile selezionare una delle seguenti modalità: <ul style="list-style-type: none"> • active - vengono applicate le regole di Controllo dell'avvio delle applicazioni; • statistics - Solo statistiche.
<code>/dll:<no yes></code>	Abilitare o disabilitare il monitoraggio del caricamento DLL.
<code>/savetofile: <percorso del file XML></code>	Esportare le regole specificate nel file indicato in formato XML.
<code>/savetofile: <nome completo del file XML></code>	Salvare l'elenco delle regole in un file.
<code>/savetofile: <nome completo del file XML> /sdc</code>	Salvare l'elenco delle regole di Controllo distribuzione software in un file.
<code>/clearsdc</code>	Elimina tutte le regole di Controllo distribuzione software dall'elenco.

Generazione regole per Controllo dell'avvio delle applicazioni KAVSHELL APPCONTROL /GENERATE

Utilizzando il comando `KAVSHELL APPCONTROL /GENERATE`, è possibile generare gli elenchi di regole di Controllo dell'avvio delle applicazioni.

Potrebbe essere richiesta la password per eseguire il comando. Immettere la chiave di utilizzo `[/pwd:<password>]` della password corrente.

Sintassi del comando KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL /GENERATE <percorso della cartella> | /source:<percorso del file con l'elenco delle cartelle> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<utente o gruppo di utenti>] [/export:<percorso del file XML>] [/import:<a|r|m>] [/prefix:<prefisso per i nomi delle regole>] [/unique]
```

Esempi di comandi KAVSHELL APPCONTROL /GENERATE

- Per generare regole per i file nelle cartelle specificate, eseguire il seguente comando:

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

- Per generare regole per i file eseguibili con tutte le estensioni disponibili nella cartella specificata e, dopo il completamento dell'attività, salvare le regole generate nel file XML specificato, eseguire il seguente comando:

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms
/export:c:\rules\appctrlrules.xml
```

A seconda della sintassi delle chiavi, è possibile configurare le impostazioni di generazione delle regole automatiche per l'attività Controllo dell'avvio delle applicazioni (vedere la seguente tabella).

Tabella 44. Chiavi del comando `KAVSHELL APPCONTROL /GENERATE`

Chiave	Descrizione
Ambito di applicazione delle regole di permesso	
<percorso della cartella>	Specifica il percorso della cartella con i file eseguibili che richiedono le regole di permesso generate automaticamente.
/source: <percorso del file con l'elenco delle cartelle>	Specifica il percorso del file TXT con l'elenco delle cartelle che contengono i file eseguibili che richiedono le regole di permesso generate automaticamente.

Chiave	Descrizione
/masks: <edms>	<p>Specifica le estensioni dei file eseguibili che richiedono le regole di permesso generate automaticamente.</p> <p>È possibile includere nell'ambito di applicazione delle regole i file con le seguenti estensioni:</p> <ul style="list-style-type: none"> • e - file EXE • d - file DLL • m - file MSI • s - script
/runapp	<p>Durante la generazione delle regole di permesso, vengono prese in considerazione le applicazioni in esecuzione in un computer protetto al momento dell'esecuzione dell'attività.</p>
Azioni durante la generazione automatica delle regole di permesso	
/rules: <ch cp h>	<p>Specifica le azioni da eseguire durante la generazione delle regole di permesso di Controllo dell'avvio delle applicazioni:</p> <ul style="list-style-type: none"> • ch - utilizza il certificato digitale. Se il certificato risulta mancante, utilizza l'hash SHA256. • cp - utilizza il certificato digitale. Se il certificato risulta mancante, utilizza il percorso del file eseguibile. • h - utilizza l'hash SHA256.
/strong	<p>Utilizza il soggetto e l'identificazione personale del certificato digitale durante la generazione automatica delle regole di permesso di Controllo dell'avvio delle applicazioni. Il comando viene eseguito se è specificata la chiave /rules: <ch cp>.</p>
/user: <utente o gruppo di utenti>	<p>Specifica il nome utente o un gruppo di utenti per cui saranno applicate le regole. Verrà monitorata qualsiasi applicazione eseguita dall'utente e/o dal gruppo di utenti specificato.</p>
Azioni al completamento di Generazione regole per Controllo dell'avvio delle applicazioni	
/export: <percorso del file XML>	<p>Salva le regole generate nel file XML.</p>
/unique	<p>Aggiunge le informazioni sul computer con le applicazioni installate che rappresentano la base per la generazione delle regole di permesso di Controllo dell'avvio delle applicazioni.</p>
/prefix: <prefisso per i nomi delle regole>	<p>Specifica il prefisso dei nomi per la generazione delle regole di permesso di Controllo dell'avvio delle applicazioni.</p>
/import: <a r m>	<p>Importa le regole generate nell'elenco delle regole di Controllo dell'avvio delle applicazioni specificate in base al principio di aggiunta selezionato. :</p> <ul style="list-style-type: none"> • a - Aggiungi alle regole esistenti (le regole con impostazioni identiche vengono duplicate) • r - Sostituisci le regole esistenti (le regole con parametri identici non vengono aggiunte: la regola viene aggiunta se almeno un parametro della regola è univoco) • m - Unisci con le regole esistenti (le regole con parametri identici non vengono aggiunte: la regola viene aggiunta se almeno un parametro della regola è univoco)

Compilazione dell'elenco delle regole di Controllo dell'avvio delle applicazioni KAVSHELL APPCONTROL

Utilizzando `KAVSHELL APPCONTROL` è possibile aggiungere regole dal file XML all'elenco di regole dell'attività Controllo dell'avvio delle applicazioni in base al principio selezionato, nonché eliminare tutte le regole impostate dall'elenco.

Potrebbe essere richiesta la password per eseguire il comando. Immettere la chiave di utilizzo `[/pwd:<password>]` della password corrente.

Sintassi del comando KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <percorso del file XML> | /replace <percorso del file XML> | /merge <percorso del file XML> | /clear
```

Esempi di comandi KAVSHELL APPCONTROL

- Per aggiungere regole da un file XML alle regole già specificate per l'attività Controllo dell'avvio delle applicazioni in base al principio *Aggiungi alle regole esistenti*, eseguire il seguente comando:

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

A seconda della sintassi delle chiavi, è possibile selezionare il principio per l'aggiunta delle nuove regole da un file XML specificato a un elenco di regole di Controllo dell'avvio delle applicazioni definite (vedere la seguente tabella).

Tabella 45. Chiavi del comando KAVSHELL SCAN

Chiave	Descrizione
<code>/append <percorso del file XML></code>	Rinnovare l'elenco delle regole di Controllo dell'avvio delle applicazioni in base a un file XML specificato. Principio di aggiunta - Aggiungi alle regole esistenti (le regole con impostazioni identiche vengono duplicate)
<code>/replace <percorso del file XML></code>	Rinnovare l'elenco delle regole di Controllo dell'avvio delle applicazioni in base a un file XML specificato. Principio di aggiunta - Sostituisci le regole esistenti (le regole con parametri identici non vengono aggiunte: la regola viene aggiunta se almeno un parametro della regola è univoco)
<code>/merge <percorso del file XML></code>	Rinnovare l'elenco delle regole di Controllo dell'avvio delle applicazioni in base a un file XML specificato. Principio di aggiunta - Unisci con le regole esistenti (le nuove regole non duplicano le regole già impostate).
<code>/clear</code>	Cancellare l'elenco delle regole di Controllo dell'avvio delle applicazioni.

Compilazione dell'elenco delle regole di Controllo dispositivi. KAVSHELL DEVCONTROL

Utilizzando `KAVSHELL DEVCONTROL` è possibile aggiungere regole dal file XML all'elenco di regole dell'attività Controllo dispositivi in base al principio selezionato, nonché eliminare tutte le regole impostate dall'elenco.

Potrebbe essere richiesta la password per eseguire il comando. Immettere la chiave di utilizzo `[/pwd:<password>]` della password corrente.

Sintassi del comando KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <percorso del file XML> | /replace <percorso del file XML> | /merge <percorso del file XML> | /clear
```

Esempi di comandi KAVSHELL DEVCONTROL

- Per aggiungere regole da un file XML alle regole già specificate per l'attività Controllo dispositivi in base al principio **Aggiungi alle regole esistenti**, eseguire il seguente comando:

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

A seconda della sintassi delle chiavi, è possibile selezionare il principio per l'aggiunta delle nuove regole da un file XML specificato a un elenco di regole di Controllo dispositivi definite (vedere la seguente tabella).

Tabella 46. Chiavi del comando `KAVSHELL DEVCONTROL`

Chiave	Descrizione
<code>/append <percorso del file XML></code>	Rinnovare l'elenco delle regole di Controllo dispositivi in base a un file XML specificato. Principio di aggiunta - Aggiungi alle regole esistenti (le regole con impostazioni identiche vengono duplicate)
<code>/replace <percorso del file XML></code>	Rinnovare l'elenco delle regole di Controllo dispositivi in base a un file XML specificato. Principio di aggiunta - Sostituisci le regole esistenti (le regole con parametri identici non vengono aggiunte: la regola viene aggiunta se almeno un parametro della regola è univoco)
<code>/merge <percorso del file XML></code>	Rinnovare l'elenco delle regole di Controllo dispositivi in base a un file XML specificato. Principio di aggiunta - Unisci con le regole esistenti (le nuove regole non duplicano le regole già impostate).
<code>/clear</code>	Cancellare l'elenco delle regole di Controllo dispositivi.

Avvio dell'attività di aggiornamento dei database di Kaspersky Embedded Systems Security 2.2. KAVSHELL UPDATE

Il comando `KAVSHELL UPDATE` può essere utilizzato per avviare il comando Aggiornamento database di Kaspersky Embedded Systems Security 2.2 nella modalità sincrona.

L'attività Aggiornamento database di Kaspersky Embedded Systems Security 2.2 eseguita tramite `KAVSHELL UPDATE` è un'attività temporanea. È visualizzata nella console dell'applicazione solo durante l'esecuzione. Il log dell'attività viene generato contemporaneamente. È visualizzato in **Log delle attività** nella console dell'applicazione. I criteri di Kaspersky Security Center possono essere applicati alle attività di aggiornamento create e avviate tramite il comando `KAVSHELL`

UPDATE e le attività di aggiornamento create nella console dell'applicazione. Per informazioni sulla gestione di Kaspersky Embedded Systems Security 2.2 nei computer tramite Kaspersky Security Center, fare riferimento alla sezione "Gestione di Kaspersky Embedded Systems Security 2.2 tramite Kaspersky Security Center".

È possibile utilizzare le variabili di ambiente durante la specificazione del percorso della sorgente degli aggiornamenti in questa attività. Se si utilizzano le variabili di ambiente di un utente, eseguire il comando KAVSHELL UPDATE con le autorizzazioni per questo utente.

Sintassi del comando per KAVSHELL UPDATE

```
KAVSHELL UPDATE < Percorso della sorgente degli aggiornamenti | /AK | /KL>
[/NOUSEKL] [/PROXY:<indirizzo>:<porta>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<nome
utente>] [/PROXYPWD:<password>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM]
[/NOFTPPASSIVE] [/TIMEOUT:<secondi>] [/REG:<codice iso3166>] [/W:<percorso del
file di log dell'attività>] [/ALIAS:<alias dell'attività>]
```

Il comando KAVSHELL UPDATE ha sia chiavi obbligatorie che facoltative (vedere la seguente tabella).

Esempi del comando KAVSHELL UPDATE

- Per avviare un'attività *Aggiornamento database personalizzata*, eseguire il seguente comando:

```
KAVSHELL UPDATE
```

- Per eseguire l'attività *Aggiornamento database utilizzando i file di aggiornamento nella cartella di rete \\server\databases*, eseguire il seguente comando:

```
KAVSHELL UPDATE \\server\databases
```

- Per avviare un'attività di aggiornamento dal server FTP <ftp://dnl-ru1.kaspersky-labs.com/> e scrivere tutti gli eventi dell'attività nel file `c:\update_report.log`, eseguire il comando:

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

- Per scaricare gli aggiornamenti del database di Kaspersky Embedded Systems Security 2.2 dal server di aggiornamento di Kaspersky Lab, connettersi alla sorgente degli aggiornamenti tramite un server proxy (indirizzo del server proxy: `proxy.company.com`, porta: 8080) per accedere al computer utilizzando l'autenticazione NTLM predefinita di Microsoft Windows con nome utente `inetuser` e password 123456, eseguire il seguente comando:

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1
/PROXYUSER:inetuser /PROXYPWD:123456
```

Tabella 47. Chiavi del comando KAVSHELL UPDATE

Chiave	Descrizione
Sorgenti degli aggiornamenti (chiave obbligatoria).	Specificare una o più sorgenti. Kaspersky Embedded Systems Security 2.2 accederà alle sorgenti nell'ordine in cui sono elencate. Delimitare le sorgenti con uno spazio.
<percorso in formato UNC>	Sorgente degli aggiornamenti definita dall'utente. Percorso della cartella degli aggiornamenti in rete nel formato UNC.

Chiave	Descrizione
<URL>	Sorgente degli aggiornamenti definita dall'utente. Indirizzo del server HTTP o FTP in cui è contenuta la cartella degli aggiornamenti.
<Cartella locale>	Sorgente degli aggiornamenti definita dall'utente. Cartella sul computer protetto.
/AK	Kaspersky Security Center Administration Server come sorgente degli aggiornamenti.
/KL	Server di aggiornamento di Kaspersky Lab come sorgenti degli aggiornamenti.
/NOUSEKL	Non utilizzare i server di aggiornamento di Kaspersky Lab se non sono disponibili altre sorgenti degli aggiornamenti (utilizzato per impostazione predefinita).
Impostazioni del server proxy	
/PROXY:<indirizzo>:<porta>	Nome di rete o indirizzo IP del server proxy e relativa porta. Se questa chiave non è specificata, Kaspersky Embedded Systems Security 2.2 rileverà automaticamente le impostazioni del server proxy utilizzato nella rete LAN.
/AUTHTYPE:<0-2>	Questa chiave specifica il metodo di autenticazione per l'accesso al server proxy. Può avere i seguenti valori: 0 - autenticazione NTLM predefinita di Microsoft Windows; Kaspersky Embedded Systems Security 2.2 contatterà il server proxy con l'account Sistema locale (SYSTEM) 1 - autenticazione NTLM predefinita di Microsoft Windows; Kaspersky Embedded Systems Security 2.2 contatterà il server proxy con l'account con il nome utente e la password specificati dalle chiavi /PROXYUSER e /PROXYPWD 2 - autenticazione tramite il nome utente e la password specificati dalle chiavi /PROXYUSER e /PROXYPWD (autenticazione di base) Se non è richiesta l'autenticazione per accedere al server proxy, non è necessario specificare una chiave.
/PROXYUSER:<nome utente>	Nome utente che sarà utilizzato per l'accesso al server proxy. Se è specificato il valore della chiave /AUTHTYPE:0, le chiavi /PROXYUSER:<nome utente> e /PROXYPWD:<password> saranno ignorate.
/PROXYPWD:<password>	Password dell'utente che sarà utilizzata per l'accesso al server proxy. Se è specificato il valore della chiave /AUTHTYPE:0, le chiavi /PROXYUSER:<nome utente> e /PROXYPWD:<password> saranno ignorate. Se la chiave /PROXYUSER è specificata e /PROXYPWD è omesso, la password sarà considerata vuota.
/NOPROXYFOR L	Non utilizzare le impostazioni del server proxy per la connessione ai server degli aggiornamenti Kaspersky Lab (utilizzato per impostazione predefinita).
/USEPROXYFOR CUSTOM	Utilizzare le impostazioni del server proxy per la connessione alle sorgenti degli aggiornamenti definite dall'utente (non utilizzato per impostazione predefinita).
/USEPROXYFOR LOCAL	Utilizzare le impostazioni del server proxy per la connessione alle sorgenti degli aggiornamenti locali. Se non è specificato, verrà applicato il valore Non utilizzare un server proxy per gli indirizzi locali .
Impostazioni generali dei server FTP e HTTP	
/NOFTPPASSIVE	Se questa chiave è specificata, Kaspersky Embedded Systems Security 2.2 utilizzerà la modalità FTP attiva per la connessione al server protetto. Se questa chiave non è specificata, Kaspersky Embedded Systems Security 2.2 utilizzerà la modalità FTP passiva, se possibile.

Chiave	Descrizione
/TIMEOUT:<numero di secondi>	Timeout della connessione al server FTP o HTTP. Se non si specifica questa chiave, Kaspersky Embedded Systems Security 2.2 utilizzerà il valore predefinito: 10 secondi. Il valore della chiave deve essere un numero intero.
/REG:<codice iso3166>	<p>Impostazioni internazionali. Questa chiave è utilizzata durante la ricezione degli aggiornamenti dai server di aggiornamento di Kaspersky Lab. Kaspersky Embedded Systems Security 2.2 ottimizza il carico degli aggiornamenti sul computer protetto selezionando il server di aggiornamento più vicino.</p> <p>Come valore di questa chiave, specificare il codice del paese in cui è posizionato il computer protetto in conformità con lo standard ISO 3166-1, ad esempio /REG: gr o /REG:RU. Se questa chiave è omessa o viene specificato un codice di paese inesistente, Kaspersky Embedded Systems Security 2.2 rileverà la posizione del computer protetto in base alle impostazioni internazionali nel computer in cui è installata la console dell'applicazione.</p>
/ALIAS:<alias dell'attività>	<p>Questa chiave consente di assegnare un nome temporaneo all'attività, da utilizzare per accedere all'attività durante la sua esecuzione. Ad esempio, le statistiche dell'attività possono essere visualizzate utilizzando il comando TASK. L'alias dell'attività deve essere univoco tra gli alias di attività di tutti i componenti funzionali di Kaspersky Embedded Systems Security 2.2.</p> <p>Se questa chiave non è specificata, sarà utilizzato update_<pid_kavshell>, ad esempio update_1234. Nella console dell'applicazione all'attività verrà automaticamente assegnato il nome Update-databases (<data ora>), ad esempio Update-databases 16/8/2007 17:41:02.</p>
/W:<percorso del file di log dell'attività>	<p>Se si specifica questa chiave, Kaspersky Embedded Systems Security 2.2 salverà il file di log dell'attività con il nome definito dal valore della chiave.</p> <p>Il file di log contiene le statistiche sull'esecuzione dell'attività, l'ora di avvio e completamento (interruzione) e le informazioni sugli eventi relativi all'attività.</p> <p>Il log viene utilizzato per registrare gli eventi definiti dalle impostazioni dei log dell'attività e del log eventi di Kaspersky Embedded Systems Security 2.2 nel "Visualizzatore eventi". È possibile specificare il percorso assoluto o relativo del file di log. Se si specifica solo il nome del file senza il percorso, il file di log verrà creato nella cartella corrente.</p> <p>Riavviando il comando con le stesse impostazioni per il log, verrà sovrascritto il file di log esistente.</p> <p>Il file di log può essere visualizzato mentre un'attività è in esecuzione.</p> <p>Il log è visualizzato nel nodo Log delle attività della console dell'applicazione.</p> <p>Se Kaspersky Embedded Systems Security 2.2 non riesce a creare il file di log, non interrompe l'esecuzione del comando né visualizza un messaggio di errore.</p>

Codici restituiti per il comando KAVSHELL UPDATE (a pagina [247](#)).

Rollback degli aggiornamenti dei database di Kaspersky Embedded Systems Security 2.2. KAVSHELL ROLLBACK

Il comando `KAVSHELL ROLLBACK` può essere utilizzato per eseguire un'attività di sistema di rollback dei database di Kaspersky Embedded Systems Security 2.2 (rollback dei database di Kaspersky Embedded Systems Security 2.2 alla versione precedentemente installata). Il comando è eseguito in modalità sincrona.

Sintassi del comando:

KAVSHELL ROLLBACK

Codici restituiti per il comando KAVSHELL ROLLBACK (a pagina [247](#)).**Gestione di Analisi log. KAVSHELL TASK LOG-INSPECTOR**

Il comando KAVSHELL TASK LOG-INSPECTOR può essere utilizzato per monitorare l'integrità dell'ambiente in base all'analisi del log eventi di Windows.

Sintassi del comando

KAVSHELL TASK LOG-INSPECTOR

Esempi di comandi

KAVSHELL TASK LOG-INSPECTOR /stop

Tabella 48. KAVSHELL TASK LOG-INSPECTOR modificatori del comando

Chiave	Descrizione
/START	Avvia l'attività specificata in modalità asincrona.
/STOP	Interrompe l'attività specificata.
/STATE	Restituisce lo stato dell'attività corrente (ad esempio <i>In esecuzione, Completata, Sospesa, Arrestata, Non riuscita, Avvio in corso, Ripristino in corso</i>).
/STATISTICS	Recupera le statistiche dell'attività - informazioni sul numero di oggetti elaborati dall'avvio dell'attività fino al momento corrente.

Codici restituiti per il comando KAVSHELL TASK LOG-INSPECTOR (vedere la sezione "Codici restituiti per il comando KAVSHELL TASK LOG-INSPECTOR" a pagina [246](#)).

Attivazione dell'applicazione. KAVSHELL LICENSE

Le chiavi e i codici di attivazione di Kaspersky Embedded Systems Security 2.2 possono essere gestiti utilizzando il comando KAVSHELL LICENSE.

Potrebbe essere richiesta la password per eseguire il comando. Immettere la chiave di utilizzo [/pwd:<password>] della password corrente.

Sintassi del comando per KAVSHELL FULLSCAN

KAVSHELL LICENSE [/ADD:<file chiave | codice di attivazione> [/R] | /DEL:<chiave | numero del codice di attivazione>]

Esempi del comando KAVSHELL SCAN

► Per attivare l'applicazione, eseguire il comando:

```
KAVSHELL.EXE LICENSE / ADD: <codice di attivazione o chiave>
```

► Per visualizzare le informazioni sulle chiavi aggiunte, eseguire il comando:

```
KAVSHELL LICENSE
```

► Per rimuovere una chiave aggiunta con il numero 0000-000000-00000001, eseguire il comando:

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

Il comando `KAVSHELL LICENSE` può essere eseguito con o senza chiavi (vedere la seguente tabella).

Tabella 49. Chiavi del comando `KAVSHELL LICENSE`

Chiave	Descrizione
Senza chiavi	Il comando restituisce le seguenti informazioni sulle chiavi aggiunte: <ul style="list-style-type: none"> • Chiave. • Tipo di licenza (commerciale). • Durata della licenza associata alla chiave. • Stato della chiave (attiva o di riserva). Se il valore specificato è *, la chiave è stata aggiunta come chiave di riserva.
/ADD:<nome del file chiave o del codice di attivazione>	Aggiunge la chiave tramite il file o il codice di attivazione specificato. Per specificare il percorso di un file chiave è possibile utilizzare le variabili di ambiente di sistema (le variabili di ambiente dell'utente non sono consentite).
/R	Il codice di attivazione o la chiave /R è un'aggiunta al codice di attivazione o alla chiave /ADD e indica che il codice di attivazione o la chiave aggiunta è un codice di attivazione o una chiave di riserva.
/DEL:<chiave o codice di attivazione>	Elimina la chiave con il numero specificato o il codice di attivazione selezionato.

Codici restituiti per il comando `KAVSHELL LICENSE` (vedere la sezione "Codici restituiti per il comando `KAVSHELL LICENSE`" a pagina [248](#)).

Abilitazione, configurazione e disabilitazione del log di traccia. KAVSHELL TRACE

Il comando `KAVSHELL TRACE` può essere utilizzato per abilitare e disabilitare il log di traccia per tutti i sottosistemi di Kaspersky Embedded Systems Security 2.2 e per impostare il livello di dettaglio del log.

Kaspersky Embedded Systems Security 2.2 scrive le informazioni nei file di traccia e nel file di dump in formato non criptato.

Sintassi del comando per `KAVSHELL TRACE`

```
KAVSHELL TRACE </ON /F:<percorso della cartella del file di log di traccia>
```

```
[/S:<dimensione massima del log in megabyte>]
[/LVL:debug|info|warning|error|critical] | /OFF>
```

Se si mantiene il log di traccia e si desidera modificarne le impostazioni, immettere il comando `KAVSHELL TRACE` con la chiave `/ON` e specificare le impostazioni del log con i valori delle chiavi `/S` e `/LVL` (vedere la seguente tabella).

Tabella 50. Chiavi del comando `KAVSHELL TRACE`

Chiave	Descrizione
<code>/ON</code>	Abilita il log di traccia.
<code>/F:<cartella con i file dei log di traccia></code>	<p>Questa chiave specifica il percorso completo della cartella in cui saranno salvati i file dei log di traccia (obbligatorio).</p> <p>Se si specifica il percorso di una cartella inesistente, il log di traccia non verrà creato. È possibile utilizzare i percorsi di rete in formato UNC (Universal Naming Convention), ma non possono essere specificati percorsi di cartelle nelle unità di rete del computer protetto.</p> <p>Se il nome della cartella di cui si specifica il percorso come valore della chiave contiene uno spazio, racchiudere il percorso della cartella tra virgolette, ad esempio: <code>/F:"C:\Trace Folder"</code>.</p> <p>Per specificare il percorso dei file di log di traccia è possibile utilizzare le variabili di ambiente di sistema (le variabili di ambiente dell'utente non sono consentite).</p>
<code>/S: <dimensione massima del file di log in megabyte></code>	<p>Questa chiave imposta la dimensione massima di un singolo file di log di traccia. Non appena il file di log raggiunge il livello massimo, Kaspersky Embedded Systems Security 2.2 avvia la registrazione delle informazioni in un nuovo file. Il file di log precedente verrà salvato.</p> <p>Se il valore di questa chiave non è specificato, la dimensione massima di un file di log sarà di 50 MB.</p>
<code>/LVL:debug info warning error critical</code>	<p>Questa chiave imposta il livello di dettaglio del log, dal livello massimo (Tutte le informazioni di debug), in cui tutti gli eventi vengono registrati nel log, al livello minimo (Eventi critici), in cui sono registrati solo gli eventi critici.</p> <p>Se questa chiave non è specificata, nel log di traccia saranno registrati gli eventi con il livello di dettaglio Tutte le informazioni di debug.</p>
<code>/OFF</code>	Questa chiave disabilita il log di traccia.

Esempi del comando KAVSHELL TRACE

- Per abilitare il log di traccia con il livello di dettaglio **Tutte le informazioni di debug** e la dimensione massima del log di 200 MB e salvare il file di log nella cartella C:\Trace Folder, eseguire il comando:

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

- Per abilitare il log di traccia con il livello di dettaglio **Eventi importanti** e salvare il file di log nella cartella C:\Trace Folder, eseguire il comando:

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

- Per disabilitare il log di traccia, eseguire il comando:

```
KAVSHELL TRACE /OFF
```

Codici restituiti per il comando KAVSHELL TRACE (vedere la sezione "Codici restituiti per il comando KAVSHELL TRACE" a pagina [248](#)).

Deframmentazione dei file di log di Kaspersky Embedded Systems Security 2.2. KAVSHELL VACUUM

Utilizzando il comando `KAVSHELL VACUUM` è possibile deframmentare i file di log dell'applicazione. Questo consente di evitare gli errori di sistema o gli errori durante l'esecuzione di Kaspersky Embedded Systems Security 2.2 correlati all'archiviazione dei log.

Potrebbe essere richiesta la password per eseguire il comando. Immettere la chiave di utilizzo [/pwd:<password>] della password corrente.

È consigliabile applicare il comando `KAVSHELL VACUUM` per ottimizzare l'archiviazione dei file di log in caso di avvii frequenti delle attività Scansione su richiesta e delle attività di aggiornamento. Durante l'esecuzione del comando, Kaspersky Embedded Systems Security 2.2 rinnova una struttura logica per i file di log dell'applicazione che sono archiviati in un computer protetto in base al percorso specificato.

Per impostazione predefinita, i file di log dell'applicazione sono archiviati nel percorso: C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security 2.2\2.2\Reports. Se è stato specificato manualmente un altro percorso per l'archiviazione dei log, il comando `KAVSHELL VACUUM` esegue la deframmentazione per i file nella cartella specificata nelle impostazioni dei log di Kaspersky Embedded Systems Security 2.2.

La deframmentazione di file di grandi dimensioni aumenta il tempo per l'esecuzione del comando `KAVSHELL VACUUM`.

Le attività Protezione in tempo reale e Controllo del computer non sono disponibili per l'esecuzione durante l'esecuzione del comando `KAVSHELL VACUUM`. Il processo di deframmentazione in corso limita l'accesso al log di Kaspersky Embedded Systems Security 2.2 e non consente la registrazione di eventi. Per evitare la riduzione del livello di sicurezza, è consigliabile pianificare l'esecuzione del comando `KAVSHELL VACUUM` in un periodo di inattività.

- Per deframmentare i file di log di Kaspersky Embedded Systems Security 2.2, eseguire il seguente comando:

```
KAVSHELL VACUUM
```

L'esecuzione del comando è possibile se questo viene avviato con diritti di amministratore locale per l'account.

Pulizia del database di iSwift. KAVSHELL FBRESET

Kaspersky Embedded Systems Security 2.2 utilizza la tecnologia iSwift, che consente all'applicazione di evitare di esaminare di nuovo i file che non sono stati modificati dall'ultima scansione (**Usa la tecnologia iSwift**).

Kaspersky Embedded Systems Security 2.2 crea nella directory %SYSTEMDRIVE%\System Volume Information i file klamfb.dat e klamfb2.dat, che contengono informazioni sugli oggetti puliti che sono già stati esaminati. Il file klamfb.dat (klamfb2.dat) aumenta di dimensioni con il numero di file esaminati da Kaspersky Embedded Systems Security 2.2. Il file contiene solo informazioni aggiornate sui file esistenti nel sistema: se un file viene rimosso, Kaspersky Embedded Systems Security 2.2 elimina le relative informazioni da klamfb.dat.

Per pulire un file, utilizzare il comando `KAVSHELL FBRESET`.

Tenere presente le specifiche seguenti per l'utilizzo del comando `KAVSHELL FBRESET`:

- Durante la pulizia del file klamfb.dat tramite il comando `KAVSHELL FBRESET`, Kaspersky Embedded Systems Security 2.2 non sospende la protezione (a differenza di quanto avviene nel caso dell'eliminazione manuale di klamfb.dat).
- Kaspersky Embedded Systems Security 2.2 può aumentare il carico di lavoro del computer dopo la cancellazione dei dati in klamfb.dat. In questo caso, il software anti-virus esamina tutti i file a cui viene eseguito l'accesso per la prima volta dopo la cancellazione di klamfb.dat. Dopo la scansione, Kaspersky Embedded Systems Security 2.2 aggiunge di nuovo a klamfb.dat le informazioni su ogni oggetto esaminato. Nel caso di nuovi tentativi di accesso all'oggetto, la tecnologia iSwift eviterà di ripetere la scansione del file, purché rimanga invariato.

L'esecuzione del comando `KAVSHELL FBRESET` è disponibile solo se la riga di comando viene avviata con l'account `SYSTEM`.

Abilitazione e disabilitazione della creazione del file di dump. KAVSHELL DUMP

La creazione di snapshot (file di dump) per i processi di Kaspersky Embedded Systems Security 2.2 nei casi di arresto anomalo può essere abilitata o disabilitata tramite il comando `KAVSHELL DUMP` (vedere la seguente tabella). In aggiunta, gli snapshot della memoria dei processi di Kaspersky Embedded Systems Security 2.2 in corso possono essere acquisiti in qualsiasi momento.

Per la corretta creazione dei file di dump è necessario eseguire il comando `KAVSHELL DUMP` con l'account di sistema locale (`SYSTEM`).

Sintassi del comando per KAVSHELL DUMP

KAVSHELL DUMP </ON /F:<cartella con il file di dump>|/SNAPSHOT /F:<cartella con il file di dump> / P:<pid> | /OFF>

Esempi del comando KAVSHELL DUMP

- Per abilitare la creazione del file di dump e salvare il file di dump nella cartella C:\Dump Folder, eseguire il comando:

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

- Per creare un dump per il processo con l'ID 1234 nella cartella C:\Dumps, eseguire il comando:

```
KAVSHELL DUMP /SNAPSHOT /F: C:\Dumps /P:1234
```

- Per disabilitare la generazione del file di dump, eseguire il comando:

```
KAVSHELL DUMP /OFF
```

Tabella 51. Chiavi del comando KAVSHELL DUMP

Chiave	Descrizione
/ON	Abilita la creazione del file di dump della memoria del processo in caso di arresto anomalo.
/F:<percorso della cartella con i file di dump>	Questa è una chiave obbligatoria. Specifica il percorso della cartella in cui verranno salvati i file di dump. Se si specifica il percorso di una cartella inesistente, il file di dump non verrà creato. È possibile utilizzare i percorsi di rete in formato UNC (Universal Naming Convention), ma non possono essere specificati percorsi di cartelle nelle unità di rete del computer protetto. Per specificare il percorso della cartella con i file di dump della memoria è possibile utilizzare le variabili di ambiente di sistema (le variabili di ambiente dell'utente non sono consentite).
/SNAPSHOT	Acquisisce uno snapshot della memoria del processo di Kaspersky Embedded Systems Security 2.2 specificato in corso e salva il file di dump nella cartella il cui percorso è specificato dalla chiave /F.
/P	L'identificatore del processo PID è visualizzato in Gestione attività di Microsoft Windows.
/OFF	Disabilita la creazione del file di dump della memoria in caso di arresto anomalo.

Codici restituiti per il comando KAVSHELL DUMP (vedere la sezione "Codici restituiti per il comando KAVSHELL DUMP" a pagina [249](#)).

Importazione delle impostazioni. KAVSHELL IMPORT

Il comando `KAVSHELL IMPORT` consente di importare le impostazioni di Kaspersky Embedded Systems Security 2.2, le relative funzionalità e attività da un file di configurazione in una copia di Kaspersky Embedded Systems Security 2.2 sul computer protetto. Un file di configurazione può essere creato utilizzando il comando `KAVSHELL EXPORT`.

Potrebbe essere richiesta la password per eseguire il comando. Immettere la chiave di utilizzo `[/pwd:<password>]` della password corrente.

Sintassi del comando per KAVSHELL IMPORT

```
KAVSHELL IMPORT <nome del file di configurazione e percorso del file>
```

Esempi del comando KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Tabella 52. Chiavi del comando KAVSHELL IMPORT

Chiave	Descrizione
<nome del file di configurazione e percorso del file>	Nome del file di configurazione utilizzato come origine di importazione per le impostazioni. Per specificare il percorso del file è possibile utilizzare le variabili di ambiente di sistema (le variabili di ambiente dell'utente non sono consentite).

Codici restituiti per il comando `KAVSHELL IMPORT` (vedere la sezione "Codici restituiti per il comando `KAVSHELL IMPORT`" a pagina [249](#)).

Esportazione delle impostazioni. KAVSHELL EXPORT

Il comando `KAVSHELL EXPORT` consente di esportare tutte le impostazioni di Kaspersky Embedded Systems Security 2.2 e le relative attività correnti in un file di configurazione per importarle in seguito in copie di Kaspersky Embedded Systems Security 2.2 installate in altri computer.

Sintassi del comando per KAVSHELL EXPORT

```
KAVSHELL EXPORT <nome del file di configurazione e percorso del file>
```

Esempi del comando KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Tabella 53. Chiavi del comando KAVSHELL EXPORT

Chiave	Descrizione
<nome del file di configurazione e percorso del file>	Nome del file di configurazione che conterrà le impostazioni. È possibile assegnare qualsiasi estensione al file di configurazione. Per specificare il percorso del file è possibile utilizzare le variabili di ambiente di sistema (le variabili di ambiente dell'utente non sono consentite).

Codici restituiti per il comando `KAVSHELL EXPORT` (vedere la sezione "Codici restituiti per il comando `KAVSHELL EXPORT`" a pagina [249](#)).

Integrazione con Microsoft Operations Management Suite. KAVSHELL OMSINFO

Utilizzando il comando KAVSHELL OMSINFO, è possibile esaminare lo stato dell'applicazione e le informazioni sulle minacce rilevate dai database anti-virus e dal servizio KSN. I dati sulle minacce sono ricavati dai log eventi disponibili.

Sintassi del comando KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <nome e percorso completo del file generato>
```

Esempi del comando KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Tabella 54. Chiavi del comando KAVSHELL OMSINFO

Chiave	Descrizione
<nome e percorso del file generato>	Nome del file generato che includerà le informazioni sullo stato dell'applicazione e le minacce rilevate.

Codici restituiti dalla riga di comando

In questa sezione

Codici restituiti per i comandi KAVSHELL START e KAVSHELL STOP.....	245
Codici restituiti per i comandi KAVSHELL SCAN e KAVSHELL SCANCritical.....	245
Codici restituiti per il comando KAVSHELL TASK LOG-INSPECTOR.....	246
Codici restituiti per il comando KAVSHELL TASK.....	246
Codici restituiti per il comando KAVSHELL RTP.....	246
Codici restituiti per il comando KAVSHELL UPDATE.....	247
Codici restituiti per il comando KAVSHELL ROLLBACK.....	247
Codici restituiti per il comando KAVSHELL LICENSE.....	248
Codici restituiti per il comando KAVSHELL TRACE.....	248
Codici restituiti per il comando KAVSHELL FBRESET.....	248
Codici restituiti per il comando KAVSHELL DUMP.....	249
Codici restituiti per il comando KAVSHELL IMPORT.....	249
Codici restituiti per il comando KAVSHELL EXPORT.....	249

Codici restituiti per i comandi KAVSHELL START e KAVSHELL STOP

Tabella 55. Codici restituiti per i comandi KAVSHELL START e KAVSHELL STOP

Codice restituito	Descrizione
0	Operazione completata
-3	Errore di autorizzazioni
-5	Sintassi del comando non valida
-6	Operazione non valida (ad esempio, il servizio di Kaspersky Embedded Systems Security 2.2 è già in esecuzione o è già stato arrestato)
-7	Servizio non registrato
-8	L'avvio del servizio automatico è disabilitato.
-9	Tentativo di avviare il computer con un altro account utente non riuscito (per impostazione predefinita, il servizio di Kaspersky Embedded Systems Security 2.2 viene eseguito con l'account utente Sistema locale)
-99	Errore sconosciuto

Codici restituiti per i comandi KAVSHELL SCAN e KAVSHELL SCANCritical

Tabella 56. Codici restituiti per i comandi KAVSHELL SCAN e KAVSHELL SCANCritical

Codice restituito	Descrizione
0	Operazione completata (nessuna minaccia rilevata)
1	Operazione annullata
-2	Servizio non in esecuzione
-3	Errore di autorizzazioni
-4	Oggetto non trovato (file con l'elenco degli ambiti della scansione non trovato)
-5	Sintassi del comando non valida o ambito della scansione non definito
-80	Oggetti infetti e di altro tipo rilevati
-81	Oggetti potenzialmente infetti rilevati
-82	Errori di elaborazione rilevati
-83	Oggetti non controllati individuati
-84	Oggetti danneggiati rilevati
-85	Creazione del file di log all'attività non riuscita
-99	Errore sconosciuto
-301	Chiave non valida

Codici restituiti per il comando KAVSHELL TASK LOG-INSPECTOR

Tabella 57. Codice restituito per il comando KAVSHELL TASK LOG-INSPECTOR

Codice restituito	Descrizione
0	Operazione completata
-6	Operazione non valida (ad esempio, il servizio di Kaspersky Embedded Systems Security 2.2 è già in esecuzione o è già stato arrestato)
402	L'attività è già in esecuzione (per il modificatore /STATE)

Codici restituiti per il comando KAVSHELL TASK

Tabella 58. Codici restituiti per il comando KAVSHELL TASK

Codice restituito	Descrizione
0	Operazione completata
-2	Servizio non in esecuzione
-3	Errore di autorizzazioni
-4	Oggetto non trovato (attività non trovata)
-5	Sintassi del comando non valida
-6	Operazione non valida (ad esempio, l'attività non è in esecuzione, è già in esecuzione o non può essere sospesa)
-99	Errore sconosciuto
-301	Chiave non valida
401	Attività non in esecuzione (per il modificatore /STATE)
402	Attività già in esecuzione (per il modificatore /STATE)
403	Attività già sospesa (per il modificatore /STATE)
-404	Errore durante l'esecuzione dell'operazione (la modifica dello stato dell'attività ha causato un arresto anomalo)

Codici restituiti per il comando KAVSHELL RTP

Tabella 59. Codici restituiti per il comando KAVSHELL RTP

Codice restituito	Descrizione
0	Operazione completata
-2	Servizio non in esecuzione
-3	Errore di autorizzazioni
-4	Oggetto non trovato (una o tutte le attività Protezione in tempo reale non trovate)

Codice restituito	Descrizione
-5	Sintassi del comando non valida
-6	Operazione non valida (ad esempio, l'attività è già in esecuzione o già stata arrestata)
-99	Errore sconosciuto
-301	Chiave non valida

Codici restituiti per il comando KAVSHELL UPDATE

Tabella 60. Codici restituiti per il comando KAVSHELL UPDATE

Codice restituito	Descrizione
0	Operazione completata
200	Tutti gli oggetti sono aggiornati (il database o i componenti del programma sono aggiornati)
-2	Servizio non in esecuzione
-3	Errore di autorizzazioni
-5	Sintassi del comando non valida
-99	Errore sconosciuto
-206	I file di estensione risultano mancanti nell'origine specificata o hanno un formato non riconosciuto
-209	Errore durante la connessione alla sorgente degli aggiornamenti
-232	Errore di autenticazione durante la connessione al server proxy
-234	Errore durante la connessione a Kaspersky Security Center
-235	Kaspersky Embedded Systems Security 2.2 non è stato autenticato durante la connessione alla sorgente degli aggiornamenti
-236	Il database dell'applicazione è danneggiato
-301	Chiave non valida

Codici restituiti per il comando KAVSHELL ROLLBACK

Tabella 61. Codici restituiti per il comando KAVSHELL ROLLBACK

Codice restituito	Descrizione
0	Operazione completata
-2	Servizio non in esecuzione
-3	Errore di autorizzazioni
-99	Errore sconosciuto
-221	Copia di backup del database non trovata o danneggiata
-222	Copia di backup del database danneggiata

Codici restituiti per il comando KAVSHELL LICENSE

Tabella 62. Codici restituiti per il comando KAVSHELL LICENSE

Codice restituito	Descrizione
0	Operazione completata
-2	Servizio non in esecuzione
-3	Privilegi insufficienti per la gestione delle chiavi
-4	Chiave con il numero specificato non trovata
-5	Sintassi del comando non valida
-6	Operazione non valida (chiave già aggiunta)
-99	Errore sconosciuto
-301	Chiave non valida
-303	La licenza si applica a un'altra applicazione

Codici restituiti per il comando KAVSHELL TRACE

Tabella 63. Codici restituiti per il comando KAVSHELL TRACE

Codice restituito	Descrizione
0	Operazione completata
-2	Servizio non in esecuzione
-3	Errore di autorizzazioni
-4	Oggetto non trovato (percorso specificato come percorso della cartella dei log di traccia non trovato)
-5	Sintassi del comando non valida
-6	Operazione non valida (tentativo di esecuzione del comando KAVSHELL TRACE /OFF se la creazione del log di traccia è già disabilitata)
-99	Errore sconosciuto

Codici restituiti per il comando KAVSHELL FBRESET

Tabella 64. Codici restituiti per il comando KAVSHELL FBRESET

Codice restituito	Descrizione
0	Operazione completata
-99	Errore sconosciuto

Codici restituiti per il comando KAVSHELL DUMP

Tabella 65. Codici restituiti per il comando KAVSHELL DUMP

Codice restituito	Descrizione
0	Operazione completata
-2	Servizio non in esecuzione
-3	Errore di autorizzazioni
-4	Oggetto non trovato (percorso specificato come percorso della cartella del file di dump non trovato; processo con il PID specificato non trovato)
-5	Sintassi del comando non valida
-6	Operazione non valida (tentativo di esecuzione del comando KAVSHELL DUMP/OFF se la creazione del file di dump è già disabilitata)
-99	Errore sconosciuto

Codici restituiti per il comando KAVSHELL IMPORT

Tabella 66. Codici restituiti per il comando KAVSHELL IMPORT

Codice restituito	Descrizione
0	Operazione completata
-2	Servizio non in esecuzione
-3	Errore di autorizzazioni
-4	Oggetto non trovato (file di configurazione da importare non trovato)
-5	Sintassi non valida
-99	Errore sconosciuto
501	L'operazione è stata completata, tuttavia si è verificato un errore/avviso durante l'esecuzione del comando, ad esempio Kaspersky Embedded Systems Security 2.2 non ha importato i parametri di alcuni componenti funzionali
-502	File importato mancante o in formato non riconosciuto
-503	Impostazioni incompatibili (file di configurazione esportato da un programma diverso o da una versione successiva e incompatibile di Kaspersky Embedded Systems Security 2.2)

Codici restituiti per il comando KAVSHELL EXPORT

Tabella 67. Codici restituiti per il comando KAVSHELL EXPORT

Codice restituito	Descrizione
0	Operazione completata
-2	Servizio non in esecuzione

Codice restituito	Descrizione
-3	Errore di autorizzazioni
-5	Sintassi non valida
-10	Impossibile creare un file di configurazione (ad esempio, nessun accesso alla cartella specificata nel percorso del file)
-99	Errore sconosciuto
501	L'operazione è stata completata, tuttavia si è verificato un errore/avviso durante l'esecuzione del comando, ad esempio Kaspersky Embedded Systems Security 2.2 non ha esportato i parametri di alcuni componenti funzionali

Integrazione con sistemi di terze parti

In questa sezione viene descritta l'integrazione di Kaspersky Embedded Systems Security 2.2 con funzionalità e tecnologie di terze parti.

In questo capitolo

Monitoraggio delle prestazioni. Contatori di Kaspersky Embedded Systems Security 2.2	251
Integrazione con WMI	265

Monitoraggio delle prestazioni. Contatori di Kaspersky Embedded Systems Security 2.2

Questa sezione fornisce informazioni sui contatori di Kaspersky Embedded Systems Security 2.2: contatori delle prestazioni di Monitor di sistema e contatori e trap SNMP.

In questo capitolo

Contatori delle prestazioni per Monitor di sistema.....	251
Contatori e trap SNMP di Kaspersky Embedded Systems Security 2.2	257

Contatori delle prestazioni per Monitor di sistema

Questa sezione contiene informazioni sui contatori delle prestazioni per Monitor di sistema di Microsoft Windows che sono registrati da Kaspersky Embedded Systems Security 2.2 durante l'installazione.

In questa sezione

Informazioni sui contatori SNMP di Kaspersky Embedded Systems Security 2.2	252
Numero totale di richieste negate	252
Numero totale di richieste ignorate	253
Numero di richieste non elaborate a causa della mancanza di risorse di sistema.....	254
Numero di richieste inviate per l'elaborazione	254
Numero medio di flussi del dispatcher di intercettazione dei file	255
Numero massimo di flussi del dispatcher di intercettazione dei file	255
Numero di elementi nella coda degli oggetti infetti	256
Numero di oggetti elaborati al secondo	256

Informazioni sui contatori SNMP di Kaspersky Embedded Systems Security 2.2

Il componente **Contatori delle prestazioni** è incluso nei componenti installati di Kaspersky Embedded Systems Security 2.2 per impostazione predefinita. Kaspersky Embedded Systems Security 2.2 registra i propri contatori delle prestazioni per Monitor di sistema di Microsoft Windows durante l'installazione.

Utilizzando i contatori di Kaspersky Embedded Systems Security 2.2, è possibile monitorare le prestazioni dell'applicazione durante l'esecuzione delle attività Protezione in tempo reale. È possibile individuare i colli di bottiglia durante l'esecuzione con altre applicazioni e le risorse in esaurimento. È possibile diagnosticare le impostazioni di Kaspersky Embedded Systems Security 2.2 non desiderate e gli arresti anomali durante la sua esecuzione.

È possibile visualizzare i contatori delle prestazioni di Kaspersky Embedded Systems Security 2.2 aprendo la console **Prestazioni** nell'elemento **Amministrazione** del Pannello di controllo di Windows.

Le sezioni seguenti elencano le definizioni dei contatori, gli intervalli consigliati per le letture, i valori di soglia e le raccomandazioni per le impostazioni di Kaspersky Embedded Systems Security 2.2 se i valori dei contatori li superano.

Numero totale di richieste negate

Tabella 68. Numero totale di richieste negate

Nome	Numero totale di richieste negate.
Definizione	Numero totale di richieste dal driver di intercettazione dei file per l'elaborazione di oggetti che non sono stati accettati dai processi dell'applicazione. Il conteggio viene effettuato a partire dall'ultimo avvio di Kaspersky Embedded Systems Security 2.2. L'applicazione ignora gli oggetti per cui le richieste di elaborazione sono negate dai processi di Kaspersky Embedded Systems Security 2.2.
Scopo	Questo contatore può consentire di rilevare: <ul style="list-style-type: none"> • Qualità inferiore di Protezione in tempo reale dovuta al rallentamento dei processi di lavoro di Kaspersky Embedded Systems Security 2.2. • Interruzione di Protezione in tempo reale a causa di errori del dispatcher di intercettazione dei file.
Valore normale / soglia	0 / 1.
Intervallo di lettura consigliato	1 ora.

Raccomandazioni per la configurazione se il valore supera la soglia	<p>Il numero di richieste di elaborazione negate corrisponde al numero di oggetti ignorati.</p> <p>Sono possibili le seguenti situazioni a seconda del comportamento del contatore:</p> <ul style="list-style-type: none"> il contatore mostra diverse richieste negate per un periodo di tempo prolungato: tutti i processi di Kaspersky Embedded Systems Security 2.2 sono completamente carichi, quindi Kaspersky Embedded Systems Security 2.2 non poteva esaminare gli oggetti. <p>Per evitare che vengano ignorati alcuni oggetti, aumentare il numero di processi dell'applicazione per le attività Protezione in tempo reale. È possibile utilizzare impostazioni di Kaspersky Embedded Systems Security 2.2 come Numero massimo di processi attivi e Numero di processi per la protezione in tempo reale.</p> <ul style="list-style-type: none"> Il numero di richieste negate supera considerevolmente la soglia critica e aumenta in modo rapido: si è verificato un arresto anomalo del dispatcher di intercettazione dei file. Kaspersky Embedded Systems Security 2.2 non esamina gli oggetti all'accesso. <p>Riavviare Kaspersky Embedded Systems Security 2.2.</p>
--	--

Numero totale di richieste ignorate

Tabella 69. Numero totale di richieste ignorate

Nome	Numero totale di richieste ignorate
Definizione	<p>Numero totale di richieste dal driver di intercettazione dei file per l'elaborazione di oggetti che sono stati ricevute da Kaspersky Embedded Systems Security 2.2, ma non hanno generato eventi di completamento dell'elaborazione. Il conteggio viene effettuato a partire dall'ultimo avvio dell'applicazione.</p> <p>Se una richiesta di elaborazione di un oggetto di questo tipo accettata da uno dei processi di lavoro non ha inviato un evento per il completamento dell'elaborazione, il driver trasferirà tale richiesta a un altro processo e il valore del contatore Numero totale di richieste ignorate aumenterà di 1. Se il driver ha esaminato tutti i processi di lavoro e nessuno di essi ha ricevuto la richiesta per l'elaborazione (era occupato) o ha inviato eventi di completamento dell'elaborazione, Kaspersky Embedded Systems Security 2.2 ignorerà tale oggetto, quindi il valore del contatore Numero totale di richieste ignorate aumenterà di 1.</p>
Scopo	Questo contatore consente di rilevare i cali delle prestazioni a causa di errori del dispatcher di intercettazione dei file.
Valore normale / soglia	0 / 1
Intervallo di lettura consigliato	1 ora
Raccomandazioni per la configurazione se il valore supera la soglia	<p>Se il valore del contatore è diverso da zero, uno o più flussi del dispatcher di intercettazione dei file si sono bloccati e risultano inattivi. Il valore del contatore corrisponde al numero di flussi attualmente inattivi.</p> <p>Se la velocità di scansione non è soddisfacente, riavviare Kaspersky Embedded Systems Security 2.2 per ripristinare i flussi offline.</p>

Numero di richieste non elaborate a causa della mancanza di risorse di sistema

Tabella 70. Numero di richieste non elaborate a causa della mancanza di risorse di sistema

Nome	Numero di richieste non elaborate a causa della mancanza di risorse.
Definizione	Numero totale di richieste dal driver di intercettazione dei file che non sono state elaborate a causa di una mancanza di risorse di sistema (ad esempio, la RAM). Il conteggio viene effettuato a partire dall'ultimo avvio di Kaspersky Embedded Systems Security 2.2. Kaspersky Embedded Systems Security 2.2 ignora le richieste di elaborazione degli oggetti che non sono elaborati dal driver di intercettazione dei file.
Scopo	Questo contatore può essere utilizzato per rilevare ed eliminare una qualità potenzialmente inferiore in Protezione in tempo reale a causa di una riduzione delle risorse di sistema.
Valore normale / soglia	0 / 1.
Intervallo di lettura consigliato	1 ora.
Raccomandazioni per la configurazione se il valore supera la soglia	Se il valore del contatore è diverso da zero, i processi di lavoro di Kaspersky Embedded Systems Security 2.2 hanno bisogno di più RAM per elaborare le richieste. I processi attivi di altre applicazioni potrebbero stare utilizzando tutta la RAM disponibile.

Numero di richieste inviate per l'elaborazione

Tabella 71. Numero di richieste inviate per l'elaborazione

Nome	Numero di richieste inviate per l'elaborazione.
Definizione	Numero di oggetti che attendono l'elaborazione da parte dei processi di lavoro.
Scopo	Questo contatore può essere utilizzato per tenere traccia del carico sui processi di lavoro di Kaspersky Embedded Systems Security 2.2 e del livello generale di attività sui file nel computer.
Valore normale / soglia	Il valore del contatore può variare a seconda del livello di attività sui file nel computer.
Intervallo di lettura consigliato	1 minuto
Raccomandazioni per la configurazione se il valore supera la soglia	No

Numero medio di flussi del dispatcher di intercettazione dei file

Tabella 72. Numero medio di flussi del dispatcher di intercettazione dei file

Nome	Numero medio di flussi del dispatcher di intercettazione dei file.
Definizione	Numero di flussi del dispatcher di intercettazione dei file in un processo e media per tutti i processi attualmente coinvolti nelle attività Protezione in tempo reale.
Scopo	Questo contatore può essere utilizzato per rilevare ed eliminare una qualità potenzialmente inferiore in Protezione in tempo reale a causa del carico sui processi di Kaspersky Embedded Systems Security 2.2.
Valore normale / soglia	Variabile / 40
Intervallo di lettura consigliato	1 minuto
Raccomandazioni per la configurazione se il valore supera la soglia	<p>Possono essere creati fino a 60 flussi del dispatcher di intercettazione dei file in ogni processo di lavoro. Se il valore del contatore si avvicina a 60, c'è il rischio che nessuno dei processi di lavoro possa elaborare la prossima richiesta in coda dal driver di intercettazione dei file e che Kaspersky Embedded Systems Security 2.2 ignori l'oggetto.</p> <p>Aumentare il numero dei processi di Kaspersky Embedded Systems Security 2.2 per le attività Protezione in tempo reale. È possibile utilizzare impostazioni di Kaspersky Embedded Systems Security 2.2 come Numero massimo di processi attivi e Numero di processi per la protezione in tempo reale.</p>

Numero massimo di flussi del dispatcher di intercettazione dei file

Tabella 73. Numero massimo di flussi del dispatcher di intercettazione dei file

Nome	Numero massimo di flussi del dispatcher di intercettazione dei file.
Definizione	Numero di flussi del dispatcher di intercettazione dei file in un processo e massimo per tutti i processi attualmente coinvolti nelle attività Protezione in tempo reale.
Scopo	Questo contatore consente di rilevare ed eliminare i cali delle prestazioni a causa della distribuzione irregolare dei carichi nei processi in esecuzione.
Valore normale / soglia	Variabile / 40
Intervallo di lettura consigliato	1 minuto
Raccomandazioni per la configurazione se il valore supera la soglia	<p>Se il valore di questo contatore supera considerevolmente e costantemente il contatore Numero medio di flussi del dispatcher di intercettazione dei file, Kaspersky Embedded Systems Security 2.2 sta distribuendo in modo irregolare il carico ai processi in esecuzione.</p> <p>Riavviare Kaspersky Embedded Systems Security 2.2.</p>

Numero di elementi nella coda degli oggetti infetti

Tabella 74. Numero di elementi nella coda degli oggetti infetti

Nome	Numero di elementi nella coda degli oggetti infetti.
Definizione	Numero di oggetti infetti attualmente in attesa di elaborazione (disinfettati o eliminati).
Scopo	<p>Questo contatore può consentire di rilevare:</p> <ul style="list-style-type: none"> • Interruzione di Protezione in tempo reale a causa di possibili errori del dispatcher di intercettazione dei file. • Sovraccarico dei processi a causa della distribuzione irregolare del tempo del processore tra i diversi processi di lavoro e Kaspersky Embedded Systems Security 2.2. • Epidemie di virus.
Valore normale / soglia	Questo valore può essere diverso da zero mentre Kaspersky Embedded Systems Security 2.2 elabora gli oggetti infetti o potenzialmente infetti, ma torna a zero al termine dell'elaborazione / Il valore rimane diverso da zero per un periodo di tempo prolungato.
Intervallo di lettura consigliato	1 minuto
Raccomandazioni per la configurazione se il valore supera la soglia	<p>Se il valore del contatore non torna a zero per un periodo di tempo prolungato:</p> <ul style="list-style-type: none"> • Kaspersky Embedded Systems Security 2.2 non elabora gli oggetti (potrebbe essersi verificato un arresto anomalo del dispatcher di intercettazione dei file). Riavviare Kaspersky Embedded Systems Security 2.2. • Tempo del processore insufficiente per elaborare gli oggetti. Verificare che Kaspersky Embedded Systems Security 2.2 riceva tempo del processore aggiuntivo (ad esempio, riducendo il carico di altre applicazioni sul computer). • Si è verificata un'epidemia di virus. <p>Un grande numero di oggetti infetti o potenzialmente infetti nell'attività Protezione dei file in tempo reale è anche un segno di un'epidemia di virus. È possibile visualizzare le informazioni sul numero di oggetti rilevati nelle statistiche dell'attività o nei log delle attività.</p>

Numero di oggetti elaborati al secondo

Tabella 75. Numero di oggetti elaborati al secondo

Nome	Numero di oggetti elaborati al secondo.
Definizione	Numero di oggetti elaborati diviso per il tempo che è stato necessario per elaborare tali oggetti (calcolato su intervalli di tempo uguali).
Scopo	Questo contatore riflette la velocità di elaborazione degli oggetti. Può essere utilizzato per rilevare ed eliminare i momenti di scarse prestazioni del computer che si verificano a causa di tempo del processore insufficiente assegnato ai processi di Kaspersky Embedded Systems Security 2.2 o di errori durante l'esecuzione di Kaspersky Embedded Systems Security 2.2.

Valore normale / soglia	Variabile / Nessuno.
Intervallo di lettura consigliato	1 minuto.
Raccomandazioni per la configurazione se il valore supera la soglia	<p>I valori di questo contatore dipendono dai valori specificati nelle impostazioni di Kaspersky Embedded Systems Security 2.2 e dal carico sul computer dei processi di altre applicazioni.</p> <p>Osservare il livello medio dei numeri del contatore durante un periodo di tempo prolungato. Se il livello generale dei valori del contatore diventa inferiore, è possibile una delle seguenti situazioni:</p> <ul style="list-style-type: none"> • I processi di Kaspersky Embedded Systems Security 2.2 non hanno tempo del processore sufficiente per l'elaborazione degli oggetti. Verificare che Kaspersky Embedded Systems Security 2.2 riceva tempo del processore aggiuntivo (ad esempio, riducendo il carico di altre applicazioni sul computer). • Si è verificato un errore di Kaspersky Embedded Systems Security 2.2 (diversi flussi sono inattivi). Riavviare Kaspersky Embedded Systems Security 2.2.

Contatori e trap SNMP di Kaspersky Embedded Systems Security 2.2

Questa sezione contiene informazioni su contatori e trap di Kaspersky Embedded Systems Security 2.2.

In questa sezione

Informazioni su contatori e trap SNMP di Kaspersky Embedded Systems Security 2.2.....	257
Contatori SNMP di Kaspersky Embedded Systems Security 2.2.....	258
Trap SNMP	260

Informazioni su contatori e trap SNMP di Kaspersky Embedded Systems Security 2.2

Se sono stati inclusi **Contatori e trap SNMP** nel set dei componenti anti-virus da installare, è possibile visualizzare i contatori e le trap di Kaspersky Embedded Systems Security 2.2 tramite SNMP (Simple Network Management Protocol).

Per visualizzare i contatori e le trap di Kaspersky Embedded Systems Security 2.2 dalla workstation di amministrazione, avviare il servizio SNMP nel computer protetto e avviare i servizi SNMP e Trap SNMP nella workstation di amministrazione.

Contatori SNMP di Kaspersky Embedded Systems Security 2.2

Questa sezione contiene tabelle con una descrizione delle impostazioni per i contatori SNMP di Kaspersky Embedded Systems Security 2.2.

In questa sezione

Contatori delle prestazioni	258
Contatori per la quarantena	258
Contatori per il backup	258
Contatori generali	259
Contatori per l'aggiornamento	259
Contatori per Protezione in tempo reale	259

Contatori delle prestazioni

Tabella 76. Contatori delle prestazioni

Contatore	Definizione
currentRequestsAmount	Numero di richieste inviate per l'elaborazione (a pagina 254)
currentInfectedQueueLength	Numero di elementi nella coda degli oggetti infetti (vedere la sezione "Numero di elementi nella coda degli oggetti infetti" a pagina 256)
currentObjectProcessingRate	Numero di oggetti elaborati al secondo (a pagina 256)
currentWorkProcessesNumber	Numero corrente di processi di lavoro utilizzati da Kaspersky Embedded Systems Security 2.2

Contatori per la quarantena

Tabella 77. Contatori per la quarantena

Contatore	Definizione
totalObjects	Numero di oggetti attualmente in Quarantena
totalSuspiciousObjects	Numero di oggetti potenzialmente infetti attualmente in Quarantena
currentStorageSize	Dimensione totale dei dati in Quarantena.(MB)

Contatori per il backup

Tabella 78. Contatori per il backup

Contatore	Definizione
currentBackupStorageSize	Dimensione totale dei dati in Backup.(MB)

Contatori generali

Tabella 79. Contatori generali

Contatore	Definizione
lastCriticalAreasScanAge	Periodo dall'ultima scansione completa delle aree critiche del computer (tempo trascorso in secondi dal completamento dell'ultima <i>attività Scansione aree critiche</i>).
licenseExpirationDate	Data di scadenza della licenza. Se sono state aggiunte chiavi attive e di riserva, è visualizzata la data di scadenza della licenza associata alla chiave di riserva.
currentApplicationUptime	Periodo di tempo per cui Kaspersky Embedded Systems Security 2.2 è stato in esecuzione dall'ultimo avvio, in centesimi di secondi.
currentFileMonitorTaskStatus	Stato dell'attività Protezione dei file in tempo reale: On - in esecuzione; Off - arrestata o sospesa.

Contatori per l'aggiornamento

Tabella 80. Contatori per l'aggiornamento

Contatore	Definizione
avBasesAge	"Età" dei database (tempo trascorso in centesimi di secondi dalla data di creazione degli ultimi database installati).

Contatori per Protezione in tempo reale

Tabella 81. Contatori per Protezione in tempo reale

Contatore	Definizione
totalObjectsProcessed	Numero totale di oggetti esaminati dall'ultima esecuzione dell'attività Protezione dei file in tempo reale
totalInfectedObjectsFound	Numero totale di oggetti infetti e di altro tipo rilevati dall'ultima esecuzione dell'attività Protezione dei file in tempo reale
totalSuspiciousObjectsFound	Numero totale di oggetti potenzialmente infetti rilevati dall'ultima esecuzione dell'attività Protezione dei file in tempo reale
totalVirusesFound	Numero totale di oggetti rilevati dall'ultima esecuzione dell'attività Protezione dei file in tempo reale
totalObjectsQuarantined	Numero totale di oggetti infetti, potenzialmente infetti e di altro tipo che sono stati messi in Quarantena da Kaspersky Embedded Systems Security 2.2; il valore è calcolato dall'ultimo avvio dell'attività Protezione dei file in tempo reale
totalObjectsNotQuarantined	Numero totale di oggetti infetti o potenzialmente infetti che Kaspersky Embedded Systems Security 2.2 ha tentato di mettere in Quarantena senza riuscirci; il valore è calcolato dall'ultimo avvio dell'attività Protezione dei file in tempo reale

Contatore	Definizione
totalObjectsDisinfected	Numero totale di oggetti infetti che sono stati disinfettati da Kaspersky Embedded Systems Security 2.2; il valore è calcolato dall'ultimo avvio dell'attività Protezione dei file in tempo reale
totalObjectsNotDisinfected	Numero totale di oggetti infetti e di altro tipo che Kaspersky Embedded Systems Security 2.2 ha tentato di disinfettare senza riuscirci; il valore è calcolato dall'ultimo avvio dell'attività Protezione dei file in tempo reale
totalObjectsDeleted	Numero totale di oggetti infetti, potenzialmente infetti e di altro tipo che sono stati disinfettati da Kaspersky Embedded Systems Security 2.2; il valore è calcolato dall'ultimo avvio dell'attività Protezione dei file in tempo reale
totalObjectsNotDeleted	Numero totale di oggetti infetti, potenzialmente infetti e di altro tipo che Kaspersky Embedded Systems Security 2.2 ha tentato di disinfettare senza riuscirci; il valore è calcolato dall'ultimo avvio dell'attività Protezione dei file in tempo reale
totalObjectsBackedUp	Numero totale di oggetti infetti e di altro tipo che sono stati inseriti in Backup da Kaspersky Embedded Systems Security 2.2; il valore è calcolato dall'ultimo avvio dell'attività Protezione dei file in tempo reale
totalObjectsNotBackedUp	Numero totale di oggetti infetti e di altro tipo che Kaspersky Embedded Systems Security 2.2 ha tentato di inserire in Backup senza riuscirci; il valore è calcolato dall'ultimo avvio dell'attività Protezione dei file in tempo reale

Trap SNMP

Le impostazioni delle trap SNMP di Kaspersky Embedded Systems Security 2.2 sono riepilogate nella seguente tabella.

Tabella 82. Trap SNMP di Kaspersky Embedded Systems Security 2.2

Trap	Descrizione	Opzioni
eventThreatDetected	Un oggetto è stato rilevato.	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty
eventBackupStorageSizeExceeds	Dimensione massima del backup superata. La dimensione totale dei dati in Backup ha superato il valore specificato da Dimensione massima backup (MB) . Kaspersky Embedded Systems Security 2.2 continua a eseguire il backup degli oggetti infetti.	eventDateAndTime eventSeverity eventSource

Trap	Descrizione	Opzioni
eventThresholdBackupStorageSizeExceeds	Soglia per lo spazio disponibile nel backup raggiunta. La quantità di spazio disponibile in Backup assegnato da Valore di soglia dello spazio disponibile (MB) è uguale o minore rispetto al valore specificato. Kaspersky Embedded Systems Security 2.2 continua a eseguire il backup degli oggetti infetti.	eventDateAndTime eventSeverity eventSource
eventQuarantineStorageSizeExceeds	Dimensione massima della quarantena superata. La dimensione totale dei dati in Quarantena ha superato il valore specificato da Dimensione massima quarantena (MB) . Kaspersky Embedded Systems Security 2.2 continua a mettere in quarantena gli oggetti potenzialmente infetti.	eventDateAndTime eventSeverity eventSource
eventThresholdQuarantineStorageSizeExceeds	Soglia per lo spazio disponibile nella quarantena raggiunta. La quantità di spazio disponibile in Quarantena assegnato da Valore di soglia dello spazio disponibile (MB) è minore del valore specificato. Kaspersky Embedded Systems Security 2.2 continua a mettere in quarantena gli oggetti potenzialmente infetti.	eventDateAndTime eventSeverity eventSource
eventObjectNotQuarantined	Errore della quarantena.	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackupid	Errore durante il salvataggio della copia di un oggetto in Backup.	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason

Trap	Descrizione	Opzioni
eventQuarantineInternalError	Errore della quarantena.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Errore del backup.	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	Il database anti-virus non è aggiornato. È in corso il calcolo del numero di giorni dall'ultima esecuzione dell'attività di aggiornamento del database (attività locale, attività di gruppo o attività per set di computer).	eventSeverity eventDateAndTime eventSource days
eventAVBasesTotallyOutdated	Il database anti-virus è obsoleto. È in corso il calcolo del numero di giorni dall'ultima esecuzione dell'attività di aggiornamento del database (attività locale, attività di gruppo o attività per set di computer).	eventSeverity eventDateAndTime eventSource days
eventApplicationStarted	Kaspersky Embedded Systems Security 2.2 è in esecuzione.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Embedded Systems Security 2.2 è arrestato.	eventSeverity eventDateAndTime eventSource
eventCriticalAreasScanWasntPerformForALongTime	La scansione aree critiche non viene eseguita da molto tempo. Il valore è calcolato come numero di giorni dall'ultimo completamento dell' <i>attività Scansione aree critiche</i> .	eventSeverity eventDateAndTime eventSource days
eventLicenseHasExpired	La licenza è scaduta.	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	La licenza sta per scadere. Il valore è calcolato come numero di giorni fino alla data di scadenza per la licenza.	eventSeverity eventDateAndTime eventSource days

Trap	Descrizione	Opzioni
eventTaskInternalError	Errore di completamento dell'attività.	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Errore durante l'esecuzione di un'attività di aggiornamento.	eventSeverity eventDateAndTime taskName updaterErrorEventReason

La seguente tabella descrive le impostazioni delle trap e i possibili valori dei parametri.

Tabella 83. Trap SNMP: valori delle impostazioni

Impostazione	Descrizione e possibili valori
eventDateAndTime	Ora dell'evento.
eventSeverity	Livello di importanza. L'impostazione può avere i seguenti valori: <ul style="list-style-type: none"> critical (1) - critico warning (2) - avviso info (3) - informativo
userName	Nome utente (ad esempio, il nome dell'utente che ha tentato di ottenere l'accesso a un file infetto).
computerName	Nome computer (ad esempio, il nome del computer da cui un utente ha tentato di ottenere l'accesso a un file infetto).
eventSource	Origine dell'evento: componente funzionale in cui è stato generato l'evento. L'impostazione può avere i seguenti valori: <ul style="list-style-type: none"> unknown (0) - componente funzionale sconosciuto quarantine (1) - Quarantena backup (2) - Backup reporting (3) - log delle attività updates (4) - Aggiornamento realTimeProtection (5) - Protezione dei file in tempo reale onDemandScanning (6) - Scansione su richiesta product (7) - evento correlato all'esecuzione di Kaspersky Embedded Systems Security 2.2 nel complesso, invece che all'esecuzione di singoli componenti systemAudit (8) - log di audit

Impostazione	Descrizione e possibili valori
eventReason	<p>Trigger dell'evento: elemento che ha provocato l'evento. L'impostazione può avere i seguenti valori:</p> <ul style="list-style-type: none"> • reasonUnknown(0) - motivo sconosciuto • reasonInvalidSettings (1) - solo per gli eventi di Backup e Quarantena, visualizzato se la Quarantena o il Backup non sono disponibili (autorizzazioni di accesso insufficienti o la cartella è specificata in modo errato nelle impostazioni della Quarantena, ad esempio è specificato un percorso di rete). In questo caso, Kaspersky Embedded Systems Security 2.2 utilizzerà la cartella predefinita per Backup o Quarantena.
objectName	Nome dell'oggetto (ad esempio, nome del file in cui è stato rilevato il virus).
threatName	Nome dell'oggetto secondo la classificazione dell'Enciclopedia dei Virus. Questo nome è incluso nel nome completo dell'oggetto rilevato che viene restituito da Kaspersky Embedded Systems Security 2.2 al momento del rilevamento di un oggetto. È possibile visualizzare il nome completo di un oggetto rilevato nel log dell'attività (vedere la sezione "Configurazione delle impostazioni dei log" a pagina 138).
detectType	<p>Tipo di oggetto rilevato.</p> <p>L'impostazione può avere i seguenti valori:</p> <ul style="list-style-type: none"> • undefined (0) - indefinito • virware - virus classici e worm di rete • trojware - Trojan • malware - altri programmi dannosi • adware - software pubblicitario • pornware - software pornografico • riskware - applicazioni legittime che possono essere utilizzate da intrusi per danneggiare il computer o i dati dell'utente
detectCertainty	<p>Livello di certezza per il rilevamento della minaccia. L'impostazione può avere i seguenti valori:</p> <ul style="list-style-type: none"> • Suspicion (potenzialmente infetto) - Kaspersky Embedded Systems Security 2.2 ha rilevato una corrispondenza parziale tra una sezione del codice dell'oggetto e una sezione di un codice dannoso noto. • Sure (infetto) - Kaspersky Embedded Systems Security 2.2 ha rilevato una corrispondenza completa tra una sezione del codice dell'oggetto e una sezione di un codice dannoso noto.
days	Numero di giorni (ad esempio, numero di giorni fino alla data di scadenza della licenza).
errorCode	Codice di errore.
knowledgeBaselId	Indirizzo di un articolo della Knowledge Base (ad esempio, indirizzo di un articolo che descrive un particolare errore).
taskName	Nome dell'attività.

Impostazione	Descrizione e possibili valori
updaterErrorEventReason	<p>Motivo dell'errore di aggiornamento. L'impostazione può avere i seguenti valori:</p> <ul style="list-style-type: none"> • reasonUnknown(0) - motivo sconosciuto • reasonAccessDenied - accesso negato • reasonUrlsExhausted - l'elenco delle sorgenti degli aggiornamenti è esaurito • reasonInvalidConfig - file di configurazione non valido • reasonInvalidSignature - firma non valida • reasonCantCreateFolder - impossibile creare la cartella • reasonFileOperError - errore del file • reasonDataCorrupted - oggetto danneggiato • reasonConnectionReset - connessione reimpostata • reasonTimeOut - timeout della connessione superato • reasonProxyAuthError - errore di autenticazione del proxy • reasonServerAuthError - errore di autenticazione del server • reasonHostNotFound - computer non trovato • reasonServerBusy - server non disponibile • reasonConnectionError - errore di connessione • reasonModuleNotFound - oggetto non trovato • reasonBlstCheckFailed(16) - errore durante la verifica della blacklist delle chiavi. È possibile che gli aggiornamenti dei database siano stati pubblicati al momento dell'aggiornamento; ripetere l'aggiornamento tra qualche minuto.
storageObjectNotAddedEventReason	<p>Motivo per cui l'oggetto non è stato sottoposto a backup o messo in quarantena. L'impostazione può avere i seguenti valori:</p> <ul style="list-style-type: none"> • reasonUnknown(0) - motivo sconosciuto • reasonStorageInternalError - errore del database; ripristinare Kaspersky Embedded Systems Security 2.2. • reasonStorageReadOnly - il database è in modalità di sola lettura; ripristinare Kaspersky Embedded Systems Security 2.2. • reasonStorageIOError - errore di input/output: a) Kaspersky Embedded Systems Security 2.2 è danneggiato, ripristinare Kaspersky Embedded Systems Security 2.2; b) il disco con i file di Kaspersky Embedded Systems Security 2.2 è danneggiato. • reasonStorageCorrupted - l'archivio è danneggiato; ripristinare Kaspersky Embedded Systems Security 2.2. • reasonStorageFull - il database è pieno, liberare su spazio su disco. • reasonStorageOpenError - impossibile aprire il file del database; ripristinare Kaspersky Embedded Systems Security 2.2. • reasonStorageOSFeatureError - alcune funzionalità del sistema operativo non corrispondono ai requisiti di Kaspersky Embedded Systems Security 2.2. • reasonObjectNotFound - l'oggetto messo in quarantena non esiste sul disco. • reasonObjectAccessError - autorizzazioni insufficienti per l'utilizzo dell'API di backup: l'account utilizzato per eseguire l'operazione non dispone delle autorizzazioni Backup Operators. • reasonDiskOutOfSpace - spazio insufficiente sul disco.

Integrazione con WMI

Kaspersky Embedded Systems Security 2.2 supporta l'integrazione con Strumentazione gestione Windows (WMI): è possibile utilizzare sistemi client che utilizzano WMI per ricevere dati tramite lo standard WBEM (Web-Based

Enterprise Management) allo scopo di raccogliere informazioni sullo stato di Kaspersky Embedded Systems Security 2.2 e dei relativi componenti.

Durante l'installazione, Kaspersky Embedded Systems Security 2.2 registra un modulo proprietario nel sistema, che semplifica la creazione di uno spazio dei nomi di Kaspersky Embedded Systems Security 2.2 nello spazio dei nomi radice WMI nel computer locale. Uno spazio dei nomi di Kaspersky Embedded Systems Security 2.2 consente di utilizzare le classi e le istanze di Kaspersky Embedded Systems Security 2.2 e le relative proprietà.

I valori di alcune proprietà delle istanze dipendono dai tipi di attività.

Un'*attività non periodica* è un'attività dell'applicazione che non è limitata nel tempo e può essere sempre in esecuzione o arrestata. Non è disponibile alcuno stato di avanzamento per queste attività. I risultati dell'esecuzione delle attività vengono registrati senza interruzioni durante l'esecuzione dell'attività come un singolo evento (ad esempio, il rilevamento di un oggetto infetto da parte di qualsiasi attività Protezione del computer in tempo reale). Questo tipo di attività è gestito tramite i criteri di Kaspersky Security Center.

Un'*attività periodica* è un'attività dell'applicazione che è limitata nel tempo e per cui viene visualizzato un avanzamento in percentuale. I risultati delle attività vengono generati dopo il completamento dell'attività e sono rappresentati come un singolo elemento o una modifica dello stato dell'applicazione (ad esempio, l'applicazione ha completato l'aggiornamento dei database o sono stati generati i file di configurazione per le attività di generazione delle regole). Diverse attività periodiche dello stesso tipo possono essere in esecuzione in un singolo computer contemporaneamente (tre attività Scansione su richiesta con diversi ambiti della scansione). Le attività periodiche possono essere gestite tramite Kaspersky Security Center come attività di gruppo.

Se si utilizzano strumenti per la generazione di query degli spazi dei nomi WMI e la ricezione di dati dinamici dagli spazi dei nomi WMI nella rete aziendale, sarà possibile ricevere le informazioni sullo stato corrente dell'applicazione (vedere la seguente tabella).

Tabella 84. Informazioni sullo stato dell'applicazione

Proprietà dell'istanza	Descrizione	Valori
ProductName	Nome dell'applicazione installata.	Nome completo dell'applicazione senza numero di versione.
ProductVersion	Versione completa dell'applicazione installata.	Numero di versione completo dell'applicazione, incluso il numero di build.
InstalledPatches	Array di nomi visualizzati di patch che sono distribuite per l'applicazione.	Elenco di correzioni critiche installate per l'applicazione.
IsLicenseInstalled	Stato di attivazione dell'applicazione.	Stato della chiave utilizzata per attivare l'applicazione. Valori possibili: <ul style="list-style-type: none"> False - Una chiave o un codice di attivazione non è stato impostato nell'applicazione. True - Una chiave o un codice di attivazione è stato aggiunto all'applicazione.

Proprietà dell'istanza	Descrizione	Valori
LicenseDaysLeft	Mostra il numero di giorni rimanenti prima della scadenza della licenza corrente.	Numero di giorni rimanenti prima della scadenza della licenza corrente. Possibili valori non positivi: <ul style="list-style-type: none"> • 0 - La licenza è scaduta. • -1 - Impossibile ottenere informazioni sulla chiave corrente o la chiave specificata non può essere utilizzata per attivare l'applicazione (ad esempio, è bloccata in base a una blacklist delle chiavi).
AVBasesDatetime	Timestamp per una versione corrente dei database anti-virus.	Data e ora di creazione del database anti-virus attualmente in uso. Se l'applicazione installata non utilizza database anti-virus, il campo contiene il valore "Non installato".
IsExploitPreventionEnabled	Stato del componente Prevenzione exploit.	Stato del componente Prevenzione exploit. Valori possibili: <ul style="list-style-type: none"> • True - Il componente Prevenzione exploit è abilitato e fornisce la protezione. • False - Il componente Prevenzione exploit non fornisce la protezione. Ad esempio: disabilitato, non installato, è stato violato il Contratto di licenza.
ProtectionTasksRunning	Array delle attività di protezione attualmente in esecuzione.	Elenco delle attività di protezione, controllo e monitoraggio attualmente in esecuzione. Questo campo elenca tutte le attività non periodiche in esecuzione. Se non è in esecuzione alcuna attività non periodica, il campo contiene il valore "No".
IsAppControlRunning	Stato dell'attività Controllo dell'avvio delle applicazioni.	Stato dell'attività Controllo dell'avvio delle applicazioni. <ul style="list-style-type: none"> • True - L'attività Controllo dell'avvio delle applicazioni è in esecuzione. • False - L'attività Controllo dell'avvio delle applicazioni non è attualmente in esecuzione o il componente Controllo dell'avvio delle applicazioni non è installato.

Proprietà dell'istanza	Descrizione	Valori
AppControlMode	Modalità dell'attività Controllo dell'avvio delle applicazioni.	Descrizione dello stato corrente del componente Controllo dell'avvio delle applicazioni e della modalità selezionata per l'attività corrispondente. Valori possibili: <ul style="list-style-type: none"> Active - Nelle impostazioni dell'attività è selezionata la modalità Attivo. Statistics Only - Nelle impostazioni dell'attività è selezionata la modalità Solo statistiche. Not installed - Il componente Controllo dell'avvio delle applicazioni non è installato
AppControlRulesNumber	Numero totale di regole di Controllo dell'avvio delle applicazioni.	Numero di regole attualmente specificate nelle impostazioni dell'attività Controllo dell'avvio delle applicazioni.
AppControlLastBlocking	Timestamp per l'ultimo blocco dell'avvio di un'applicazione da parte dell'attività Controllo dell'avvio delle applicazioni in qualsiasi modalità.	Data e ora in cui il componente Controllo dell'avvio delle applicazioni ha bloccato l'ultimo avvio di un'applicazione. Questo campo include tutte le applicazioni bloccate, indipendentemente dalla modalità dell'attività. Se non sono registrate istanze di avvii di applicazioni bloccati al momento dell'elaborazione della query WMI, al campo viene assegnato il valore "No".
PeriodicTasksRunning	Array delle attività periodiche attualmente in esecuzione.	Elenco delle attività Scansione su richiesta, di aggiornamento e di inventario attualmente in esecuzione. Questo campo dovrebbe includere tutte le attività periodiche in esecuzione. Se non sono attualmente in esecuzione attività periodiche, il campo contiene il valore "No".
ConnectionState	Stato della connessione tra il componente Provider WMI e il servizio di Kaspersky Security (KAVFS).	Informazioni sullo stato della connessione tra il modulo del Provider WMI e il servizio di Kaspersky Security. Valori possibili: <ul style="list-style-type: none"> Success - La connessione è stata stabilita correttamente: il client WMI può ricevere informazioni sullo stato dell'applicazione. Failed. Error Code: <codice> - Non è stato possibile stabilire la connessione a causa di un errore con il codice specificato.

Questi dati rappresentano le proprietà dell'istanza KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security, dove:

- KasperskySecurity_ProductInfo è il nome della classe di Kaspersky Embedded Systems Security 2.2
- .ProductName=Kaspersky Embedded Systems Security è il parametro della chiave di Kaspersky Embedded Systems Security 2.2

L'istanza viene creata nello spazio dei nomi ROOT\Kaspersky\Security.

Come contattare il Servizio di assistenza tecnica

Questa sezione descrive i modi e le condizioni per ottenere assistenza tecnica.

In questo capitolo

Come ottenere assistenza tecnica.....	269
Assistenza tecnica tramite Kaspersky CompanyAccount	269
Utilizzo di file di traccia e script AVZ.....	270

Come ottenere assistenza tecnica

Se non è possibile trovare una soluzione per il proprio problema nella documentazione dell'applicazione o in una delle fonti di informazioni sull'applicazione, è consigliabile contattare l'Assistenza tecnica. Gli specialisti dell'Assistenza tecnica risponderanno a tutte le domande relative all'installazione e all'utilizzo dell'applicazione.

L'Assistenza tecnica è disponibile solo per gli utenti che hanno acquistato una licenza commerciale per l'applicazione. L'Assistenza tecnica non è disponibile per gli utenti che dispongono di una licenza di prova.

Prima di contattare l'Assistenza tecnica, consultare le regole dell'Assistenza tecnica.

È possibile contattare l'Assistenza tecnica in uno dei seguenti modi:

- Contattando telefonicamente l'Assistenza tecnica.
- Inviando una richiesta al Servizio di assistenza tecnica di Kaspersky Lab tramite il portale Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

Assistenza tecnica tramite Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) è un portale per le aziende che utilizzano le applicazioni Kaspersky Lab. Kaspersky CompanyAccount è progettato per agevolare l'interazione tra utenti e specialisti di Kaspersky Lab tramite richieste online. Kaspersky CompanyAccount consente di monitorare lo stato di avanzamento dell'elaborazione delle richieste elettroniche da parte degli specialisti di Kaspersky Lab e di memorizzare una cronologia delle richieste elettroniche.

È possibile registrare tutti i dipendenti dell'organizzazione con un unico account utente in Kaspersky CompanyAccount. Un singolo account consente di gestire in modo centralizzato le richieste online inviate a Kaspersky Lab dai dipendenti registrati e di gestire i privilegi dei dipendenti tramite Kaspersky CompanyAccount.

Kaspersky CompanyAccount è disponibile nelle seguenti lingue:

- Inglese
- Spagnolo
- Italiano
- Tedesco
- Polacco
- Portoghese
- Russo
- Francese
- Giapponese

Per ulteriori informazioni su Kaspersky CompanyAccount, visitare il sito Web dell'Assistenza tecnica http://support.kaspersky.com/faq/companyaccount_help.

Utilizzo di file di traccia e script AVZ

Dopo avere segnalato un problema agli specialisti dell'Assistenza tecnica di Kaspersky Lab, è possibile che questi richiedano di generare un rapporto con le informazioni sull'esecuzione di Kaspersky Embedded Systems Security 2.2 e di inviarlo all'Assistenza tecnica di Kaspersky Lab. Gli specialisti dell'Assistenza tecnica di Kaspersky Lab possono anche richiedere di creare un file di traccia. Il file di traccia consente di seguire il processo con cui vengono eseguiti i comandi dell'applicazione, passo dopo passo, per determinare la fase dell'esecuzione dell'applicazione in cui si verifica un errore.

Dopo avere analizzato i dati inviati, gli specialisti dell'Assistenza tecnica di Kaspersky Lab possono creare uno script AVZ e inviarlo all'utente. Con gli script AVZ è possibile analizzare i processi attivi alla ricerca di minacce, esaminare le minacce nel computer, disinfettare o eliminare i file infetti e creare rapporti sulle scansioni del sistema.

Per poter fornire supporto e risolvere più efficacemente i problemi dell'applicazione, gli specialisti dell'Assistenza tecnica possono richiedere di modificare temporaneamente le impostazioni dell'applicazione a scopo di debug durante la diagnostica. A tale scopo potrebbero essere necessarie le seguenti operazioni:

- Attivazione della funzionalità per l'elaborazione e l'archiviazione delle informazioni di diagnostica estese.
- Ottimizzazione delle impostazioni dei singoli componenti software, non disponibili tramite gli elementi dell'interfaccia utente standard.
- Modifica delle impostazioni di archiviazione e trasmissione delle informazioni di diagnostica elaborate.
- Configurazione dell'intercettazione e della registrazione del traffico di rete.

AO Kaspersky Lab

Kaspersky Lab è un fornitore noto a livello mondiale di sistemi di protezione dei computer dalle minacce digitali, tra cui virus e altro malware, messaggi e-mail indesiderati (spam), attacchi di rete e di hacker.

Nel 2008 Kaspersky Lab è stata classificata tra i primi quattro produttori a livello mondiale di soluzioni software di protezione delle informazioni per gli utenti finali (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab è il fornitore preferito di sistemi di protezione dei computer per utenti home in Russia (IDC Endpoint Tracker 2014).

Kaspersky Lab è stata fondata in Russia nel 1997. Nel tempo si è evoluta in un gruppo internazionale di aziende con 38 sedi in 33 Paesi. L'azienda impiega più di 3.000 specialisti qualificati.

Prodotti. I prodotti Kaspersky Lab offrono protezione per tutti i sistemi, dagli home computer alle reti aziendali di grandi dimensioni.

La gamma di prodotti personali include applicazioni di protezione per computer desktop, portatili e tablet, smartphone e altri dispositivi mobili.

L'azienda offre tecnologie e soluzioni per il controllo e la protezione destinate a workstation e dispositivi mobili, macchine virtuali, file server e server Web, gateway di posta e firewall. L'offerta aziendale contiene inoltre prodotti specializzati per la protezione dagli attacchi DDoS, per la protezione di sistemi di controllo industriali e la prevenzione delle frodi finanziarie. Utilizzate in combinazione con strumenti di gestione centralizzati, queste soluzioni assicurano una protezione efficace e automatizzata dalle minacce per i computer per aziende e organizzazioni di qualsiasi dimensione. I prodotti Kaspersky Lab sono certificati dai più importanti laboratori di testing, sono compatibili con il software di svariati fornitori e sono ottimizzati per l'esecuzione in numerose piattaforme hardware.

Gli analisti anti-virus di Kaspersky Lab lavorano 24 ore su 24. Ogni giorno scoprono centinaia di migliaia di nuove minacce per i computer, creano strumenti per rilevarle e disinfettarle e includono le firme di tali minacce nei database utilizzati dalle applicazioni di Kaspersky Lab.

Tecnologie. Molte delle tecnologie che oggi sono parte integrante dei moderni strumenti anti-virus sono state originariamente sviluppate da Kaspersky Lab. Non è un caso che il motore di Kaspersky Anti-Virus sia utilizzato nei prodotti realizzati da molti altri sviluppatori, tra cui: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu e ZYXEL. Molte delle tecnologie innovative dell'azienda sono coperte da brevetto.

Risultati. Nel corso degli anni, Kaspersky Lab ha ottenuto centinaia di riconoscimenti per il proprio impegno nella lotta contro le minacce per i computer. Nel 2014, i test e le ricerche condotti da AV-Comparatives, un rinomato laboratorio anti-virus austriaco, hanno determinato la designazione di Kaspersky Lab come uno dei due produttori leader per il numero di certificati Advanced+ conseguiti, che hanno permesso all'azienda di ottenere il certificato Top Rated. Tuttavia, il principale risultato ottenuto da Kaspersky Lab è la fedeltà dei suoi clienti di tutto il mondo. I prodotti e le tecnologie di Kaspersky Lab proteggono più di 400 milioni di utenti e i suoi clienti aziendali sono oltre 270.000.

Sito Web di Kaspersky Lab:

<https://www.kaspersky.it>

Enciclopedia dei virus:

<https://securelist.it/>

Virus Lab:

<https://virusdesk.kaspersky.com> (per l'analisi di file e siti Web sospetti)

Forum Web di Kaspersky Lab:

<https://forum.kaspersky.com>

Informazioni sul codice di terze parti

Le informazioni sul codice di terze parti sono contenute nel file denominato legal_notices.txt, disponibile nella cartella di installazione dell'applicazione.

Note relative ai marchi

I marchi registrati e i marchi di servizi appartengono ai rispettivi proprietari.

Intel e Pentium sono marchi di Intel Corporation negli Stati Uniti e/o in altri paesi.

Microsoft, Active Directory, Excel, Internet Explorer, Outlook, Windows, Windows Server e Windows Vista sono marchi registrati di Microsoft Corporation negli Stati Uniti e in altri paesi.

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti e in altri paesi.

Glossario

A

Administration Server

Un componente di Kaspersky Security Center che archivia in modo centralizzato le informazioni su tutte le applicazioni Kaspersky Lab installate nei computer della rete. Può essere utilizzato anche per gestire tali applicazioni.

Aggiornamento

Procedura di sostituzione/aggiunta di nuovi file (database o moduli dell'applicazione) recuperati dai server degli aggiornamenti di Kaspersky Lab.

Analizzatore euristico

Tecnologia per il rilevamento delle minacce per cui non sono ancora state aggiunte informazioni ai database di Kaspersky Lab. L'analizzatore euristico rileva gli oggetti il cui comportamento nel sistema operativo può costituire una minaccia alla sicurezza. Gli oggetti rilevati dall'analizzatore euristico sono considerati potenzialmente infetti. Un oggetto può ad esempio essere considerato potenzialmente infetto se contiene sequenze di comandi tipiche degli oggetti dannosi (apertura di file, scrittura in file).

Archivio

Uno o più file compressi in un singolo file. Per la compressione e la decompressione dei dati, è necessaria un'applicazione dedicata denominata utilità di archiviazione.

Attività

Le funzioni eseguite dall'applicazione Kaspersky Lab sono implementate come attività, ad esempio: Protezione dei file in tempo reale, Scansione completa, Aggiornamento database.

Attività locale

Attività definita e in esecuzione in un singolo computer client.

B

Backup

Uno speciale archivio per le copie di backup dei file create prima del tentativo di disinfezione o eliminazione.

C

Chiave attiva

Chiave attualmente utilizzata dall'applicazione.

Criterio

Un criterio determina le impostazioni di un'applicazione e gestisce l'accesso alla configurazione di un'applicazione installata nei computer di un gruppo di amministrazione. Per ogni applicazione è necessario creare un singolo criterio. È possibile creare un numero illimitato di criteri per le applicazioni installate nei computer di ogni gruppo di amministrazione, ma un solo criterio alla volta può essere applicato a ogni applicazione all'interno di un gruppo di amministrazione.

D

Database anti-virus

Database che contengono informazioni sulle minacce per la protezione del computer note a Kaspersky Lab al momento del rilascio dei database anti-virus. Le voci contenute nei database anti-virus consentono il rilevamento del codice dannoso negli oggetti esaminati. I database anti-virus sono creati dagli specialisti di Kaspersky Lab e vengono aggiornati ogni ora.

Disinfezione

Metodo di elaborazione degli oggetti infetti che determina un ripristino parziale o completo dei dati. Non tutti gli oggetti infetti possono essere disinfettati.

F

Falso positivo

Situazione in cui un'applicazione Kaspersky Lab considera infetto un oggetto non infetto perché il codice è simile a quello di un virus.

File infettabile

Un file che, a causa della struttura o del formato, può essere utilizzato da utenti malintenzionati come "contenitore" per archiviare e diffondere codice dannoso. In genere si tratta di file eseguibili, con estensioni come .com, .exe e .dll. Il rischio di penetrazione di codice dannoso in tali file è piuttosto alto.

G

Gravità di un evento

Proprietà di un evento che si è verificato durante l'esecuzione di un'applicazione Kaspersky Lab. Esistono quattro livelli di gravità:

- Evento critico.
- Errore.
- Avviso.
- Informazioni.

Eventi dello stesso tipo possono avere diversi livelli di gravità, a seconda della situazione in cui si è verificato l'evento.

I

Impostazioni delle attività

Impostazioni dell'applicazione specifiche per ogni tipo di attività.

K

Kaspersky Security Network (KSN)

Un'infrastruttura di servizi cloud che consente di accedere al database di Kaspersky Lab, con informazioni sempre aggiornate sulla reputazione di file, risorse Web e software. Kaspersky Security Network assicura una risposta più rapida da parte delle applicazioni Kaspersky Lab alle minacce, migliora l'efficacia di alcuni componenti di protezione e riduce la probabilità di falsi positivi.

L

Livello di sicurezza

Il livello di sicurezza è definito come un set preconfigurato di impostazioni dei componenti dell'applicazione.

M

Maschera per i file

Rappresentazione del nome di un file tramite caratteri jolly. I due caratteri jolly standard utilizzati nelle maschere di file sono * e ?, dove * rappresenta qualsiasi numero di caratteri e ? indica qualsiasi carattere singolo.

O

Oggetti di avvio

Set di applicazioni necessarie per l'avvio e il corretto funzionamento del sistema operativo e del software installato nel computer. Questi oggetti vengono eseguiti a ogni avvio del sistema operativo. Esistono virus in grado di infettare questi oggetti in particolare e bloccare, ad esempio, l'accesso al sistema operativo.

Oggetto infetto

Oggetto contenente una parte di codice che corrisponde completamente a una parte di codice di un malware noto.

Kaspersky Lab consiglia di evitare di accedere a tali oggetti.

Oggetto OLE

Un oggetto allegato a un altro file o incorporato in un altro file tramite l'utilizzo della tecnologia OLE (Object Linking and Embedding). Un esempio di oggetto OLE è un foglio di calcolo di Microsoft Office Excel® incorporato in un documento di Microsoft Office Word.

P

Periodo di validità della licenza

Periodo di tempo per cui è possibile avere accesso alle funzionalità e ai servizi aggiuntivi dell'applicazione. I servizi che è possibile utilizzare dipendono dal tipo di licenza.

Protezione in tempo reale

Modalità di esecuzione dell'applicazione in cui gli oggetti vengono esaminati in tempo reale alla ricerca di codice dannoso.

L'applicazione intercetta tutti i tentativi di aprire un oggetto (lettura, scrittura o esecuzione) ed esamina l'oggetto per determinare se presenta minacce. Gli oggetti non infetti vengono passati all'utente, mentre gli oggetti che contengono minacce o gli oggetti potenzialmente infetti vengono elaborati in base alle impostazioni dell'attività (disinfectati, eliminati o messi in quarantena).

Q

Quarantena

Cartella in cui l'applicazione Kaspersky Lab sposta gli oggetti potenzialmente infetti che sono stati rilevati. Gli oggetti vengono archiviati in quarantena in formato criptato per evitare qualsiasi impatto sul computer.

S

SIEM

Tecnologia che analizza gli eventi di sicurezza originati da diversi dispositivi di rete e applicazioni.

Stato della protezione

Stato corrente della protezione, che riflette il livello di protezione del computer.

V

Vulnerabilità

Un difetto di un sistema operativo o di un'applicazione che può essere utilizzato dagli autori di malware per penetrare nel sistema operativo o nell'applicazione e danneggiarne l'integrità. La presenza di un numero elevato di vulnerabilità rende un sistema operativo inaffidabile, dal momento che i virus penetrati possono causare interruzioni del sistema operativo stesso e delle applicazioni installate.

Indice

D

Default deny.....	193
Dispositivi attendibili.....	193