

Kaspersky Embedded Systems Security

管理手冊

應用程式版本 : 2.3.0.754

親愛的使用者：

感謝您選擇 Kaspersky Lab 作為您的安全軟體提供商。我們希望本文件能幫助您使用我們的產品。

注意！本文件是 AO Kaspersky Lab (以下簡稱 Kaspersky Lab) 的資產。根據俄羅斯聯邦的版權法和國際條約保留對本文件的所有權利。根據相關法律，非法複製和散佈本文件或其所含部分需要承擔民事、行政或刑事責任。

使用本文中任何資料進行任何類型的複製或發佈 (包括翻譯) ，必須經過 Kaspersky Lab 的書面授權之後始可進行。

本文件及其相關圖片影像只能用於資訊參考、非商業和個人用途。

Kaspersky Lab 保留在沒有事先通知的情況下修改本文件的權利。

關於本文件中任何協力廠商資源的內容、品質、相關性與準確性，以及使用此類資源而可能導致的任何直接或間接損失，Kaspersky Lab 將不承擔任何相關責任與損失。

本文件使用的註冊商標和服務標誌均為其各自所有者擁有的專利權。

文件修訂日期：2019 年 4 月 19 日

© 2019 年 AO Kaspersky Lab 版權所有。保留所有權利。

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

內容

關於本手冊	21
本手冊說明主旨	21
文件說明	24
有關 Kaspersky Embedded Systems Security 的資訊來源	26
可供自行查詢的資料來源	26
在社區中討論 Kaspersky Lab 應用程式	27
Kaspersky Embedded Systems Security	28
關於 Kaspersky Embedded Systems Security	28
新增功能	31
分發套件	31
硬體和軟體需求	34
功能要求和限制	37
安裝和移除	37
檔案完整性監控	38
防火牆管理	39
其他限制	40
安裝和移除應用程式	42
適用於 Windows Installer 服務的 Kaspersky Embedded Systems Security 軟體元件程式碼	42
Kaspersky Embedded Systems Security 軟體元件	43
軟體元件的“管理工具”集	45
安裝 Kaspersky Embedded Systems Security 後系統的變更	46
Kaspersky Embedded Systems Security 處理程序	51
Windows Installer 服務的安裝和移除設定及命令列選項	52
Kaspersky Embedded Systems Security 安裝和移除記錄	56
安裝排程	56
選擇管理工具	57
選擇安裝類型	58
基於精靈安裝和移除應用程式	60
使用安裝精靈進行安裝	60

Kaspersky Embedded Systems Security 安裝	61
Kaspersky Embedded Systems Security 主控台安裝	64
在其他電腦上安裝應用程式主控台以後的進階設定	65
在安裝 Kaspersky Embedded Systems Security 後執行的操作	69
修改元件集和修復 Kaspersky Embedded Systems Security.....	73
使用安裝精靈移除	75
Kaspersky Embedded Systems Security 移除	75
Kaspersky Embedded Systems Security 主控台移除	76
透過命令列安裝或移除應用程式	77
關於從命令列安裝和移除 Kaspersky Embedded Systems Security.....	78
安裝 Kaspersky Embedded Systems Security 的指令範例	78
在安裝 Kaspersky Embedded Systems Security 後執行的操作	80
新增/移除元件。指令範例.....	81
Kaspersky Embedded Systems Security 移除。指令範例	82
回傳代碼	83
使用卡巴斯基安全管理中心安裝和移除應用程式	84
透過卡巴斯基安全管理中心安裝的一般資訊	85
安裝或移除 Kaspersky Embedded Systems Security 的權限.....	85
透過卡巴斯基安全管理中心安裝 Kaspersky Embedded Systems Security	86
在安裝 Kaspersky Embedded Systems Security 後執行的操作	88
透過卡巴斯基安全管理中心安裝應用程式主控台	88
透過卡巴斯基安全管理中心移除 Kaspersky Embedded Systems Security	89
透過 Active Directory® 群組政策進行安裝和解除安裝	90
透過 Active Directory 群組政策安裝 Kaspersky Embedded Systems Security.....	90
在安裝 Kaspersky Embedded Systems Security 後執行的操作	91
透過 Active Directory 群組政策移除 Kaspersky Embedded Systems Security.....	92
檢查 Kaspersky Embedded Systems Security 功能。使用 EICAR 測試病毒	93
關於 EICAR 測試病毒	93
檢查即時防護和自訂掃描功能.....	94

應用程式介面	97
應用程式授權	98
關於最終使用者產品授權協議	98
關於產品授權	99
關於產品授權憑證	100
關於金鑰	101
關於金鑰檔案	101
關於啟動碼	102
關於資料提供	102
使用產品授權金鑰啟動應用程式	105
使用啟動碼啟動應用程式	106
檢視有關目前產品授權的資訊	107
產品授權到期後的功能限制	110
續約產品授權	110
刪除金鑰	111
使用管理外掛程式	113
從卡斯基安全管理中心管理 Kaspersky Embedded Systems Security	113
管理應用程式設定	114
從卡斯基安全管理中心管理 Kaspersky Embedded Systems Security	115
導航	116
透過政策開啟一般設定	117
在應用程式內容視窗中開啟一般設定	117
在卡斯基安全管理中心中設定一般應用程式設定	118
在卡斯基安全管理中心中配置延展性和介面	118
在卡斯基安全管理中心中配置安全性設定	120
使用卡斯基安全管理中心配置連線設定	122
設定本機系統工作的排程啟動	123
在卡斯基安全管理中心中配置隔離和備份設定	125
配置記錄和通知	126
配置記錄設定	127

安全記錄	128
配置 SIEM 整合設定	128
配置通知設定	132
配置與管理伺服器的互動	134
建立和設定政策	135
建立政策	136
Kaspersky Embedded Systems Security 政策設定部分	139
設定政策	144
使用卡巴斯基安全管理中心建立和管理工作	146
關於卡巴斯基安全管理中心中的工作建立	146
使用卡巴斯基安全管理中心建立工作	147
在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作	150
在卡巴斯基安全管理中心中設定群組工作	151
啟動應用程式工作	157
更新工作	158
應用程式完整性控制	160
在卡巴斯基安全管理中心中設定當機診斷設定	161
管理工作排程	164
配置工作啟動排程設定	164
啟用和停用排程工作	166
在卡巴斯基安全管理中心中報告	167
Kaspersky Embedded Systems Security 主控台	170
應用程式主控台內的 Kaspersky Embedded Systems Security 設定	171
關於 Kaspersky Embedded Systems Security 主控台	179
Kaspersky Embedded Systems Security 主控台介面	180
通知區域中的系統欄圖示	184
透過其他電腦上的應用程式主控台管理 Kaspersky Embedded Systems Security	186
管理 Kaspersky Embedded Systems Security 工作	186
Kaspersky Embedded Systems Security 工作類別	187
變更工作設定後儲存工作	188

手動啟動/暫停/還原/停止工作	188
管理工作排程	189
配置工作啟動排程設定	189
啟用和停用排程工作	191
使用使用者帳戶啟動工作	191
關於使用帳戶啟動工作	192
指定使用者帳戶以啟動工作	192
匯入和匯出設定.....	193
關於匯入和匯出設定	193
匯出設定	195
匯入設定	196
使用安全性設定範本	197
關於安全性設定範本	197
建立安全性設定範本	198
檢視範本中的安全性設定	199
套用安全性設定範本	199
刪除安全性設定範本	200
檢視防護狀態和 Kaspersky Embedded Systems Security 資訊.....	201
小型診斷視窗	207
關於小型診斷視窗	207
透過小型診斷視窗檢視 Kaspersky Embedded Systems Security 狀態	208
檢視安全事件統計	209
檢視目前應用程式活動.....	210
配置傾印和偵錯檔案寫入	211
更新 Kaspersky Embedded Systems Security 資料庫和軟體模組.....	212
關於更新工作	213
關於 Kaspersky Embedded Systems Security 軟體模組更新	214
關於 Kaspersky Embedded Systems Security 資料庫更新	215
組織內所使用的病毒防護程式資料庫和模組的更新方案	216
配置更新工作	219

配置使用 Kaspersky Embedded Systems Security 更新來源的設定	220
在執行資料庫更新工作時最佳化磁碟 I/O 的使用	223
配置複製更新工作設定	224
配置軟體模組更新工作設定	225
回溯 Kaspersky Embedded Systems Security 資料庫更新	227
回溯應用程式模組更新	227
更新工作統計	228
物件隔離和備份複製	228
隔離可疑感染物件。隔離	229
關於隔離可疑感染的物件	229
檢視隔離物件	229
隔離區掃描	232
還原隔離的物件	234
將物件移到隔離	236
從隔離區刪除物件	237
傳送可疑感染物件到 Kaspersky Lab 以供分析	237
配置隔離設定	239
隔離統計	240
製作物件的備份副本。備份	241
關於備份物件之後再解毒或刪除	241
檢視備份中儲存的檔案	242
從備份還原檔案	244
從備份刪除檔案	247
配置備份設定	247
備份統計	249
事件註冊。Kaspersky Embedded Systems Security 記錄	250
註冊 Kaspersky Embedded Systems Security 事件的方式	250
系統稽核記錄	251
在系統稽核記錄中排序事件	252
在系統稽核記錄中篩選事件	252

刪除系統稽核記錄中的事件	253
工作記錄	254
關於工作記錄	254
在工作記錄中檢視事件清單	255
排序工作記錄中的事件	255
在工作記錄中篩選事件	256
在工作記錄中檢視有關 Kaspersky Embedded Systems Security 工作的統計和資訊	257
匯出工作記錄中的資訊	257
刪除工作記錄中的事件	258
安全記錄	259
在事件檢視器中檢視 Kaspersky Embedded Systems Security 事件記錄	259
在 Kaspersky Embedded Systems Security 主控台中配置記錄設定	260
關於 SIEM 整合	264
配置 SIEM 整合設定	265
通知設定	267
通知管理員和使用者的方式	268
設定管理員和使用者通知	269
啟動和停止 Kaspersky Embedded Systems Security	272
啟動 Kaspersky Embedded Systems Security 管理外掛程式	272
從開始功能表啟動 Kaspersky Embedded Systems Security 主控台	272
啟動和停止 Kaspersky Security 服務	273
在作業系統安全模式下啟動 Kaspersky Embedded Systems Security	275
關於在作業系統安全模式下工作的 Kaspersky Embedded Systems Security	275
在安全模式下啟動 Kaspersky Embedded Systems Security	276
Kaspersky Embedded Systems Security 自我防護	277
關於 Kaspersky Embedded Systems Security 自我防護	277
防止包含已安裝的 Kaspersky Embedded Systems Security 元件的資料夾被變更	277
防止 Kaspersky Embedded Systems Security 登錄機碼被變更	278
將 Kaspersky Security 服務註冊為受防護服務	278
管理 Kaspersky Embedded Systems Security 功能的存取權限	280

關於 Kaspersky Embedded Systems Security 的管理權限	280
關於管理註冊服務的權限	282
關於 Kaspersky Security 服務的管理權限	284
關於 Kaspersky Security 管理服務的存取權限	286
配置用於管理 Kaspersky Embedded Systems Security 和 Kaspersky Security 服務的存取權限	286
對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取	290
在卡斯基安全管理中心中設定存取權限	291
即時檔案防護	292
關於“即時檔案防護”工作	292
關於工作防護範圍和安全設定	293
關於虛擬防護範圍	294
預設的防護範圍	295
預設安全等級	296
“即時檔案防護”工作中預設掃描的檔案副檔名	298
“即時檔案防護”工作預設值	303
透過管理外掛程式管理“即時檔案防護”工作	304
導航	304
開啟“即時檔案防護”工作的政策設定	304
開啟“即時檔案防護”工作內容	305
配置“即時檔案防護”工作	306
選擇防護模式	307
配置啟發式分析以及與其他應用程式元件的整合	308
配置工作啟動排程設定	310
建立和配置工作防護範圍	312
手動配置安全性設定	313
配置一般工作設定	314
配置操作	318
配置效能	320
透過應用程式主控台管理“即時檔案防護”工作	323
導航	323

開啟“即時檔案防護”範圍設定	323
開啟“即時檔案防護”工作設定	324
配置“即時檔案防護”工作	324
選擇防護模式	325
配置啟發式分析以及與其他應用程式元件的整合	326
配置工作啟動排程設定	328
建立防護範圍	329
建立防護範圍	330
建立虛擬防護範圍	332
手動配置安全性設定	333
配置一般工作設定	334
配置操作	338
配置效能	341
即時檔案防護工作統計	343
KSN 使用	346
關於“KSN 使用”工作	346
“KSN 使用”工作預設設定	348
透過管理外掛程式管理“KSN 使用”	349
透過管理外掛程式配置“KSN 使用”工作	350
透過管理外掛程式配置資料處理	352
透過應用程式主控台管理“KSN 使用”	354
透過應用程式主控台配置“KSN 使用”工作	354
透過應用程式主控台配置資料處理	356
設定其他資料傳輸	358
“KSN 使用”工作統計	360
應用程式啟動控制	362
關於“應用程式啟動控制”工作	362
關於應用程式啟動控制規則	364
關於軟體分發控制	366
關於“應用程式啟動控制”工作的 KSN 使用	369

產生應用程式啟動控制規則.....	370
“應用程式啟動控制”工作預設設定.....	372
透過管理外掛程式管理應用程式啟動控制.....	376
導航.....	376
開啟“應用程式啟動控制”工作的政策設定.....	376
開啟應用程式啟動控制規則清單.....	377
開啟“應用程式啟動控制規則產生器”工作精靈和內容.....	377
配置“應用程式啟動控制”工作設定.....	378
配置軟體分發控制.....	383
配置“應用程式啟動控制規則產生器”工作.....	386
透過卡巴斯基安全管理中心配置應用程式啟動控制規則.....	389
新增應用程式啟動控制規則.....	389
啟用預設允許模式.....	393
從卡巴斯基安全管理中心事件建立允許規則.....	393
從有關受封鎖應用程式的卡巴斯基安全管理中心報告中匯入規則.....	395
從 XML 設定檔匯入應用程式啟動控制規則.....	397
檢查應用程式啟動.....	399
建立“應用程式啟動控制規則產生器”工作.....	399
限制工作使用範圍.....	401
自動規則產生期間要執行的操作.....	402
自動規則產生完成後要執行的操作.....	404
透過應用程式主控台管理應用程式啟動控制.....	405
導航.....	406
開啟“應用程式啟動控制”工作設定.....	406
開啟應用程式啟動控制規則視窗.....	406
開啟“應用程式啟動控制規則產生器”工作設定.....	407
伺服器配置“應用程式啟動控制”工作設定.....	407
選擇“應用程式啟動控制”工作的模式.....	408
配置“應用程式啟動控制”工作的範圍.....	410
配置 KSN 使用.....	411

軟體分發控制	413
配置應用程式啟動控制規則	416
新增應用程式啟動控制規則	416
啟用預設允許模式	420
根據“應用程式啟動控制”工作事件建立允許規則	420
匯出應用程式啟動控制規則	421
從 XML 設定檔匯入應用程式啟動控制規則	421
刪除應用程式啟動控制規則	422
配置“應用程式啟動控制規則產生器”工作	423
限制工作使用範圍	424
自動規則產生期間要執行的操作	425
自動規則產生完成後要執行的操作	427
裝置控制	429
關於裝置控制工作	429
關於裝置控制規則	431
關於裝置控制規則清單填充	433
關於裝置控制規則產生器工作	435
裝置控制規則建立方案	435
“裝置控制”工作預設設定	436
透過管理外掛程式管理裝置控制	437
導航	438
開啟“裝置控制”工作的政策設定	438
開啟裝置控制規則清單	438
開啟“裝置控制規則產生器”工作精靈和內容	439
配置“裝置控制”工作	440
透過卡巴斯基安全管理中心建立所有電腦的裝置控制規則	441
配置“裝置控制規則產生器”工作	443
透過卡巴斯基安全管理中心配置裝置控制規則	444
基於卡巴斯基安全管理中心政策中的系統資料建立允許規則	444
為已連線的裝置建立規則	445

從有關被封鎖裝置的卡巴斯基安全管理中心報告中匯入規則	445
使用“裝置控制規則產生器”工作建立規則	447
將建立的規則新增到裝置控制規則清單	449
透過應用程式主控台管理裝置控制	450
導航	451
開啟“裝置控制”工作設定	451
開啟“裝置控制規則”視窗	452
開啟“裝置控制規則產生器”工作設定	452
配置裝置控制工作設定	453
配置裝置控制規則	454
從 XML 檔案匯入裝置控制規則	454
基於裝置控制工作事件填寫規則清單	455
為一個或多個外部裝置新增允許規則	456
刪除裝置控制規則	456
匯出裝置控制規則	457
啟動和停用裝置控制規則	457
延伸裝置控制規則使用範圍	458
配置裝置控制規則產生器工作	459
防火牆管理	462
關於防火牆管理工作	462
關於防火牆規則	463
防火牆管理工作預設設定	465
透過管理外掛程式管理防火牆規則	466
啟用和停用防火牆規則	466
手動新增防火牆規則	468
刪除防火牆規則	469
透過應用程式主控台管理防火牆規則	471
啟用和停用防火牆規則	471
手動新增防火牆規則	472
刪除防火牆規則	473

檔案完整性監控.....	474
關於“檔案完整性監控”工作.....	474
關於檔案操作監控規則.....	475
“檔案完整性監控”工作設定.....	478
透過管理外掛程式管理“檔案完整性監控”.....	479
配置“檔案完整性監控”工作設定.....	479
配置監控規則.....	480
透過應用程式主控台管理“檔案完整性監控”.....	484
配置“檔案完整性監控”工作設定.....	485
配置監控規則.....	486
記錄審查.....	491
關於“記錄審查”工作.....	491
“記錄審查”工作預設設定.....	493
透過管理外掛程式管理記錄審查規則.....	493
透過管理外掛程式管理預定義工作規則.....	494
透過管理外掛程式新增記錄審查規則.....	496
透過應用程式主控台管理記錄審查規則.....	498
透過應用程式主控台管理預定義工作規則.....	498
配置記錄審查規則.....	500
自訂掃描.....	502
關於自訂掃描工作.....	502
關於掃描範圍.....	503
預設的掃描範圍.....	504
雲端儲存檔案掃描.....	506
自訂掃描工作中所選節點的安全性設定.....	508
為自訂掃描工作的預設安全等級.....	508
關於卸除式磁碟機掃描.....	510
預設自訂掃描工作設定.....	512
透過管理外掛程式管理自訂掃描工作.....	514
導航.....	514

開啟自訂掃描工作精靈	514
開啟自訂掃描工作內容	516
建立自訂掃描工作	516
為自訂掃描工作指定關鍵區域掃描的工作狀態	520
執行背景自訂掃描工作	521
記錄關鍵區域掃描執行記錄	522
配置工作掃描範圍	523
為自訂掃描工作選擇預設的安全等級	524
手動配置安全性設定	525
配置一般工作設定	526
配置操作	530
配置效能	533
配置卸除式磁碟機掃描	535
透過應用程式主控台管理自訂掃描工作	536
導航	536
開啟自訂掃描工作設定	537
建立和配置自訂掃描工作	537
自訂掃描工作中的掃描範圍	540
配置網路檔案資源的視圖模式	540
建立掃描範圍	541
在掃描範圍內包含網路物件	543
建立虛擬掃描範圍	544
為自訂掃描工作選擇預設的安全等級	545
手動配置安全性設定	546
配置一般工作設定	547
配置操作	551
配置效能	553
配置分級儲存	555
掃描卸除式磁碟。	556
自訂掃描工作統計	557

信任區域.....	559
關於信任區域.....	559
透過管理外掛程式管理信任區域.....	561
導航.....	561
透過卡巴斯基安全管理中心管理應用程式.....	562
開啟信任區域內容視窗.....	562
透過管理外掛程式配置信任網域設定.....	563
新增排除.....	564
新增受信任處理程序.....	566
套用 not-a-virus 遮罩.....	569
透過應用程式主控台管理信任區域.....	569
在應用程式主控台中對工作套用信任區域.....	570
在應用程式主控台中配置信任區域設定.....	571
將排除新增至信任區域.....	571
信任處理程序.....	573
套用 not-a-virus 遮罩.....	576
弱點利用防禦.....	578
關於弱點利用防禦.....	578
透過管理外掛程式管理弱點利用防禦.....	580
導航.....	580
開啟弱點利用防禦的政策設定.....	581
開啟弱點利用防禦內容視窗.....	581
配置處理程序記憶體防護設定.....	582
新增進行防護的處理程序.....	584
透過應用程式主控台管理弱點利用防禦.....	585
導航.....	586
開啟弱點利用防禦一般設定.....	586
開啟弱點利用防禦處理程序防護設定.....	586
配置處理程序記憶體防護設定.....	587
新增進行防護的處理程序.....	588

弱點利用防禦技術	590
與協力廠商系統整合	592
監控效能。Kaspersky Embedded Systems Security 計數器	592
系統監視器的效能計數器	592
關於 Kaspersky Embedded Systems Security 效能計數器	593
拒絕需求總數	594
略過需求總數	595
因為系統資源不足而未處理的需求數	595
傳送以供處理的需求數	596
檔案截取調度程式執行緒的平均數	597
檔案截取調度程式執行緒的最大數	597
已感染物件佇列中的元素數	598
每秒處理的物件數	599
Kaspersky Embedded Systems Security SNMP 計數器和 TRAP	600
關於 Kaspersky Embedded Systems Security SNMP 計數器和 TRAP	600
Kaspersky Embedded Systems Security SNMP 計數器	601
Kaspersky Embedded Systems Security SNMP TRAP	604
與 WMI 整合	613
從命令列使用 Kaspersky Embedded Systems Security	618
命令列指令	618
顯示 Kaspersky Embedded Systems Security 指令說明。KAVSHELL HELP	621
啟動和停止 Kaspersky Security 服務 KAVSHELL START , KAVSHELL STOP	622
掃描指定區域。KAVSHELL SCAN.....	623
啟動“掃描關鍵區域”工作 KAVSHELL SCANCritical	629
以非同步模式管理指定的工作 KAVSHELL TASK.....	630
將 KAVFS 註冊為系統防護處理程序。KAVSHELL CONFIG	632
啟動及停止即時防護工作。KAVSHELL RTP	632
管理應用程式啟動控制工作 KAVSHELL APPCONTROL /CONFIG.....	633
應用程式啟動控制規則產生器 KAVSHELL APPCONTROL /GENERATE	634
填寫應用程式啟動控制規則清單 KAVSHELL APPCONTROL.....	637

填寫裝置控制規則清單。KAVSHELL DEVCONTROL	638
啟動 Kaspersky Embedded Systems Security 資料庫更新工作。KAVSHELL UPDATE	639
回溯 Kaspersky Embedded Systems Security 資料庫更新。KAVSHELL ROLLBACK.....	644
管理記錄審查。KAVSHELL TASK LOG-INSPECTOR	644
啟用、設定和停用偵錯記錄。KAVSHELL TRACE.....	645
Kaspersky Embedded Systems Security 記錄檔案磁碟整理。KAVSHELL VACUUM.....	646
清除 iSwift 庫。KAVSHELL FBRESET.....	647
啟用和停用建立傾印檔案。KAVSHELL DUMP	648
匯入設定。KAVSHELL IMPORT.....	650
匯出設定。KAVSHELL EXPORT	650
與 Microsoft Operations Management Suite 整合。KAVSHELL OMSINFO	651
命令列回傳代碼.....	652
KAVSHELL START 和 KAVSHELL STOP 指令的回傳代碼	652
KAVSHELL SCAN 和 KAVSHELL SCANCritical 指令的回傳代碼	653
KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼	654
KAVSHELL TASK 指令的回傳代碼.....	654
KAVSHELL RTP 指令的回傳代碼.....	655
KAVSHELL UPDATE 指令的回傳代碼	656
KAVSHELL ROLLBACK 指令的回傳代碼.....	656
KAVSHELL LICENSE 指令的回傳代碼	657
KAVSHELL TRACE 指令的回傳代碼.....	658
KAVSHELL FBRESET 指令的回傳代碼	658
KAVSHELL DUMP 指令的回傳代碼	658
KAVSHELL IMPORT 指令的回傳代碼	659
KAVSHELL EXPORT 指令的回傳代碼	660
聯絡技術支援	661
如何獲取技術支援.....	661
透過電話獲取技術支援.....	662
透過 Kaspersky CompanyAccount 取得技術支援.....	662
使用偵錯檔案和 AVZ 指令碼	663

詞彙表	664
AO Kaspersky Lab	668
有關協力廠商程式碼資訊	670
商標聲明	671
索引	672

關於本手冊

Kaspersky Embedded Systems Security 2.3 (下文稱為“Kaspersky Embedded Systems Security”、“應用程式”) 管理手冊的編寫目的是，供在所有受防護裝置上安裝和管理 Kaspersky Embedded Systems Security 的專家，以及使用 Kaspersky Embedded Systems Security 為各組織提供技術支援的專家使用。

本管理手冊包含有關設定和使用 Kaspersky Embedded Systems Security 的資訊。

本手冊還可協助您瞭解有關應用程式的資訊來源以及獲得技術支援的方法。

本章內容

本手冊說明主旨	21
文件說明	24

本手冊說明主旨

Kaspersky Embedded Systems Security 管理手冊由以下章節組成：

有關 Kaspersky Embedded Systems Security 的資訊來源

本章節介紹程式的相關資訊來源。

Kaspersky Embedded Systems Security

本節介紹了 Kaspersky Embedded Systems Security 的功能、元件以及分發套件，並提供了 Kaspersky Embedded Systems Security 的硬體和軟體需求清單。

安裝和移除應用程式

本節提供安裝和移除 Kaspersky Embedded Systems Security 的逐步說明。

應用程式介面

本節包含有關 Kaspersky Embedded Systems Security 介面元素的資訊。

應用程式授權

本章節提供與應用程式產品授權有關的主要概念的資訊。

啟動和停止 Kaspersky Embedded Systems Security

本節包含有關啟動和停止 Kaspersky Embedded Systems Security 管理外掛程式(下文稱為管理外掛程式) 和 Kaspersky Security Service 的資訊。

關於 Kaspersky Embedded Systems Security 功能的存取權限

本節包含有關 Kaspersky Embedded Systems Security 和應用程式註冊的 Windows® 服務的管理權限的資訊，以及如何設定這些權限的說明。

建立和設定政策

本節包含有關使用卡斯基安全管理中心政策在台電腦上管理 Kaspersky Embedded Systems Security 的資訊。

使用卡斯基安全管理中心建立和管理工作

本節包含有關 Kaspersky Embedded Systems Security 工作、如何建立工作、配置工作設定，以及啟動和停止工作的資訊。

管理應用程式設定

本章節包含有關在卡斯基安全管理中心中配置 Kaspersky Embedded Systems Security 一般設定的資訊。

即時電腦防護

本節提供有關即時電腦元件(即時檔案防護、KSN 使用和弱點利用防禦)的資訊。還提供有關如何設定即時電腦防護工作和管理受防護電腦的安全性設定說明。

本機行為控制

本節提供有關用於控制應用程式啟動和透過 USB 連線到外部裝置的 Kaspersky Embedded Systems Security 功能的資訊。

網路行為控制

本節包含有關防火牆工作的資訊。

系統稽核

本節包含有關檔案完整性監控工作以及稽核作業系統記錄功能的資訊。

與協力廠商系統整合

本節介紹 Kaspersky Embedded Systems Security 與協力廠商功能和技術的整合。

從命令列使用 Kaspersky Embedded Systems Security

本節敘述從命令列使用 Kaspersky Embedded Systems Security。

聯絡技術支援

本章節提供有關如何與 Kaspersky Lab 技術支援服務聯絡的資訊。

詞彙表

本章節包含文件中提到的專業術語及其自訂的清單。

AO Kaspersky Lab

本章節包含有關 AO Kaspersky Lab 的資訊。

有關協力廠商程式碼資訊

本章節提供有關程式中使用的協力廠商代碼資訊。

商標聲明

本章節列出本文中協力廠商的商標聲明。

索引

本章節使您可以在文件中快速尋找所需的資訊。

文件說明

本文件使用以下約定 (參閱下表) 。

表 1. 文件說明

範例文件	文件約定的說明
<p>注意...</p>	警告使用紅色字型 and 括號來註明。警告含有可能造成您的資料遺失以及硬體或作業系統故障的潛在危險資訊。
<p>我們建議您使用...</p>	註釋使用括號表示。註釋包含補充和參考資訊。
<p>範例： ...</p>	示範區域採用藍色背景，並且帶有“示範”標題。
<p>更新是指... 發生了“資料庫已過期”事件。</p>	<p>下列的項目使用斜體字來註明：</p> <ul style="list-style-type: none"> • 新的專有名詞 • 程式狀態和事件名稱
<p>點擊 ENTER 鍵。 點擊 ALT+F4 組合鍵。</p>	<p>鍵盤鍵名稱用粗體顯示並採用大寫。 以“+”號相連的按鍵名稱表示按鍵組合。這些按鍵必須同時點擊。</p>
<p>點擊“啟用”按鈕。</p>	應用程式介面內容 (例如，輸入欄位、選單項和按鈕) 的名稱以粗體顯示。
<p>► 要設定工作排程：</p>	步驟標題以斜體顯示，並伴以箭頭符號。

範例文件	文件約定的說明
<p>在命令列中，輸入 help</p> <p>隨後會出現以下訊息：</p> <p>使用 dd:mm:yy 格式指定日期。</p>	<p>下列類型的文件內容用特殊字型顯示：</p> <ul style="list-style-type: none">• 命令列語法• 應用程式顯示在視窗中的資訊文字• 使用者必須輸入的資料。
<p><使用者名稱></p>	<p>變數放在角括號中。如果不是變數名稱，應插入相應的值並省略尖括號。</p>

有關 Kaspersky Embedded Systems Security 的資訊來源

本章節介紹程式的相關資訊來源。

您可依據問題的緊急性或重要等級，來選取最適宜的來源。

本章內容

可供自行查詢的資料來源	26
在社區中討論 Kaspersky Lab 應用程式	27

可供自行查詢的資料來源

您可以使用以下來源尋找有關 Kaspersky Embedded Systems Security 的資訊：

- Kaspersky Lab 網站上的 Kaspersky Embedded Systems Security 頁面。
- 技術支援網站 (知識庫) 上的 Kaspersky Embedded Systems Security 頁面。
- 手冊。

如果您有無法自行排除的問題，請聯絡 Kaspersky Lab 技術支援部門

<https://support.kaspersky.com/>。

若要使用 Kaspersky Lab 網站資訊來源，您必須連線網際網路。

Kaspersky Lab 網站上的 Kaspersky Embedded Systems Security 頁面

在 Kaspersky Embedded Systems Security 頁面 <https://www.kaspersky.com/enterprise-security/embedded-systems> 上，您可以檢視有關程式、它的功能和特色的基本資訊。

Kaspersky Embedded Systems Security 頁面包含指向 eStore 的連結。您可以在此購買或續約產品授權。

知識庫中的 Kaspersky Embedded Systems Security 頁面

知識庫是技術支援網站的一部分。

知識庫中的 Kaspersky Embedded Systems Security 頁面 <https://support.kaspersky.com/kess2/> 包含一些文章，這些文章提供實用的資訊、建議以及有關如何購買、安裝和使用程式的常見問題解答。

知識庫文章不僅可以解答與 Kaspersky Embedded Systems Security 有關的問題，而且還可以解答與其他 Kaspersky Lab 應用程式有關的問題。它們還可能包含來自技術支援服務的新聞。

Kaspersky Embedded Systems Security 文件

《Kaspersky Embedded Systems Security 管理手冊》包含有關應用程式安裝、移除、設定配置和使用的資訊。

在社區中討論 Kaspersky Lab 應用程式

如果您的問題不需要立即性的回答，您可以在我們的社區 <https://community.kaspersky.com/> 中與 Kaspersky Lab 專家及其他使用者進行討論。

在此社區中，您可以檢視現有主題、留下評論和建立新討論主題。

Kaspersky Embedded Systems Security

本節介紹了 Kaspersky Embedded Systems Security 的功能、元件以及分發套件，並提供了 Kaspersky Embedded Systems Security 的硬體和軟體需求清單。

本章內容

關於 Kaspersky Embedded Systems Security.....	28
新增功能.....	31
分發套件.....	31
硬體和軟體需求.....	34
功能要求和限制.....	37

關於 Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security 可防護執行 Microsoft® Windows 的電腦和其他嵌入式系統免受病毒和其他電腦威脅的攻擊。Kaspersky Embedded Systems Security 管理者是負責公司網路病毒防護的系統管理員和專業人員。

您可以在執行 Windows 的各種嵌入式系統上安裝 Kaspersky Embedded Systems Security，包括以下裝置類型：

- ATM (自動櫃員機)；
- POS (銷售點)。

可透過以下方式管理 Kaspersky Embedded Systems Security：

- 透過與 Kaspersky Embedded Systems Security 安裝在同一台電腦上或安裝在其他電腦上的應用程式主控台來管理。
- 在命令列中使用指令。

- 透過卡巴斯基安全管理中心管理主控台。

卡巴斯基安全管理中心也可以用於集中管理執行 Kaspersky Embedded Systems Security 的多台電腦。

您可以檢視針對“系統監控器”應用的 Kaspersky Embedded Systems Security 效能計數器以及 SNMP 計數器和 TRAP。

Kaspersky Embedded Systems Security 元件和功能

應用程式包含以下元件：

- **即時防護。** Kaspersky Embedded Systems Security 在物件被存取時掃描物件。Kaspersky Embedded Systems Security 掃描以下物件：
 - 檔案
 - 交換檔案系統執行緒 (NTFS 執行緒)
 - 本機硬碟磁碟機和卸除式裝置上的主開機紀錄區和啟動磁區。
- **自訂掃描。** Kaspersky Embedded Systems Security 可在指定區域執行單獨的掃描，以偵測病毒和其他電腦安全威脅。應用程式會掃描受防護電腦上的檔案、RAM 和自動執行物件。
- **應用程式啟動控制。** 該元件可跟蹤使用者啟動應用程式的嘗試並控制受防護電腦上的應用程式啟動。
- **裝置控制。** 該元件可控制大容量儲存裝置和 CD/DVD 磁碟機的註冊和使用，以便防護電腦在與 USB 連線的快閃記憶體磁碟機或其他類型的外部裝置交換檔案時，免受可能產生的電腦安全威脅。
- **防火牆管理。** 此元件提供管理 Windows 防火牆的能力：配置設定和作業系統防火牆規則，並封鎖從外部配置防火牆的任何可能性。
- **檔案完整性監控。** Kaspersky Embedded Systems Security 可以偵測工作設定中指定的監控範圍內的檔案變更。這些變更可能表示受防護電腦遭到安全入侵。
- **記錄審查。** 此元件根據 Windows 事件記錄的審查結果，對受防護環境的完整性進行監控。

應用程式中佈署了以下功能：

- **資料庫更新和軟體模組更新。** Kaspersky Embedded Systems Security 會從 Kaspersky Lab 的 FTP 或 HTTP 更新伺服器、卡斯基安全管理中心管理伺服器或其他更新來源中下載應用程式資料庫和模組更新。
- **隔離。** Kaspersky Embedded Systems Security 透過將疑似感染的物件從原始位置移動到 **隔離區** 資料夾來進行隔離。出於安全考慮，物件以加密形式儲存在隔離區資料夾中。
- **備份。** 對於被歸類為“已感染”的物件，Kaspersky Embedded Systems Security 會在對其進行解毒或刪除之前，在 **備份** 中儲存這些物件的加密副本。
- **管理員和使用者通知。** 您可以設定程式通知受防護電腦的管理員和使用者，有關 Kaspersky Embedded Systems Security 操作中的事件和電腦上病毒防護的狀態。
- **匯入和匯出設定。** 可以將 Kaspersky Embedded Systems Security 設定匯出到 XML 設定檔，也可以將設定檔中的設定匯入到 Kaspersky Embedded Systems Security 中。可以將所有應用程式設定或僅將單個元件的設定儲存到設定檔。
- **套用範本。** 可以在電腦的檔案資源樹狀目錄或清單中手動配置節點的安全性設定，並將配置好的設定值儲存為範本。然後可在 Kaspersky Embedded Systems Security 防護和掃描工作中使用該範本來設定其他節點的安全設定。
- **管理 Kaspersky Embedded Systems Security 功能的存取權限。** 您可以為使用者和使用者群組設定管理 Kaspersky Embedded Systems Security 的權限和管理應用程式註冊的 Windows 服務的權限。
- **將事件寫入到應用程式事件記錄。** Kaspersky Embedded Systems Security 將記錄有關軟體元件設定的資訊、目前工作狀態、工作執行過程中發生的事件、與 Kaspersky Embedded Systems Security 管理相關的事件，以及 Kaspersky Embedded Systems Security 錯誤診斷所需的資訊。
- **信任區域。** 您可以從防護範圍或掃描範圍中建立排除清單，Kaspersky Embedded Systems Security 將在自訂和即時防護工作中套用該清單。
- **弱點利用防禦。** 您可以使用注入處理程序的代理來防護處理程序記憶體免受弱點利用。

新增功能

Kaspersky Embedded Systems Security 提供以下新功能和改進：

- 支援新版本的 Microsoft Windows 作業系統。
Windows 10 Redstone 6 (x32 和 x64) 。
- 在應用程式 GUI 中無法看到完整的啟動碼。
已新增的啟動碼在應用程式 GUI 中顯示時會部分隱藏，任何使用者都無法看到全部。

分發套件

分發套件包含常用的應用程式，您可以用它來執行以下操作：

- 啟動 Kaspersky Embedded Systems Security 安裝精靈。
- 啟動 Kaspersky Embedded Systems Security 主控台安裝精靈。
- 啟動將安裝 Kaspersky Embedded Systems Security 管理外掛程式的安裝精靈以透過卡巴斯基安全管理中心管理應用程式。
- 閱讀《管理手冊》。
- 轉到 Kaspersky Lab 網站上的 Kaspersky Embedded Systems Security 頁面。
- 存取技術支援網站 <https://support.kaspersky.com/>。
- 閱讀有關 Kaspersky Embedded Systems Security 目前版本的資訊。

\console 資料夾包含用於安裝應用程式主控台的檔案(元件的“Kaspersky Embedded Systems Security 管理工具”集)。

\product 資料夾包含：

- 用於在執行 32 位元或 64 位元 Microsoft Windows 作業系統的電腦上安裝 Kaspersky Embedded Systems Security 元件的檔案。

- 用於安裝管理外掛程式的檔案，以便透過卡斯基安全管理中心管理 Kaspersky Embedded Systems Security。
- 程式發佈時最新病毒資料庫的壓縮檔案。
- 包含最終使用者產品授權協議和隱私政策文字的檔案。

\product_no_avbases 資料夾包含 Kaspersky Embedded Systems Security 元件和管理外掛程式的安裝檔案，不含病毒資料庫。

\setup 資料夾包含問候程式啟動檔案。

分發套件檔案儲存在不同的資料夾中，具體位置取決於它們的目標用途（請參見以下表格）。

表 2. Kaspersky Embedded Systems Security 分發套件檔案

檔案	用途
autorun.inf	從卸除式介質安裝應用程式時，Kaspersky Embedded Systems Security 安裝精靈的自動執行檔案。
ess_admin_guide_zh.pdf	管理手冊。
release_notes.txt	該檔案包含發佈資訊。
setup.exe	程式安裝檔（啟動 setup.hta）。
\console\esstools_x86(x64).msi	Windows Installer 安裝套件；在受防護電腦上安裝應用程式主控台。
\console\setup.exe	該檔案啟動元件的“管理工具”元件集（包括應用程式主控台）的安裝精靈；它可使用在安裝精靈中指定的設定啟動 esstools.msi 安裝套件檔案。

檔案	用途
\product\bases.cab	程式發佈時最新病毒資料庫的壓縮檔案。
\product\setup.exe	用於透過精靈在受防護電腦上安裝 Kaspersky Embedded Systems Security 的檔案；它會啟動安裝套件檔案 ess.msi 並使用精靈中指定的安裝設定。
\product\less_x86(x64).msi	Windows Installer 安裝套件；在受防護電腦上安裝 Kaspersky Embedded Systems Security。
\product\less.kud	Kaspersky Unicode 定義格式的檔案，帶有用於透過卡巴斯基安全管理中心遠端安裝 Kaspersky Embedded Systems Security 的安裝套件的說明。
\product\klcfginst.exe	管理外掛程式的安裝程式，以便透過卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security。如果您預計用它來管理 Kaspersky Embedded Systems Security，請在每台已安裝卡巴斯基安全管理中心管理主控台的電腦上安裝該管理外掛程式。
\product\license.txt	最終使用者產品授權協議和隱私政策的文字。
\product\migration.txt	該檔案介紹從以前的應用程式版本進行移轉。
\setup\setup.hta	程式安裝檔。

硬體和軟體需求

在安裝 Kaspersky Embedded Systems Security 之前，您必須先從電腦移除其他防毒程式。

對受防護電腦的軟體需求

您可以在執行 32 位元或 64 位元 Microsoft Windows 作業系統的電腦上安裝 Kaspersky Embedded Systems Security。

在執行 Microsoft Windows XP 的電腦上正常安裝和使用應用程式需要 Windows Installer 3.1。

要在執行嵌入式作業系統的電腦上安裝和使用 Kaspersky Embedded Systems Security，需要“篩選管理器”元件。

您可以在執行下列 32 位元或 64 位元 Microsoft Windows 作業系統之一的伺服器上安裝 Kaspersky Embedded Systems Security：

- Windows XP Embedded SP3 (32 位元)
- Windows Embedded POSReady 2009 (32 位元)
- Windows XP Professional SP2 / SP3 (32 位元、64 位元)
- Windows Embedded Standard 7 SP1 (32 位元、64 位元)
- Windows Embedded Enterprise 7 SP1 (32 位元、64 位元)
- Windows Embedded POSReady 7 (32 位元、64 位元)
- Windows 7 Professional / Enterprise SP1 (32 位元、64 位元)
- Windows Embedded 8.1 Industry Professional / Enterprise (32 位元、64 位元)
- Windows Embedded 8.0 Standard (32 位元、64 位元)
- Windows 8 Professional / Enterprise (32 位元、64 位元)
- Windows 8.1 Professional / Enterprise (32 位元、64 位元)

- Windows 10 Professional / Enterprise (32 位元、64 位元)
- Windows 10 IoT Enterprise (32 位元、64 位元)
- Windows 10 Redstone 1 Professional / Enterprise / IoT Enterprise (32 位元、64 位元)
- Windows 10 Redstone 2 Professional / Enterprise / IoT Enterprise (32 位元、64 位元)
- Windows 10 Redstone 3 Professional / Enterprise / IoT Enterprise (32 位元、64 位元)
- Windows 10 Redstone 4 Professional / Enterprise / IoT Enterprise (32 位元、64 位元)
- Windows 10 Redstone 5 Professional / Enterprise / IoT Enterprise (32 位元、64 位元)
- Windows 10 Redstone 6 Professional / Enterprise / IoT Enterprise (32 位元、64 位元)

對受防護電腦的硬體需求

對受防護電腦的硬體要求有所不同，具體取決於安裝的 Windows 作業系統：

- 對執行 Windows XP (32/64 位元)、Windows 7 (32 位元)、Windows 8 (32 位元)、Windows Embedded XP、Windows Embedded POSReady 2009 或 Windows Embedded POSReady 7 作業系統的電腦的硬體要求：
 - 最低需求：
 - 磁碟空間需求：
 - 安裝“應用程式啟動控制”元件 – 50 MB。
 - 安裝所有 Kaspersky Embedded Systems Security 元件 – 2 GB。
 - RAM：
 - 256 MB - 在執行 Microsoft Windows 作業系統的電腦上只安裝“應用程式啟動控制”元件。
 - 512 MB - 完全安裝所有元件。

- 處理器要求：
 - 對於 32 位元 Microsoft Windows 作業系統：1.4 GHz 單核處理器 Intel® Pentium® III。
 - 對於 64 位元 Microsoft Windows 作業系統：1.4 GHz 單核處理器 Intel Pentium IV。
- 建議需求：
 - 磁碟空間需求：
 - 安裝“應用程式啟動控制”元件 – 2 GB。
 - 安裝所有 Kaspersky Embedded Systems Security 元件 – 4 GB。
 - RAM：2 GB。
 - 處理器要求：2.4 GHz 四核處理器。
- 對執行 Windows 7(64 位元), Windows 8(64 位元), Windows 10(64 位元), Windows Embedded 7 或 Windows Embedded 8 作業系統的電腦的硬體要求：
 - 最低需求：
 - 磁碟空間需求：
 - 安裝“應用程式啟動控制”元件 – 50 MB。
 - 安裝所有 Kaspersky Embedded Systems Security 元件 – 2 GB。
 - RAM：1 GB。
 - 處理器要求：
 - 對於 32 位元 Microsoft Windows 作業系統：1.4 GHz 單核處理器 Intel Pentium III。
 - 對於 64 位元 Microsoft Windows 作業系統：1.4 GHz 單核處理器 Intel Pentium IV。
 - 建議配置
 - 磁碟空間需求：
 - 安裝“應用程式啟動控制”元件 – 2 GB。
 - 安裝所有 Kaspersky Embedded Systems Security 元件 – 4 GB。

- RAM : 2 GB。
- 處理器要求 : 2.4 GHz 四核處理器。

功能要求和限制

本節介紹 Kaspersky Embedded Systems Security 元件的附加功能要求和現有限制。

本章節說明項目

安裝和移除	37
檔案完整性監控	38
防火牆管理	39
其他限制	40

安裝和移除

- 在應用程式安裝過程中，如果 Kaspersky Embedded Systems Security 安裝資料夾的新路徑包含超過 150 個符號，將顯示一條警告。該警告不會影響安裝過程：Kaspersky Embedded Systems Security 將成功安裝並執行。
- 要安裝 SNMP 協議支援元件，必須重新啟動 SNMP 服務（如果其正在執行）。
- 要在嵌入式作業系統管理的裝置上安裝 Kaspersky Embedded Systems Security 並使其執行，必須安裝“篩選管理器”元件。

- Kaspersky Embedded Systems Security 管理工具不能透過 Microsoft Active Directory® 群組政策安裝。
- 在執行無法定期接收更新的較舊作業系統的電腦上安裝應用程式時，需要檢查以下根憑證：DigiCert Assured ID Root CA、DigiCert_High_Assurance_EV_Root_CA、DigiCertAssuredIDRootCA。缺少指定憑證可能導致應用程式執行錯誤。建議以任何可能的方式安裝指定憑證。
- Kaspersky Embedded Systems Security 主控台不能透過“開始”功能表移除。您可以使用“新增/移除程式”視窗中的連結移除 Kaspersky Embedded Systems Security 主控台。

檔案完整性監控

預設情況下，“檔案完整性監控”不監控系統資料夾或檔案系統清理檔案的變化，以防止有關由作業系統不斷執行的例行檔案變更的資訊進入工作報告。使用者無法手動在監控範圍中包含此類資料夾。

以下資料夾/檔案從監控範圍中排除：

- 檔案 id 從 0 到 33 的 NTFS 清理檔案
- "%SystemRoot%\Prefetch\"
- "%SystemRoot%\ServiceProfiles\LocalService\AppData\Local\"
- "%SystemRoot%\System32\LogFiles\Scm\"
- "%SystemRoot%\Microsoft.NET\Framework\v4.0.30319\"
- "%SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\"
- "%SystemRoot%\Microsoft.NET\"
- "%SystemRoot%\System32\config\"
- "%SystemRoot%\Temp\"
- "%SystemRoot%\ServiceProfiles\LocalService\"
- "%SystemRoot%\System32\winevt\Logs\"
- "%SystemRoot%\System32\wbem\repository\"

- "%SystemRoot%\System32\wbem\Logs\"
- "%ProgramData%\Microsoft\Windows\WER\ReportQueue\"
- "%SystemRoot%\SoftwareDistribution\DataStore\"
- "%SystemRoot%\SoftwareDistribution\DataStore\Logs\"
- "%ProgramData%\Microsoft\Windows\AppRepository\"
- "%ProgramData%\Microsoft\Search\Data\Applications\Windows\"
- "%SystemRoot%\Logs\SystemRestore\"
- "%SystemRoot%\System32\Tasks\Microsoft\Windows\TaskScheduler\"

應用程式會排除頂層資料夾。

該元件不監控繞過 ReFS/NTFS 檔案系統的檔案變更 (透過 BIOS、LiveCD 等進行的檔案變更)。

防火牆管理

- 當指定的應用規則範圍包含一個位址時，不能使用 IPv6 格式的 IP 位址。
- 預設的防火牆政策只提供本機電腦與管理伺服器之間的基本互動方案的執行。要完全使用卡巴斯基安全管理中心功能，需要手動設定連接埠規則。有關連接埠號、協定及其功能的資訊包含在卡巴斯基安全管理中心知識庫 (文章 ID : 9297) 中。
- 如果在安裝應用程式時未將 Windows 防火牆規則和規則群組新增到防火牆管理工作配置中，則在該工作的每分鐘查詢期間，應用程式不對這些規則的修改進行控制。要更新狀態和包含此類規則，必須重新啟動防火牆管理工作。
- 啟動“防火牆管理”工作後，以下類型的規則會自動從作業系統的防火牆設定中刪除：
 - 拒絕規則；
 - 監控傳出流量的規則。

其他限制

自訂掃描，即時檔案防護：

- 已連線 MTP 裝置掃描不可用。
- 如果沒有 SFX 壓縮檔案掃描，壓縮檔案物件掃描不可用：如果 Kaspersky Embedded Systems Security 的防護設定中啟用了壓縮檔案掃描，應用程式會自動掃描壓縮檔案和 SFX 壓縮檔案中的物件。如果沒有壓縮檔案掃描，SFX 壓縮檔案掃描仍可用。

授權：

- 如果金鑰儲存在使用 SUBST 指令建立的磁碟上，或者指定了金鑰檔案的網路路徑，則無法透過安裝精靈使用金鑰啟動應用程式。

更新：

- 安裝 Kaspersky Embedded Systems Security 關鍵模組更新後，應用程式圖示預設隱藏。
- 執行 Windows XP 或 Windows 2003 作業系統的電腦不支援 KLRAMDISK。

介面：

- 在“隔離”、“備份”、“系統稽核記錄”或“工作記錄”中，如果在應用程式主控台中使用篩選，則應保持大小寫。
- 在應用程式主控台中配置防護範圍或掃描範圍時，只能使用一個遮罩且只能在路徑末尾使用。正確的遮罩使用範例：“C:\Temp\Temp*”或“C:\Temp\Temp????.doc”或“C:\Temp\Temp*.doc”。限制不影響信任區域配置。

安全性：

- 如果作業系統設定中啟動了使用者帳戶控制，則使用者帳戶必須屬於 KAVWSEE 管理員群組，才能透過點擊工作列通知區域中的應用程式圖示來開啟應用程式主控台。在其他情況下，需要以被允許開啟小型診斷視窗或 Microsoft 管理控制台管理單元的使用者身分登入。
- 如果啟動了使用者帳戶控制，則無法透過 Microsoft Windows 的“程式和功能”視窗移除應用程式。

與卡斯基安全管理中心整合：

- 管理伺服器在收到更新套件時會先檢查資料庫更新有效性，然後才將更新傳送到網路電腦。管理伺服器不檢查收到的軟體模組更新的有效性。
- 當借助網路清單（隔離、備份）使用將動態變化的資料傳輸到卡斯基安全管理中心的元件時，確保在與管理伺服器設定的互動中選中所需核取方塊。

弱點利用防禦：

- 如果目前環境配置中未載入 apphelp.dll 庫，則“弱點利用防禦”不可用。
- “弱點利用防禦”元件與執行 Microsoft Windows 10 作業系統的電腦上的 Microsoft EMET 實用程式不相容：如果在安裝了 EMET 的電腦上安裝“弱點利用防禦”元件，Kaspersky Embedded Systems Security 會封鎖 EMET。

安裝和移除應用程式

本節提供安裝和移除 Kaspersky Embedded Systems Security 的逐步說明。

本章內容

適用於 Windows Installer 服務的 Kaspersky Embedded Systems Security 軟體元件程式碼	42
Kaspersky Embedded Systems Security 安裝後的系統變更	46
Kaspersky Embedded Systems Security 處理程序	51
Windows Installer 服務的安裝和移除設定及命令列選項	52
Kaspersky Embedded Systems Security 安裝和移除記錄	56
安裝排程	56
基於精靈安裝和移除應用程式	60
透過命令列安裝或移除應用程式	77
使用卡斯基安全管理中心安裝和移除應用程式	84
透過 Active Directory 群組政策安裝和移除	90
檢查 Kaspersky Embedded Systems Security 功能。使用 EICAR 測試病毒	93

適用於 Windows Installer 服務的 Kaspersky Embedded Systems Security 軟體元件程式碼

預設情況下，\product\ess_x86.msi 和 \product\ess_x64.msi 檔案會安裝所有 Kaspersky Embedded Systems Security 元件。您可透過在自訂安裝中包含這些元件來安裝它們。

\console\esstools_x86.msi 和 \console\esstools_x64.msi 檔案安裝“管理工具”集內的所有軟體元件。

以下各節列出了適用於 Windows Installer 服務的 Kaspersky Embedded Systems Security 元件程式碼。透過命令列安裝 Kaspersky Embedded Systems Security 時，可使用這些代碼來定義要安裝的元件清單。

本章節說明項目

Kaspersky Embedded Systems Security 軟體元件.....	43
軟體元件的“管理工具”集	45

Kaspersky Embedded Systems Security 軟體元件

下表含有 Kaspersky Embedded Systems Security 軟體元件的代碼和說明。

表 3. Kaspersky Embedded Systems Security 軟體元件的說明

元件	識別碼	執行功能
基本功能	Core	此元件包含基本應用程式功能集合並確保其操作。
應用程式啟動控制	AppCtrl	此元件監控使用者執行應用程式的嘗試，並根據指定的應用程式啟動控制規則來允許或拒絕這些應用程式啟動。 它在“應用程式啟動控制”工作中執行。
裝置控制	DevCtrl	此元件跟蹤將 USB 大容量儲存器連線到受防護電腦的嘗試，並根據指定的裝置控制規則來允許或拒絕這些裝置的使用。 該元件在“裝置控制”工作中實施。
病毒防護	AVProtection	此元件確保病毒防護並包含以下元件： <ul style="list-style-type: none"> • 自訂掃描 • 即時檔案防護

元件	識別碼	執行功能
自訂掃描	Ods	此元件安裝 Kaspersky Embedded Systems Security 系統檔案並提供自訂掃描工作(依要求掃描受防護電腦的物件)。如果您從命令列安裝 Kaspersky Embedded Systems Security 時，指定其他 Kaspersky Embedded Systems Security 元件，但未指定 Core 元件，將自動安裝 Core 元件。
即時檔案防護	Oas	此元件在受防護電腦上的檔案被存取時對這些檔案執行病毒防護掃描。 其執行“即時檔案防護”工作。
卡巴斯基安全網路使用	Ksn	此元件基於 Kaspersky Lab 雲端技術提供防護。它執行“KSN 使用”工作(向卡巴斯基安全網路服務傳送請求及從該服務接收結論)。
檔案完整性監控	Fim	此元件可記錄指定監控範圍內針對檔案執行的操作。 該元件執行檔案完整性監控工作。
弱點利用防禦	AntiExploit	此元件可管理設定，以便防護受防護電腦記憶體中的處理程序所使用的記憶體。
防火牆管理	Firewall	此元件可透過 Kaspersky Embedded Systems Security 圖形化使用者介面來管理 Windows 防火牆。 關於防火牆管理工作。
整合卡巴斯基安全管理中心網路代理模組	AKIntegration	此元件提供 Kaspersky Embedded Systems Security 與卡巴斯基安全管理中心網路代理之間的連線。 如果想透過卡巴斯基安全管理中心管理應用程式，請在受防護電腦上安裝此元件。

元件	識別碼	執行功能
記錄審查	LogInspector	此元件根據 Windows 事件記錄的審查結果，對受防護環境的完整性進行監控。
“系統監控器”效能計數器群組	PerfMonCounters	此元件可安裝一組系統監控效能計數器。效能計數器可用來衡量 Kaspersky Embedded Systems Security 的效能，並在使用 Kaspersky Embedded Systems Security 與其他程式時找出電腦上的潛在影響。
SNMP 計數器與 TRAP	SnmpSupport	此元件可透過 Microsoft Windows 中的簡單網路管理通訊協定 (SNMP) 發佈 Kaspersky Embedded Systems Security 計數器與 TRAP。只有受防護電腦上安裝了 Microsoft SNMP 服務時，才能在同一電腦上安裝此元件。
通知區域中的 Kaspersky Embedded Systems Security 圖示	TrayApp	此元件在受防護電腦的工作列通知區域顯示 Kaspersky Embedded Systems Security 圖示。Kaspersky Embedded Systems Security 圖示除了會顯示電腦防護的狀態，還可在 MMC (如果已安裝) 和“關於應用程式”視窗中開啟 Kaspersky Embedded Systems Security 主控台。

軟體元件的“管理工具”集

下表含有“管理工具”集軟體元件的代碼及說明。

表 4. “管理工具”軟體元件說明

元件	代碼	元件功能
Kaspersky Embedded Systems Security 嵌入式管理	MmcSnapin	此元件透過 Kaspersky Embedded Systems Security 主控台安裝 Microsoft 管理主控台管理單元。 如果您透過命令列安裝管理工具時，指定其他元件，但未指定 MmcSnapin 元件，將自動安裝此元件。

元件	代碼	元件功能
說明	Help	這是儲存在包含 Kaspersky Embedded Systems Security 管理工具檔案資料夾中的 .chm 說明檔案。您可以使用“開始”功能表或透過在應用程式主控台視窗處於開啟狀態時按 F1 鍵，來開啟說明檔案。
文件	Help	Kaspersky Embedded Systems Security 新增了 Kaspersky Lab 網站的捷徑，其中提供了 PDF 格式的《管理手冊》。該捷徑在“開始”功能表中提供。

安裝 Kaspersky Embedded Systems Security 後系統的變更

當 Kaspersky Embedded Systems Security 和“管理工具”集(包括應用程式主控台)同時安裝時，Windows Installer 服務將對受防護電腦進行以下變更：

- 在受防護電腦與安裝了應用程式主控台的電腦上建立 Kaspersky Embedded Systems Security 資料夾。
- 註冊 Kaspersky Embedded Systems Security 服務。
- 建立一個 Kaspersky Embedded Systems Security 使用者群組。
- 在系統登錄檔中註冊 Kaspersky Embedded Systems Security 項。

下文介紹了這些變更。

受防護電腦上的 Kaspersky Embedded Systems Security 資料夾

安裝 Kaspersky Embedded Systems Security 後，在受防護電腦上建立以下資料夾：

- Kaspersky Embedded Systems Security 預設安裝資料夾，其中包含 Kaspersky Embedded Systems Security 可執行檔，具體取決於作業系統位集。因此，預設安裝資料夾如下所示：
 - 在 32 位元版本的 Microsoft Windows 中：`%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\`

- 資料庫的備份副本；每次更新資料庫時將會覆寫這些副本：
 - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Backup\
- 執行更新工作時所建立的暫存檔：
 - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Temp\
- 隔離的物件（預設資料夾）：
 - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Quarantine\
- 備份中的物件（預設資料夾）：
 - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Backup\
- 從備份區和隔離區還原的物件（還原物件的預設資料夾）：
 - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored\

在應用程式主控台安裝過程中建立的資料夾

應用程式主控台預設安裝資料夾，其中包含“管理工具”檔案，具體取決於作業系統位集。因此，預設安裝資料夾如下所示：

- 在 32 位元版本的 Microsoft Windows 中：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\
- 在 64 位元版本的 Microsoft Windows 中：%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\

Kaspersky Embedded Systems Security 服務

以下 Kaspersky Embedded Systems Security 服務使用本機系統 (SYSTEM) 帳戶啟動：

- Kaspersky Security 服務 (KAVFS) – 用於管理 Kaspersky Embedded Systems Security 工作和工作流的基本 Kaspersky Embedded Systems Security 服務。
- Kaspersky Security 管理服務 (KAVFSGT) – 此服務用於透過應用程式主控台進行 Kaspersky Embedded Systems Security 應用程式。
- Kaspersky Security 弱點利用防禦服務 (KAVFSSLP) – 用作將安全設定傳輸給外部安全代理並接收有關安全事件資料的媒介的服務。

Kaspersky Embedded Systems Security

“ESS 管理員”是受防護電腦上的使用者群組，其中的使用者對 Kaspersky Security 管理服務和所有 Kaspersky Embedded Systems Security 功能擁有完全存取權限。

系統登錄註冊參數

安裝 Kaspersky Embedded Systems Security 後，將建立以下系統登錄機碼：

- Kaspersky Embedded Systems Security 的內容：
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Kaspersky Embedded Systems Security 事件記錄設定 (Kaspersky 事件記錄)：
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Kaspersky Embedded Systems Security 管理服務的內容：
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- 效能計數器設定：
 - 在 32 位元版本的 Microsoft Windows 中：[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
 - 在 64 位元版本的 Microsoft Windows 中：[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- SNMP 協定支援元件設定：
 - 在 32 位元版本的 Microsoft Windows 中：[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\SnmpAgent]
 - 在 64 位元版本的 Microsoft Windows 中：[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\SnmpAgent]
- 傾印檔案設定：
 - 在 32 位元版本的 Microsoft Windows 中：[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\CrashDump]
 - 在 64 位元版本的 Microsoft Windows 中：[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\CrashDump]

- 偵錯檔案設定：
 - 在 32 位元版本的 Microsoft Windows 中：[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\Trace]
 - 在 64 位元版本的 Microsoft Windows 中：[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Trace]
- 應用程式的工作和功能的設定：[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Environment]

Kaspersky Embedded Systems Security 處理程序

Kaspersky Embedded Systems Security 將啟動下表中敘述的處理程序。

表 5. Kaspersky Embedded Systems Security 處理程序

檔案名稱	用途
kavfswp.exe	Kaspersky Embedded Systems Security 工作流
kavtray.exe	系統欄圖示的處理程序
kavfsmui.exe	小型診斷視窗元件的處理程序
kavshell.exe	命令列實用工具處理程序
kavfsrcn.exe	Kaspersky Embedded Systems Security 遠端管理處理程序
kavfs.exe	Kaspersky Security 服務處理程序
kavfsgt.exe	Kaspersky Security 管理服務處理程序
kavfswh.exe	Kaspersky Security 弱點利用防禦服務處理程序

Windows Installer 服務的安裝和移除設定及命令列選項

本節包含安裝和移除 Kaspersky Embedded Systems Security 的設定說明和預設值，以及變更安裝設定值及可變動參數。透過命令列安裝 Kaspersky Embedded Systems Security 時，您可以使用參數及 Windows Installer 服務中 `msiexec` 指令適用的標準指令。

Windows Installer 中的安裝設定和命令列選項

- 接受最終使用者產品授權協議的條款：您必須接受條款才能安裝 Kaspersky Embedded Systems Security。

EULA=<值> 命令列選項的可能值如下：

- 0 - 不同意接受最終使用者產品授權協議條款（預設值）。
- 1 - 同意接受最終使用者產品授權協議條款。
- 接受隱私政策的條款：您必須接受條款才能安裝 Kaspersky Embedded Systems Security。

PRIVACYPOLICY=<值> 命令列選項的可能值如下：

- 0 - 拒絕隱私政策條款（預設值）。
- 1 - 接受隱私政策條款。
- 安裝 Kaspersky Embedded Systems Security 並初步掃描啟動的處理程序與本機磁碟機的開機磁區。

PRESCAN=<值> 命令列選項的可能值如下：

- 0 - 在安裝過程中不執行對活動處理程序和本機磁碟機引導扇區的初步掃描（預設值）。
- 1 - 在安裝過程中執行對活動處理程序和本機磁碟機引導扇區的初步掃描。

- 安裝過程中將儲存在 Kaspersky Embedded Systems Security 檔案的目標資料夾。您可指定不同的資料夾。

INSTALLDIR=<資料夾的完整路徑> 命令列選項的預設值如下：

- Kaspersky Embedded Systems Security : %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
- 管理工具 : %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
- 在 x64 位元版本的 Microsoft Windows 中 : %ProgramFiles(x86)%
- “即時檔案防護”工作在 Kaspersky Embedded Systems Security 啟動後立即啟動。開啟該設定可在 Kaspersky Embedded Systems Security 啟動時啟動“即時檔案防護”（建議）。

RUNRTP=<值> 命令列選項的可能值如下：

- 1 – 啟動（預設值）。
- 0 – 不啟動。
- Microsoft Corporation 推薦的防護排除項目。在“即時檔案防護”範圍中排除 Microsoft Corporation 建議電腦排除的物件。當防毒應用程式攔截或修改檔案時，電腦上某些應用程式可能變得較不穩定。例如，當 Microsoft Corporation 將某些網域控制站應用程式納入此類物件清單時。

ADDMSEXCLUSION=<值> 命令列選項的可能值如下：

- 1 – 排除（預設值）。
- 0 – 不排除。
- 按照 Kaspersky Lab 建議從防護範圍中排除的物件。在“即時檔案防護”範圍中排除 Kaspersky Lab 建議電腦排除的物件。

ADDKLEXCLUSION=<值> 命令列選項的可能值如下：

- 1 – 排除（預設值）。
- 0 – 不排除。

- 允許遠端連線到應用程式主控台。預設情況下，不允許遠端連線到安裝在受防護電腦上的應用程式主控台。安裝過程中，可允許連線。Kaspersky Embedded Systems Security 針對所有連接埠使用 TCP 協定為處理程序 kavfsgt.exe 建立允許規則。

ALLOWREMOTECON=<值> 命令列選項的可能值如下：

- 1 – 允許。
- 0 – 拒絕 (預設值)。
- 金鑰檔案的路徑。預設情況下，Windows Installer 會嘗試在分發套件的 \product 資料夾中尋找副檔名為 .key 的檔案。如果 \product 資料夾包含多個金鑰檔案，Windows Installer 將選擇到期日期最晚的金鑰檔案。可以預先將金鑰檔案儲存在 \product 資料夾中，也可以使用“**新增金鑰**”設定為金鑰檔案指定其他路徑。您可以在安裝 Kaspersky Embedded Systems Security 後使用所選的管理工具 (例如，應用程式主控台) 新增金鑰。如果您在應用程式安裝期間未新增金鑰，Kaspersky Embedded Systems Security 將不會發揮功能。
- 設定檔的路徑。Kaspersky Embedded Systems Security 從在應用程式中建立的指定設定檔匯入設定。Kaspersky Embedded Systems Security 無法從設定檔匯入密碼，例如，用來啟動工作的帳戶密碼或用來連線代理伺服器的密碼。一旦匯入設定，將需手動輸入所有密碼。如果未指定設定檔，安裝後應用程式將開始使用預設設定。

CONFIGPATH=<設定檔名稱> 的預設值未指定。

- 為應用程式主控台啟用網路連線。使用該選項在另一台電腦上安裝 Kaspersky Embedded Systems Security。您可以從安裝了 Kaspersky Embedded Systems Security 主控台的另一台電腦遠端管理電腦防護。在 Microsoft Windows 防火牆中開放連接埠 135 (TCP)，允許透過網路連線到可執行檔 kavfsrcn.exe 以遠端管理 Kaspersky Embedded Systems Security，並授予對 DCOM 應用程式的存取權限。安裝完成後，向“ESS 管理員”群組新增使用者，以允許他們遠端管理應用程式，並允許透過網路連線到電腦上的 Kaspersky Security 管理服務 (kavfsgt.exe 檔案)。您可以閱讀有關 Kaspersky Embedded Systems Security 主控台安裝到其他電腦上時的附加配置的詳細資訊 (請參見第 65 頁上的“在其他電腦上安裝應用程式主控台以後的進階設定”部分)。

ADDWFEXCLUSION=<值> 命令列選項的可能值如下：

- 1 – 允許。

- 0 – 拒絕 (預設值)。
- 停用不相容軟體檢查。使用此設定可啟用或停用在電腦上背景安裝應用程式期間對不相容軟體的檢查。不管此設定的值如何，在 Kaspersky Embedded Systems Security 安裝期間，應用程式始終會針對電腦上安裝的其他版本的應用程式發出警告。

SKIPINCOMPATIBLESW=<值> 命令列選項的可能值如下：

- 0 – 執行不相容軟體檢查 (預設值)。
- 1 – 不執行不相容軟體檢查。

Windows Installer 中的移除設定和命令列選項

- 還原隔離的物件。

RESTOREQTN=<值> 命令列選項的可能值如下：

- 0 – 刪除隔離內容 (預設值)。
- 1 – 將隔離內容還原到 RESTOREPATH 參數所指定的資料夾的 \Quarantine 子資料夾中。
- 還原備份內容。

RESTOREBCK=<值> 命令列選項的可能值如下：

- 0 – 刪除備份內容 (預設值)。
- 1 – 將備份內容還原到 RESTOREPATH 參數所指定的資料夾 \Backup 子資料夾中。
- 輸入目前密碼以確認移除 (如果已啟用密碼防護)。

UNLOCK_PASSWORD=<指定密碼> 的預設值未指定。

- 還原物件的資料夾。還原的物件將儲存到指定的資料夾。

RESTOREPATH=<資料夾的完整路徑> 命令列選項的預設值為 %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored。

Kaspersky Embedded Systems Security 安裝和移除記錄

如果使用安裝 (移除) 精靈安裝 (移除) Kaspersky Embedded Systems Security , Windows Installer 服務會建立安裝 (移除) 記錄。一個名為 `ess_install_<uid>.log` (其中 `<uid>` 是唯一的八個字元記錄識別碼) 的記錄檔案將儲存在用於啟動 `setup.exe` 檔案的帳戶所屬使用者的 `%temp%` 資料夾中。

如果從“開始”功能表執行應用程式主控台或 Kaspersky Embedded Systems Security 的“修改或移除 Kaspersky Embedded Systems Security 2.3 管理工具”選項，將在 `%temp%` 資料夾中自動建立一個名為 `ess_2.3_maintenance.log` 的記錄檔案。

預設情況下，若您是從命令列安裝或移除 Kaspersky Embedded Systems Security，就不會建立該安裝記錄檔案。

► 要安裝 *Kaspersky Embedded Systems Security* 並在磁碟 `C:\` 上建立記錄檔案：

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

安裝排程

本節包含 Kaspersky Embedded Systems Security 管理工具集以及 使用精靈 (請參見第 60 頁上的“使用精靈安裝和移除應用程式”部分)、命令列 (請參見第 77 頁上的“從命令列安裝和移除應用程式”部分)、透過卡巴斯基安全管理中心 (請參見第 84 頁上的“使用卡巴斯基安全管理中心安裝和移除應用程式”部分) 以及透過 Active Directory 群組政策 (請參見第 90 頁上的“透過 Active Directory 群組政策安裝和移除”部分) 安裝和移除 Kaspersky Embedded Systems Security 的特殊方面。

在開始安裝 Kaspersky Embedded Systems Security 前，請計劃安裝的主要階段。

1. 確定管理和設定 Kaspersky Embedded Systems Security 所使用的管理工具。
2. 選擇必須安裝的應用程式元件 (請參閱第 42 頁上的“適用於 Windows Installer 服務的 Kaspersky Embedded Systems Security 軟體元件程式碼”部分)。
3. 選擇安裝方式。

本章節說明項目

選擇管理工具.....	57
選擇安裝類型.....	58

選擇管理工具

確定將用於配置 Kaspersky Embedded Systems Security 設定和管理該應用程式的管理工具。可以使用應用程式主控台、命令列實用工具和卡斯基安全管理中心管理主控台管理 Kaspersky Embedded Systems Security。

Kaspersky Embedded Systems Security 主控台

Kaspersky Embedded Systems Security 主控台是新增到 Microsoft 管理主控台的獨立管理元件。您可以透過安裝在受防護電腦或公司網路中其他電腦上的應用程式主控台來管理 Kaspersky Embedded Systems Security。

您可以將多個 Kaspersky Embedded Systems Security 管理元件新增到在作者模式中開啟單獨的 Microsoft 管理主控台中，以使用它來管理多台已安裝 Kaspersky Embedded Systems Security 的電腦防護。

應用程式主控台含在“管理工具”應用程式元件集內。

命令列實用工具

您可以從受防護電腦的命令列管理 Kaspersky Embedded Systems Security。

命令列實用工具包含在 Kaspersky Embedded Systems Security 軟體元件群組中。

卡斯基安全管理中心

若您為了集中管理公司電腦的病毒防護工作而使用卡斯基安全管理中心，您可使用卡斯基安全管理中心的管理主控台來管理 Kaspersky Embedded Systems Security。

必須安裝下列元件：

- **整合卡巴斯基安全管理中心網路代理模組。**此元件包含在 Kaspersky Embedded Systems Security 軟體元件群組中。它允許 Kaspersky Embedded Systems Security 與網路代理通信。請在受防護電腦上安裝與卡巴斯基安全管理中心網路代理程式整合的模組。
- **卡巴斯基安全管理中心網路代理。**在每台受防護電腦上安裝該元件。該元件支援電腦上安裝的 Kaspersky Embedded Systems Security 與卡巴斯基安全管理中心管理主控台之間的互動。網路代理程式安裝檔案包含在卡巴斯基安全管理中心的分發套件資料夾中。
- **Kaspersky Embedded Systems Security 2.3 管理外掛程式。**此外，安裝該外掛程式，以在安裝了卡巴斯基安全管理中心管理電腦的電腦上透過管理主控台管理 Kaspersky Embedded Systems Security。此外掛程式提供了透過卡巴斯基安全管理中心進行應用程式管理的介面。管理外掛程式安裝檔案 `\product\klcfginst.exe` 包含在 Kaspersky Embedded Systems Security 分發套件中。

選擇安裝類型

指定 Kaspersky Embedded Systems Security 安裝的軟體元件後（請參閱第 42 頁上的“適用於 Windows Installer 服務的 Kaspersky Embedded Systems Security 軟體元件程式碼”部分），您需要選擇應用程式安裝方法。

根據網路架構並參考下列情況選擇安裝方法：

- 是需要特殊的 Kaspersky Embedded Systems Security 安裝設定，還是建議的安裝設定（請參見第 52 頁上的“Windows Installer 服務的安裝和移除設定及命令列選項”部分）。
- 所有電腦是否採用相同的安裝設定或個別為每個電腦使用不同的設定。

使用者可使用背景模式在命令列指定適當的安裝設定，或利用互動式安裝精靈安裝 Kaspersky Embedded Systems Security。您可使用 Active Directory 群組政策或卡巴斯基安全管理中心遠端安裝工作，以遠端方式統一安裝 Kaspersky Embedded Systems Security。

可以在單台電腦上安裝和設定 Kaspersky Embedded Systems Security，其設定會儲存到一個設定檔中；該檔案隨後可用於在其他電腦上安裝 Kaspersky Embedded Systems Security。請注意，使用 Active Directory 群組政策安裝應用程式時，此功能不存在。

啟動安裝精靈

您可使用安裝精靈安裝下列內容：

- 將 Kaspersky Embedded Systems Security 元件 (請參見第 [43](#) 頁上的“Kaspersky Embedded Systems Security 軟體元件”部分) 從分發套件中包含的 \product\setup.exe 檔案安裝到受防護電腦上。
- 將 Kaspersky Embedded Systems Security 主控台 (請參見第 [64](#) 頁上的“Kaspersky Embedded Systems Security 主控台安裝”部分) 從安裝套件的 \console\setup.exe 檔案安裝到受防護電腦或其他 LAN 主機上。

透過命令列使用必要的安裝設定來啟動安裝套件檔案

如果不以任何命令列選項啟動安裝套件檔案，則 Kaspersky Embedded Systems Security 將以預設設定安裝。可以使用 Kaspersky Embedded Systems Security 選項修改安裝設定。

應用程式主控台可以安裝在受防護電腦和/或管理員工作站上。

您還可以使用示例指令安裝 Kaspersky Embedded Systems Security 和應用程式主控台(請參見第 [77](#) 頁上的“從命令列安裝和移除應用程式”部分)。

透過卡巴斯基安全管理中心集中安裝

如果卡巴斯基安全管理中心在您的網路中的用途是管理網路電腦的病毒防護，則可以使用遠端安裝工作在一台或多台電腦上安裝 Kaspersky Embedded Systems Security。

您希望使用卡巴斯基安全管理中心安裝 Kaspersky Embedded Systems Security (請參見第 [84](#) 頁上的“使用卡巴斯基安全管理中心安裝和移除應用程式”部分) 的電腦可以與卡巴斯基安全管理中心在同一網域中，也可以在不同的網域中，或完全不在任何網域中。

使用 Active Directory 群組政策集中安裝

您可使用 Active Directory 群組政策在受防護電腦上安裝 Kaspersky Embedded Systems Security。應用程式主控台可以安裝在受防護電腦或管理員工作站上。

可以僅使用建議的安裝設定安裝 Kaspersky Embedded Systems Security。

使用 Active Directory 群組政策安裝 Kaspersky Embedded Systems Security (請參見第 90 頁上的“透過 Active Directory 群組政策安裝和移除”部分) 的電腦必須位於相同網域和相同的組織單元中。安裝作業會在電腦啟動，登入 Microsoft Windows 之前執行。

基於精靈安裝和移除應用程式

本節介紹透過安裝精靈安裝和移除 Kaspersky Embedded Systems Security 和應用程式主控台，並包含有關 Kaspersky Embedded Systems Security 的附加配置以及要在安裝後執行的操作的資訊。

本章節說明項目

使用安裝精靈安裝	60
修改元件集和修復 Kaspersky Embedded Systems Security	73
使用安裝精靈移除	75

使用安裝精靈進行安裝

以下各節包含有關安裝 Kaspersky Embedded Systems Security 和應用程式主控台的資訊。

► 要安裝及使用 *Kaspersky Embedded Systems Security* 服務，請執行以下步驟：

1. 在受防護電腦上安裝 Kaspersky Embedded Systems Security。
2. 在您打算用來管理 Kaspersky Embedded Systems Security 的電腦上安裝應用程式主控台。
3. 如果應用程式主控台已經安裝在網路中的其他電腦上，而不是安裝在受防護電腦上，請執行附加配置以允許應用程式主控台使用者遠端管理 Kaspersky Embedded Systems Security。
4. 安裝 Kaspersky Embedded Systems Security 後執行操作。

本章節說明項目

Kaspersky Embedded Systems Security 安裝.....	61
Kaspersky Embedded Systems Security 主控台安裝.....	64
在其他電腦上安裝應用程式主控台以後的進階設定.....	65
在安裝 Kaspersky Embedded Systems Security 後執行的操作.....	69

Kaspersky Embedded Systems Security 安裝

在安裝 Kaspersky Embedded Systems Security 之前，請執行以下步驟：

確認電腦上未安裝任何防毒程式。

- 確認用來啟動安裝精靈的帳戶屬於受防護電腦上的管理員群組。

完成上述操作後，繼續安裝程式。依照安裝精靈的指示，指定安裝 Kaspersky Embedded Systems Security 的安裝設定。可以在安裝精靈的任何一個步驟停止 Kaspersky Embedded Systems Security 安裝過程。若要停止安裝，請在安裝精靈視窗中點擊“取消”按鈕。

您可閱讀更多有關安裝（移除）設定的詳細資訊（請參閱第 [52](#) 頁上的“Windows Installer 服務的安裝和移除設定及命令列選項”部分）。

► 使用安裝精靈安裝 Kaspersky Embedded Systems Security：

1. 在電腦上啟動 setup.exe 檔案。
2. 在開啟的視窗中的“安裝”部分，點擊“**此 EULA 的條款和條件**”連結。
3. 在 Kaspersky Embedded Systems Security 安裝精靈的歡迎頁面，點擊“**下一步>**”按鈕。
將開啟“**EULA 和隱私政策**”視窗。
4. 檢視產品授權協議和隱私政策的條款。
5. 如果您同意最終使用者產品授權協議和隱私政策的條款和條件，請選中“**此 EULA 的條款和條件**”和“**描述資料處理的隱私政策**”核取方塊以繼續安裝。

如果您不接受最終使用者產品授權協議和/或隱私政策，安裝將中止。

6. 點擊“**下一步>**”按鈕。

“在安裝前快速掃描電腦”視窗將開啟。

7. 在“在安裝前快速掃描電腦”中，選中“掃描電腦病毒”核取方塊以掃描系統記憶體和電腦本機磁碟機的引導扇區是否存在威脅。點擊“**下一步>**”按鈕。完成掃描程序時，該精靈會開啟一個結果報告視窗。

此視窗顯示有關已掃描電腦物件有關的資訊，包括：已掃描的物件總數、偵測到的威脅數目、偵測到的已感染和可疑物件數目、Kaspersky Embedded Systems Security 從記憶體中刪除的危險或可疑處理程序數目，以及此應用程式無法刪除的危險和可疑處理程序數目。

若要檢視究竟掃描了哪些物件，請點擊“**已處理物件清單**”按鈕。

8. 點擊“在安裝前快速掃描電腦”視窗中的“**下一步>**”按鈕。

將開啟“**自訂安裝**”視窗。

9. 請選擇您想安裝的元件，

預設情況下，建議安裝集包括除“防火牆管理”元件外的所有 Kaspersky Embedded Systems Security 元件。

只有在電腦安裝了 Microsoft Windows SNMP 服務的情況下，建議的安裝元件清單中才會出現 Kaspersky Embedded Systems Security 的“SNMP 協定支援”元件。

10. 要取消所有變更，請從“自訂安裝”視窗中點擊“**重設**”按鈕。點擊“**下一步>**”按鈕。

11. 在“選擇目的資料夾”視窗中：

- 如果需要，指定 Kaspersky Embedded Systems Security 檔案將複製到的資料夾。
- 如果需要，點擊“**磁碟**”按鈕檢視有關本地磁碟機上可用空間的資訊。

點擊“**下一步>**”按鈕。

12. 在“進階安裝設定”視窗中，配置以下安裝設定：

- 安裝應用程式後啟用即時防護。
- 將 Microsoft 建議的檔案新增到排除清單。
- 將 Kaspersky Lab 建議的檔案新增到排除清單。

點擊“下一步>”按鈕。

13. 在“從設定檔匯入設定”視窗中：

- a. 指定設定檔以從在任何先前相容版本的應用程式中建立的現有設定檔匯入 Kaspersky Embedded Systems Security 設定。
- b. 點擊“下一步>”按鈕。

14. 在“啟動應用程式”視窗中，執行下列操作之一：

- 如果您想要啟動應用程式，請指定 Kaspersky Embedded Systems Security 金鑰檔案以啟動應用程式。
- 如果您想要稍後啟動應用程式，請點擊“下一步>”按鈕。
- 如果金鑰案之前已儲存在分發套件的 \product 資料夾中，該檔案的名稱將顯示在“金鑰”欄位中。

若要使用儲存在其他資料夾的金鑰檔案新增金鑰，請指定金鑰檔案。

新增金鑰檔案後，視窗中將顯示授權資訊。Kaspersky Embedded Systems Security 會顯示計算出的產品授權到期日期。此日期自啟用金鑰開始計算，並於金鑰檔案的“有效期間”到期前結束。

點擊“下一步>”按鈕在應用程式中套用金鑰檔案。

15. 在“已準備安裝”視窗中點擊“安裝”按鈕。精靈將開始安裝 Kaspersky Embedded Systems Security 元件。

16. 完成安裝時，會開啟“安裝完成”視窗。

17. 選中“檢視發佈說明”核取方塊，可於安裝精靈完成安裝時檢視發佈資訊。

18. 點擊“完成”。

安裝精靈關閉。完成安裝後，如果已新增啟動金鑰，即可使用 Kaspersky Embedded Systems Security。

Kaspersky Embedded Systems Security 主控台安裝

依照安裝精靈說明配置應用程式主控台的安裝設定。您可於安裝精靈的任何一個步驟停止安裝程序。若要停止安裝，請在安裝精靈視窗中點擊“取消”按鈕。

► 若要安裝應用程式主控台，請執行以下步驟：

1. 確認用來執行安裝精靈的帳戶屬於電腦上的管理員群組。
2. 在電腦上執行 setup.exe 檔案。
隨即會開啟一個歡迎安裝程式視窗。
3. 點擊“安裝 Kaspersky Embedded Systems Security 主控台”連結。
隨即會開啟“安裝精靈”歡迎視窗。
4. 點擊“下一步>”按鈕。
5. 在開啟的視窗中瀏覽最終使用者產品授權協議的條款，然後選中“我確認我已完全閱讀、理解並接受此最終使用者產品授權協議的條款和條件”核取方塊以繼續安裝。
6. 點擊“下一步>”按鈕。
將開啟“進階安裝設定”視窗。
7. 在“進階安裝設定”視窗中：
 - 如果希望使用應用程式主控台管理遠端電腦上安裝的 Kaspersky Embedded Systems Security，請選中“允許遠端存取”核取方塊。
 - 將開啟“自訂安裝”視窗並選擇元件：
 - a. 點擊“進階”按鈕。
將開啟“自訂安裝”視窗。
 - b. 從清單中選擇“管理工具”元件。
預設情況下，安裝所有元件。

- c. 點擊“**下一步>**”按鈕。

您可以找到有關 Kaspersky Embedded Systems Security 元件的更多詳細資訊(請參閱第 42 頁上的“適用於 Windows Installer 服務的 Kaspersky Embedded Systems Security 軟體元件代碼”部分)。

8. 在“**選擇目的資料夾**”視窗中：
 - a. 如有需要，指定要安裝的檔案應儲存到的其他資料夾。
 - b. 點擊“**下一步>**”按鈕。

9. 在“**已準備安裝**”視窗中點擊“**安裝**”按鈕。

該精靈將開始安裝所選的元件。

10. 點擊“**完成**”。

安裝精靈關閉。將在受防護電腦上安裝應用程式主控台。

如果“管理工具”集已經安裝在網路中的其他電腦上，而不是安裝在受防護電腦上，請調整“進階設定”(請參閱第 65 頁上的“在其他電腦上安裝應用程式主控台以後的進階設定”部分)。

在其他電腦上安裝應用程式主控台以後的進階設定

如果應用程式主控台已經安裝在網路中的其他電腦上，而不是安裝在受防護電腦上，請執行以下操作，以允許使用者遠端管理 Kaspersky Embedded Systems Security：

- 在受防護電腦上將 Kaspersky Embedded Systems Security 使用者新增到 ESS 管理員群組中。
- 如果受防護電腦使用 Windows 防火牆或協力廠商防火牆，則允許 Kaspersky Security 管理服務 (kavfsgt.exe) 進行網路連線(請參見第 286 頁上的“關於 Kaspersky Security 管理服務的存取權限”部分)。
- 如果在執行 Microsoft Windows 的電腦上安裝應用程式主控台期間未選中“**允許遠端存取**”核取方塊，則透過電腦的防火牆手動允許應用程式主控台的網路連線。

遠端電腦上的應用程式主控台將使用 DCOM 協議從受防護電腦上的 Kaspersky Security 管理服務接收關於 Kaspersky Embedded Systems Security 事件的資訊 (如物件掃描、工作完成等)。需要在“Windows 防火牆設定”中允許應用程式主控台的網路連線，才能在應用程式主控台和 Kaspersky Security 管理服務之間建立連線。

在安裝了應用程式主控台的遠端電腦上，執行以下操作：

- 確保允許遠端匿名存取 COM 應用程式 (但不是遠端啟動和啟動 COM 應用程式)。
- 在 Windows 防火牆中開放 TCP 連接埠 135 並允許 Kaspersky Embedded Systems Security 遠端管理處理程序的可執行檔 kavfsrcn.exe 的網路連線。

安裝應用程式主控台的用戶端電腦將使用連接埠 TCP 135 存取受防護電腦並接收電腦回應。

- 設定 Windows 防火牆的輸出規則以允許連線。

與單個協定具有固定連接埠的傳統 TCP/IP 和 UDP/IP 服務不同，DCOM 會為遠端 COM 物件動態分配連接埠。如果用戶端 (其中安裝了應用程式主控台) 與 DCOM 端點 (受防護電腦) 之間存在防火牆，則必須開放很大範圍的連接埠。

設定任何其他軟體或硬體防火牆應該套用相同步驟。

► 如果在配置受防護電腦與安裝了應用程式主控台的電腦之間的連線時，應用程式主控台處於開啟狀態：

1. 關閉應用程式主控台。
2. 等待至 Kaspersky Embedded Systems Security 遠端管理處理程序 kavfsrcn.exe 結束。
3. 重新啟動應用程式主控台。

將套用新的連線設定。

本章節說明項目

允許匿名遠端存取 COM 應用程式.....	67
允許 Kaspersky Embedded Systems Security 遠端管理處理程序的網路連線.....	67
新增 Windows 防火牆的輸出規則.....	69

允許匿名遠端存取 COM 應用程式

設定的名稱可能有所不同，具體取決於安裝的 Windows 作業系統。

► 為了允許匿名遠端存取 COM 應用程式，請執行以下步驟：

1. 在安裝了 Kaspersky Embedded Systems Security 主控台的遠端電腦上，開啟元件服務主控台。
2. 選擇“開始 → 執行”。
3. 輸入指令 dcomcnfg。
4. 點擊“確定”。
5. 展開電腦上元件服務主控台中的“電腦”節點。
6. 開啟“我的電腦”節點的內容功能表。
7. 選擇“內容”。
8. 在“內容”視窗的“COM 安全”標籤上，點擊“存取權限”設定群組中的“編輯限制”按鈕。
9. 請確認在“允許遠端存取”視窗中為“匿名登入”使用者選定“允許遠端存取”的核取方塊。
10. 點擊“確定”。

允許 Kaspersky Embedded Systems Security 遠端管理處理程序的網路連線

設定的名稱可能有所不同，具體取決於安裝的 Windows 作業系統。

► 要在 Windows 防火牆中開放 TCP 連接埠 135 並允許 Kaspersky Embedded Systems Security 遠端管理處理程序的網路連線，請執行以下步驟：

1. 關閉遠端電腦上的 Kaspersky Embedded Systems Security 主控台。
2. 執行以下步驟之一：
 - 在 Microsoft Windows XP SP2 或更高版本中：
 - a. 選擇“開始 > Windows 防火牆”。
 - b. 在“Windows 防火牆”視窗 (或“Windows 防火牆設定”) 中點擊“排除”選項上的“新增連接埠”按鈕。
 - c. 在“名稱”欄位中指定連接埠名稱 RPC (TCP/135) 或輸入其他名稱，例如“Kaspersky Embedded Systems Security DCOM”，並在“連接埠名稱”欄位中指定埠號 (135)。
 - d. 選擇“TCP”協定。
 - e. 點擊“確定”。
 - f. 點擊“排除”標籤上的“新增”按鈕。
 - 在 Microsoft Windows 7 或更高版本中：
 - a. 選擇“開始 > 控制台 > Windows 防火牆”。
 - b. 在“Windows 防火牆”視窗中，選擇“允許程式或功能透過 Windows 防火牆”。
 - c. 在“允許程式透過 Windows 防火牆通訊”視窗中點擊“允許其他程式...”按鈕。
3. 在“新增程式”視窗中指定 kavfsrnc.exe 檔案。在使用 MMC 安裝 Kaspersky Embedded Systems Security 的過程中，該檔案位於指定為目的資料夾的資料夾中。
4. 點擊“確定”。
5. 在“Windows 防火牆 (Windows 防火牆設定) ”視窗中，點擊“確定”按鈕。

新增 Windows 防火牆的輸出規則

設定的名稱可能有所不同，具體取決於安裝的 Windows 作業系統。

► 要新增 Windows 防火牆的輸出規則，請執行以下步驟：

1. 選擇“開始 > 控制台 > Windows 防火牆”。
2. 在“Windows 防火牆”視窗中，點擊“進階設定”連結。
將開啟“進階安全 Windows 防火牆”視窗。
3. 選擇“輸出規則”子節點。
4. 在“操作”窗格中點擊“新建規則”選項。
5. 在開啟的“新建輸出規則精靈”視窗中，選擇“連接埠”選項，然後點擊“下一步”。
6. 選擇“TCP”協定。
7. 在“特定遠端連接埠”欄位中，指定以下允許傳出連線的連接埠範圍：1024-65535。
8. 在“操作”視窗中，選擇“允許連線”選項。
9. 儲存新規則，然後關閉“進階安全 Windows 防火牆”視窗。

Windows 防火牆現在將允許應用程式主控台與 Kaspersky Security 管理服務之間進行網路連線。

在安裝 Kaspersky Embedded Systems Security 後執行的操作

如果您已啟動 Kaspersky Embedded Systems Security，該應用程式在安裝後立即啟動防護和掃描工作。

如果在安裝 Kaspersky Embedded Systems Security 期間選中“安裝應用程式後啟用即時防護”(預設選項)，當電腦的檔案系統物件被存取時，應用程式會掃描這些物件。Kaspersky Embedded Systems Security 將在每週五的 20:00 執行“關鍵區域掃描”工作。

建議在安裝 Kaspersky Embedded Systems Security 後執行下列步驟：

- 啟動應用程式資料庫更新工作。安裝後 Kaspersky Embedded Systems Security 將使用應用程式發行套件中的資料庫掃描物件。

我們建議立即更新 Kaspersky Embedded Systems Security 資料庫，因為它們可能已過期。

之後，應用程式將根據預設排程每小時更新一次資料庫。

- 如果安裝 Kaspersky Embedded Systems Security 之前受防護電腦上未安裝任何具有即時檔案防護的病毒防護軟體，請在電腦上執行“關鍵區域掃描”。
- 配置有關 Kaspersky Embedded Systems Security 事件的管理員通知。

本章節說明項目

啟動和配置 Kaspersky Embedded Systems Security 資料庫更新工作.....	70
關鍵區域掃描.....	73

啟動和配置 Kaspersky Embedded Systems Security 資料庫更新工作

► 要在安裝後更新應用程式資料庫，請執行以下操作：

1. 在“資料庫更新”工作設定中，配置與更新來源的連線 – Kaspersky Lab HTTP 或 FTP 更新伺服器。
2. 啟動“資料庫更新”工作。

您的網路中可能未配置 Web 代理自動發現協議 (WPAD) 以在 LAN 中自動偵測代理伺服器設定。而且，在存取代理伺服器時，您的網路可能需要身分驗證。

► 要為存取代理伺服器指定可選的代理伺服器設定和身分驗證設定，請執行以下操作：

1. 開啟“Kaspersky Embedded Systems Security”節點的上下文功能表。
2. 選擇“內容”項。

將開啟“應用程式設定”視窗。
3. 選擇“連線設定”標籤。
4. 在“代理伺服器設定”部分中，選中“使用自訂代理伺服器設定”核取方塊。
5. 在“位址”欄位中輸入代理伺服器位址，在“埠號”欄位中輸入代理伺服器的埠號。
6. 在“代理伺服器身分驗證設定”部分的下拉清單中選擇必要的身分驗證方法：
 - 如果代理伺服器支援內建 Microsoft Windows NTLM 驗證方式，請使用 **NTLM 身分驗證** 方式。Kaspersky Embedded Systems Security 將使用工作設定中指定的使用者帳戶存取代理伺服器（預設情況下，該工作會在本機系統（**SYSTEM**）使用者帳戶下執行）。
 - 如果代理伺服器支援內建 Microsoft Windows NTLM 驗證方式，請使用帶使用者名稱和密碼的 **NTLM 身分驗證** 方式。Kaspersky Embedded Systems Security 將使用您指定的帳戶來存取代理伺服器。輸入使用者名稱與密碼，或從清單選擇一個使用者。
 - **套用使用者名稱和密碼**，以選擇基本身分驗證。輸入使用者名稱與密碼，或從清單選擇一個使用者。
7. 在“應用程式設定”視窗中點擊“確定”。

► 要設定與 Kaspersky Lab 的更新伺服器的連線，在“資料庫更新”工作中：

1. 透過以下方式之一啟動應用程式主控台：
 - 在受防護電腦上開啟應用程式主控台。要執行此操作，請選取“開始 > 所有程式 > Kaspersky Embedded Systems Security > 管理工具 > Kaspersky Embedded Systems Security 2.3 主控台”。

- 如果應用程式主控台已在不受防護的電腦上啟動，請連線到受防護的電腦：
 - a. 在應用程式主控台樹狀目錄中開啟“Kaspersky Embedded Systems Security”節點的內容功能表。
 - b. 選擇“連線至其他電腦”項。
 - c. 在“選擇電腦”視窗中，選擇“其他電腦”，然後在文字欄位中，指定受防護電腦的網路名稱。

如果用於登入到 Microsoft Windows 的帳戶沒有 Kaspersky Security 管理服務的存取權限（請參見第 286 頁上的“關於 Kaspersky Security 管理服務的存取權限”部分），請指定具有所需權限的帳戶。

將開啟應用程式主控台視窗。

2. 在應用程式主控台樹狀目錄中，展開“更新”節點。
3. 選擇“資料庫更新”子節點。
4. 在詳細資訊視窗中點擊“內容”連結。
5. 在開啟的“工作設定”視窗中，開啟“連線設定”標籤。
6. 選中“使用指定的代理伺服器設定以連線至 Kaspersky Lab 更新伺服器”。
7. 在“工作設定”視窗中點擊“確定”。

將儲存“資料庫更新”工作中連線更新來源的設定。

► 要執行“資料庫更新”工作，請執行以下操作：

1. 在應用程式主控台樹狀目錄中，展開“更新”節點。
2. 在“資料庫更新”子節點的內容功能表中，選擇“啟動”項。

“資料庫更新”工作啟動。

工作成功完成後，您可以在 **Kaspersky Embedded Systems Security** 節點的詳細資訊視窗中檢視安裝的最新資料庫更新的發佈日期。

關鍵區域掃描

更新 Kaspersky Embedded Systems Security 資料庫後，使用“掃描關鍵區域”工作掃描電腦是否有惡意軟體。

▶ 若要執行“關鍵區域掃描”工作，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中展開“自訂掃描”節點。
2. 在“關鍵區域掃描”子節點的內容功能表中，選擇“啟動”指令。

工作啟動；詳細資訊窗格中顯示工作狀態“正在執行”。

▶ 要檢視工作記錄，請執行下列操作：

在“關鍵區域掃描”節點的詳細資訊視窗中，點擊“開啟工作記錄”連結。

修改元件集和修復 Kaspersky Embedded Systems Security

可以新增或移除 Kaspersky Embedded Systems Security 元件。您需要先停止“即時檔案防護”工作，才能刪除“即時檔案防護”元件。其他情況下，將不需停止即時檔案防護工作或 Kaspersky Security 服務。

如果應用程式管理受密碼防護，Kaspersky Embedded Systems Security 會在您在安裝精靈中嘗試移除元件或修改元件集時請求密碼。

▶ 要修改 Kaspersky Embedded Systems Security 元件集：

1. 在“開始”功能表中，選擇“所有程式”>“Kaspersky Embedded Systems Security”>“修改或移除 Kaspersky Embedded Systems Security”。

將開啟安裝精靈的“修改、修復或移除安裝”視窗。

2. 選擇“修改元件集”。點擊“下一步>”按鈕。

將開啟“自訂安裝”視窗。

3. 在“**自訂安裝**”視窗的可用元件清單中，選擇要從 Kaspersky Embedded Systems Security 新增或移除的元件。為此，請執行以下操作：

- 要變更元件集，請點擊所選元件名稱旁邊的按鈕。然後在右鍵選單中選取：
 - “**元件將被安裝在本機硬碟上**”（如果您想要安裝一個元件）；
 - “**程式將在本機磁碟上安裝元件及其子元件**”（如果您想要安裝一組元件）。
- 要移除先前安裝的元件，請點擊所選元件名稱旁邊的按鈕。然後在上下文功能表中選擇“**元件將變為不可用**”。

點擊“**下一步>**”按鈕。

4. 在“**已準備安裝**”視窗中，透過點擊“**安裝**”按鈕確認軟體元件集的變更。

5. 在安裝完成後開啟的視窗中，點擊“**確定**”按鈕。

將根據指定設定修改 Kaspersky Embedded Systems Security 元件集。

如果 Kaspersky Embedded Systems Security 於運作時發生問題（Kaspersky Embedded Systems Security 當機；工作損毀或無法啟動），您可嘗試修復 Kaspersky Embedded Systems Security。您可在儲存 Kaspersky Embedded Systems Security 的目前設定時執行修復，或選擇一個選項以將所有 Kaspersky Embedded Systems Security 設定重設為預設值。

► 要在應用程式或工作崩潰後修復 Kaspersky Embedded Systems Security，請執行以下步驟：

1. 在“**開始**”功能表中，選擇“**所有程式**”。
2. 選擇“**Kaspersky Embedded Systems Security**”。
3. 選擇“**修改或移除 Kaspersky Embedded Systems Security**”。

將開啟安裝精靈的“**修改、修復或移除安裝**”視窗。

4. 選擇“**修復已安裝元件**”。點擊“**下一步>**”按鈕。

這會開啟“**修復已安裝元件**”視窗。

5. 在“**修復已安裝元件**”視窗中，如果您希望重設應用程式設定並使用其預設設定還原 Kaspersky Embedded Systems Security，則選中“**還原建議的應用程式設定**”核取方塊。點擊“**下一步>**”按鈕。

6. 在“準備進行修復”視窗中，透過點擊“安裝”按鈕確認修復操作。

7. 在修復操作完成後開啟的視窗中，點擊“確定”按鈕。

將使用指定設定修復 Kaspersky Embedded Systems Security。

使用安裝精靈移除

本節包含有關使用安裝/移除精靈從受防護電腦上移除 Kaspersky Embedded Systems Security 和應用程式主控台的說明。

本章節說明項目

Kaspersky Embedded Systems Security 移除.....	75
Kaspersky Embedded Systems Security 主控台移除.....	76

Kaspersky Embedded Systems Security 移除

在不同 Windows 作業系統中，設定的名稱可能會有所不同。

可以使用安裝/移除精靈從受防護電腦移除 Kaspersky Embedded Systems Security。

從受防護電腦移除 Kaspersky Embedded Systems Security 後，可能需要重新啟動電腦。重新啟動可以推遲。

如果作業系統使用 UAC 功能（使用者帳戶控制）或對應用程式的存取受密碼防護，則不能透過 Windows 主控台移除、修復和安裝應用程式。

如果應用程式管理受密碼防護，Kaspersky Embedded Systems Security 會在您在安裝精靈中嘗試移除元件或修改元件集時請求密碼。

► **要移除 Kaspersky Embedded Systems Security :**

1. 在“**開始**”功能表中，選擇“**所有程式**”。
2. 選擇“**Kaspersky Embedded Systems Security**”。
3. 選擇“**修改或移除 Kaspersky Embedded Systems Security**”。

將開啟安裝精靈的“**修改、修復或移除安裝**”視窗。

4. 選擇“**移除軟體元件**”。點擊“**下一步>**”按鈕。

將開啟“**進階應用程式移除設定**”視窗。

5. 如有必要，在“**進階應用程式移除設定**”視窗中：

- a. 選中“**匯出隔離區物件**”核取方塊以使 Kaspersky Embedded Systems Security 匯出已隔離的物件。預設取消選定該核取方塊。
- b. 選中“**匯出備份區物件**”核取方塊，以從 Kaspersky Embedded Systems Security 備份區匯出物件。預設取消選定該核取方塊。
- c. 點擊“**儲存到**”按鈕並選擇您希望將物件匯出到的資料夾。預設情況下，會將物件匯出到 %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall。
點擊“**下一步>**”按鈕。

6. 在“**已準備移除**”視窗中，透過點選“**移除**”按鈕確認移除。

7. 在移除完成後開啟的視窗中，點擊“**確定**”按鈕。

Kaspersky Embedded Systems Security 將從受防護電腦移除。

Kaspersky Embedded Systems Security 主控台移除

在不同 Windows 作業系統中，設定的名稱可能會有所不同。

您可以使用安裝/移除精靈，從電腦移除應用程式主控台。

移除應用程式主控台後，無需重新啟動電腦。

► 要移除應用程式主控台，請執行下列步驟：

1. 在“開始”功能表中，選擇“所有程式”。
2. 選擇“Kaspersky Embedded Systems Security”。
3. 選擇“修改或移除 Kaspersky Embedded Systems Security 2.3 管理工具”。

將開啟精靈的“修改、修復或移除安裝”視窗。

4. 選擇“移除軟體元件”並點擊“下一步>”按鈕。
5. 將開啟“已準備移除”視窗。點擊“移除”按鈕。

將開啟“移除完成”視窗。

6. 點擊“確定”。

此時，移除完成，且安裝精靈關閉。

透過命令列安裝或移除應用程式

本章節介紹從命令列安裝和移除 Kaspersky Embedded Systems Security 的詳細資訊，包含從命令列安裝和移除 Kaspersky Embedded Systems Security 的指令範例，以及從命令列新增和移除 Kaspersky Embedded Systems Security 元件的指令範例。

本章節說明項目

關於從命令列安裝和移除 Kaspersky Embedded Systems Security	78
安裝 Kaspersky Embedded Systems Security 的指令範例	78
在安裝 Kaspersky Embedded Systems Security 後執行的操作	80
新增/移除元件指令範例	81
Kaspersky Embedded Systems Security 移除。指令範例	82
回傳代碼	83

關於從命令列安裝和移除 Kaspersky Embedded Systems Security

在使用金鑰指定安裝設定後，可透過命令列執行 `\product\ess_x86(x64).msi` 安裝套件檔案，來安裝或移除 Kaspersky Embedded Systems Security，以及新增或移除其元件。

您可在受防護電腦或網路的另一台電腦上安裝“管理工具”集，以本機或遠端方式和應用程式主控台搭配使用。要執行此操作，請使用 `\console\esstools.msi` 安裝套件。

在安裝了該應用程式的電腦上，使用包含在管理員群組中的帳戶執行安裝。

如果在沒有備用金鑰的受防護電腦上執行 `\product\ess_x86.msi` 或 `\product\ess_x64.msi` 檔案中的一個，將使用建議的安裝設定安裝 Kaspersky Embedded Systems Security。

您可使用 `ADDLOCAL` 命令列選項，透過列出所選的元件或元件集的代碼，來指定要安裝的元件集。

安裝 Kaspersky Embedded Systems Security 的指令範例

本章節提供安裝 Kaspersky Embedded Systems Security 所使用的指令範例。

在執行 32 位元版本的 Microsoft Windows 的電腦上，執行分發套件中帶有 x86 尾碼的檔案。在執行 64 位元版本的 Microsoft Windows 的電腦上，執行分發套件中帶有 x64 尾碼的檔案。

有關使用 Windows Installer 標準指令和命令列選項的詳細資訊，提供在 Microsoft 提供的文件中。

從 `setup.exe` 檔案安裝 Kaspersky Embedded Systems Security 的範例

- ▶ 若不想以使用者互動模式安裝 Kaspersky Embedded Systems Security，而想以預設的安裝設定來安裝，請執行以下指令：

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

可以使用以下設定安裝 Kaspersky Embedded Systems Security：

- 僅安裝“即時檔案防護”和“自訂掃描”元件；

- 在啟動 Kaspersky Embedded Systems Security 時不執行即時檔案防護；
- 不排除 Microsoft Corporation 建議從掃描範圍中排除的檔案；

要執行此操作，請執行以下指令：

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

用於安裝的指令範例：執行 .msi 檔案

- ▶ 若不想以使用者互動模式安裝 Kaspersky Embedded Systems Security，而想以預設的安裝設定來安裝，請執行以下指令：

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

- ▶ 若要以預設安裝設定安裝 Kaspersky Embedded Systems Security 並顯示安裝介面，請執行以下指令：

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

- ▶ 若要以 C:\0000000A.key 的金鑰檔案安裝 Kaspersky Embedded Systems Security：

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

- ▶ 若要安裝 Kaspersky Embedded Systems Security 並初步掃描啟動的處理程序與本機磁碟機的開機磁區，請執行以下指令：

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

- ▶ 要將 Kaspersky Embedded Systems Security 安裝在安裝資料夾 C:\ESS 中，請執行以下指令：

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

- ▶ 若要安裝 Kaspersky Embedded Systems Security 並將名稱為 ess.log 的安裝記錄檔案儲存在儲存 Kaspersky Embedded Systems Security msi 檔案的資料夾中，請執行以下指令：

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

- ▶ 若要安裝 Kaspersky Embedded Systems Security 主控台，請執行以下指令：

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

- ▶ 若要使用 C:\0000000A.key 檔案的金鑰安裝 Kaspersky Embedded Systems Security，並根據 C:\settings.xml 設定檔中的設定配置 Kaspersky Embedded Systems Security，請執行以下指令：

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

- ▶ 若要在 Kaspersky Embedded Systems Security 受密碼防護的情況下安裝應用程式修補程式，請執行以下指令：

```
msiexec /p "<msp 檔案名及路徑>" UNLOCK_PASSWORD=<密碼>
```

在安裝 Kaspersky Embedded Systems Security 後執行的操作

如果您已啟動 Kaspersky Embedded Systems Security，該應用程式在安裝後立即啟動防護和掃描工作。

如果在安裝 Kaspersky Embedded Systems Security 期間選中“安裝應用程式後啟用即時防護”，當電腦的檔案系統物件被存取時，應用程式會掃描這些物件。Kaspersky Embedded Systems Security 將在每週五晚上 8 點鐘執行“關鍵區域掃描”工作。

建議在安裝 Kaspersky Embedded Systems Security 後執行下列步驟：

- 啟動 Kaspersky Embedded Systems Security 資料庫更新工作。安裝後，Kaspersky Embedded Systems Security 會使用其分發套件中的資料庫掃描物件。我們建議立即更新 Kaspersky Embedded Systems Security 資料庫。若要進行更新，您必須執行“資料庫更新”工作。之後，資料庫將根據預設排程，每小時更新一次。

例如，您可執行以下指令來啟動“資料庫更新”工作：

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

在此情況下，將從 Kaspersky Lab 更新伺服器下載 Kaspersky Embedded Systems Security 資料庫。透過代理伺服器（代理伺服器位址：proxy.company.com，連接埠：8080）與更新來源建立連線，使用內置 Windows NTLM 身分驗證存取伺服器（登入帳戶的使用者名稱：inetuser；密碼：123456）。

- 如果安裝 Kaspersky Embedded Systems Security 之前受防護電腦上未安裝任何具有即時檔案防護的病毒防護軟體，請對電腦執行“關鍵區域掃描”。

▶ 若要使用命令列啟動“關鍵區域掃描”工作：

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

此指令會將工作記錄儲存在目前資料夾內名為 scancritical.log 檔案中。

- 配置有關 Kaspersky Embedded Systems Security 事件的管理員通知。

新增/移除元件。指令範例

“自訂掃描”元件將自動安裝。您不必透過新增或移除 Kaspersky Embedded Systems Security 元件，在 ADDLOCAL 指令設定值清單中指定此元件。

▶ 要將“應用程式啟動控制”元件新增到已安裝的元件，請執行以下指令：

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

或

```
\product\setup.exe /s /p "ADDLOCAL=Oas,AppCtrl"
```

如果將要安裝的元件與已安裝的元件列在一起，則 Kaspersky Embedded Systems Security 將重新安裝現有的元件。

- ▶ 要刪除已安裝的元件，請執行以下指令：

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

Kaspersky Embedded Systems Security 移除。指令範例

- ▶ 要從受防護電腦移除 Kaspersky Embedded Systems Security，請執行以下指令：

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

或

- 對於 32 位元作業系統：

```
msiexec /x {51AACF7F-421E-40FA-B2B7-FCFE0BACF505} /qn
```

- 對於 64 位元作業系統：

```
msiexec /x {673F3697-9D6C-4CF4-BB28-478492F45DDC} /qn
```

- ▶ 要移除 Kaspersky Embedded Systems Security 主控台，請執行以下指令：

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

或

- 對於 32 位元作業系統：

```
msiexec /x {26E7C356-E535-4434-9AB1-F1EA4E8A70F4} /qn
```

- 對於 64 位元作業系統：

```
msiexec /x {7EC1A40D-52F4-4F8F-93BA-F6E68B152C26} /qn
```

► 要從已啟用密碼防護的受防護電腦上移除 Kaspersky Embedded Systems Security，請執行以下指令：

- 對於 32 位元作業系統：

```
msiexec /x {51AACF7F-421E-40FA-B2B7-FCFE0BACF505} UNLOCK_PASSWORD=*** /qn
```

- 對於 64 位元作業系統：

```
msiexec /x {673F3697-9D6C-4CF4-BB28-478492F45DDC} UNLOCK_PASSWORD=*** /qn
```

回傳代碼

下表包含了命令列的回傳代碼清單。

表 6. 回傳代碼

代碼	敘述
1324	目的資料夾名稱包含無效的字元。
25001	沒有足夠權限安裝 Kaspersky Embedded Systems Security。要安裝該應用程式，請使用本機管理員權限啟動安裝精靈。
25003	Kaspersky Embedded Systems Security 不能安裝在執行此版本的 Microsoft Windows 的電腦上。請啟動用於 64 位元版本 Microsoft Windows 的安裝精靈。
25004	偵測到不相容的軟體。要繼續安裝，請移除以下軟體：<不相容的軟體清單>。
25010	指定的路徑不能用於儲存已隔離的物件。
25011	用於儲存已隔離的物件的資料夾名包含無效的字元。
26251	無法下載效能計數器 DLL。

代碼	敘述
26252	無法下載效能計數器 DLL。
27300	不能安裝驅動程式。
27301	不能移除驅動程式。
27302	不能安裝網路元件。已達到所支援的篩選裝置的最大數量。
27303	無法找到病毒特徵碼資料庫。

使用卡斯基安全管理中心安裝和移除應用程式

本章節包含有關透過卡斯基安全管理中心安裝 Kaspersky Embedded Systems Security 的一般資訊。同時也介紹如何透過卡斯基安全管理中心安裝和移除 Kaspersky Embedded Systems Security 以及安裝 Kaspersky Embedded Systems Security 後執行的操作。

本章節說明項目

有關透過卡斯基安全管理中心安裝的一般資訊	85
安裝或移除 Kaspersky Embedded Systems Security 的權限.....	85
透過卡斯基安全管理中心安裝 Kaspersky Embedded Systems Security	86
在安裝 Kaspersky Embedded Systems Security 後執行的操作	88
透過卡斯基安全管理中心安裝應用程式主控台	88
透過卡斯基安全管理中心移除 Kaspersky Embedded Systems Security	89

透過卡巴斯基安全管理中心安裝的一般資訊

您可以透過卡巴斯基安全管理中心，使用遠端安裝工作來安裝 Kaspersky Embedded Systems Security。

完成遠端安裝工作後，將可在多台電腦上使用相同的設定安裝 Kaspersky Embedded Systems Security。

所有電腦可以整合到一個管理群組中，並且可以建立群組工作來在該群組的電腦上安裝 Kaspersky Embedded Systems Security。

您可以建立一個工作，在不屬於相同管理群組的一組電腦上遠端安裝 Kaspersky Embedded Systems Security。建立此工作時，您必須建立一份要安裝 Kaspersky Embedded Systems Security 的各個電腦的清單。

有關遠端安裝工作的詳細資訊，請參閱 [卡巴斯基安全管理中心說明](#)。

安裝或移除 Kaspersky Embedded Systems Security 的權限

遠端安裝（移除）工作中所指定的帳戶必須加入每一台受管理電腦的管理員群組中，但以下情況除外：

- 如果卡巴斯基安全管理中心網路代理已安裝在要安裝 Kaspersky Embedded Systems Security 的電腦上（不論這些電腦位於哪個網域，或它們是否屬於任何網域）。

如果電腦上尚未安裝網路代理，您可使用遠端安裝工作安裝網路代理程式與 Kaspersky Embedded Systems Security。安裝網路代理程式前，請確保要在該工作中指定的帳戶包含在每台電腦的管理員群組中。

- 要安裝 Kaspersky Embedded Systems Security 的電腦都在相同網域中作為管理伺服器使用，且管理伺服器以“網域管理員”帳戶身分註冊（如果此帳戶在該網域電腦上有本機管理員權限）。

預設情況下，使用“遠端安裝”方式進行安裝時，遠端安裝工作會在執行管理伺服器下的帳戶執行。

以強制安裝（移除）模式執行群組工作或整組電腦的工作時，用戶端電腦上的帳戶必須有下列權限：

- 遠端執行應用程式的權限。
- Admin\$ 共用的權限。

- 作為服務登入的權限。

透過卡斯基安全管理中心安裝 Kaspersky Embedded Systems Security

如需更多有關建立安裝套件和遠端安裝工作的資訊，請參閱《卡斯基安全管理中心實施手冊》。

如果希望以後透過卡斯基安全管理中心管理 Kaspersky Embedded Systems Security，請確保符合以下條件：

- 安裝了卡斯基安全管理中心管理電腦的電腦上還安裝了管理外掛程式（Kaspersky Embedded Systems Security 分發套件中的 \product\klcfginst.exe 檔案）。
- 請在受防護電腦上安裝卡斯基安全管理中心網路代理。如果卡斯基安全管理中心網路代理未安裝在受防護電腦上，可以使用遠端安裝工作同時安裝它與 Kaspersky Embedded Systems Security。

也可以將多台電腦整合在同一個管理群組中，以便之後使用卡斯基安全管理中心政策和群組工作管理防護設定。

► 要使用遠端安裝工作安裝 Kaspersky Embedded Systems Security：

1. 啟動卡斯基安全管理中心管理主控台。
2. 在卡斯基安全管理中心中，展開“進階”節點。
3. 展開“遠端安裝”子節點。
4. 在“安裝套件”子節點的詳細資訊窗格中，點擊“建立安裝套件”按鈕。
5. 選擇“建立 Kaspersky Lab 應用程式的安裝套件”安裝套件類型。
6. 輸入安裝套件名稱。
7. 指定 Kaspersky Embedded Systems Security 分發套件中的 ess.kud 檔案為安裝套件檔案。
將開啟“最終使用者產品授權協議和隱私政策”視窗。
8. 如果您同意最終使用者產品授權協議和隱私政策的條款和條件，請選中“此最終使用者產品授權協議的條款和條件”和“描述資料處理的隱私政策”核取方塊以繼續安裝。

您必須接受產品授權協議和隱私政策才能繼續。

9. 要變更要安裝的 Kaspersky Embedded Systems Security 元件集 (請參見第 73 頁上的“修改元件集和修復 Kaspersky Embedded Systems Security”部分) 以及安裝套件中的預設安裝設定 (請參見第 52 頁上的“Windows Installer 服務的安裝和移除設定及命令列選項”部分)：
 - a. 在卡巴斯基安全管理中心中，展開“遠端安裝”節點。
 - b. 在“安裝套件”子節點的詳細資訊窗格中，開啟已建立 Kaspersky Embedded Systems Security 安裝套件的內容功能表，然後選擇“內容”。
 - c. 在“設定”部分的“內容: <安裝套件名稱>”視窗中，執行以下操作：
 - a. 在“要安裝的元件”設定群組中，選中要安裝的 Kaspersky Embedded Systems Security 元件名稱旁邊的核取方塊。
 - b. 要指定預設資料夾以外的目的資料夾，請在“目的資料夾”欄位指定資料夾名稱和路徑。
目的資料夾的路徑可能包含系統環境變數。電腦上若沒有您指定的資料夾，就會建立資料夾。
 - c. 在“進階安裝設定”群組中，配置以下設定：
 - 在安裝之前對電腦進行病毒掃描。
 - 安裝應用程式後啟用即時防護。
 - 將 Microsoft 建議的檔案新增到排除清單。
 - d. 將 Kaspersky Lab 建議的檔案新增到排除清單。
 - d. 在“內容: <安裝套件名稱>”視窗，點擊“確定”。
10. 在“安裝套件”節點中，建立一個工作，於選定電腦 (管理群組) 上遠端安裝 Kaspersky Embedded Systems Security。配置工作設定。

要瞭解建立和配置遠端安裝工作的詳細資訊，請參見 *卡巴斯基安全管理中心說明*。
11. 執行 Kaspersky Embedded Systems Security 遠端安裝工作。

Kaspersky Embedded Systems Security 將安裝於在工作中指定的電腦上。

在安裝 Kaspersky Embedded Systems Security 後執行的操作

安裝 Kaspersky Embedded Systems Security 後，建議更新電腦上的 Kaspersky Embedded Systems Security 資料庫；若安裝 Kaspersky Embedded Systems Security 前，電腦上未安裝任何防毒應用程式並啟用即時防護功能，則還建議掃描電腦的關鍵區域。

如果安裝了 Kaspersky Embedded Systems Security 的電腦在卡巴斯基安全管理中心中屬於同一個管理群組，您可以使用以下方法執行這些工作：

1. 為安裝了 Kaspersky Embedded Systems Security 的電腦群組建立“資料庫更新”工作。將卡巴斯基安全管理中心管理伺服器設定為更新來源。
2. 依需要使用“關鍵區域掃描”狀態建立“自訂掃描”群組工作。卡巴斯基安全管理中心根據此工作的結果（而不是根據關鍵區域掃描工作的結果）評估群組中每台電腦的安全狀態。
3. 替一組電腦建立新的政策。在政策內容的“應用程式設定”部分中，停用系統自訂掃描工作的排程啟動，並在“執行系統工作”子部分的設定中停用對管理群組電腦的資料庫更新工作。

您還可以配置有關 Kaspersky Embedded Systems Security 事件的管理員通知。

透過卡巴斯基安全管理中心安裝應用程式主控台

如需更多有關建立套件和遠端安裝工作的資訊，請參閱《卡巴斯基安全管理中心實施手冊》。

► 要使用遠端安裝工作安裝應用程式主控台，請執行下列操作：

1. 在卡巴斯基安全管理中心管理主控台中，展開“進階”節點。
2. 展開“遠端安裝”子節點。
3. 在“安裝套件”子節點的詳細資訊窗格中，點擊“建立安裝套件”按鈕。建立新的安裝套件時：
 - a. 在“新建安裝套件精靈”視窗中，選擇“建立指定可執行檔的安裝套件”作為安裝套件類型。
 - b. 輸入新安裝套件名稱。
 - c. 選擇 Kaspersky Embedded Systems Security 分發套件資料夾中的 `\console\setup.exe` 檔案，然後選中“將整個資料夾複製到安裝套件”核取方塊。

- d. 如有需要，可以使用 ADDLOCAL 命令列選項來修改要在“可執行檔啟用設定”（可選）欄位中安裝的元件集，並修改目的資料夾。

例如，若要在 C:\KasperskyConsole 資料夾中安裝應用程式主控台但不安裝說明檔案和文件，請使用以下命令列選項：

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

4. 在“安裝套件”子節點中，建立一個工作，於選定電腦（管理群組）上遠端安裝應用程式主控台。配置工作設定。

要瞭解建立和配置遠端安裝工作的詳細資訊，請參見卡巴斯基安全管理中心說明。

5. 執行遠端安裝工作。

應用程式主控台安裝到此工作指定的電腦上。

透過卡巴斯基安全管理中心移除 Kaspersky Embedded Systems Security

如果網路電腦上的 Kaspersky Embedded Systems Security 管理受密碼防護，在建立用於移除多個應用程式的工作時請輸入密碼。如果未透過卡巴斯基安全管理中心政策集中管理密碼防護，Kaspersky Embedded Systems Security 將從受防護電腦成功移除，在該電腦上輸入的密碼與設定值比對。不會從其他電腦移除 Kaspersky Embedded Systems Security。

► 要移除 Kaspersky Embedded Systems Security，請在卡巴斯基安全管理中心管理主控台中執行下列步驟：

1. 在卡巴斯基安全管理中心管理主控台中，建立並啟動應用程式刪除工作。
2. 在該工作中，選擇移除方法（與選擇安裝方法類似，請參見上一節）並指定管理電腦將用來存取電腦的帳戶。您可以僅使用預設移除設定移除 Kaspersky Embedded Systems Security（請參閱第 52 頁上的“Windows Installer 服務的安裝和移除設定及命令列選項”部分）。

透過 Active Directory® 群組政策進行安裝和解除安裝

本章節介紹透過 Active Directory 群組政策安裝和移除 Kaspersky Embedded Systems Security。同時也包含有關透過群組政策安裝 Kaspersky Embedded Systems Security 後執行的操作的資訊。

本章節說明項目

透過 Active Directory 群組政策安裝 Kaspersky Embedded Systems Security	90
在安裝 Kaspersky Embedded Systems Security 後執行的操作	91
透過 Active Directory 群組政策移除 Kaspersky Embedded Systems Security	92

透過 Active Directory 群組政策安裝 Kaspersky Embedded Systems Security

您可以透過 Active Directory 群組政策在多台電腦上安裝 Kaspersky Embedded Systems Security。您可以以相同的方式安裝應用程式主控台。

要安裝 Kaspersky Embedded Systems Security 或應用程式主控台的電腦必須在同一個網域中和一個組織單元中。

要使用政策安裝 Kaspersky Embedded Systems Security 的電腦的作業系統必須為相同的位數 (32 位元或 64 位元)。

您必須有該網域的管理員權限。

要安裝 Kaspersky Embedded Systems Security，請使用 `ess_x86(x64).msi` 安裝套件。要安裝應用程式主控台，請使用 `esstools.msi` 安裝套件。

有關使用 Active Directory 群組政策的詳細資訊，提供在 Microsoft 提供的文件中。

► 若要安裝 *Kaspersky Embedded Systems Security* (或應用程式主控台) :

1. 將對應於已安裝的 Microsoft Windows 作業系統版本位元數 (32 位元或 64 位元) 的 msi 檔案儲存到網域控制站上的公共資料夾中。
2. 將金鑰檔案(請參加第 [101](#) 頁上的“關於金鑰檔案”部分)儲存在網域控制器上的同一公共資料夾中。
3. 在網域控制器上的相同公共資料夾中，建立一個包含以下內容的 install_props.json 檔案，表示您接受產品授權協議和隱私政策的條款。

```
{
  "EULA": "1",
  "PRIVACYPOLICY": "1"
}
```

4. 在網域控制器上替一組整合的電腦建立新的政策。
5. 使用“**群組政策物件編輯器**”，在“**電腦設定**”節點中建立新的安裝套件。以 UNC 格式(通用命名慣例) 指定 *Kaspersky Embedded Systems Security* (或應用程式主控台) msi 檔案的路徑。
6. 如同所選群組的“**使用者設定**”與“**電腦設定**”節點一樣，選中 Windows Installer 的“**永遠以較高的權限安裝**”核取方塊。
7. 使用 gpupdate /force 指令採納變更。

Kaspersky Embedded Systems Security 將在該群組的電腦重新啟動後安裝到這些電腦上。

在安裝 *Kaspersky Embedded Systems Security* 後執行的操作

在受防護電腦上安裝 *Kaspersky Embedded Systems Security* 後，建議您立即更新應用程式資料庫並執行關鍵區域掃描。您可以從應用程式主控台執行這些操作 (請參見第 [69](#) 頁上的“在安裝 *Kaspersky Embedded Systems Security* 後執行的操作”部分)。

您還可以配置有關 *Kaspersky Embedded Systems Security* 事件的管理員通知。

透過 Active Directory 群組政策移除 Kaspersky Embedded Systems Security

如果在電腦群組中使用了 Active Directory 群組政策安裝 Kaspersky Embedded Systems Security (或應用程式主控台) , 則可以使用該政策移除 Kaspersky Embedded Systems Security (或應用程式主控台) 。

您可以僅使用預設的移除參數來移除應用程式。

有關使用 Active Directory 群組政策的詳細資訊，提供在 Microsoft 提供的文件中。

如果應用程式管理受密碼防護，則無法使用 Active Directory 群組政策移除 Kaspersky Embedded Systems Security。

► 要移除 *Kaspersky Embedded Systems Security (或應用程式主控台)* :

1. 在網域控制器上，從要移除 Kaspersky Embedded Systems Security 或應用程式主控台的電腦中選擇組織單元。
2. 在“**群組政策編輯器**”中選擇為安裝 Kaspersky Embedded Systems Security 所建立的政策，在“**軟體安裝**”節點 (“**電腦配置** > **軟體設定** > **軟體安裝**”) 中開啟 Kaspersky Embedded Systems Security (或應用程式主控台) 安裝套件的內容功能表，然後選擇“**所有工作** > **刪除**”指令。
3. 選擇移除方法“**立即從使用者處和電腦中移除軟體**”。
4. 使用 `gpupdate /force` 指令採納變更。

Kaspersky Embedded Systems Security 將在電腦重啟後和登入 Microsoft Windows 前從電腦中移除。

檢查 Kaspersky Embedded Systems Security 功能。使用 EICAR 測試病毒

本章節介紹 EICAR 測試病毒以及如何使用 EICAR 測試病毒檢查 Kaspersky Embedded Systems Security 的即時防護和自訂掃描功能。

本章節說明項目

關於 EICAR 測試病毒.....	93
檢查即時防護和自訂掃描功能.....	94

關於 EICAR 測試病毒

測試病毒的設計目的在於驗證防毒應用程式的運作功能，它由歐洲電腦防毒研究協會 (EICAR) 開發。

測試病毒不是惡意物件，不包含針對電腦的可執程式碼。不過，大部份廠商的防毒應用程式可透過它來辨認威脅。

含有此測試病毒的檔案稱為 eicar.com。您可從 EICAR 網站 http://www.eicar.org/anti_virus_test_file.htm 下載此檔案。

在您將該檔案下載到電腦硬碟中的資料夾前，請確認已停用該磁碟機的即時防護設定。

eicar.com 檔案含有一行文字。掃描檔案時，Kaspersky Embedded Systems Security 會偵測到這行文字中有“威脅”等字，接著對檔案指派“受感染”狀態並刪除檔案。檔案中偵測到的威脅資訊將出現在應用程式主控台及工作記錄中。

您可使用 eicar.com 檔案來檢查 Kaspersky Embedded Systems Security 解毒已感染物件及偵測潛在可疑危險物件的方法。要進行檢查，使用文字編輯器開啟 eicar.com 檔案，將該檔案開頭幾行文字所列的前置詞加入另一個新建檔案中，然後以新的檔案名稱（例如 eicar_cure.com）儲存。

為確保 Kaspersky Embedded Systems Security 處理帶有首碼的 eicar.com 檔案，在“物件防護”安全設定部分中，為 Kaspersky Embedded Systems Security 的“即時檔案防護”工作和“預設自訂掃描”工作設定“所有物件”值。

表 7. EICAR 檔案前置詞

前置詞	掃描後的檔案狀態及 Kaspersky Embedded Systems Security 操作
無前置詞	Kaspersky Embedded Systems Security 會指派“ 受感染 ”狀態給物件並刪除物件。
SUSP-	Kaspersky Embedded Systems Security 向啟發式分析偵測到的物件分配“ 疑似感染 ”狀態並刪除它，因為不會解毒疑似感染物件。
WARN-	Kaspersky Embedded Systems Security 向物件（物件的程式碼與已知威脅的程式碼部分比對）分配“ 疑似感染 ”狀態並刪除它，因為不會解毒疑似感染物件。
CURE-	Kaspersky Embedded Systems Security 會指派“ 受感染 ”狀態給物件並解毒物件。如果解毒成功，則檔案中整段文字將以 "CURE" 取代。

檢查即時防護和自訂掃描功能

安裝 Kaspersky Embedded Systems Security 後，您可以確認 Kaspersky Embedded Systems Security 發現包含惡意程式碼的物件。要進行檢查，您可以使用 EICAR 測試病毒（請參見第 93 頁上的“關於 EICAR 測試病毒”部分）。

► 若要檢查“即時防護”，請執行以下步驟：

1. 從 EICAR 網站 (http://www.eicar.org/anti_virus_test_file.htm) 下載 eicar.com 檔案。將它儲存到網路上任一電腦的本機磁碟機上的公用資料夾中。

在您將檔案儲存到資料夾前，請確認已停用該資料夾的即時檔案防護設定。

2. 如果要檢查網路使用者通知是否正常工作，請確保受防護電腦和儲存 eicar.com 檔案的電腦均啟用了 Microsoft Windows Messenger 服務。
3. 開啟應用程式主控台。
4. 使用以下其中一種方法，將儲存的 eicar.com 檔案複製到受防護電腦的本機磁碟上：
 - 若要透過“終端服務”視窗進行通知測試，請在使用遠端桌面連線實用程式連線到電腦後，將 eicar.com 檔案複製到電腦。
 - 若要透過“Microsoft Windows Messenger 服務”進行測試通知，請使用電腦的網路位置從您儲存 eicar.com 檔案的電腦複製它。

“即時檔案防護”工作只有在下列條件符合時才會運作：

- 受防護電腦上的 eicar.com 檔已刪除。
- 在應用程式主控台中，工作記錄的狀態為“緊急”。記錄有一行新行，其中包含 eicar.com 檔案中的威脅的資訊。（要檢視工作記錄，請在應用程式主控台樹狀目錄中，展開“即時電腦防護”節點，選擇“即時檔案防護”工作，然後在節點的詳細資訊面板中點擊“開啟工作記錄”連結）。
- 您從中複製該檔案的電腦上會顯示以下 Microsoft Windows Messenger 服務訊息：Kaspersky Embedded Systems Security 已在 <事件發生時間> 封鎖對電腦 <電腦的網路名稱> 上的 <電腦上的檔案路徑>\eicar.com 的存取。原因：偵測到威脅。病毒名稱：EICAR-Test-File。使用者名稱：<使用者名稱>。電腦名稱：<從中複製該檔案的電腦網路名稱>。

在從中複製 eicar.com 檔案的電腦上，確保 Microsoft Windows Messenger Service 正在執行。

► 要檢查“自訂掃描”功能，請執行以下步驟：

1. 從 EICAR 網站 (http://www.eicar.org/anti_virus_test_file.htm) 下載 eicar.com 檔案。將它儲存到網路上任一電腦的本機磁碟機上的公用資料夾中。

在您將檔案儲存到資料夾前，請確認已停用該資料夾的即時檔案防護設定。

2. 開啟應用程式主控台。
3. 執行以下操作：
 - a. 在應用程式主控台樹狀目錄中展開“自訂掃描”節點。
 - b. 選擇“**關鍵區域掃描**”子節點。
 - c. 在“**設定掃描範圍**”標籤上，開啟“**網路**”節點上的內容功能表，並選擇“**新增網路檔案**”。
 - d. 以 UNC 格式（通用命名慣例）輸入 eicar.com 檔在遠端電腦中的網路路徑。
 - e. 選取將網路路徑新增到掃描範圍的核取方塊。
 - f. 執行“**關鍵區域掃描**”工作。

自訂掃描只有在下列條件符合時才會運作：

- eicar.com 檔案已從電腦的硬碟磁碟機中刪除。
- 在應用程式主控台中，工作記錄的狀態為“**緊急**”。“**關鍵區域掃描**”工作記錄有一行新行，其中包含 eicar.com 檔案中的威脅的資訊。（要檢視工作記錄，請展開應用程式主控台樹狀結構與“**自訂掃描**”節點，選擇“**關鍵區域掃描**”工作並在詳細資訊面板上的“**開啟工作記錄**”進行點擊。）

應用程式介面

您可以使用管理外掛程式和本機應用程式主控台控制 Kaspersky Embedded Systems Security。

“使用應用程式主控台”部分中介紹了本機應用程式主控台介面中的操作（請參見第 [170](#) 頁上的“使用 Kaspersky Embedded Systems Security 主控台”部分）。

卡斯基安全管理中心管理主控台介面用於使用管理外掛程式執行操作。有關卡斯基安全管理中心介面的詳細資訊，請參見 *卡斯基安全管理中心說明*。

應用程式授權

本章節提供與應用程式產品授權有關的主要概念的資訊。

本章內容

關於最終使用者產品授權協議	98
關於產品授權	99
關於產品授權憑證	100
關於金鑰	101
關於金鑰檔案	101
關於啟動碼	102
關於資料提供	102
使用產品授權金鑰啟動應用程式	105
使用啟動碼啟動應用程式	106
檢視有關目前產品授權的資訊	107
產品授權到期後的功能限制	110
續約產品授權	110
刪除金鑰	111

關於最終使用者產品授權協議

*最終使用者產品授權協議*是您和 AO Kaspersky Lab 之間達成的約束協議，它規定了您在使用所購買的軟體時須遵循的條款。

請仔細檢視最終使用者產品授權協議的條款，然後再開始使用程式。

您可以透過以下方法檢視使用者產品授權協議的條款：

- 在 Kaspersky Embedded Systems Security 安裝期間
- 閱讀 license.txt 檔案。本檔案包含在應用程式的安裝套件中

一旦在安裝程式時確認您同意最終使用者產品授權協議，即表示您接受最終使用者產品授權協議的條款。如果您不接受最終使用者產品授權協議的條款，則必須中止程式安裝，且不得使用程式。

關於產品授權

產品授權是根據使用者授權協議在有限時間內授予您使用本程式的權利。

有效的產品授權可使您享有以下各種服務：

- 依照最終使用者產品授權協議的條款使用應用程式
- 技術支援

服務範圍和應用程式使用期取決於用來應用程式的產品授權類型。

應用程式使用購買的正式產品授權的金鑰檔案或啟動碼啟動。

正式產品授權是指購買應用程式時授予的付費產品授權。

Kaspersky Embedded Systems Security 包括以下正式產品授權：

- Kaspersky Embedded Systems Security 標準產品授權。

- Kaspersky Embedded Systems Security Compliance Edition 延伸產品授權，包括兩個額外的系統審查元件：“檔案完整性監控”和“記錄審查”。

在正式產品授權到期時，應用程式將繼續執行，但其某些功能會變為不可用（例如，無法更新 Kaspersky Embedded Systems Security 資料庫）。要繼續在全功能模式下使用 Kaspersky Embedded Systems Security，您必須對您的正式版產品授權進行續約。

為確保最大限度防護您的電腦免受安全威脅，我們建議您在產品授權到期之前進行續約。

確保您新增的備用金鑰的到期日期晚於啟動金鑰。

關於產品授權憑證

產品授權憑證是您與金鑰檔案或啟動碼（如果適用）一起收到的文件。

產品授權憑證包含以下有關所提供的產品授權的相關資訊：

- 訂單號
- 有關被授予產品授權的使用者的資訊
- 有關可以使用所提供的產品授權啟動的應用程式的資訊
- 授權單元數限制（例如，執行可以使用所提供的產品授權的應用程式的裝置數量）
- 產品授權有效開始日期
- 產品授權到期日期或產品授權期限
- 產品授權類型

關於金鑰

金鑰是一串位資料，您可以依照最終使用者產品授權協議的條款透過該金鑰來啟動並在啟動後使用程式。

金鑰是由 Kaspersky Lab 建立的。

您可以透過金鑰檔案在應用程式中新增產品授權。在應用程式中新增金鑰後，將在應用程式介面中以唯一的字母數字序列形式顯示。

Kaspersky Lab 可能會由於某個產品授權違反產品授權協議而將其新增到黑名單中。如果封鎖了您的金鑰，則必須新增其他金鑰以使應用程式正常工作。

金鑰可以是“啟動金鑰”或“備用金鑰”。

*啟動金鑰*是指目前正在使用的金鑰檔案以使應用程式正常工作。可以將正式產品授權或試用產品授權的金鑰新增為啟動金鑰。應用程式只能有一個啟動金鑰。

*備用金鑰*使用者可新增一組目前尚未使用的金鑰。在與目前啟動金鑰關聯的產品授權到期時，備用金鑰將自動變為啟動金鑰。只有在具有啟動金鑰時，才能新增備用金鑰。

關於金鑰檔案

金鑰檔案是 Kaspersky Lab 提供的帶有 .key 副檔名的檔案。金鑰檔案旨在透過新增產品授權金鑰來啟動應用程式。

您在購買 Kaspersky Embedded Systems Security 或訂購 Kaspersky Embedded Systems Security 試用版時提供的電子郵件信箱會收到金鑰檔案。

您不需要連線到 Kaspersky Lab 啟動伺服器，即可利用金鑰檔案啟動應用程式。

如果意外刪除了金鑰檔案，您可以將其還原。例如，您可能需要金鑰檔案來註冊 Kaspersky CompanyAccount。

要還原金鑰檔案，請執行以下任一操作：

- 聯絡產品授權銷售商。
- 使用您的可用啟動碼透過 Kaspersky Lab 網站 (<https://keyfile.kaspersky.com/en/>) 接收金鑰檔案。

關於啟動碼

啟動碼是由 20 個字母和數字組成的唯一序列。您必須輸入啟動碼才能新增用於啟動 Kaspersky Embedded Systems Security 的金鑰。您在購買 Kaspersky Embedded Systems Security 時提供的電子郵件信箱會收到啟動碼。

要使用啟動碼啟動應用程式，您需要網際網路存取權限以連線到 Kaspersky Lab 啟動伺服器。

如果您在安裝應用程式後遺失了啟動碼，可以將其還原。例如，您可能需要啟動碼才能註冊 Kaspersky CompanyAccount。要還原啟動碼，請聯絡 Kaspersky Lab 技術支援。

關於資料提供

Kaspersky Embedded Systems Security 的產品授權協議（特別是“資料處理條款”部分）指定了本手冊中指示的傳送和處理資料的條款、責任及過程。在接受產品授權協議前，請仔細檢視其條款以及產品授權協議連結到的所有文件。

Kaspersky Lab 在您使用應用程式時收到的資料受到防護並按照隱私政策 www.kaspersky.com/Products-and-Services-Privacy-Policy 進行處理。

接受產品授權協議的條款，即表示您同意自動將以下資料傳送到 Kaspersky Lab：

- 為支援接收更新的機制 - 有關已安裝的應用程式及其啟動的資訊：已安裝的應用程式及其完全版本的識別碼，包括內部版本號、類型以及產品授權識別碼、安裝識別碼、更新工作識別碼。
- 為在應用程式出錯時使用導航到知識庫文章的功能（重定向器服務）- 有關應用程式和連結類型的資訊，具體為：名稱、區域設定以及應用程式的完全版本號、重定向連結的類型和錯誤識別碼。
- 為管理資料處理的確認 - 有關授權協議和規定了資料傳輸條款的其他文件的接受狀態的資訊：授權協議或其他文件（接受或拒絕作為其一部分的資料處理條款）的識別碼和版本；表示使用者操作（確認或撤銷接受條款）的內容；資料處理條款接受的狀態變更的日期和時間。

您可以透過以下方法檢視使用者產品授權協議的條款：

- 在應用程式安裝過程中，Kaspersky Embedded Systems Security 安裝精靈將在請求接受產品授權協議條款的步驟中顯示產品授權協議的全文。
- 隨時檢視 TXT 檔案 (license.txt)，其中包含產品授權協議全文。此檔案連同應用程式安裝檔案一同包含在 Kaspersky Embedded Systems Security 分發套件中。

本機資料處理

在執行本手冊所述的應用程式主要功能時，Kaspersky Embedded Systems Security 會在受防護電腦上本機處理和儲存一系列資料類型。應用程式本機處理的資料不會自動傳送到 Kaspersky Lab 或其他協力廠商系統。

Kaspersky Embedded Systems Security 本機處理並儲存以下資料：

- 有關掃描的檔案和偵測的物件的資訊，例如，被處理檔案的名稱和內容以及它們在被掃描介質上的完整路徑、對掃描的檔案執行的操作、對受防護網路或受防護電腦執行任何操作的使用者的帳戶、被掃描裝置的名稱和相關資料、有關係統上執行的處理程序的資訊、核對總和（MD5、SHA-256）、時間戳記、數位憑證內容、關於已執行指令碼的資料。
- 有關作業系統活動和設定的資訊，例如，Windows 防火牆設定、Windows 事件記錄項目、使用者帳戶的名稱、可執行檔的啟動，這些檔案的核對總和以及內容。

作為應用程式基本功能的一部分，Kaspersky Embedded Systems Security 處理並儲存資料，包括記錄應用程式事件和接收診斷資料。本機處理的資料按照配置和應用的應用程式設定進行防護。

Kaspersky Embedded Systems Security 允許您為本機處理的資料配置防護等級：您可以變更存取處理程序資料的使用者權限，變更此類別資料的資料保留期，完全或部分停用涉及資料記錄的功能，以及變更磁碟機上用於記錄資料的資料夾的路徑和內容。

有關對涉及資料處理的應用程式功能進行配置以及處理的資料儲存的預設設定的詳細資訊，請參見本手冊的相應章節。

預設情況下，從電腦移除 Kaspersky Embedded Systems Security 後，將移除該應用程式執行期間本機處理的所有資料。

帶偵錯資訊的檔案（偵錯和傾印檔案）以及 Windows 事件記錄中的應用程式事件除外 - 建議手動刪除這些檔案。

有關處理包含應用程式偵錯資料的檔案的詳細資訊，請參閱本手冊的相應章節。

您可以透過作業系統的標準方式刪除包含 Kaspersky Embedded Systems Security 程式事件的 Windows 事件記錄檔案。

透過應用程式協助元件處理本機資料

Kaspersky Embedded Systems Security 安裝套件包含應用程式協助元件，這些協助元件可以安裝在伺服器或電腦上，即使該伺服器或電腦未安裝 Kaspersky Embedded Systems Security。這些協助元件為：

- 應用程式主控台。該元件包含在 Kaspersky Embedded Systems Security 管理工具集中，由 Microsoft 管理主控台管理單元表示。
- 管理外掛程式。該元件提供與卡巴斯基安全管理中心應用程式的完全整合。

當執行本手冊所述的主要應用程式功能時，應用程式協助元件本機處理一群組資料並將資料儲存在安裝了這些元件的電腦上，即使它們與 Kaspersky Embedded Systems Security 分開安裝也是如此。

這些應用程式元件本機處理並存儲以下資料：

- 應用程式主控台：應用程式主控台上次遠端連線到的安裝了 Kaspersky Embedded Systems Security 的電腦的名稱 (IP 位址或網域名稱) ；在 Microsoft 管理主控台管理單元中配置的顯示參數；使用者上次透過應用程式主控台在其中選擇了物件 (使用透過點擊“瀏覽”按鈕開啟的系統對話方塊) 的資料夾的相關資料。應用程式主控台偵錯檔案還可能包含以下資料：建立了遠端連線的安裝了 Kaspersky Embedded Systems Security 應用程式的電腦的名稱，以及用於建立遠端連線的使用者帳戶的名稱。
- 管理外掛程式可以處理和暫時儲存 Kaspersky Embedded Systems Security 處理的資料；例如，應用程式工作和元件的配置參數、卡巴斯基安全管理中心政策的參數、網路清單中傳送的資料。

協助元件處理的資料不會自動傳送到 Kaspersky Lab 或其他協力廠商系統。

預設情況下，在移除這些應用程式協助元件後，這些元件在執行期間本機處理的資料都將被刪除。

應用程式協助元件的偵錯檔案是例外，建議手動刪除這些檔案。

有關處理包含應用程式協助元件診斷資料的檔案的詳細資訊，請參閱本手冊的相應章節。

使用產品授權金鑰啟動應用程式

您可以透過套用金鑰檔案來啟動 Kaspersky Embedded Systems Security。

如果已經向 Kaspersky Embedded Systems Security 新增了啟動金鑰，並且您又另外新增一個金鑰作為啟動金鑰，則新金鑰會替換之前新增的金鑰。之前新增的金鑰將被刪除。

如果已經向 Kaspersky Embedded Systems Security 新增了備用金鑰，並且您又另外新增一個金鑰作為備用金鑰，則新金鑰會替換之前新增的金鑰。之前新增的備用金鑰會被刪除。

如果已經向 Kaspersky Embedded Systems Security 新增了啟動金鑰和備用金鑰，並且您又另外新增一個新金鑰作為啟動金鑰，則新金鑰會替換之前新增的啟動金鑰；備用金鑰不會被刪除。

► 要使用金鑰檔案啟動 Kaspersky Embedded Systems Security，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“授權”節點。
2. 在“授權”節點的詳細資訊窗格中，點擊“新增金鑰”連結。
3. 在開啟的視窗中，點擊“瀏覽”按鈕並選擇具有 .key 副檔名的授權檔案。

還可以新增金鑰作為備用金鑰。若要新增金鑰作為備用金鑰，請選中“作為備用金鑰使用”核取方塊。

4. 點擊“確定”。

將會套用選定的金鑰檔案。“授權”節點將提供有關新增的金鑰的資訊。

使用啟動碼啟動應用程式

要使用啟動碼啟動應用程式，電腦必須連線到網際網路。

您可以透過使用啟動碼來啟動 Kaspersky Embedded Systems Security。

使用此方法啟動應用程式時，Kaspersky Embedded Systems Security 會將資料傳送到啟動伺服器來驗證所輸入的代碼：

- 如果啟動碼驗證成功，應用程式將啟動。
- 如果啟動碼驗證失敗，將顯示相應通知。在這種情況下，您必須聯絡您向其購買 Kaspersky Embedded Systems Security 產品授權的軟體供應商。
- 如果超過了啟動碼的啟動次數，將顯示相應通知。應用程式啟動過程將中斷，應用程式會建議您聯絡 Kaspersky Lab 技術支援。

► 要獲得金鑰以使用啟動碼啟動 Kaspersky Embedded Systems Security，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“授權”節點。

2. 在“授權”節點的詳細資訊窗格中，點擊“新增啟動碼”連結。
3. 在開啟的視窗的“啟動碼”欄位中，輸入啟動碼。
 - 如果要將啟動碼作為備用金鑰使用，請啟用“作為備用金鑰使用”核取方塊。
 - 如果要檢視產品授權資訊，請點擊“顯示產品授權資訊”按鈕；相應資訊將顯示在“產品授權資訊”組框中。
4. 點擊“確定”。

Kaspersky Embedded Systems Security 會將有關套用的啟動碼的資訊傳送到管理伺服器。

檢視有關目前產品授權的資訊

檢視授權資訊

有關目前產品授權的資訊顯示在應用程式主控台的 **Kaspersky Embedded Systems Security** 節點的詳細資訊窗格中。金鑰可以具有以下狀態：

- **檢查金鑰狀態** – Kaspersky Embedded Systems Security 正在檢查已套用的金鑰檔案或啟動碼，等待有關目前金鑰狀態的回應。
- **產品授權到期日期** – Kaspersky Embedded Systems Security 已啟動，且在指定日期和時間之前有效。在以下情況下，金鑰狀態突出顯示為黃色：
 - 產品授權將在 14 天後到期，並且未套用任何備用金鑰。
 - 新增的金鑰已被列入黑名單且將被封鎖。
- **產品授權已到期** – 由於產品授權已到期，Kaspersky Embedded Systems Security 未啟動。狀態紅色高亮顯示。
- **已違反最終使用者產品授權協議** – 由於違反了最終使用者產品授權協議（請參見第 98 頁上的“關於最終使用者產品授權協議”部分）的條款，Kaspersky Embedded Systems Security 未啟動。狀態紅色高亮顯示。
- **金鑰已被列入黑名單** – 新增的金鑰已被 Kaspersky Lab 封鎖並列入黑名單，例如，金鑰被協力廠商用來非法啟動程式。狀態紅色高亮顯示。

檢視有關目前產品授權的資訊

- ▶ 要檢視有關目前產品授權的資訊，

在應用程式主控台樹狀目錄中，展開“授權”節點。

有關目前產品授權的一般資訊顯示在“授權”節點的詳細資訊視窗中（請參見下表）。

表 8. “授權”節點中有關產品授權的一般資訊

欄位	敘述
啟動碼	啟動碼。如果您使用啟動碼啟動應用程式時，則填寫此欄位。
啟動狀態	有關應用程式的啟動狀態的資訊。“授權”節點的詳細資訊窗格中“啟動”列可具有以下狀態： <ul style="list-style-type: none"> • 已套用 – 如果您已使用啟動碼或金鑰檔案啟動應用程式。 • 啟動 – 如果您已套用啟動碼啟動應用程式，但啟動過程尚未最終完成。應用程式啟動完成並且節點的詳細資訊窗格的內容重新整理後，狀態變更為“已套用”。 • 啟動錯誤 – 如果應用程式啟動失敗。您可在工作記錄中檢視啟動不成功的原因。
金鑰	用於啟動應用程式的金鑰。
產品授權類型	產品授權類型：正式或試用。
到期日期	與啟動金鑰相關聯的產品授權的到期日期和時間。
啟動碼狀態或金鑰狀態	啟動碼狀態或金鑰狀態：啟動或備用。

- ▶ 要檢視有關產品授權的詳細資訊，

在“授權”節點上，開啟包含您要展開的產品授權資料的行的內容功能表，然後選擇“內容”。

在“內容：<啟動碼狀態或金鑰狀態>”視窗中，“一般”標籤顯示有關目前產品授權的詳細資訊，“進階”標籤顯示有關客戶的資訊以及 Kaspersky Lab 或向您出售 Kaspersky Embedded Systems Security 的轉銷商的聯絡人詳細資訊（請參見下表）。

表 9. “內容 <啟動碼狀態或金鑰狀態>”視窗中的詳細產品授權資訊

欄位	敘述
“一般”標籤	
金鑰	用於啟動應用程式的金鑰。
金鑰新增日期	金鑰新增到應用程式的日期。
產品授權類型	產品授權類型：正式或試用。
到期剩餘天數	與啟動授權相關的產品授權在到期前剩餘的天數。
到期日期	與啟動金鑰相關聯的產品授權的到期日期和時間。如果在無期限訂購下啟動應用程式，此欄位的值為 <i>無期限</i> 。如果 Kaspersky Embedded Systems Security 無法確定產品授權到期日期，則此欄位的值設定為 <i>未知</i> 。
應用程式	使用金鑰檔案或啟動碼啟動的應用程式的名稱。
金鑰使用限制	對使用金鑰的限制（如果有）。
符合技術支援需求	有關 Kaspersky Lab 或合作夥伴之一是否將在產品授權期限下提供技術支援的資訊。
“進階”標籤	
關於產品授權的資訊	目前產品授權編號。
支援資訊	Kaspersky Lab 或其提供技術支援的合作夥伴的聯絡人詳細資訊。如果不提供技術支援，則此欄位可為空。
所有者資訊	有關產品授權所有者的資訊：客戶名稱和獲取產品授權的組織的名稱。

產品授權到期後的功能限制

產品授權到期後，以下限制將套用於功能元件：

- 除了“即時檔案防護”、“自訂掃描”和“應用程式完整性控制”工作以外，所有工作都將停止。
- 無法啟動除了“即時檔案防護”、“自訂掃描”和“應用程式完整性控制”以外的所有工作。這些工作繼續使用舊的病毒資料庫執行。
- 弱點利用防禦功能受限制：
 - 處理程序受防護至重新啟動為止。
 - 新處理程序無法新增到防護範圍中。

其他功能（儲存區、記錄、診斷資訊）仍將可用。

續約產品授權

預設情況下，當產品授權還有 14 天就要到期時，Kaspersky Embedded Systems Security 會通知您即將到期的情況。在這種情況下，“Kaspersky Embedded Systems Security”節點的詳細資訊視窗中將以黃色突出顯示“**產品授權到期日期**”狀態。

您可以在到期日期前使用備用金鑰檔案或啟動碼續約產品授權。這可確保在目前產品授權到期後和您使用新的產品授權啟動應用程式之前繼續防護您的電腦。

► 若要更新產品授權，請執行以下步驟：

1. 獲取新的啟動碼或金鑰檔案。
2. 在應用程式主控台樹狀目錄中，開啟“**授權**”節點。
3. 在“**授權**”節點的詳細資訊視窗中執行以下操作之一：
 - 如果您想要使用備用金鑰續約產品授權：
 - a. 點擊“**新增**”連結。
 - b. 在開啟的視窗中，點擊“**瀏覽**”按鈕並使用 .key 副檔名選擇新的授權檔案。

- c. 選中“**作為備用金鑰使用**”核取方塊。
- 如果您想要使用啟動碼續約產品授權：
 - a. 點擊“**新增啟動碼**”連結。
 - b. 在開啟的視窗中輸入購買的啟動碼。
 - c. 選中“**作為備用金鑰使用**”核取方塊。

套用啟動碼需要網際網路連線。

4. 點擊“**確定**”。

目前 Kaspersky Embedded Systems Security 產品授權到期後，會新增並自動套用備用金鑰。

刪除金鑰

您可以刪除新增的金鑰。

如果向 Kaspersky Embedded Systems Security 新增了備用金鑰，並且您刪除了啟動金鑰，則備用金鑰會自動變為啟動金鑰。

如果您刪除所新增的金鑰，則可以透過重新套用金鑰檔案來將其還原。

▶ 刪除所新增的金鑰：

1. 在應用程式主控台樹狀目錄中，選擇“**授權**”節點。
2. 在包含有關已新增金鑰的資訊的表格中的“**授權**”節點的詳細資訊窗格中，選擇您要刪除的金鑰。
3. 在包含有關所選金鑰的資訊的行的內容功能表中，選擇“**刪除**”。
4. 在確認視窗中點擊“**是**”按鈕以確認您希望刪除該金鑰。

選定的金鑰將被刪除。

使用管理外掛程式

本節提供有關 Kaspersky Embedded Systems Security 管理外掛程式的資訊，並介紹如何管理受防護電腦或電腦群組上安裝的應用程式。

本章內容

從卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security.....	113
管理應用程式設定.....	114
建立和設定政策.....	135
使用卡巴斯基安全管理中心建立和管理工作.....	146
在卡巴斯基安全管理中心中報告.....	167

從卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security

透過 Kaspersky Embedded Systems Security 管理外掛程式可以集中管理多台已安裝 Kaspersky Embedded Systems Security 並包括在管理群組中的電腦。卡巴斯基安全管理中心還可以單獨配置管理群組中包括的每台電腦的操作設定。

“*管理群組*”透過卡巴斯基安全管理中心手動建立並包含您要為其設定相同的控制和防護設定的已安裝 Kaspersky Embedded Systems Security 的多台電腦。有關使用管理群組的詳細資訊，請參閱 *卡巴斯基安全管理中心說明*。

如果 Kaspersky Embedded Systems Security 在某台電腦上的執行受活動卡巴斯基安全管理中心政策的控制，則該電腦的應用程式設定不可用。

可透過以下方式透過卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security：

- **使用卡巴斯基安全管理中心政策。**可使用卡巴斯基安全管理中心政策為一組電腦遠端設定相同的防護設定。在活動政策中指定的工作設定的優先順序高於在應用程式主控台中本機設定或在卡巴斯基安全管理中心的“內容：<電腦名稱>”視窗中遠端配置的工作設定。

您可使用政策設定一般應用程式設定、即時防護工作設定、本機行為控制工作設定、排程的系統工作啟動設定和設定檔使用設定。

- **使用卡巴斯基安全管理中心群組工作。**卡巴斯基安全管理中心群組工作允許為一組電腦遠端配置具有過期期限的工作的通用設定。
- 您可使用工作群組啟動應用程式，設定“自訂掃描”工作設定，更新工作設定，以及“應用程式啟動控制規則產生器”工作設定。
- **使用一組裝置的工作。**針對一組裝置的工作允許為不屬於任何一個管理群組的電腦遠端配置具有有限執行期限的通用工作設定。
- **使用單個電腦的內容視窗。**在“內容：<電腦名稱>”視窗中，您可遠端配置管理群組中包含的單個電腦的工作設定。如果選定電腦不受活動卡巴斯基安全管理中心政策的控制，您可配置一般應用程式設定和所有 Kaspersky Embedded Systems Security 工作的設定。

卡巴斯基安全管理中心可以配置應用程式設定、進階功能，並允許您使用記錄和通知。您可以為一組電腦也可以為單台電腦配置這些設定。

管理應用程式設定

本章節包含有關在卡巴斯基安全管理中心中配置 Kaspersky Embedded Systems Security 一般設定的資訊。

本章內容

從卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security	115
導航	116
在卡巴斯基安全管理中心中設定一般應用程式設定	118
在卡巴斯基安全管理中心中配置隔離和備份設定	125
配置記錄和通知	126

從卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security

透過 Kaspersky Embedded Systems Security 管理外掛程式可以集中管理多台已安裝 Kaspersky Embedded Systems Security 並包括在管理群組中的電腦。卡巴斯基安全管理中心還可以單獨配置管理群組中包括的每台電腦的操作設定。

“**管理群組**”透過卡巴斯基安全管理中心手動建立並包含您要為其設定相同的控制和防護設定的已安裝 Kaspersky Embedded Systems Security 的多台電腦。有關使用管理群組的詳細資訊，請參閱 *卡巴斯基安全管理中心說明*。

如果 Kaspersky Embedded Systems Security 在某台電腦上的執行受活動卡巴斯基安全管理中心政策的控制，則該電腦的應用程式設定不可用。

可透過以下方式透過卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security：

- **使用卡巴斯基安全管理中心政策。**可使用卡巴斯基安全管理中心政策為一組電腦遠端設定相同的防護設定。在活動政策中指定的工作設定的優先順序高於在應用程式主控台中本機設定或在卡巴斯基安全管理中心的“內容：<電腦名稱>”視窗中遠端配置的工作設定。
您可使用政策設定一般應用程式設定、即時防護工作設定、本機行為控制工作設定、排程的系統工作啟動設定和設定檔使用設定。
- **使用卡巴斯基安全管理中心群組工作。**卡巴斯基安全管理中心群組工作允許為一組電腦遠端配置具有過期期限的工作的通用設定。
- 您可使用工作群組啟動應用程式，設定“自訂掃描”工作設定，更新工作設定，以及“應用程式啟動控制規則產生器”工作設定。
- **使用一組裝置的工作。**針對一組裝置的工作允許為不屬於任何一個管理群組的電腦遠端配置具有有限執行期限的通用工作設定。
- **使用單個電腦的內容視窗。**在“內容：<電腦名稱>”視窗中，您可遠端配置管理群組中包含的單個電腦的工作設定。如果選定電腦不受活動卡巴斯基安全管理中心政策的控制，您可配置一般應用程式設定和所有 Kaspersky Embedded Systems Security 工作的設定。

卡巴斯基安全管理中心可以配置應用程式設定、進階功能，並允許您使用記錄和通知。您可以為一組電腦也可以為單台電腦配置這些設定。

導航

學習如何透過介面導航到所需工作設定。

本章節說明項目

透過政策開啟一般設定.....	117
在應用程式內容視窗中開啟一般設定.....	117

透過政策開啟一般設定

► 要透過政策開啟 *Kaspersky Embedded Systems Security* 的應用程式設定：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“**政策**”標籤。
4. 點擊要設定的政策名稱。
5. 在開啟的“**內容：<政策名稱>**”視窗中，選擇“**應用程式設定**”部分。
6. 在您要配置的設定的子部分中點擊“**設定**”按鈕。

在應用程式內容視窗中開啟一般設定

► 要開啟單台電腦的 *Kaspersky Embedded Systems Security* 內容視窗：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“**裝置**”標籤。
4. 採用以下方法之一開啟“**內容：<電腦名稱>**”視窗：
 - 點擊受防護電腦的名稱。
 - 在受防護電腦的上下文功能表中選擇“**內容**”項。

將開啟“**內容：<電腦名稱>**”視窗。

5. 在“**應用程式**”部分中，選擇“**Kaspersky Embedded Systems Security**”。
6. 點擊“**內容**”按鈕。

將開啟“**Kaspersky Embedded Systems Security**’應用程式設定”視窗。

7. 選擇“**應用程式設定**”部分。

在卡巴斯基安全管理中心中設定一般應用程式設定

您可以透過卡巴斯基安全管理中心為一組電腦或一個電腦配置 Kaspersky Embedded Systems Security 一般設定。

本章節說明項目

在卡巴斯基安全管理中心中配置延展性和介面.....	118
在卡巴斯基安全管理中心中配置安全性設定.....	120
使用卡巴斯基安全管理中心配置連線設定.....	122
設定本機系統工作的排程啟動.....	123

在卡巴斯基安全管理中心中配置延展性和介面

► 要配置延伸性設定和應用程式介面：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 144 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 150 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**應用程式設定**”部分的“**延伸性和介面**”部分，點擊“**設定**”。

5. 在“進階程式設定”視窗中“一般”標籤上，配置以下設定：

- 在“延伸性設定”部分中，配置用於定義 Kaspersky Embedded Systems Security 使用的處理程序數的設定：

- **自動偵測延伸性設定。**

Kaspersky Embedded Systems Security 自動控制使用的處理程序數量。

這是預設值。

- **手動設定工作處理程序數。**

Kaspersky Embedded Systems Security 根據指定的值控制有效的工作處理程序數。

- **最大活動處理程序數。**

Kaspersky Embedded Systems Security 使用的最大處理程序數。如果選擇了“手動設定工作處理程序數”選項，該輸入欄位才可用。

- **用於即時防護的程序數。**

即時防護工作元件使用的最大處理程序數。如果選擇了“手動設定工作處理程序數”選項，該輸入欄位才可用。

- **背景自訂掃描工作的處理程序數。**

在背景模式下執行“自訂掃描”工作時“自訂掃描”元件使用的最大處理程序數。如果選擇了“手動設定工作處理程序數”選項，該輸入欄位才可用。

- 在“使用者互動”部分中，配置通知區域中應用程式系統欄圖示顯示：清除或選中“在工作列中顯示系統匣圖示”核取方塊。

6. 在“分級儲存”標籤上，選擇存取分級儲存的選項。

7. 點擊“確定”。

將儲存設定的應用程式設定。

在卡斯基安全管理中心中配置安全性設定

► 若要手動設定安全性設定，請執行以下步驟：

1. 展開卡斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 144 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 150 頁上的“在卡斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**應用程式設定**”部分，點擊“**安全**”設定下的“**設定**”按鈕。
5. 在“**安全性設定**”視窗中，配置以下設定：
 - 在“**可靠性設定**”部分，您可以配置當應用程式返回錯誤或終止時 Kaspersky Embedded Systems Security 工作的還原設定。
 - **重新啟動工作**

該核取方塊用於允許或禁止當應用程式返回錯誤或終止時 Kaspersky Embedded Systems Security 工作的還原。

如果選中該核取方塊，則當應用程式返回錯誤或終止時，Kaspersky Embedded Systems Security 會自動還原 Kaspersky Embedded Systems Security 工作。

如果清除該核取方塊，則當應用程式返回錯誤或終止時，Kaspersky Embedded Systems Security 不會還原 Kaspersky Embedded Systems Security 工作。

預設將會選定該核取方塊。
 - **還原自訂掃描工作的次數不超過 (次)**

Kaspersky Embedded Systems Security 傳回錯誤後嘗試還原“自訂掃描”工作的次數。如果選中“重新啟動工作”核取方塊，則該輸入欄位才可用。

- 在“轉換到 UPS 備份電源時的操作”部分，指定在轉換為 UPS 備份電源後 Kaspersky Embedded Systems Security 對電腦產生的負荷的限制：

- **不啟動排程掃描工作**

該核取方塊用於啟用或停用在電腦轉換為 UPS 電源後、還原標準電源模式前啟動排程掃描工作。

如果選中該核取方塊，在電腦轉換為 UPS 電源後、還原標準電源模式前 Kaspersky Embedded Systems Security 不會啟動排程掃描工作。

如果清除該核取方塊，不論電源模式如何，Kaspersky Embedded Systems Security 都會啟動排程掃描工作。

預設將會選定該核取方塊。

- **停止目前掃描工作**

該核取方塊用於啟用或停用在電腦轉換為 UPS 電源後執行執行掃描工作的選項。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會在電腦轉換為 UPS 電源後暫停執行掃描工作。

如果清除該核取方塊，Kaspersky Embedded Systems Security 會在電腦轉換為 UPS 電源後繼續執行掃描工作。

預設將會選定該核取方塊。

- 在“密碼防護設定”部分中，設定用於防護存取 Kaspersky Embedded Systems Security 功能的密碼。

6. 點擊“確定”。

將儲存延伸性和可靠性設定。

使用卡巴斯基安全管理中心配置連線設定

設定的連線設定用於將 Kaspersky Embedded Systems Security 連線到更新和啟動伺服器，以及在將應用程式與 KSN 服務整合期間使用。

► 若要設定連線設定，請執行以下步驟：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“政策”標籤，然後開啟“內容：<政策名稱>”視窗（請參見第 144 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“裝置”標籤，然後開啟“應用程式設定”視窗（請參見第 150 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“應用程式設定”視窗中編輯這些設定。

4. 在“應用程式設定”部分中，點擊“連線”設定塊中的“設定”按鈕。

將開啟“連線設定”視窗。

5. 在“連線設定”視窗中，配置以下設定：

- 在“代理伺服器設定”部分中，選擇代理伺服器使用設定：

- 不使用代理伺服器。

如果選擇此選項，Kaspersky Embedded Systems Security 會直接連線到 KSN 服務，而不使用任何代理伺服器。

- 使用自訂代理伺服器設定。

如果選擇此選項，Kaspersky Embedded Systems Security 會使用手動指定的代理伺服器設定連線到 KSN。

- 代理伺服器和埠號的 IP 位址或符號名稱。

- 對於本機位址不使用代理伺服器。

該核取方塊用於在存取與安裝了 Kaspersky Embedded Systems Security 的電腦位於同一網路上的電腦時啟用/停用代理伺服器。

如果選中該核取方塊，則會直接透過託管已安裝了 Kaspersky Embedded Systems Security 的電腦的網路存取電腦。而不使用代理伺服器。

如果取消選中該核取方塊，將套用代理伺服器以連線到本機電腦。

預設將會選定該核取方塊。

- 在“代理伺服器身分驗證設定”部分中，指定身分驗證設定：
 - 在下拉清單中選擇身分驗證設定。
 - **不使用身分驗證** - 不執行身分驗證。預設選擇該方式。
 - **使用 NTLM 身分驗證** - 使用由 Microsoft 開發的 NTLM 網路身分驗證協定執行身分驗證。
 - **使用帶使用者名稱和密碼的 NTLM 身分驗證** - 透過由 Microsoft 開發的 NTLM 網路身分驗證協定，使用名稱和密碼執行身分驗證。
 - **套用使用者名稱和密碼** - 使用使用者名和密碼執行身分驗證。
 - 需要時，輸入使用者名稱和密碼。
- 在“授權”塊中，清除或選中“**啟動應用程式時使用卡斯基安全管理中心作為代理伺服器**”。

6. 點擊“確定”。

將儲存設定的連線設定。

設定本機系統工作的排程啟動

您可以使用政策，根據管理群組中的每個電腦上本機配置的以下排程，允許或封鎖啟動本機系統自訂掃描工作和更新工作：

- 如果特定類型的本機系統工作的排程啟動受到政策禁止，則這些工作將不會按照排程在本機電腦上執行。您可以手動啟動該本機系統工作。

- 如果特定類型的本機系統工作的排程啟動被政策允許，則這些工作將按照為此工作進行的本機配置的排程參數來執行。

預設情況下，政策會禁止本機系統工作的啟動。

如果更新或自訂掃描受卡巴斯基安全管理中心群組工作的管理，我們建議不要允許本機系統工作啟動。

如果不使用群組更新或自訂掃描工作，則在政策中允許本機系統工作啟動：Kaspersky Embedded Systems Security 將執行應用程式資料庫和模組更新，並根據預設排程啟動所有本機系統的自訂掃描工作。

您可使用政策允許或封鎖以下本機系統工作的排程啟動：

- 自訂掃描工作：關鍵區域掃描、隔離區掃描、在作業系統啟動時掃描、應用程式完整性控制。
- 更新工作：資料庫更新、軟體模組更新和複製更新。

如果受防護電腦從管理群組中排除，則系統工作排程將自動啟用。

► 要在政策中允許或封鎖 Kaspersky Embedded Systems Security 系統工作的排程啟動，請執行以下步驟：

1. 展開管理主控台中的“**管理服務**”節點，展開所需的群組並在“**政策**”節點中選擇該群組。
2. 在“**政策**”標籤上，在用於配置電腦群組上的 Kaspersky Embedded Systems Security 系統工作排程啟動的政策右鍵選單中，選擇“**內容**”項
3. 在“**內容：<政策名稱>**”視窗中，開啟“**應用程式設定**”部分。在“**執行系統工作**”部分中，點擊“**設定**”按鈕並執行以下操作：
 - 選中“**允許啟動自訂掃描工作**”和“**允許啟動更新工作和複製更新工作**”核取方塊以允許所列工作的排程啟動。
 - 清除“**允許啟動自訂掃描工作**”和“**允許啟動更新工作和複製更新工作**”核取方塊以停用所列工作的排程啟動。

選擇或清除該核取方塊將不會影響任何此類本機自訂工作的啟動設定。

4. 確保您所配置的政策為活動政策且套用於選定電腦群組。

5. 點擊“確定”。

將為選定工作應用配置的排程工作啟動設定。

在卡巴斯基安全管理中心中配置隔離和備份設定

► 在卡巴斯基安全管理中心中管理一般備份設定：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“政策”標籤，然後開啟“內容：<政策名稱>”視窗（請參見第 144 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“裝置”標籤，然後開啟“應用程式設定”視窗（請參見第 150 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“應用程式設定”視窗中編輯這些設定。

4. 在“選項”部分中，點擊“儲存”子部分中的“設定”按鈕。
5. 使用“儲存”設定視窗的“備份”標籤配置以下備份設定：
 - 若要指定備份資料夾，請使用“備份資料夾”欄位在受防護電腦的本機硬碟上選擇所需的資料夾，或輸入資料夾的完整路徑。
 - 若要設定最大備份容量，請選定“最大備份空間(MB)”選擇方塊，然後在輸入欄位中指定此參數的值（單位為 MB）。
 - 若要設置備份中的可用空間值，請定義“最大備份空間(MB)”的設定值，選定“可用空間上限值(MB)”核取方塊並以 MB 為單位指定備份檔案夾中的最小可用空間值。
 - 若要為還原的物件指定資料夾，請在“還原設定”部分中選擇受防護電腦的本機硬碟上的相關資料夾，或者在“還原物件的指定資料夾”欄位中輸入資料夾名稱及其完整路徑。

6. 在“儲存”設定視窗的“隔離”標籤上，配置以下隔離設定：

- 若要變更隔離資料夾，請在“隔離”資料夾輸入欄位中指定受防護電腦本機硬碟上的資料夾完整路徑。
- 若要設定最大隔離容量，請選定“最大隔離區空間(MB)”核取方塊，然後在輸入欄位中指定此參數的值（單位為 MB）。
- 若要設定隔離儲存中的最小可用空間量，請選定“最大隔離區空間(MB)”核取方塊和“可用空間上限值(MB)”核取方塊，然後在輸入欄位中指定此參數值（單位為 MB）。
- 若要變更將隔離中的物件還原到指定資料夾，請在“還原物件的指定資料夾”輸入欄位中指定在受防護電腦本機硬碟上的資料夾完整路徑。

7. 點擊“確定”。

將儲存配置的隔離和備份設定。

配置記錄和通知

可以使用卡巴斯基安全管理中心管理主控台為管理員和使用者設定通知，以使其瞭解下列與 Kaspersky Embedded Systems Security 和受防護電腦上的防毒防護狀態有關的事件：

- 管理員可以收到有關選定類型事件的資訊；
- 存取受防護電腦的區域網路使用者和終端電腦使用者可以收到與偵測到的物件類型事件有關的資訊。

可使用選定電腦的“內容：<電腦名稱>”視窗為單個電腦，或使用選定管理群組的“內容：<政策名稱>”視窗中為一組電腦配置有關 Kaspersky Embedded Systems Security 事件的通知。

在“事件通知”標籤上或在“通知設定”視窗中，可以配置以下類型的通知：

- 可以使用“事件通知”選項（卡巴斯基安全管理中心應用程式的標準標籤）配置有關選定類型事件的管理員通知。有關通知方法的詳細資訊，請參閱 *卡巴斯基安全管理中心說明*。
- 在“通知設定”視窗中，可以配置管理員通知和使用者通知。

您可在視窗中或僅在標籤上配置某些事件種類的通知；您可使用視窗和標籤配置其他事件種類的通知。

如果同時在兩個標籤（“**事件通知**”標籤上和“**通知設定**”視窗中）上使用相同模式配置關於同一類型事件的通知，系統管理員將以相同的模式收到兩次這些事件的通知。

本章節說明項目

配置記錄設定.....	127
安全記錄.....	128
配置 SIEM 整合設定.....	128
配置通知設定.....	132
配置與管理伺服器的互動.....	134

配置記錄設定

► 要設定 Kaspersky Embedded Systems Security 記錄，請執行下列步驟：

1. 展開卡斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 [144](#) 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 [150](#) 頁上的“在卡斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**記錄和通知**”部分中，點擊“**工作記錄**”的“**設定**”按鈕。

5. 在“**記錄設定**”視窗中，根據您的需要定義以下 Kaspersky Embedded Systems Security 設定：
 - 配置記錄中的事件詳細等級。為此，請執行以下操作：
 - a. 在“**元件**”清單中，選擇您要設定其詳細等級的 Kaspersky Embedded Systems Security 元件。
 - b. 若要定義選定元件的工作記錄和系統稽核記錄中的詳細等級，請從“**重要性等級**”中選擇所需等級。
 - 要變更記錄的預設位置，請指定資料夾的絕對路徑，或點擊“**瀏覽**”按鈕進行選擇。
 - 指定工作記錄的儲存天數。
 - 指定“**系統稽核記錄**”節點中顯示的資訊儲存天數。
6. 點擊“**確定**”。

已儲存配置的記錄設定。

安全記錄

Kaspersky Embedded Systems Security 保持有與受防護電腦上的安全入侵或嘗試進行安全入侵相關的事件的記錄。本記錄中記錄以下事件：

- 弱點利用防禦事件。
- 關鍵記錄檢查事件。
- 表示嘗試進行安全入侵的緊急事件（對於“即時電腦防護”、“自訂掃描”、“檔案完整性監控”、“應用程式啟動控制”和“裝置控制”工作）。

您可以清除安全記錄以及系統稽核記錄（請參見第 [253](#) 頁上的“刪除系統稽核記錄中的事件”部分）。此外，Kaspersky Embedded Systems Security 記錄與清除安全記錄相關的系統稽核記錄事件。

配置 SIEM 整合設定

為了減小低效能裝置上的負載和降低由於應用程式記錄量增大而造成系統效能降級的風險，可以透過 Syslog 協定將稽核事件和工作效能事件的發佈配置到 *syslog 伺服器*。

syslog 伺服器是用於聚合事件 (SIEM) 的外部伺服器。它可以收集和分析接收到的事件，還可以執行管理記錄的其他操作。

可以在兩種模式中使用 SIEM 整合：

- **syslog 伺服器上的重複事件**：此模式指定其發佈在記錄設定中進行配置的所有工作效能事件，以及即使被傳送到 SIEM 後仍繼續儲存到本機電腦上的所有系統系統稽核記錄事件。

建議使用此模式，以便能夠最大限度地減小受防護電腦上的負載。

- **刪除事件的本機副本**：此模式指定將從本機電腦上刪除在應用程式執行過程中註冊和已發佈到 SIEM 的所有事件。

應用程式永遠不會刪除安全記錄的本機版本。

Kaspersky Embedded Systems Security 可以將應用程式記錄中的事件轉換為 syslog 伺服器支援的格式，以便這些事件能夠被傳輸和被 SIEM 成功識別。應用程式支援轉換為結構化資料格式和 JSON 格式。

為了降低將事件傳輸到 SIEM 不成功的風險，可以定義連線到映像 syslog 伺服器的設定。

映像 syslog 伺服器是一個額外的 syslog 伺服器，如果與主 syslog 伺服器的連線不可用或不能使用主要伺服器，應用程式會自動轉換到該伺服器。

預設情況下，不使用 SIEM 整合。可以啟用和停用 SIEM 整合，並配置功能性設定（請參見以下表格）。

表 10. SIEM 整合設定

設定	預設值	敘述
透過 syslog 協定傳送事件到遠端 syslog 伺服器	未套用	可以分別透過選擇或清除該核取方塊來啟用或停用 SIEM 整合。
刪除已被傳送到遠端 syslog 伺服器的事件本機副本	未套用	可以為儲存記錄的本機副本配置設定（透過選擇或清除該核取方塊將它們傳送到 SIEM 後）。
事件格式	結構化資料	可以選擇以下兩種格式之一，應用程式在將事件傳送到 syslog 伺服器以便 SIEM 能夠更好進行識別之前，將其事件轉換為該格式。

設定	預設值	敘述
連線協定	TCP	可以使用下拉清單來配置透過 UDP 或 TCP 協定與主 syslog 伺服器的連線，以及透過 TCP 協定與映像 syslog 伺服器的連線。
主 syslog 伺服器 連線設定	IP 位址： 127.0.0.1 連接埠：514	可以使用適當的欄位來配置用於連線到主 syslog 伺服器的 IP 位址和連接埠。 可以指定 IP 位址僅為 IPv4 格式。
如果無法存取主伺 服器則使用映像 syslog 伺服器	未套用	可以使用核取方塊來啟用或停用映像 syslog 伺服器。
映像 syslog 伺 服器連線設定	IP 位址： 127.0.0.1 連接埠：514	可以使用適當的欄位來配置用於連線到映像 syslog 伺服器的 IP 位址和連接埠。 可以指定 IP 位址僅為 IPv4 格式。

► 要配置 SIEM 整合設定：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“政策”標籤，然後開啟“內容：<政策名稱>”視窗（請參見第 144 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“裝置”標籤，然後開啟“應用程式設定”視窗（請參見第 150 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“應用程式設定”視窗中編輯這些設定。

4. 在“記錄和通知”部分中，點擊“工作記錄”的“設定”按鈕。

將開啟“記錄和通知設定”視窗。

5. 選擇“**SIEM 整合**”標籤。
6. 在“**整合設定**”部分中，選擇“**透過 syslog 協定傳送事件到遠端 syslog 伺服器**”核取方塊。

該核取方塊可啟用或停用將已發佈的事件傳送到外部 syslog 伺服器的功能。

如果選中該核取方塊，則應用程式將根據配置的 SIEM 整合設定將已發佈的事件傳送到 SIEM。

如果清除該核取方塊，則應用程式不執行 SIEM 整合。如果該核取方塊已被清除，則無法配置 SIEM 整合設定。

預設取消選定該核取方塊。

7. 如果需要，在“**整合設定**”部分中，選擇“**刪除已被傳送到遠端 syslog 伺服器的事件本機副本**”核取方塊。

該核取方塊可啟用或停用傳送到 SIEM 後記錄本機副本的刪除。

如果選中該核取方塊，則應用程式在事件被成功發佈到 SIEM 後刪除事件的本機副本。建議在低效能電腦上使用此模式。

如果清除該核取方塊，則應用程式僅將事件傳送到 SIEM。記錄的副本將繼續儲存在本機。

預設取消選定該核取方塊。

“**刪除已被傳送到遠端 syslog 伺服器的事件本機副本**”核取方塊的狀態不會影響儲存安全記錄檔案事件的設定：應用程式永遠不會自動刪除安全記錄事件。

8. 在“**事件格式**”部分中，指定您要將應用程式操作事件轉換為該格式的格式，以便能夠將它們傳送到 SIEM。

預設情況下，應用程式將它們轉換為結構化資料格式。

9. 在“**連線設定**”部分中：

- 指定 SIEM 連線協定。
- 指定用於連線到主 syslog 伺服器的設定。

可以僅指定 IP 位址為 IPv4 格式。

- 當無法傳送事件到主 syslog 伺服器時，如果想讓應用程式使用其他連線設定，請選中“**如果無法存取主伺服器則使用映像 syslog 伺服器**”核取方塊。

- 指定用於連線到映像 syslog 伺服器的設定：“**IP 位址**”和“**埠號**”。

如果已清除“**如果無法存取主伺服器則使用映像 syslog 伺服器**”核取方塊，則無法編輯映像 syslog 伺服器的“**IP 位址**”和“**埠號**”欄位。

可以僅指定 IP 位址為 IPv4 格式。

10. 點擊“**確定**”。

將套用已配置的 SIEM 整合設定。

配置通知設定

► 要設定 Kaspersky Embedded Systems Security 通知，請執行下列步驟：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 [144](#) 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 [150](#) 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“應用程式設定”視窗中編輯這些設定。

4. 在“記錄和通知”部分中，點擊“事件通知”子部分中的“設定”按鈕。
 5. 在“通知設定”視窗中，根據您的需要定義以下 Kaspersky Embedded Systems Security 設定：
 - 在“通知設定”清單中，選擇想要配置其設定的通知類型。
 - 在“通知使用者”部分中，配置使用者通知方式。如有必要，輸入通知訊息的文字。
 - 在“通知管理員”部分中，配置管理員通知方式。如有必要，輸入通知訊息的文字。如有必要，透過點擊“設定”按鈕配置附加通知設定。
 - 在“事件產生上限值”部分中，指定 Kaspersky Embedded Systems Security 記錄“應用程式資料庫已過期”、“應用程式資料庫已嚴重過期”和“已很長時間未執行關鍵區域掃描”事件的時間間隔。
 - **應用程式資料庫已過期 (天)**

自上次資料庫更新以來的天數。

預設值為 7 天。
 - **資料庫已長時間未更新 (天)**

自上次資料庫更新以來的天數。

預設值為 14 天。
 - **已很長時間未執行關鍵區域掃描 (天)**

上次成功完成關鍵區域掃描後的天數。

預設值為 30 天。
 6. 點擊“確定”。
- 將儲存設定的通知設定。

配置與管理伺服器的互動

► 要選擇 *Kaspersky Embedded Systems Security* 將其有關資訊傳送到卡斯基安全管理中心管理伺服器的物件類型：

1. 展開卡斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“政策”標籤，然後開啟“內容：<政策名稱>”視窗（請參見第 144 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“裝置”標籤，然後開啟“應用程式設定”視窗（請參見第 150 頁上的“在卡斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“應用程式設定”視窗中編輯這些設定。

4. 在“記錄和通知”部分中，點擊“與管理伺服器互動”設定塊中的“設定”按鈕。
將開啟“管理伺服器網路清單”視窗。
5. 在“管理伺服器網路清單”視窗中，選擇 *Kaspersky Embedded Systems Security* 將其有關資訊傳送到卡斯基安全管理中心管理伺服器的物件類型：
 - 隔離的物件。
 - 已備份物件。
6. 點擊“確定”。

Kaspersky Embedded Systems Security 會將有關選定物件類型的資訊傳送到管理伺服器。

建立和設定政策



本節提供有關使用卡斯基安全管理中心政策在多個電腦上管理 Kaspersky Embedded Systems Security 的資訊。



可以建立全域性卡斯基安全管理中心政策，以便管理多台已安裝 Kaspersky Embedded Systems Security 的電腦防護。


政策在一個管理群組中所有受防護電腦上實行該政策中指定的 Kaspersky Embedded Systems Security 設定、功能和工作。

可以為一個管理群組依次建立和實行多個政策。在管理主控台中，目前對某個群組有效的政策具有活動狀態。

Kaspersky Embedded Systems Security 系統稽核記錄中記錄了有關政策實行情況的資訊。可在應用程式主控台的“系統稽核記錄”節點中檢視該資訊。

卡斯基安全管理中心提供一種在本機電腦上套用政策的方式：**禁止變更設定**。當某個政策啟動時，Kaspersky Embedded Systems Security 將使用政策內容中所選  圖示旁的設定值，而不是使用套用政策前的這些設定值。Kaspersky Embedded Systems Security 不會套用政策內容中在其旁邊選擇了  圖示的活動政策設定的值。

如果政策為活動的，則政策中標記  圖示的設定的值在應用程式主控台中顯示，但無法編輯。其他設定的值（政策中標記  圖示）可在應用程式主控台中編輯。

活動政策中配置的且標記  圖示的設定也會封鎖在“內容：<電腦名稱>”視窗中變更一台電腦的卡斯基安全管理中心。

在停用活動政策後，使用活動政策指定併傳送到本機電腦的設定將儲存在本機工作設定中。

如果政策為任何“即時電腦防護”工作定義設定時，此工作若正在執行中，則一旦套用政策，便將立即修改該政策所定義的設定。如果該工作未執行，就會在啟動時套用其設定。

本章內容



建立政策	136
Kaspersky Embedded Systems Security 政策設定部分	139
設定政策	144

建立政策

建立政策的過程涉及下列步驟：

1. 使用政策精靈建立政策。可以使用精靈對話方塊配置即時電腦防護工作設定。
 2. 配置政策設定。在已建立政策的“內容：<政策名稱>”視窗中，您可以定義即時電腦防護工作設定、Kaspersky Embedded Systems Security 一般設定、隔離和備份設定、工作記錄的詳細等級以及有關 Kaspersky Embedded Systems Security 事件的使用者和管理員通知。
- 若要為一組執行已安裝 Kaspersky Embedded Systems Security 的電腦建立政策，請執行以下步驟：
1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點，然後選擇包含您希望為其建立政策的電腦的管理群組。
 2. 在選定管理群組的詳細資訊視窗中，選擇“政策”標籤，然後點擊“建立政策”連結以啟動精靈並建立政策。
將開啟“新建政策精靈”視窗。
 3. 在“選擇要為其建立群組政策的應用程式”視窗中，選擇 Kaspersky Embedded Systems Security，然後點擊“下一步”。
 4. 在“名稱”欄位中輸入群組政策名稱。

政策名稱不能包含以下符號：" * < : > ? \ |。

5. 要套用先前應用程式版本使用的政策設定：
 - a. 選中“使用先前應用程式版本的政策設定”核取方塊。
 - b. 點擊“選擇”按鈕。
 - c. 選擇要套用的政策。
 - d. 點擊“下一步”。
6. 在“選擇操作類型”視窗中，選擇以下選項之一：
 - “新增”，以建立具有預設設定的新政策。
 - “匯入使用以前版本的 Kaspersky Embedded Systems Security 建立的政策”，以將該版本政策用作範本。
 - 點擊“瀏覽”，然後選擇儲存現有政策的設定檔。
7. 在“即時電腦防護”視窗中，根據需要配置“即時檔案防護”、“KSN 使用”工作和弱點利用防禦功能。允許或封鎖在網路上的本機電腦上使用配置的政策工作：
 - 點擊  按鈕允許變更網路電腦上的工作設定，並封鎖套用政策中配置的工作設定。
 - 點擊  按鈕拒絕變更網路電腦上的工作設定，並允許套用政策中配置的工作設定。

新建立的政策使用即時電腦防護工作的預設設定。

- 要編輯“即時檔案防護”工作的預設設定，請點擊“即時檔案防護”子部分中的“設定”按鈕。在開啟的視窗中，根據需要設定工作。點擊“確定”。
- 要編輯“KSN 使用”工作的預設設定，請點擊“KSN 使用”子部分中的“設定”按鈕。在開啟的視窗中，根據需要設定工作。點擊“確定”。

要啟動“KSN 使用”工作，您需要接受“資料處理”視窗中的 KSN 聲明（請參見第 [352](#) 頁上的“透過管理外掛程式配置資料處理”部分）。

- 要編輯“弱點利用防禦”元件的預設設定，請點擊“弱點利用防禦”子部分中的“設定”按鈕。在開啟的視窗中，根據需要設定該功能。點擊“確定”。

8. 在“為應用程式建立群組政策”視窗中選擇下列之一的政策狀態：

- “活動政策”，如果您希望在建立政策後立即套用該政策。如果群組中已經存在活動政策，則會將其停用並套用新政策。
- “非活動政策”，如果您不希望立即套用所建立的政策。在此情況下，可在之後啟動該政策。
- 選中“建立政策後立即開啟政策內容”核取方塊以在點擊“下一步”按鈕後自動關閉新建政策精靈並設定新建立的政策。

9. 點擊“完成”按鈕。

所建立的政策將顯示在選定管理群組的“政策”標籤上的政策清單中。在“內容：<政策名稱>”視窗中，您可配置 Kaspersky Embedded Systems Security 的其他設定、工作和功能。

Kaspersky Embedded Systems Security 政策設定部分

一般

在“一般”部分中，您可配置以下政策設定：

- 指定政策狀態。
- 為子政策設定繼承父政策的設定。

事件配置

在“事件配置”部分中，您可配置以下事件類別的設定：

- 緊急事件
- 功能故障
- 警告
- 資訊訊息

可以使用“內容”按鈕來配置選定事件的以下設定：

- 指定有關記錄事件的資訊的儲存位置和保留期限。
- 指定有關記錄事件的通知方式。

應用程式設定

表 11. 應用程式設定的設定部分

部分	選項
延伸性和介面	<p>在“延伸性和介面”子部分中，可以點擊“設定”按鈕來配置以下設定：</p> <ul style="list-style-type: none"> • 選擇手動或自動配置延伸性設定。 • 配置應用程式圖示顯示設定。
安全性	<p>在“安全性”子部分中，可以點擊“設定”按鈕來配置以下設定：</p> <ul style="list-style-type: none"> • 配置工作執行設定。 • 指定當電腦使用 UPS 電源執行時應用程式的行為。 • 啟用或停用應用程式功能的密碼防護。

部分	選項
連線	<p>在“連線”子部分中，可以使用“設定”按鈕來配置與更新伺服器、啟動伺服器和 KSN 連線的以下代理伺服器設定：</p> <ul style="list-style-type: none"> • 配置代理伺服器設定 • 指定代理伺服器身分驗證設定。
執行系統工作	<p>在“執行系統工作”子部分中，可以使用“設定”按鈕來根據本機電腦上配置的排程允許或封鎖啟動以下系統工作：</p> <ul style="list-style-type: none"> • 自訂掃描工作。 • 更新工作和複製更新工作。

選項

表 12. 選項的設定部分

部分	選項
信任區域	<p>點擊“信任區域”子部分上的“設定”按鈕，以配置以下信任區域應用程式設定：</p> <ul style="list-style-type: none"> • 建立信任區域排除項目清單。 • 啟用或停用檔案備份操作的掃描。 • 建立受信任處理程序清單。
卸除式磁碟機掃描	<p>在“卸除式磁碟機掃描”子部分中，可以使用“設定”按鈕來配置卸除式 USB 磁碟機的掃描設定。</p>
應用程式管理的使用者存取權限	<p>在“應用程式管理的使用者存取權限”子部分中，可以配置管理 Kaspersky Embedded Systems Security 的使用者權限和使用者的群組權限。</p>
Security 服務管理的使用者存取權限	<p>在“Security 服務管理的使用者存取權限”子部分中，可以配置管理 Kaspersky Security 服務的使用者權限和使用者的群組權限。</p>

部分	選項
儲存	<p>在“儲存”子部分中，點擊“設定”按鈕以配置以下“隔離”、“備份”和“封鎖的主機”設定：</p> <ul style="list-style-type: none"> • 指定想要放置隔離或備份物件的資料夾路徑。 • 設定備份和隔離的最大大小，並指定可用空間上限值。 • 指定想要放置隔離或備份還原物件的資料夾路徑。 • 配置主機封鎖期限。

即時電腦防護

表 13. “即時電腦防護的設定”部分

部分	選項
即時檔案防護	<p>在“即時檔案防護”子部分中，可以點擊“設定”按鈕來配置以下工作設定：</p> <ul style="list-style-type: none"> • 指定防護模式。 • 配置啟發式分析的使用。 • 配置信任區域的使用。 • 指定防護範圍。 • 設定選定防護範圍的安全等級：您可選擇預設的安全等級或手動配置安全性設定。 • 配置工作啟動設定。

KSN 使用	<p>在“KSN 使用”子部分中，可以點擊“設定”按鈕來配置以下工作設定：</p> <ul style="list-style-type: none"> • 指定要對 KSN 不信任的物件執行的操作。 • 配置卡斯基安全管理中心作為 KSN 代理伺服器的資料傳輸和使用。 <p>點擊“資料處理”按鈕可接受或拒絕 KSN 聲明和 KMP 聲明，並設定可靠的資料交換設定。</p>
弱點利用防禦	<p>在“弱點利用防禦”子部分中，可以點擊“設定”按鈕來配置以下工作設定：</p> <ul style="list-style-type: none"> • 選擇處理程序記憶體防護模式。 • 指定降低弱點利用風險的操作。 • 新增到和編輯受防護的處理程序清單。

本機行為控制

表 14. “本機行為控制的設定”部分

部分	選項
應用程式啟動控制	<p>在“應用程式啟動控制”子部分中，可以點擊“設定”按鈕來配置以下工作設定：</p> <ul style="list-style-type: none"> • 選擇工作執行模式。 • 配置控制隨後應用程式啟動的設定。 • 指定應用程式啟動控制規則的套用範圍。 • 配置 KSN 的使用。 • 配置工作啟動設定。
裝置控制	<p>在“裝置控制”子部分中，可以點擊“設定”按鈕來配置以下工作設定：</p> <ul style="list-style-type: none"> • 選擇工作執行模式。 • 配置工作啟動設定。

網路行為控制

表 15. 網路行為控制的設定部分

部分	選項

防火牆管理	<p>在“防火牆管理”子部分中，可以點擊“設定”按鈕來配置以下工作設定：</p> <ul style="list-style-type: none"> • 刪除防火牆規則。 • 配置工作啟動設定。
--------------	--

系統稽核

表 16. 系統稽核的設定部分

部分	選項
檔案完整性監控	<p>在“檔案完整性監控”子部分中，可以配置表示受防護電腦上存在安全衝突的檔案變更的控制。</p>
記錄審查	<p>在“記錄審查”子部分中，可以根據 Windows 事件記錄分析結果配置受防護電腦的完整性控制。</p>

記錄和通知

表 17. 記錄和通知的設定部分

部分	選項
工作記錄	<p>在“工作記錄”子部分中，可以點擊“設定”按鈕以配置以下設定：</p> <ul style="list-style-type: none"> • 為選定的軟體元件指定記錄事件的重要性等級。 • 指定工作記錄儲存設定。 • 指定 SIEM 與卡巴斯基安全管理中心整合的設定。
事件通知	<p>在“事件通知”子部分中，可以點擊“設定”按鈕以配置以下設定：</p> <ul style="list-style-type: none"> • 指定“偵測到物件”事件、“偵測到並限制不受信任的大容量儲存”事件和“主機已列為不受信任”事件的使用者通知設定。 • 為“通知設定”部分中的事件清單中選定的任何事件指定管理員通知設定。

與管理伺服器 互動	在“ 與管理伺服器互動 ”部分中，可以點擊“ 設定 ”按鈕來選擇 Kaspersky Embedded Systems Security 將報告給管理伺服器的物件類型。您還可以配置關於隔離和備份物件到管理伺服器的資訊的傳輸。
----------------------	--

要檢視有關“網路附加儲存防護”工作的詳細資訊，請參見 [Kaspersky Embedded Systems Security 網路附加儲存防護實施手冊](#)。

修訂歷史

在“**修訂歷史**”部分中，可以管理修訂：與目前版本或其他政策對比、新增修訂說明、儲存修訂到檔案或執行回溯。

設定政策

在現有政策的“**內容 :<政策名稱>**”視窗中，您可以配置一般 Kaspersky Embedded Systems Security 設定、隔離和備份設定、信任區域設定、即時電腦防護設定、本機行為控制設定、工作記錄的詳細等級以及有關 Kaspersky Embedded Systems Security 事件的使用者和管理員通知，用於管理應用程式和 Kaspersky Security 服務的存取權限以及政策設定檔應用程式設定。

► 要配置政策設定：

1. 在卡斯基安全管理中心的管理主控台樹狀目錄中展開“**受管理裝置**”節點。
2. 展開您希望為其配置關聯政策設定的管理群組，然後開啟詳細資訊視窗中的“**政策**”標籤。
3. 選擇您想要設定的政策，然後使用以下方法之一開啟“**內容 :<政策名稱>**”視窗：
 - 在政策的內容功能表中選擇“**內容**”選項。
 - 在所選政策的右側詳細資訊視窗中，點擊“**配置政策**”連結。
 - 點擊所選政策。

4. 在“**政策狀態**”部分的“**一般**”標籤下，啟用或停用政策。為此，請選擇以下一個選項：
 - **活動政策**，如果您希望在選定管理群組內的所有電腦上套用政策。
 - **非活動政策**，如果您不希望以後在選定管理群組內的所有電腦上啟動政策。

當管理 Kaspersky Embedded Systems Security 時，“**漫遊政策**”設定不可用。

5. 在“**事件配置**”、“**應用程式設定**”、“**選項**”、“**記錄和通知**”以及“**修訂歷程**”部分中，可以修改應用程式配置（請參見以下表格）。
6. 在“**即時電腦防護**”、“**本機行為控制**”、“**網路行為控制**”和“**系統稽核**”部分中，配置應用程式設定和應用程式啟動設定（請參見以下表格）。

您可透過卡巴斯基安全管理中心政策啟用或停用在管理群組內的所有電腦上執行任何工作。
您可為每個單個軟體元件配置在所有網路電腦上套用政策設定。

7. 點擊“**確定**”。

將在政策中套用配置的設定。

使用卡巴斯基安全管理中心建立和管理工作

本節包含有關 Kaspersky Embedded Systems Security 工作、如何建立工作、配置工作設定，以及啟動和停止工作的資訊。

本章內容

關於卡巴斯基安全管理中心中的工作建立.....	146
使用卡巴斯基安全管理中心建立工作.....	147
在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作.....	150
在卡巴斯基安全管理中心中設定群組工作.....	151
在卡巴斯基安全管理中心中設定當機診斷設定.....	161
管理工作排程.....	164

關於卡巴斯基安全管理中心中的工作建立

您可為管理群組和電腦集建立群組工作。您可建立以下工作類型：

- 啟動應用程式
- 複製更新
- 資料庫更新
- 軟體模組更新
- 資料庫更新回溯
- 自訂掃描
- 應用程式完整性控制
- 應用程式啟動控制規則產生器
- 裝置控制規則產生器

您可採用以下方式建立本機和群組工作：

- 對於一台電腦：在“內容 <電腦名稱>”視窗的“工作”部分中。
- 對於管理群組：在選定電腦群組的節點的詳細資訊視窗中的“工作”標籤上。
- 對於一組電腦：在“裝置選擇”節點的詳細資訊視窗中。

使用政策可以停用同一管理群組的所有受防護電腦上的更新和自訂掃描本機系統工作的排程（請參見第 123 頁上的“配置本機系統工作的排程啟動”部分）。

有關卡巴斯基安全管理中心工作的一般資訊，請參閱 *卡巴斯基安全管理中心說明*。

使用卡巴斯基安全管理中心建立工作

► 要在卡巴斯基安全管理中心管理主控台中建立新工作：

1. 採用以下方式之一啟動工作精靈：
 - 若要建立本機工作，請執行以下步驟：
 - a. 展開管理主控台樹狀目錄中的“受管理裝置”節點，然後選擇受防護電腦所屬的群組。
 - b. 在詳細資訊視窗的“裝置”標籤上，開啟受防護電腦的內容功能表，然後選擇“內容”。
 - c. 在開啟的視窗中，點擊“工作”部分中的“新增”按鈕。
 - 建立群組工作：
 - a. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
 - b. 選取要為其建立工作的管理群組。
 - c. 在詳細資訊視窗中，開啟“工作”標籤，然後選擇“建立工作”。
 - 要為自訂的一組電腦建立工作：
 - a. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
 - b. 選擇包含這些電腦的管理群組。

- c. 選擇一台或自訂的一組電腦。
- d. 從“**執行操作**”下拉清單中，選擇“**建立工作**”選項。

將開啟工作精靈視窗。

2. 在標題 **Kaspersky Embedded Systems Security** 下的“**選擇工作類型**”視窗中，選擇要建立的工作的類型。
3. 如果選擇了除“**資料庫更新回溯**”、“**應用程式完整性控制**”或“**應用程式啟動**”外的任何工作類型，將開啟“**設定**”視窗。根據工作類型，設定可能有所變化：
 - 建立自訂掃描工作（請參見第 [516](#) 頁上的“**建立自訂掃描工作**”部分）。
 - 要建立更新工作，請根據您的需要配置工作設定：
 - a. 在“**更新來源**”視窗中選擇更新來源。
 - b. 點擊“**連線設定**”按鈕。將開啟“**連線設定**”視窗。
 - c. 在“**連線設定**”視窗上：
 - 指定用於連線到受防護電腦的 FTP 伺服器模式。
 - 根據需要修改連線到更新源來時的連線逾時值。
 - 配置連線到更新來源時的代理伺服器存取設定。
 - 指定受防護電腦的位置，以便最佳化更新下載。
 - 若要建立“**軟體模組更新**”工作，請在“**有關應用程式軟體模組更新的設定**”視窗中配置所需程式模組更新設定：
 - a. 選擇複製並安裝關鍵軟體模組更新，或者僅檢查它們的可用性而不安裝。
 - b. 如果選擇了“**複製並安裝軟體模組的重要更新**”：可能需要重新開機電腦才能套用已安裝的軟體模組。如果希望工作完成時 Kaspersky Embedded Systems Security 自動重新啟動電腦，請選定“**允許作業系統重新啟動**”核取方塊。
 - c. 若要獲得有關 Kaspersky Embedded Systems Security 模組升級的資訊，請選擇“**接收有關可用的排程軟體模組更新的資訊**”。

Kaspersky Lab 不會在更新伺服器上發佈排程的軟體更新套件以供自動安裝；您可以手動從 Kaspersky Lab 網站下載這些軟體更新套件。您可以設定有關“有新的排程軟體模組更新可用”事件的管理員通知。該通知將包含我們網站的 URL，以便您從中下載排程的更新。

- 若要建立“複製更新”工作，請在“複製更新設定”視窗中指定更新和目的資料夾。
 - 要建立“應用程式啟動”工作：
 - a. 在“啟動設定”視窗中，指定您要使用的金鑰檔案來啟動應用程式。
 - b. 如果您想要建立用於續約產品授權的工作，請選中“作為備用金鑰使用”核取方塊。
 - 建立“應用程式啟動控制規則產生器”工作（請參見第 [399](#) 頁上的“建立‘應用程式啟動控制規則產生器’工作”部分）。
 - 建立“裝置控制規則產生器”工作（請參見第 [447](#) 頁上的“建立‘裝置控制規則產生器’工作”部分）。
4. 配置工作啟動（請參見第 [164](#) 頁上的“配置工作啟動排程設定”部分）（您可以為除了“資料庫更新回溯”工作外的所有工作類型配置排程）。
 5. 點擊“確定”。
 6. 如果是為一組電腦建立的工作，則請選擇將在其中執行此工作的電腦網路（或群組）。
 7. 在“選擇帳戶以執行工作”視窗中，指定您希望執行工作的帳戶。
 8. 在“定義工作名稱”視窗中，輸入工作名稱（不超過 100 個字元），不包含符號 “* < > ? \ | :”。
建議將工作類型新增到它的名稱中（例如，“共用資料夾的自訂掃描”）。
 9. 如果希望在建立工作後不久啟動它，則在“完成建立工作”視窗中，選中“精靈完成後執行工作”核取方塊。點擊“完成”按鈕。

建立的工作將會在“工作”清單中顯示。

在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作

► 要設定單台網路電腦的本機工作或一般應用程式設定：

1. 展開卡巴斯基安全管理中心管理電腦樹狀結構中的“**受管理裝置**”節點，選擇受防護電腦所屬的群組。
2. 在詳細資訊視窗中，選擇“**裝置**”標籤。
3. 採用以下方法之一開啟“**內容：<電腦名稱>**”視窗：
 - 點擊受防護電腦的名稱。
 - 開啟受防護電腦名稱的內容功能表，然後選擇“**內容**”。

將開啟“**內容：<電腦名稱>**”視窗。

4. 若要設定本機工作設定，請執行以下步驟：
 - a. 轉至“**工作**”部分。
 - 在工作清單中，選擇要配置的本機工作。
 - 在工作清單中點擊工作名稱。
 - 選擇工作名稱，然後點擊“**內容**”按鈕。
 - 在所選工作的內容功能表中，選擇“**內容**”。

將開啟“**內容：<工作名稱>**”視窗。

5. 若要設定應用程式設定，請執行以下步驟：
 - a. 轉至“**應用程式**”部分。
 - 在安裝的應用程式清單中，選擇要配置的應用程式。
 - 在安裝的應用程式清單中點兩下應用程式名稱。
 - 在安裝的應用程式清單中選擇應用程式名稱，然後點擊“**內容**”按鈕。
 - 在安裝程式的單中開啟應用程式名稱的內容功能表，然後選擇“**內容**”項。

將開啟“**<應用程式名稱>設定**”視窗。

如果應用程式目前受卡斯基安全管理中心政策管控，且該政策禁止變更應用程式設定，則無法透過“<應用程式名稱>設定”視窗編輯這些設定。

在卡斯基安全管理中心中設定群組工作

► 要為多台電腦配置群組工作：

1. 在卡斯基安全管理中心管理主控台樹狀目錄中，展開“受管理裝置”節點，然後選擇要為其配置應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“工作”標籤。
3. 在先前建立的組工作清單中，選擇您要配置的工作。採用以下方法之一開啟“內容：<工作名稱>”視窗：
 - 在建立的工作清單中點擊工作名稱。
 - 在建立的工作清單中選擇工作名稱，然後點擊“配置工作”連結。
 - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇“內容”項。
4. 在“通知”部分中，配置工作事件通知設定。

關於此節中配置設定的詳細資訊，請參見卡斯基安全管理中心說明。

5. 根據配置的工作類型，執行下列一種操作：
 - 要設定自訂掃描工作：
 - a. 在“掃描範圍”部分中，配置掃描範圍。
 - b. 在“選項”部分中，配置工作優先順序水準及與其他軟體元件的整合。
 - 要配置更新工作，請根據您的需要調整工作設定：
 - a. 在“設定”部分中，配置更新來源設定和磁碟子系統使用情況最佳化。
 - b. 點擊“連線設定”按鈕以配置更新來源連線設定。

- 若要配置“軟體模組更新”工作，在“**有關應用程式軟體模組更新的設定**”部分中選擇要執行的操作：複製並安裝應用程式模組的重要更新或僅進行檢查。
 - 若要配置“複製更新”工作，請在“**複製更新設定**”視窗中指定更新和目的資料夾。
 - 若要配置“應用程式啟動工作”，在“**啟動設定**”部分中套用要用於啟動應用程式的金鑰檔案。如果您想要新增用於續約產品授權的啟動碼或金鑰檔案，請選中“**作為備用金鑰使用**”核取方塊。
 - 若要配置電腦控制的允許規則的自動建立，請在“**設定**”部分中，指定建立允許規則清單所依據的設定。
6. 在“**排程**”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。
 7. 在“**帳戶**”部分中，指定將使用其權限執行工作的帳戶。關於此節中配置設定的詳細資訊，請參見 *卡巴斯基安全管理中心說明*。
 8. 如有需要，在“**工作範圍的排除項目**”部分中指定要從工作範圍中排除的物件。關於此節中配置設定的詳細資訊，請參見 *卡巴斯基安全管理中心說明*。
 9. 在“**內容：<工作名稱>**”視窗中，點擊“**確定**”。

將儲存新配置的群組工作設定。

下表匯總了可用於配置的群組工作設定。

表 18. *Kaspersky Embedded Systems Security* 群組工作設定

Kaspersky Embedded Systems Security 工作類型	“內容：<工作名稱>”視窗中的部分	工作設定
應用程式啟動控制規則產生器	設定	在配置“應用程式啟動控制規則產生器”工作設定時，您可以： <ul style="list-style-type: none"> • 基於正在執行的應用程式建立允許規則； • 為以下資料夾中的應用程式建立允許規則；

Kaspersky Embedded Systems Security 工作類型	“內容 :<工作名稱>” 視窗中的部分	工作設定
	選項	當建立應用程式啟動控制的允許規則時，您可以指定執行的操作： <ul style="list-style-type: none"> • 使用數位憑證 • 使用數位憑證主旨和指紋 • 憑證遺失則使用 • 使用 SHA256 雜湊 • 為使用者或使用者群組產生規則 您可以使用 Kaspersky Embedded Systems Security 在工作完成時建立的允許規則清單為設定檔配置設定。
	排程	您可以配置排程的工作啟動設定。
裝置控制規則產生器	設定	<ul style="list-style-type: none"> • 選擇執行模式：考慮有關之前曾連線過的所有大容量儲存的系統資料，或僅考慮目前連線的大容量儲存。 • 使用 Kaspersky Embedded Systems Security 在工作完成時建立的允許規則清單為設定檔配置設定。
	排程	您可以配置排程的工作啟動設定。
應用程式啟動（請參見第 157 頁上的“應用程式啟動工作”部分）	啟動設定	若要啟動應用程式或續約產品授權，可以新增金鑰檔案。
	排程	您可以配置排程的工作啟動設定。

Kaspersky Embedded Systems Security 工作類型	“內容 :<工作名稱>”視窗中的部分	工作設定
複製更新 (請參見第 158 頁上的“更新工作”部分)	更新來源	<p>您可以將卡斯基安全管理中心管理伺服器或 Kaspersky Lab 更新伺服器指定為應用程式更新來源。您也可以建立自訂更新來源清單：透過手動新增自訂 HTTP 和 FTP 伺服器或網路資料夾，並將他們設定為更新來源。</p> <p>如果手動自訂的伺服器不可用，您可指定使用 Kaspersky Lab 更新伺服器。</p>
	“連線設定”視窗	<p>在連結自“更新來源”部分的“連線設定”視窗中，您可指定是否應透過代理伺服器與 Kaspersky Lab 更新伺服器或任何其他伺服器建立連線。</p>
	複製更新設定	<p>您可指定用於複製的更新集。</p> <p>在“用於本機儲存已複製更新的資料夾”欄位中，指定 Kaspersky Embedded Systems Security 將用於儲存已複製更新的資料夾的路徑。</p>
	排程	<p>您可以配置排程的工作啟動設定。</p>

Kaspersky Embedded Systems Security 工作類型	“內容 :<工作名稱>”視窗中的部分	工作設定
資料庫更新 (請參見第 158 頁上的“更新工作”部分)	設定	<p>您可在“更新來源”部分中將卡斯基安全管理中心管理伺服器或 Kaspersky Lab 更新伺服器指定為應用程式更新來源。您也可以建立自訂更新來源清單：透過手動新增自訂 HTTP 和 FTP 伺服器或網路資料夾，並將他們設定為更新來源。</p> <p>如果手動自訂的伺服器不可用，您可指定使用 Kaspersky Lab 更新伺服器。</p> <p>在“磁碟 I/O 使用最佳化”部分中，您可以配置能夠減少磁碟子系統工作負載的功能：</p> <ul style="list-style-type: none"> • 降低磁碟 I/O 上的負載 • 用於最佳化 RAM(MB)
	“連線設定”視窗	<p>在連結自“更新來源”部分的“連線設定”視窗中，您可指定是否應透過代理伺服器與 Kaspersky Lab 更新伺服器或任何其他伺服器建立連線。</p>
	排程	<p>您可以配置排程的工作啟動設定。</p>
軟體模組更新 (請參見第 158 頁上的“更新工作”部分)	更新來源	<p>您可以將卡斯基安全管理中心管理伺服器或 Kaspersky Lab 更新伺服器指定為應用程式更新來源。您也可以建立自訂更新來源清單：透過手動新增自訂 HTTP 和 FTP 伺服器或網路資料夾，並將他們設定為更新來源。</p> <p>如果手動自訂的伺服器不可用，您可指定使用 Kaspersky Lab 更新伺服器。</p>
	“連線設定”視窗	<p>在“更新來源連線設定”部分中，您可指定是否應透過代理伺服器與 Kaspersky Lab 更新伺服器或任何其他伺服器建立連線。</p>

Kaspersky Embedded Systems Security 工作類型	“內容 :<工作名稱>”視窗中的部分	工作設定
	有關應用程式軟體模組更新的設定	您可指定關鍵軟體模組更新可用或已安裝時 Kaspersky Embedded Systems Security 應執行的操作，還可指定 Kaspersky Embedded Systems Security 是否應接收有關排程的更新的資訊。
	排程	您可以配置排程的工作啟動設定。
自訂掃描設定 (請參見第 516 頁上的“建立自訂掃描工作”部分)	掃描範圍	您可指定“自訂掃描”工作的掃描範圍，並配置安全等級設定。
	“自訂掃描設定”視窗	在連結自“掃描範圍”部分的“自訂掃描設定”視窗中，可以選擇預定義安全等級之一，或手動自訂安全等級。
	選項	您可啟動或取消啟動為“自訂掃描”工作使用啟發式分析，並在“ 啟發式分析 ”部分中使用滑塊設定分析等級。 在“ 與其他元件整合 ”部分中，可以配置以下設定： <ul style="list-style-type: none"> • “為自訂掃描套用信任區域”工作。 • “為自訂掃描應用 KSN 使用”工作。 • 設定“自訂掃描”工作的優先順序：在背景模式下執行工作 (低優先順序) 或將工作視為關鍵區域掃描。
	排程	您可以配置排程的工作啟動設定。
應用程式完整性控制 (請參見第 160 頁)	排程	您可以配置排程的工作啟動設定。

對於“資料庫更新回溯”工作，可以在“通知”和“工作範圍的排除項目”部分中僅配置標準工作設定（由卡巴斯基安全管理中心控制）。

有關這些部分的設定配置的詳細資訊，請參閱 *卡巴斯基安全管理中心說明*。

本章節說明項目

啟動應用程式工作	157
更新工作	158
應用程式完整性控制	160

啟動應用程式工作

► 若要配置啟動應用程式工作，請執行以下步驟：

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開“受管理裝置”節點，然後選擇要為其配置應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“工作”標籤。
3. 在先前建立的組工作清單中，選擇您要配置的工作。採用以下方法之一開啟“內容：<工作名稱>”視窗：
 - 在建立的工作清單中點擊工作名稱。
 - 在建立的工作清單中選擇工作名稱，然後點擊“配置工作”連結。
 - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇“內容”項。
4. 在“通知”部分中，配置工作事件通知設定。

關於此節中配置設定的詳細資訊，請參見 *卡巴斯基安全管理中心說明*。

5. 在“**啟動設定**”部分中，指定您要使用的金鑰檔案來啟動應用程式。如果您想要新增用於延長產品授權的金鑰，請選中“**作為備用金鑰使用**”核取方塊。
6. 在“**排程**”部分中配置工作排程（您可以為除“**資料庫更新回溯**”以外的所有工作類型配置排程）。
7. 在“**帳戶**”部分中，指定將使用其權限執行工作的帳戶。
8. 如有需要，在“**工作範圍的排除項目**”部分中指定要從工作範圍中排除的物件。

有關此節中配置設定的詳細資訊，請參見 [卡巴斯基安全管理中心說明](#)。

9. 在“**內容：<工作名稱>**”視窗中，點擊“**確定**”。

將儲存新配置的群組工作設定。

更新工作

► 要配置複製更新、資料庫更新或軟體模組更新工作，請執行以下操作：

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開“**受管理裝置**”節點，然後選擇要為其配置應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“**工作**”標籤。
3. 在先前建立的組工作清單中，選擇您要配置的工作。採用以下方法之一開啟“**內容：<工作名稱>**”視窗：
 - 在建立的工作清單中點擊工作名稱。
 - 在建立的工作清單中選擇工作名稱，然後點擊“**配置工作**”連結。
 - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇“**內容**”項。
4. 在“**通知**”部分中，配置工作事件通知設定。

關於此節中配置設定的詳細資訊，請參見 [卡巴斯基安全管理中心說明](#)。

5. 根據配置的工作類型，執行下列一種操作：
 - 在“**更新來源**”部分中，配置更新來源設定和磁碟子系統使用方式最佳化。

- a. 您可在“**更新來源**”部分中將卡斯基安全管理中心管理伺服器或 Kaspersky Lab 更新伺服器指定為應用程式更新來源。您也可以建立自訂更新來源清單：透過手動新增自訂 HTTP 和 FTP 伺服器或網路資料夾，並將他們設定為更新來源。

如果手動自訂的伺服器不可用，您可指定使用 Kaspersky Lab 更新伺服器。

- b. 在資料庫更新工作的“**磁碟 I/O 使用最佳化**”部分中，可以配置能夠減少磁碟子系統工作負載的功能：

- **降低磁碟 I/O 上的負載**

使用此核取方塊可以啟用或停用透過將更新檔案儲存在記憶體中的虛擬磁碟機上實現磁碟子系統最佳化的功能。

如果選中該核取方塊，則啟用該功能。

預設取消選定該核取方塊。

- **用於最佳化 RAM(MB)**

應用程式用於儲存更新檔案的記憶體的大小（以 MB 為單位）。預設記憶體大小為 512 MB。最小記憶體大小為 400 MB。

- c. 點擊“**連線設定**”按鈕，然後在開啟的“**連線設定**”視窗中，為連線到 Kaspersky Lab 更新伺服器和其他伺服器配置代理伺服器的使用。
- 在軟體模組更新工作的“**有關應用程式軟體模組更新的設定**”部分中，可以指定當有可用的關鍵軟體模組更新或有可用的關於排程更新的資訊時，Kaspersky Embedded Systems Security 執行什麼操作，還可以指定當安裝關鍵更新時 Kaspersky Embedded Systems Security 應執行哪種操作。
 - 在“**複製更新設定**”部分中，為“複製更新”工作指定更新集和目的資料夾。
6. 在“**排程**”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。
 7. 在“**帳戶**”部分中，指定將使用其權限執行工作的帳戶。

有關此節中配置設定的詳細資訊，請參見卡斯基安全管理中心說明。

8. 在“內容：<工作名稱>”視窗中，點擊“確定”。

將儲存新配置的群組工作設定。

對於“資料庫更新回溯”工作，可在“通知”和“工作範圍的排除項目”部分中僅配置由卡巴斯基安全管理中心控制的標準工作設定。有關此節中配置設定的詳細資訊，請參見 *卡巴斯基安全管理中心說明*。

應用程式完整性控制

► 要配置“應用程式完整性控制”群組工作：

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開“受管理裝置”節點，然後選擇要為其配置應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟“工作”標籤。
3. 在先前建立的組工作清單中，選擇您要配置的工作。採用以下方法之一開啟“內容：<工作名稱>”視窗：
 - 在建立的工作清單中點擊工作名稱。
 - 在建立的工作清單中選擇工作名稱，然後點擊“配置工作”連結。
 - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇“內容”項。
4. 在“通知”部分中，配置工作事件通知設定。

關於此節中配置設定的詳細資訊，請參見 *卡巴斯基安全管理中心說明*。

5. 在“裝置”部分中，選擇要為其配置“應用程式完整性控制”工作的裝置。
6. 在“排程”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。
7. 在“帳戶”部分中，指定將使用其權限執行工作的帳戶。
8. 如有需要，在“工作範圍的排除項目”部分中指定要從工作範圍中排除的物件。

有關此節中配置設定的詳細資訊，請參見 *卡巴斯基安全管理中心說明*。

9. 在“內容：<工作名稱>”視窗中，點擊“確定”。

將儲存新配置的群組工作設定。

在卡巴斯基安全管理中心中設定當機診斷設定

如果 Kaspersky Embedded Systems Security 執行期間發生問題（例如，Kaspersky Embedded Systems Security 當機），且您想要進行診斷，您可啟用建立 Kaspersky Embedded Systems Security 處理程序的偵錯檔案和傾印檔案，並將這些檔案傳送到 Kaspersky Lab 技術支援進行分析。

Kaspersky Embedded Systems Security 不會自動傳送任何偵錯或傾印檔案。診斷資料只能由具有相應權限的使用者傳送。

Kaspersky Embedded Systems Security 會以未加密的形式將資訊寫入到偵錯檔案和傾印檔案。儲存檔案的資料夾由使用者選擇，由作業系統配置和 Kaspersky Embedded Systems Security 設定管理。您可以配置存取權限（請參見第 280 頁上的“管理 Kaspersky Embedded Systems Security 功能的存取權限”部分）並僅允許所需使用者存取記錄、偵錯和傾印檔案。

► 要在卡巴斯基安全管理中心中配置當機診斷設定：

1. 在卡巴斯基安全管理中心的管理主控台中，開啟“應用程式設定”（請參見第 150 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）視窗。
2. 開啟“故障診斷”部分，然後執行以下操作：
 - 如果您要應用程式將調試資訊寫入檔案，請選中“將診斷資訊寫入至檔案”核取方塊。
 - 在下面的欄位中指定 Kaspersky Embedded Systems Security 將會儲存偵錯檔案的資料夾。
 - 設定診斷資訊的詳細等級。

透過該下拉清單，您可以選擇 Kaspersky Embedded Systems Security 儲存到偵錯檔案的調試資訊的詳細等級。

您可以選擇以下一種詳細等級：

- **緊急事件** - Kaspersky Embedded Systems Security 僅將和緊急事件有關的資訊儲存到偵錯檔案。
- **錯誤** - Kaspersky Embedded Systems Security 將和緊急事件及錯誤有關的資訊儲存到偵錯檔案。
- **重要事件** - Kaspersky Embedded Systems Security 將和緊急事件、錯誤及重要事件有關的資訊儲存到偵錯檔案。
- **資訊事件** - Kaspersky Embedded Systems Security 將和緊急事件、錯誤、重要事件及資訊事件有關的資訊儲存到偵錯檔案。
- **所有診斷資訊** - Kaspersky Embedded Systems Security 將所有調試資訊儲存到偵錯檔案。

技術支援代表確定為解決出現的問題而需要設定的詳細等級。

預設的詳細等級設定為“**所有診斷資訊**”。

如果選中“**將診斷資訊寫入至檔案**”核取方塊，該下拉清單才可用。

- 指定偵錯檔案的最大大小。
- 指定要診斷的元件。元件代碼必須用分號分隔。代碼區分大小寫（請參見下表）。

表 19. Kaspersky Embedded Systems Security 子系統代碼

元件代碼	元件名稱
*	所有元件。
gui	使用者介面子系統，Microsoft 管理主控台內的 Kaspersky Embedded Systems Security 管理單元。
ak_conn	整合網路代理和卡斯基安全管理中心的子系統。
bl	控制處理程序，執行 Kaspersky Embedded Systems Security 控制工作。
wp	工作處理程序，處理病毒防護工作。
blgate	Kaspersky Embedded Systems Security 遠端管理處理程序。

元件代碼	元件名稱
ods	自訂掃描子系統。
oas	即時檔案防護子系統。
qb	隔離和備份子系統。
scandll	病毒防護掃描輔助模組。
core	基本病毒防護功能子系統。
avscan	病毒防護處理子系統。
avserv	控制病毒防護內核子系統。
prague	基本功能子系統。
updater	更新資料庫和軟體模組的子系統。
snmp	SNMP 協定支援子系統
perfcount	效能計數器子系統。

Kaspersky Embedded Systems Security 管理單元 (gui) 和卡巴斯基安全管理中心的管理外掛程式 (ak_conn) 的偵錯設定在這些元件重新啟動後應用。SNMP 協定支援子系統 (snmp) 的偵錯設定在 SNMP 服務重新啟動後應用。效能計數器子系統 (perfcount) 的偵錯設定在所有使用效能計數器的處理程序都重新開機之後應用。當機診斷設定儲存後，其他 Kaspersky Embedded Systems Security 子系統的偵錯設定就會立刻應用。

預設情況下，Kaspersky Embedded Systems Security 記錄所有 Kaspersky Embedded Systems Security 元件的調試資訊。

如果選中“將診斷資訊寫入至檔案”核取方塊，則該輸入欄位才可用。

- 如果您希望應用程式建立傾印檔案，請選中“建立傾印檔案”核取方塊。
 - 在下面的欄位中，指定 Kaspersky Embedded Systems Security 將用於儲存傾印檔案的資料夾。

3. 點擊“確定”。

將在受防護電腦上套用已配置的應用程式設定。

管理工作排程

您可以配置 Kaspersky Embedded Systems Security 工作的啟動排程，並配置按排程執行的工作的設定。

本章節說明項目

配置工作啟動排程設定	164
啟用和停用排程工作	166

配置工作啟動排程設定

您可以在應用程式主控台中配置本機系統和自訂工作的啟動排程。您不能為群組工作配置啟動排程。

► 要配置群組工作啟動排程設定，請執行以下操作：

1. 在卡斯基安全管理中心管理主控台樹狀目錄中，展開“受管理裝置”節點。
2. 選取受防護伺服器所屬的群組。
3. 在詳細資訊窗格中，選取“工作”標籤。
4. 採用以下方法之一開啟“內容：<工作名稱>”視窗：
 - 點擊工作的名稱。
 - 開啟工作名稱的上下文功能表，然後選取“內容”項。
5. 選取“排程”部分。
6. 在“排程設定”設定塊中，選中“依排程執行”核取方塊。

如果卡斯基安全管理中心政策封鎖按排程啟動自訂掃描工作和更新工作，則這些工作的排程設定的欄位不可用。

7. 根據需要配置排程設定。為此，請執行以下操作：

a. 在“週期”清單中，選擇以下值之一：

- **每小時**，如果您希望該工作在指定的小時數內間隔執行，請在“每 <數量> 小時”欄位中指定小時數。
- **每天**，如果您希望該工作在指定的天數內間隔執行，請在“每 <數量> 天”欄位中指定天數。
- **每週**，如果您希望該工作在指定的週數內間隔執行，請在“每 <數量> 週”欄位中指定週數。指定工作啟動的星期中的日期（預設在星期一啟動工作）。
- **在應用程式啟動時**，如果您希望在每次啟動 Kaspersky Embedded Systems Security 時執行該工作。
- **應用程式資料庫更新後**，如果您希望在每次更新應用程式資料庫後執行該工作。

b. 在“開始時間”欄位中指定首次啟動工作的時間。

c. 在“開始日期”欄位中，指定套用排程的開始日期。

指定了工作啟動頻率之後，將在視窗頂部的“下次開始”欄位中顯示工作的首次啟動時間、排程的開始套用日期以及預計下一個工作啟動時間的相關資訊。每次開啟“工作設定”視窗的“排程”標籤時，將顯示有關工作的下一次預計啟動時間的最新資訊。

如果卡斯基安全管理中心的活動政策設定禁止活動排程的系統工作，則將在“下次開始”欄位中顯示值“政策不允許”（請參見第 123 頁上的“配置本機預設工作的排程啟動”一節）。

8. 根據需要使用“進階”標籤來配置以下排程設定。

• 在“工作停止設定”部分中：

- a. 選中“持續時間”核取方塊，並輸入右側欄位中輸入所需的小時數和分鐘數以指定工作執行的最大持續時間。
- b. 選中“暫停開始於”核取方塊，並在右側欄位中輸入時間間隔的開始和結束值，以指定在工作執行的 24 小時中將暫停執行工作的時間間隔。

- 在“進階設定”部分中：
 - a. 選中“取消排程開始於”核取方塊，並指定停止執行排程的日期。
 - b. 選定“執行錯過的工作”核取方塊以允許啟動略過的工作。
 - c. 選中“在該時間間隔內隨機化工作開始時間”核取方塊，並按分鐘指定該值。

9. 點擊“確定”。

10. 點擊“套用”按鈕儲存工作啟動設定。

如果要使用卡斯基安全管理中心配置單個工作的應用程式設定，請執行第 150 頁上的“在卡斯基安全管理中心的應用程式設定視窗中配置本機工作”部分中介紹的步驟。

啟用和停用排程工作

可在配置排程設定之前或之後啟用和停用排程工作。

► 要啟用或停用工作啟動排程，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，開啟要為其配置啟動排程的工作名稱的內容功能表。
2. 選擇“內容”。

將開啟“工作設定”視窗。

3. 在開啟的視窗中的“排程”標籤上，執行以下操作之一：
 - 如果您希望啟用工作的啟動排程，請選中“依排程執行”核取方塊。
 - 如果您希望停用工作的啟動排程，請清除“依排程執行”核取方塊。

不會刪除已配置的工作啟動排程設定，並將在排程的下一次工作啟動時間套用該設定。

4. 點擊“確定”。

5. 點擊“套用”按鈕。

將儲存已配置的工作啟動排程設定。

在卡巴斯基安全管理中心中報告

卡巴斯基安全管理中心中的報告包含有關受管理裝置狀態的資訊。報告基於管理伺服器上儲存的資訊。

從卡巴斯基安全管理中心 11 開始，對於 Kaspersky Embedded Systems Security，以下類型的報告可用：

- 有關應用程式元件狀態的資訊
- 有關已禁止的應用程式的報告
- 有關在測試模式下禁止的應用程式的報告

有關所有卡巴斯基安全管理中心報告以及如何配置它們的詳細資訊，請參見 [卡巴斯基安全管理中心說明](#)。

有關應用程式元件狀態的資訊

您可以監視所有網路裝置的防護狀態，並獲得每個裝置上的元件集的結構化概覽。

報告為每個元件顯示以下狀態之一：*正在執行*、*已暫停*、*已停止*、*故障*、*未安裝*、*正在啟動*。

*未安裝*狀態指的是元件，而不是應用程式本身。如果未安裝應用程式，卡巴斯基安全管理中心會分配 N/A (不可用) 狀態。

您可以建立元件選擇並使用篩選來顯示具有定義的元件集的網路裝置及其狀態。

有關建立和使用選擇的詳細資訊，請參閱 [卡巴斯基安全管理中心說明](#)。

► 要在應用程式設定中檢視元件狀態：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點，然後選擇您希望為其配置應用程式設定的管理群組。

2. 選擇“裝置”標籤，然後開啟“應用程式設定”視窗（請參見第 [150](#) 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。
3. 選擇“元件”部分。
4. 檢視狀態表。

► 要檢視卡巴斯基安全管理中心標準報告：

1. 在管理主控台樹狀目錄中選擇“管理伺服器 <電腦名稱>”節點。
2. 開啟“報告”標籤。
3. 點擊“有關應用程式元件狀態的報告”清單項。

將建立報告。

4. 檢視以下報告詳細資訊：
 - 圖形化圖表。
 - 元件和安裝了每個元件的網路裝置總數以及裝置所屬的組的匯總表格。
 - 指定了元件狀態、版本、裝置和群組的詳細表格。

有關在活動模式和統計模式下封鎖的應用程式的報告

根據“應用程式啟動控制”工作的執行結果，可以建立兩種類型的報告：有關已禁止的應用程式的報告（如果在活動模式下啟動該工作）、有關在測試模式下禁止的應用程式的報告（如果在僅統計資訊模式下啟動該工作）。這些報告顯示了有關網路的受防護電腦上封鎖的應用程式的資訊。每個報告都針對所有管理組建立，並累積來自受防護裝置上安裝的所有 Kaspersky Lab 應用程式的資料。

► 要檢視有關在測試模式下禁止的應用程式的報告：

1. 在“僅統計”模式下啟動“應用程式控制”工作（請參見第 [378](#) 頁上的“配置應用程式啟動控制工作設定”部分）。
2. 在管理主控台樹狀目錄中選擇“管理伺服器 <電腦名稱>”節點。
3. 開啟“報告”標籤。

4. 點擊“有關在測試模式下禁止的應用程式的報告”清單項。

將建立報告。

5. 檢視以下報告詳細資訊：

- 顯示封鎖啟動次數最多的前十個應用程式的圖形化圖表。
- 發生的應用程式封鎖的匯總表格，其中指定可執行檔名稱、原因、封鎖時間和發生封鎖的裝置數量。
- 指定了有關裝置、檔案路徑和封鎖條件的資料的詳細表格。

► 要檢視有關在活動模式下禁止的應用程式的報告：

1. 在“活動”模式下啟動“應用程式控制”工作（請參見第 [378](#) 頁上的“配置應用程式啟動控制工作設定”部分）。
2. 在管理主控台樹狀目錄中選擇“管理伺服器 <電腦名稱>”節點。
3. 開啟“報告”標籤。
4. 點擊“有關禁止的應用程式的報告”清單項。

將建立報告。

此報告與有關在測試模式下禁止的應用程式的報告包含相同的資料塊。

Kaspersky Embedded Systems Security 主控台

本節提供有關 Kaspersky Embedded Systems Security 主控台的資訊，並介紹了如何使用安裝在受防護電腦或其他電腦上的應用程式主控台來管理該應用程式。

本章內容

應用程式主控台內的 Kaspersky Embedded Systems Security 設定	171
關於 Kaspersky Embedded Systems Security 主控台	179
Kaspersky Embedded Systems Security 主控台介面	180
通知區域中的系統欄圖示	184
透過其他電腦上的應用程式主控台管理 Kaspersky Embedded Systems Security	186
管理 Kaspersky Embedded Systems Security 工作	186
檢視防護狀態和 Kaspersky Embedded Systems Security 資訊	201
小型診斷視窗	207
更新 Kaspersky Embedded Systems Security 資料庫和軟體模組	212
物件隔離和備份複製	228
事件註冊。Kaspersky Embedded Systems Security 記錄	250
通知設定	267

應用程式主控台中的 Kaspersky Embedded Systems Security 設定

Kaspersky Embedded Systems Security 設定中的一般設定和故障診斷設定設定了程式執行的一般條件。您可以透過這些設定來控制 Kaspersky Embedded Systems Security 所使用的工作處理程序數，在異常終止後還原 Kaspersky Embedded Systems Security 工作，維護跟蹤記錄，在異常終止時建立 Kaspersky Embedded Systems Security 處理程序的傾印檔案，以及設定其他一般設定。

如果卡巴斯基安全管理中心活動政策封鎖對這些設定的變更，則無法在應用程式主控台中配置應用程式設定。

► 要配置 Kaspersky Embedded Systems Security 設定：

1. 在應用程式主控台樹狀目錄中，選擇“**Kaspersky Embedded Systems Security**”節點並執行以下操作之一：
 - 在節點的詳細資訊視窗中，點擊“**應用程式內容**”連結。
 - 在節點的內容功能表中選擇“**內容**”。

將開啟“**應用程式設定**”視窗。

2. 在開啟的視窗中，根據需要配置 Kaspersky Embedded Systems Security 設定：
 - 可在“**延伸性和介面**”標籤上配置以下設定：
 - 在“**延伸性設定**”部分：
 - Kaspersky Embedded Systems Security 可以執行的最大工作處理程序數

表 20. 最大活動程序數

設定	最大活動程序數

敘述	<p>該設定屬於 Kaspersky Embedded Systems Security 的延伸性設定群組。它設定應用程式可同時執行的最大活動處理程序數量。</p> <p>增加並行執行的處理程序數量可提高檔案掃描速度以及改善 Kaspersky Embedded Systems Security 的故障安全性。然而，如果此設定的值過高，它可能會降低一般電腦效能並提高 RAM 使用率。</p> <p>在卡巴斯基安全管理中心應用程式的管理主控台中，您只能變更在獨立電腦上安裝的 Kaspersky Embedded Systems Security 的“最大活動程序數”設定（使用“應用程式設定”對話方塊）；然而，您不能在電腦群組的政策設定中修改此設定。</p>								
可能的值	1 – 8								
預設值	<p>應用程式會根據電腦上的處理器數量自動處理延伸性：</p> <table border="1" data-bbox="293 958 1377 1249"> <thead> <tr> <th data-bbox="293 958 834 1037">處理器數量</th> <th data-bbox="834 958 1377 1037">最大活動程序數</th> </tr> </thead> <tbody> <tr> <td data-bbox="293 1037 834 1093">1</td> <td data-bbox="834 1037 1377 1093">1</td> </tr> <tr> <td data-bbox="293 1093 834 1171">1 < 處理器數量 < 4</td> <td data-bbox="834 1093 1377 1171">2</td> </tr> <tr> <td data-bbox="293 1171 834 1249">4 個或更多</td> <td data-bbox="834 1171 1377 1249">4</td> </tr> </tbody> </table>	處理器數量	最大活動程序數	1	1	1 < 處理器數量 < 4	2	4 個或更多	4
處理器數量	最大活動程序數								
1	1								
1 < 處理器數量 < 4	2								
4 個或更多	4								

- 用於即時電腦防護的處理程序數

表 21. 用於即時防護的程序數

設定	用於即時防護的程序數						
敘述	<p>該設定屬於 Kaspersky Embedded Systems Security 的延伸性設定群組。</p> <p>您可以使用此設定指定 Kaspersky Embedded Systems Security 將在其中執行即時防護工作的固定處理程序數。</p> <p>此設定的值較高將提高即時防護工作中的掃描速度。然而，Kaspersky Embedded Systems Security 使用的處理程序越多，它對受防護電腦和 RAM 資源利用率的一般效能影響就越大。</p> <p>在卡斯基安全管理中心應用程式的管理主控台中，您只能變更在獨立電腦上安裝的 Kaspersky Embedded Systems Security 的“用於即時防護的程序數”設定(使用“應用程式設定”視窗)；然而，您不能在電腦群組的政策設定中修改此設定。</p>						
可能的值	<p>可能的值：1-N，其中 N 是使用“最大活動程序數”設定指定的值。</p> <p>如果您將“用於即時防護的程序數”設定的值設定為等於最大活動處理程序數，則將降低 Kaspersky Embedded Systems Security 對電腦與電腦之間的檔案交換速度的影響，從而進一步改善其在即時防護期間的效能。然而，將在已執行的 Kaspersky Embedded Systems Security 處理程序中執行具有“中度掃描 (正常)”基本優先順序的更新工作和自訂掃描工作。自訂掃描工作的執行速度將降低。如果執行工作會導致處理程序異常終止，則重新開機將花費更長的時間。</p> <p>具有“低”基本優先順序的自訂掃描工作始終在一個或多個單獨的處理程序中執行。</p>						
預設值	<p>Kaspersky Embedded Systems Security 會根據電腦上的處理器數量自動處理延伸性：</p> <table border="1" data-bbox="293 1659 1337 1892"> <thead> <tr> <th data-bbox="293 1659 815 1733">處理器數量</th> <th data-bbox="820 1659 1337 1733">用於即時防護的程序數</th> </tr> </thead> <tbody> <tr> <td data-bbox="293 1740 815 1814">=1</td> <td data-bbox="820 1740 1337 1814">1</td> </tr> <tr> <td data-bbox="293 1821 815 1895">>1</td> <td data-bbox="820 1821 1337 1895">2</td> </tr> </tbody> </table>	處理器數量	用於即時防護的程序數	=1	1	>1	2
處理器數量	用於即時防護的程序數						
=1	1						
>1	2						

- 執行背景掃描工作的程序數量

表 22. 背景自訂掃描工作的程序數

設定	背景自訂掃描工作的程序數
敘述	<p>該設定屬於 Kaspersky Embedded Systems Security 的延伸性設定群組。</p> <p>您可以使用此設定指定應用程式將用於在背景模式執行自訂掃描工作的最大處理程序數。</p> <p>此設定指定的處理程序數不包含在“最大活動程序數”設定指定的 Kaspersky Embedded Systems Security 處理程序總數中。</p> <p>例如，如果您指定以下設定值：</p> <ul style="list-style-type: none"> • 最大活動處理程序數 - 3； • 用於即時防護工作的處理程序數- 3； • 背景自訂掃描工作的處理程序數- 1； <p>然後在背景模式下啟動多個即時防護工作和一個自訂掃描工作，則 Kaspersky Embedded Systems Security 的 kavfswp.exe 處理程序總數為 4。</p> <p>可在一個處理程序中執行多個具有低優先順序的自訂掃描工作。</p> <p>例如，如果您在背景模式下執行多個工作以便為每個工作分配一個單獨的處理程序，則您可增加處理程序數。為工作分配單獨的處理程序會提高工作執行可靠性和速度。</p>
可能的值	1-4
預設值	1

- 在“**使用者互動**”部分中，選擇在每個應用程式啟動後，系統欄圖示是否將顯示在工作列中(請參見第 [184](#) 頁上的“通知區域中的系統欄圖示”部分)。
- 可在“**安全性和可靠性**”標籤上配置以下設定：
 - 在“**可靠性設定**”部分中，指定自訂掃描工作崩潰後還原該工作的嘗試次數。

表 23. 工作還原

設定	工作還原 (重新啟動工作)
----	------------------------

敘述	<p>此設定屬於 Kaspersky Embedded Systems Security 中的“可靠性設定”群組。它會在工作緊急終止的情況下啟用工作還原，並定義用於還原自訂掃描工作的嘗試次數。</p> <p>當工作當機時，Kaspersky Embedded Systems Security 的 kavfs.exe 處理程序會嘗試重新啟動當機時正在執行工作的處理程序。</p> <p>如果工作還原被停用，應用程式不會還原“即時防護”和“自訂掃描”工作。</p> <p>如果工作還原被啟用，應用程式會嘗試還原“即時防護”工作直到它們成功啟動，並會試圖使用設定中指定的嘗試次數還原“自訂掃描”工作。</p>
可能的值	<p>啟用/停用。</p> <p>自訂掃描工作還原嘗試次數：1 - 10。</p>
預設值	<p>啟動工作還原。自訂掃描工作還原嘗試次數：2。</p>

- 在“**轉換至 UPS 備份電源時的操作**”部分，指定在轉換為 UPS 備份電源後 Kaspersky Embedded Systems Security 執行的操作：

表 24. 使用不斷電供應系統

設定	<p>轉換到 UPS 備份電源時的操作。</p>
敘述	<p>此設定確定當電腦轉換到不斷電供應系統時 Kaspersky Embedded Systems Security 執行的操作。</p>
可能的值	<p>執行或不執行根據排程要啟動的自訂掃描工作。</p> <p>執行或停止所有活動的自訂掃描工作。</p>
預設值	<p>預設情況下，如果使用不間斷電源為電腦供電，Kaspersky Embedded Systems Security：</p> <ul style="list-style-type: none"> 不會執行根據排程執行的自訂掃描工作。 自動停止所有活動的自訂掃描工作。

- 在“**密碼防護設定**”部分中，配置應用程式功能的密碼防護設定（請參見第 [290](#) 頁上的“對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取”部分）。
- 在“**連線設定**”選項上：
 - 在“**代理伺服器設定**”部分中，指定代理伺服器使用設定。
 - 在“**代理伺服器身分驗證設定**”部分中，指定在代理伺服器上進行身分驗證所需的身分驗證類型和詳細資訊。
 - 在“**授權**”部分中，指定是否將卡巴斯基安全管理中心用作應用程式啟動的代理伺服器。
- 在“**故障診斷**”選項上：
 - 如果您要應用程式將調試資訊寫入檔案，請選中“**將診斷資訊寫入至檔案**”核取方塊。
 - 在下面的欄位中指定 Kaspersky Embedded Systems Security 將會儲存偵錯檔案的資料夾。
 - 設定診斷資訊的詳細等級。

透過該下拉清單，您可以選擇 Kaspersky Embedded Systems Security 儲存到偵錯檔案的調試資訊的詳細等級。

您可以選擇以下一種詳細等級：

- **緊急事件** - Kaspersky Embedded Systems Security 僅將和緊急事件有關的資訊儲存到偵錯檔案。
- **錯誤** - Kaspersky Embedded Systems Security 將和緊急事件及錯誤有關的資訊儲存到偵錯檔案。
- **重要事件** - Kaspersky Embedded Systems Security 將和緊急事件、錯誤及重要事件有關的資訊儲存到偵錯檔案。
- **資訊事件** - Kaspersky Embedded Systems Security 將和緊急事件、錯誤、重要事件及資訊事件有關的資訊儲存到偵錯檔案。
- **所有診斷資訊** - Kaspersky Embedded Systems Security 將所有調試資訊儲存

到偵錯檔案。

技術支援代表確定為解決出現的問題而需要設定的詳細等級。

預設的詳細等級設定為“所有診斷資訊”。

如果選中“將診斷資訊寫入至檔案”核取方塊，該下拉清單才可用。

- 指定偵錯檔案的最大大小。
- 指定要診斷的元件。

應用程式將其調試資訊儲存到偵錯檔案的 Kaspersky Embedded Systems Security 元件的代碼清單。元件代碼必須用分號分隔。代碼區分大小寫（請參見下表）。

表 25. Kaspersky Embedded Systems Security 子系統代碼

元件代碼	元件名稱
*	所有元件。
gui	使用者介面子系統，Microsoft 管理主控台中的 Kaspersky Embedded Systems Security 管理單元。
ak_conn	整合網路代理和卡巴斯基安全管理中心的子系統。
bl	控制處理程序，執行 Kaspersky Embedded Systems Security 控制工作。
wp	工作處理程序，處理病毒防護工作。
blgate	Kaspersky Embedded Systems Security 遠端管理處理程序。
ods	自訂掃描子系統。
oas	即時檔案防護子系統。
qb	隔離和備份子系統。
scandll	病毒防護掃描輔助模組。
core	基本病毒防護功能子系統。
avscan	病毒防護處理子系統。

avserv	控制病毒防護內核子系統。
prague	基本功能子系統。
updater	更新資料庫和軟體模組的子系統。
snmp	SNMP 協定支援子系統
perfcoun	效能計數器子系統。

Kaspersky Embedded Systems Security 管理單元 (gui) 和卡斯基安全管理中心的 Kaspersky Embedded Systems Security 管理外掛程式 (ak_conn) 的偵錯設定在這些元件重新啟動後應用。SNMP 協定支援子系統 (snmp) 的偵錯設定在 SNMP 服務重新啟動後應用。效能計數器子系統 (perfcoun) 的偵錯設定在所有使用效能計數器的處理程序都重新開機之後應用。當機診斷設定儲存後，其他 Kaspersky Embedded Systems Security 子系統的偵錯設定就會立刻應用。

預設情況下，Kaspersky Embedded Systems Security 記錄所有 Kaspersky Embedded Systems Security 元件的調試資訊。

如果選中“將診斷資訊寫入至檔案”核取方塊，則該輸入欄位才可用。

- 如果您希望應用程式建立傾印檔案，請選中“建立當機傾印檔案”核取方塊。

Kaspersky Embedded Systems Security 不會自動傳送任何偵錯或傾印檔案。診斷資料只能由具有相應權限的使用者傳送。

- 在下面的欄位中，指定 Kaspersky Embedded Systems Security 將用於儲存記憶體傾印檔案的資料夾。

Kaspersky Embedded Systems Security 會以未加密的形式將資訊寫入到偵錯檔案和傾印檔案。儲存檔案的資料夾由使用者選擇，由作業系統配置和 Kaspersky Embedded Systems Security 設定管理。您可以配置存取權限（請參見第 280 頁上的“管理 Kaspersky Embedded Systems Security 功能的存取權限”部分）並僅允許所需使用者存取記錄、偵錯和傾印檔案。

3. 點擊“確定”。

Kaspersky Embedded Systems Security 設定即被儲存。

關於 Kaspersky Embedded Systems Security 主控台

Kaspersky Embedded Systems Security 主控台是新增到 Microsoft 管理主控台的獨立管理元件。

可以透過安裝在受防護電腦或公司網路中其他電腦上的應用程式主控台來管理應用程式。

在其他電腦上安裝應用程式主控台後，需要進行進階配置。

如果應用程式主控台和 Kaspersky Embedded Systems Security 分別安裝在不同網域的不同電腦上，則從應用程式到應用程式主控台的資訊傳遞可能會存在一些限制。例如，任何應用程式工作啟動之後，其在應用程式主控台中的狀態可能保持不變。

在應用程式主控台安裝過程中，安裝精靈在安裝資料夾中建立了 kavfs.msc 檔案並將 Kaspersky Embedded Systems Security 管理單元新增到 Microsoft Windows 獨立管理單元的清單。

您可以從“開始”功能表啟動應用程式主控台。可以執行 Kaspersky Embedded Systems Security 管理單元 msc 檔案，也可以將其作為樹狀目錄中的一個新項目新增到現有 Microsoft 管理主控台中。

在 64 位元版本的 Microsoft Windows 下，Kaspersky Embedded Systems Security 管理元件只能新增到 32 位元版本的 Microsoft 管理主控台中。若要執行此操作，請透過命令列執行指令 `mmc.exe /32` 從命令列開啟 Microsoft 管理主控台。

您可以將多個 Kaspersky Embedded Systems Security 管理元件新增到在作者模式中開啟單獨的 Microsoft 管理主控台中，以使用它來管理多台已安裝 Kaspersky Embedded Systems Security 的電腦防護。

Kaspersky Embedded Systems Security 主控台介面

Kaspersky Embedded Systems Security 主控台以節點的形式顯示在 Microsoft 管理主控台樹狀目錄中。

與其他電腦上安裝的 Kaspersky Embedded Systems Security 建立連線後，將在節點名稱後面附加已安裝應用程式的電腦的名稱和建立連線時所使用的使用者帳戶名稱：**Kaspersky Embedded Systems Security <電腦名稱> as <帳戶名稱>**。透過應用程式主控台連線到同一台電腦上安裝的 Kaspersky Embedded Systems Security 時，節點名稱為 **Kaspersky Embedded Systems Security**。

預設情況下，應用程式主控台視窗包含以下元素：

- 應用程式主控台樹狀目錄
- 詳細資訊視窗
- 工具列

應用程式主控台樹狀目錄

應用程式主控台樹狀目錄顯示 **Kaspersky Embedded Systems Security** 節點和應用程式功能元件的子節點。

Kaspersky Embedded Systems Security 掃描以下物件：

- **即時電腦防護**：管理即時防護工作和 KSN 服務。“**即時電腦防護**”節點允許配置以下工作：
 - 即時檔案防護
 - KSN 使用
- **電腦控制**：控制受防護電腦上安裝的應用程式的啟動以及外部裝置連線。“**電腦控制**”節點允許配置以下工作：
 - 應用程式啟動控制
 - 裝置控制
 - 防火牆管理
- **自動規則產生器**：配置“應用程式啟動控制”工作和“裝置控制”工作的群組和系統規則的自動產生。
 - 應用程式啟動控制規則產生器

- **裝置控制規則產生器**
- 規則產生群組工作<工作名稱> (如果有)

使用卡斯基安全管理中心建立群組工作 (請參見第 [187](#) 頁上的“Kaspersky Embedded Systems Security 工作類別”)。您無法透過應用程式主控台管理群組工作。

- **系統稽核**：設定檔操作控制和 Windows 事件記錄審查設定。

- **檔案完整性監控**
- **記錄審查**

- **自訂掃描**：管理自訂掃描工作。每個工作具有單獨的節點：

- **在作業系統啟動時掃描**
- **關鍵區域掃描**
- **隔離區掃描**
- **應用程式完整性控制**
- 自訂工作<工作名稱> (如有)

該節點顯示安裝應用程式時建立的系統工作 (請參見第 [187](#) 頁上的“Kaspersky Embedded Systems Security 工作類別”部分)、自訂工作，以及使用卡斯基安全管理中心建立並傳送到電腦的群組自訂掃描工作。

- **更新**：管理 Kaspersky Embedded Systems Security 資料庫和模組更新以及將更新複製到本機更新的原始資料夾中。此節點包含一些子節點，以管理每個更新工作和上次資料庫更新回溯工作：

- **資料庫更新**
- **軟體模組更新**
- **複製更新**
- **資料庫更新回溯**

該節點顯示使用卡斯基安全管理中心建立並傳送到電腦的所有自訂和群組更新工作 (請參見第 [187](#) 頁上的“Kaspersky Embedded Systems Security 工作類別”部分)。

- **儲存**：管理“隔離”和“備份”設定。
 - 隔離
 - 備份
- **記錄和通知**：管理本機工作記錄、安全記錄和 Kaspersky Embedded Systems Security 系統稽核記錄。
 - 安全記錄
 - 系統稽核記錄
 - 工作記錄
- **授權**：新增或刪除 Kaspersky Embedded Systems Security 金鑰和啟動碼，檢視產品授權詳細資訊。

詳細資訊視窗

詳細資訊視窗顯示有關選定節點的資訊。如果選擇 **Kaspersky Embedded Systems Security** 節點，該窗格將顯示有關目前電腦防護狀態的資訊（請參見第 [201](#) 頁上的“檢視防護狀態和 Kaspersky Embedded Systems Security 資訊”部分），以及有關 Kaspersky Embedded Systems Security、其功能元件的防護狀態和產品授權到期日期的資訊。

Kaspersky Embedded Systems Security 節點的內容功能表

可使用 **Kaspersky Embedded Systems Security** 節點的內容功能表項執行以下操作：

- **連線至其他電腦**。連線至其他電腦（請參見第 [186](#) 頁上的“透過其他電腦上的應用程式主控台管理 Kaspersky Embedded Systems Security”部分）以管理其上安裝的 Kaspersky Embedded Systems Security。也可以點擊 **Kaspersky Embedded Systems Security** 節點的詳細資訊視窗右下角的連結來執行此操作。
- **啟動服務 / 停止服務**。啟動或停止應用程式或選定工作（請參見第 [188](#) 頁上的“手動啟動/暫停/還原/停止工作”部分）。要執行這些操作，您還可以使用工具列上的按鈕。也可以在程式工作的內容功能表中執行這些操作。

- **配置卸除式磁碟機掃描設定。**配置透過 USB 連接埠連線到受防護電腦的卸除式磁碟機掃描 (請參見第 [510](#) 頁上的“關於卸除式磁碟機掃描”部分)。
- **弱點利用防禦：一般設定。**配置弱點利用防禦模式並設定防禦操作。
- **弱點利用防禦：處理程序防護設定。**新增要防護的處理程序並選擇弱點利用防禦技術(請參見第 [590](#) 頁上的“弱點利用防禦技術”部分)。
- **配置信任區域設定。**檢視和配置信任區域設定 (請參見第 [559](#) 頁上的“關於信任區域”部分)。
- **修改應用程式管理的使用者權限。**檢視和配置 Kaspersky Embedded Systems Security 功能的存取權限 (請參見第 [280](#) 頁上的“管理 Kaspersky Embedded Systems Security 功能的存取權限”部分)。
- **修改 Kaspersky Security 服務管理的使用者權限。**檢視和配置 Kaspersky Security Service 管理使用者權限 (請參見第 [286](#) 頁上的“配置用於管理 Kaspersky Embedded Systems Security 和 Kaspersky Security 服務的存取權限”部分)。
- **匯出設定。**將程式設定儲存到 XML 格式的設定檔中 (請參見第 [195](#) 頁上的“匯出設定”部分)。也可以在應用程式工作的內容功能表中執行此操作。
- **匯入設定。**從 XML 格式的設定檔中匯入應用程式設定 (請參見第 [196](#) 頁上的“匯入設定”部分)。也可以在應用程式工作的內容功能表中執行此操作。
- **關於應用程式和可用模組更新的資訊。**檢視有關 Kaspersky Embedded Systems Security 和目前可用應用程式模組更新的資訊。
- **重新整理。**重新整理應用程式主控台視窗的內容。也可以在應用程式工作的內容功能表中執行此操作。
- **內容。**檢視和配置 Kaspersky Embedded Systems Security 或選定工作的設定。也可以在應用程式工作的內容功能表中執行此操作。

也可以使用 **Kaspersky Embedded Systems Security** 節點的詳細資訊視窗中“應用程式內容”連結或工具列上的按鈕執行此操作。

- **說明。**檢視 Kaspersky Embedded Systems Security 說明資訊。也可以在應用程式工作的內容功能表中執行此操作。


Kaspersky Embedded Systems Security 工作的工具列和內容功能表

可以使用應用程式主控台樹狀目錄中每個工作的內容功能表項來管理 Kaspersky Embedded Systems Security 工作。

可使用內容功能表項執行以下操作：

- **啟動 / 停止。**啟動或停止工作 (請參見第 [188](#) 頁上的“手動啟動/暫停/還原/停止工作”部分) 執行。要執行這些操作，您還可以使用工具列上的按鈕。
- **繼續/暫停。**還原或暫停執行工作 (請參見第 [188](#) 頁上的“手動啟動/暫停/還原/停止工作”部分)。要執行這些操作，您還可以使用工具列上的按鈕。此操作適用於“即時防護”和“自訂掃描”工作。
- **新增工作。**新建自訂工作 (請參見第 [537](#) 頁上的“建立和配置自訂掃描工作”部分)。此操作適用於自訂掃描工作。
- **工作執行記錄。**檢視和管理工作記錄 (請參見第 [254](#) 頁上的“關於工作記錄”部分)。此操作適用於所有工作。
- **刪除工作。**刪除自訂工作。此操作適用於自訂掃描工作。
- **範本設定。**管理範本 (請參見第 [197](#) 頁上的“使用安全性設定範本”部分)。此操作適用於“即時檔案防護”和“自訂掃描”。


通知區域中的系統欄圖示

每次重新啟動電腦之後，當 Kaspersky Embedded Systems Security 自動啟動時，系統欄圖示將顯示在工作列通知區域  中。如果在應用程式安裝期間安裝了“系統欄圖示”元件，則預設情況下將顯示該圖示。

系統欄圖示的外觀反映了目前的電腦防護狀態。可能的狀態為以下兩種：



活動 (彩色圖示)，如果目前至少有一項工作正在執行：即時檔案防護、應用程式啟動控制

 不活動（黑白圖示），如果目前未執行任何工作：即時檔案防護、應用程式啟動控制

右鍵點擊系統欄圖示可開啟該圖示的內容功能表。

內容功能表提供了多個可用於顯示應用程式視窗的指令（請參見下表）。

表 26. 系統欄圖示中顯示的內容功能表指令

指令	敘述
開啟應用程式主控台	開啟 Kaspersky Embedded Systems Security 主控台（如已安裝）。
開啟小型診斷視窗	開啟小型診斷視窗。
關於應用程式	開啟“關於應用程式”視窗，其中包含有關 Kaspersky Embedded Systems Security 的資訊。 對於註冊的 Kaspersky Embedded Systems Security 使用者，“關於應用程式”視窗包含有關已安裝的緊急更新的資訊。
隱藏	隱藏工作列通知區域中的系統欄圖示。

您可以隨時重新顯示隱藏的系統欄圖示。

► **重新顯示程式圖示：**

在 Microsoft Windows 的“開始”功能表中，選擇“**所有程式 > Kaspersky Embedded Systems Security > 系統欄圖示**”。

設定的名稱可能有所不同，具體取決於安裝的作業系統。

在 Kaspersky Embedded Systems Security 的一般設定中，您可以啟用或停用系統欄圖示在每次電腦重新啟動後應用程式自動啟動時的顯示。

透過其他電腦上的應用程式主控台管理 Kaspersky Embedded Systems Security

您可透過遠端電腦上安裝的應用程式主控台管理 Kaspersky Embedded Systems Security。

要使用遠端電腦上的 Kaspersky Embedded Systems Security 主控台管理應用程式，請確保：

- 遠端電腦上的應用程式主控台使用者已新增到受防護電腦上的 ESS 管理員群組。
- 如果在受防護電腦上啟用 Windows 防火牆，將允許 Kaspersky Security 管理服務處理程序 (kavfsgt.exe) 連線網路。
- 在安裝 Kaspersky Embedded Systems Security 的過程中，在“安裝精靈”視窗中選中“允許遠端存取”核取方塊。

如果遠端電腦上的 Kaspersky Embedded Systems Security 受密碼防護，輸入密碼以透過應用程式主控台獲取對應用程式管理的存取權限。

管理 Kaspersky Embedded Systems Security 工作

本節包含有關 Kaspersky Embedded Systems Security 工作、如何建立工作、配置工作設定，以及啟動和停止工作的資訊。

本章節說明項目

Kaspersky Embedded Systems Security 工作類別.....	187
變更工作設定後儲存工作	188
手動啟動/暫停/還原/停止工作.....	188
管理工作排程.....	189
使用使用者帳戶啟動工作	191
匯入和匯出設定	193
使用安全性設定範本	197

Kaspersky Embedded Systems Security 工作類別

Kaspersky Embedded Systems Security 中的即時電腦防護、電腦控制、自訂掃描和更新功能作為工作實現。

您可以使用應用程式主控台樹狀目錄中的工作內容功能表、工具列和快速存取工作列來管理工作。可在詳細資訊窗格中檢視工作狀態資訊。工作管理操作記錄在系統稽核記錄中。

Kaspersky Embedded Systems Security 工作分為兩種類型：本機和群組。

本機工作

本機工作僅在建立該工作的受防護電腦上執行。根據啟動方式，存在以下幾種類型的本機工作：

- **本機系統工作。**在安裝 Kaspersky Embedded Systems Security 的過程中自動建立。您可以編輯除“隔離區掃描”和“資料庫更新回溯”工作之外的所有系統工作的設定。無法重命名或刪除系統工作。您可以同時執行系統和自訂自訂掃描工作。
- **本機自訂工作。**在應用程式主控台中，您可建立自訂掃描工作。在卡巴斯基安全管理中心中，您可建立自訂掃描、資料庫更新、資料庫更新回溯和複製更新工作。此類工作稱為“自訂工作”。可以重新命名、配置和刪除自訂工作。可同時執行多個自訂工作。

群組工作

使用卡斯基安全管理中心建立的群組工作和針對電腦群組的工作顯示在應用程式主控台中。此類工作稱為群組工作。可透過卡斯基安全管理中心管理和配置群組工作。在應用程式主控台中，只能檢視群組工作的狀態。

變更工作設定後儲存工作

可以修改正在執行或已停止（暫停）的工作的設定。新設定生效條件如下：

- 如果變更正在執行的工作的設定，在儲存該工作後，將立即套用新設定。
- 如果變更已停止（已暫停）的工作的設定，將在下次啟動該工作時套用新設定。

► 儲存已修改的工作設定：

在工作的內容功能表中，選擇“儲存工作”。

變更工作設定之後，如果未先選擇“儲存工作”指令，而選擇應用程式主控台樹狀目錄中的另一個節點，則會顯示儲存設定視窗。

► 要在轉換到另一個應用程式主控台節點時儲存已修改的設定，

在儲存設定視窗中，點擊“是”。

手動啟動/暫停/還原/停止工作

您可以只暫停和還原即時電腦防護和自訂掃描工作。

► 要開始/暫停/還原/停止某个工作，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中開啟工作的內容功能表。
2. 選擇以下選項之一：“啟動”、“暫停”、“繼續”或“停止”。

將執行該操作並將該操作註冊到系統稽核記錄中（請參見第 [251](#) 頁）。

還原自訂掃描工作時，Kaspersky Embedded Systems Security 將繼續掃描暫停工作時正在掃描的物件。

管理工作排程

您可以配置 Kaspersky Embedded Systems Security 工作的啟動排程，並配置按排程執行的工作的設定。

本章節說明項目

配置工作啟動排程設定	189
啟用和停用排程工作	191

配置工作啟動排程設定

您可以在應用程式主控台中配置本機系統和自訂工作的啟動排程。您不能為群組工作配置啟動排程。

► 要配置工作啟動排程設定：

1. 開啟要配置啟動排程工作的內容功能表。
2. 選擇“內容”。

將開啟“工作設定”視窗。

3. 在開啟的視窗中的“排程”標籤上，選中“依排程執行”核取方塊。
4. 根據需要配置排程設定。為此，請執行以下操作：
 - a. 在“週期”中，選擇以下值之一：
 - 每小時，如果您希望該工作在指定的小時數內間隔執行，請在“每 <數量> 小時”欄位中指定小時數。
 - 每天，如果您希望該工作在指定的天數內間隔執行，請在“每 <數量> 天”欄位中指定天數。

- **每週**，如果您希望該工作在指定的週數內間隔執行，請在“每 <數量> 週”欄位中指定週數。指定工作啟動的星期中的日期（預設在星期一啟動工作）。
 - **在應用程式啟動時**，如果您希望在每次啟動 Kaspersky Embedded Systems Security 時執行該工作。
 - **應用程式資料庫更新後**，如果您希望在每次更新應用程式資料庫後執行該工作。
- b. 在“**開始時間**”欄位中指定首次啟動工作的時間。
- c. 在“**開始日期**”欄位中，指定套用排程的開始日期。

指定了工作啟動頻率之後，將在視窗頂部的“**下次開始**”欄位中顯示工作的首次啟動時間、排程的開始套用日期以及預計下一個工作啟動時間的相關資訊。每次開啟“**工作設定**”視窗的“**排程**”標籤時，將顯示有關工作的下一次預計啟動時間的最新資訊。

在卡斯基安全管理中心政策設定中設定了按排程啟動系統工作，則“**政策不允許**”顯示在“**下次開始**”欄位中。

5. 根據需要使用“**進階**”標籤來配置以下排程設定。

- 在“**工作停止設定**”部分中：
 - a. 選中“**持續時間**”核取方塊，並輸入右側欄位中輸入所需的小時數和分鐘數以指定工作執行的最大持續時間。
 - b. 選中“**暫停開始於**”核取方塊，並在右側欄位中輸入時間間隔的開始和結束值，以指定在工作執行的 24 小時中將暫停執行工作的時間間隔。
- 在“**進階設定**”部分中：
 - a. 選中“**取消排程開始於**”核取方塊，並指定停止執行排程的日期。
 - b. 選定“**執行錯過的工作**”核取方塊以允許啟動略過的工作。
 - c. 選中“**在該時間間隔內隨機啟動工作**”核取方塊，並按分鐘指定該值。

6. 點擊“**確定**”。

將儲存已配置的工作啟動設定。

啟用和停用排程工作

可在配置排程設定之前或之後啟用和停用排程工作。

► 要啟用或停用工作啟動排程，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，開啟要為其配置啟動排程的工作名稱的內容功能表。
2. 選擇“內容”。

將開啟“工作設定”視窗。

3. 在開啟的視窗中的“排程”標籤上，執行以下操作之一：
 - 如果您希望啟用工作的啟動排程，請選中“依排程執行”核取方塊。
 - 如果您希望停用工作的啟動排程，請清除“依排程執行”核取方塊。

不會刪除已配置的工作啟動排程設定，並將在排程的下一次工作啟動時間套用該設定。

4. 點擊“確定”。

將儲存已配置的工作啟動排程設定。

使用使用者帳戶啟動工作

您可以在系統帳戶下啟動工作，也可以指定其他帳戶。

本章節說明項目

關於使用帳戶啟動工作	192
指定使用者帳戶以啟動工作	192

關於使用帳戶啟動工作

您可以指定要在其下為 Kaspersky Embedded Systems Security 的下列功能元件執行所選工作的帳戶：

- 應用程式啟動控制規則產生器和裝置控制規則產生器工作
- 自訂掃描工作
- 更新工作

預設情況下，使用系統帳戶權限運行這些工作。

在以下情況下，建議您使用具有正確存取權限的其他帳戶：

- 在更新工作中，如果您已指定在網路上其他電腦的公共資料夾作為更新來源；
- 在更新工作中，如果使用帶有內建 Windows NTLM 身分驗證的代理伺服器來存取更新來源；
- 在自訂掃描工作中，如果系統帳戶對已掃描的物件（例如，對電腦上的共用資料夾中的檔案）不具有存取權限。
- 在應用程式啟動控制規則產生器工作中，如果在完成工作後，將建立的規則匯出到位於系統帳戶無法存取的路徑（例如，電腦上的某個共用資料夾）中的設定檔。

您可以使用系統帳戶權限執行更新、自訂掃描和規則產生器工作。在執行這些工作的過程中，如果 Kaspersky Embedded Systems Security 需存取網路中的另一台電腦上的共用資料夾，且此電腦與受防護電腦在同一個網域中註冊。在這種情況下，系統帳戶必須具有對這些資料夾的存取權限。Kaspersky Embedded Systems Security 將使用帳戶 <網域名稱\電腦名稱> 的權限存取該電腦。

指定使用者帳戶以啟動工作

► 要指定帳戶啟動工作，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，開啟要為其配置啟動帳戶權限的工作名稱的內容功能表。
2. 選擇“內容”。

將開啟“工作設定”視窗。

3. 在開啟的視窗中的“**執行帳戶**”標籤上，執行以下操作：
 - a. 選擇“**使用者**”。
 - b. 輸入您要使用的帳戶的使用者名稱和密碼。

選定使用者必須在受防護電腦上註冊，或者與該電腦在同一網域中。

- c. 確認輸入的密碼。
4. 點擊“**確定**”。

將儲存修改後的工作執行使用者帳戶權限設定。

匯入和匯出設定

本節提供有關如何將 Kaspersky Embedded Systems Security 的設定或特定軟體元件的設定匯出到 XML 格式的設定檔，以及如何將該設定檔的這些設定匯回到程式的資訊。

本章節說明項目

關於匯入和匯出設定	193
匯出設定	195
匯入設定	196

關於匯入和匯出設定

可以將 Kaspersky Embedded Systems Security 設定匯出到 XML 設定檔，也可以將設定檔中的設定匯入到 Kaspersky Embedded Systems Security 中。可以將所有應用程式設定或僅將單個元件的設定儲存到設定檔。

在將 Kaspersky Embedded Systems Security 的所有設定匯出到檔案時，將儲存一般程式設定以及下列 Kaspersky Embedded Systems Security 元件和功能的設定：

- 即時檔案防護
- KSN 使用
- 裝置控制
- 應用程式啟動控制
- 裝置控制規則產生器
- 應用程式啟動控制規則產生器
- 自訂掃描工作
- 檔案完整性監控
- 記錄審查器
- Kaspersky Embedded Systems Security 資料庫和軟體模組更新
- 隔離
- 備份
- 記錄
- 管理員和使用者通知
- 信任區域
- 弱點利用防禦
- 密碼防護

此外，還可以在檔案中儲存 Kaspersky Embedded Systems Security 一般設定及使用者帳戶的權限。

無法匯出群組工作設定。

Kaspersky Embedded Systems Security 將匯出程式所使用的所有密碼，例如，用於執行工作或連線代理伺服器的帳戶資料。匯出的密碼以加密的形式儲存在設定檔中。您只能使用此電腦上安裝的 Kaspersky Embedded Systems Security 匯入密碼，且該程式未進行重新安裝或更新。

您無法使用安裝在其他電腦上的 Kaspersky Embedded Systems Security 匯入之前儲存的密碼。將設定匯入至其他電腦之後，必須手動輸入所有密碼。

如果在匯出時卡斯基安全管理中心政策有效，則應用程式將匯出該政策所使用的指定值。

可以從包含 Kaspersky Embedded Systems Security 個別元件參數的設定檔（例如從未安裝完整元件的 Kaspersky Embedded Systems Security 建立的檔案）匯入設定。匯入設定後，只有該設定檔中包含的那些 Kaspersky Embedded Systems Security 設定會發生變化。所有其他設定保持不變。

匯入設定時，已被封鎖的活動卡斯基安全管理中心政策的設定不會發生變更。

匯出設定

► 若要將設定匯出到設定檔，請執行下列步驟：

1. 在應用程式主控台樹狀目錄中，執行以下操作之一：

- 在 **Kaspersky Embedded Systems Security** 節點的內容功能表中，選擇“**匯出設定**”可匯出所有 Kaspersky Embedded Systems Security 設定。
- 在要匯出其設定的工作的內容功能表中，選擇“**匯出設定**”可匯出程式的單個功能元件的設定。
- 匯出“信任區域”元件的設定：
 - a. 在應用程式主控台樹狀目錄中，開啟 **Kaspersky Embedded Systems Security** 節點的內容功能表。
 - b. 選擇“**配置信任區域設定**”。

將開啟“信任區域”視窗。

c. 點擊“**匯出**”按鈕。

將開啟設定匯出精靈的歡迎視窗。

2. 請按照精靈的說明操作：指定作為儲存設定目標的設定檔名稱及其路徑。

指定路徑時可以使用系統環境變數；不允許使用者環境變數。

如果安全管理中心政策在匯出時啟用，則應用程式將匯出在套用此政策前啟用的設定值。

3. 點擊“程式設定匯出已完成”視窗中的“關閉”按鈕。

關閉精靈時，將儲存匯出的設定。

匯入設定

► 若要從儲存的設定檔匯入設定，請執行下列步驟：

1. 在應用程式主控台樹狀目錄中，執行以下操作之一：
 - 在 **Kaspersky Embedded Systems Security** 節點的內容功能表中，選擇“匯入設定”可匯入所有 Kaspersky Embedded Systems Security 設定。
 - 在要匯入其設定的工作的內容功能表中，選擇“匯入設定”可匯入程式的單個功能元件的設定。
 - 若要匯出“信任區域”元件的設定：
 - a. 在應用程式主控台樹狀目錄中，開啟 **Kaspersky Embedded Systems Security** 節點的內容功能表。
 - b. 選擇“配置信任區域設定”。
將開啟“信任區域”視窗。
 - c. 點擊“匯入”按鈕。
將開啟設定匯入精靈的歡迎視窗。
2. 請按照精靈的說明操作：指定作為匯入的設定檔名稱及其路徑。

在電腦匯入 Kaspersky Embedded Systems Security 或及功能元件的一般設定後，您將無法還原之前的設定值。

3. 在“程式設定匯入已完成”視窗中，點擊“關閉”按鈕。

關閉精靈後，將儲存匯入的設定。

4. 在應用程式主控台的工具列中，點擊“重新整理”按鈕。

將在應用程式主控台視窗中顯示匯入的設定。

如果電腦上的 Kaspersky Embedded Systems Security 進行了重新安裝或更新，Kaspersky Embedded Systems Security 不會從在其他電腦上或同一電腦上建立的檔案匯入密碼（用於啟動工作或連線到代理電腦的帳戶資料）。在匯入操作完成時，必須手動輸入密碼。

使用安全性設定範本

本節包含有關在 Kaspersky Embedded Systems Security 防護和掃描工作中使用安全性設定範本的資訊。

本章節說明項目

關於安全性設定範本	197
建立安全性設定範本	198
檢視範本中的安全性設定	199
套用安全性設定範本	199
刪除安全性設定範本	200

關於安全性設定範本

可以在電腦的檔案資源樹狀目錄或清單中手動配置節點的安全性設定，並將配置好的設定值儲存為範本。然後可在 Kaspersky Embedded Systems Security 防護和掃描工作中使用該範本來設定其他節點的安全性設定。

可使用範本來配置以下 Kaspersky Embedded Systems Security 工作的安全性設定：

- 即時檔案防護
- 在作業系統啟動時掃描
- 關鍵區域掃描
- 自訂掃描工作

套用到電腦檔案資源樹狀目錄中的父節點的範本中的安全性設定將套用到所有子節點中。以下情況中父節點的範本不套用於子節點：

- 如果子節點的安全性設定單獨進行配置（請參見第 [199](#) 頁上的“套用安全性設定範本”部分）。
- 如果子節點為虛擬節點。您必須針對每個虛擬節點單獨套用範本。

建立安全性設定範本

► 手動儲存節點的安全性設定並將這些設定儲存到範本中：

1. 在應用程式主控台樹狀目錄中，選擇要對其套用安全性設定範本的工作。
2. 在所選工作的詳細資訊視窗中，點擊“配置防護範圍”或“配置掃描範圍”連結。
3. 在電腦的網路檔案資源樹狀目錄或清單中，選擇要檢視的範本。
4. 在“安全等級”標籤上，點擊“另存為範本”按鈕。

將開啟“範本內容”視窗。

5. 在“範本名稱”欄位中，輸入範本名稱。
6. 在“敘述”欄位中，輸入範本其他資訊。
7. 點擊“確定”。

將儲存帶有一組安全性設定的範本。

檢視範本中的安全性設定

► 若要檢視已建立範本中的安全設定，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，選擇要檢視其安全範本的工作。
2. 在選定工作的內容功能表中，選擇“**範本設定**”。

將開啟“**範本**”視窗。

3. 在開啟的視窗中的範本清單中，選擇要檢視的範本。
4. 點擊“**檢視**”按鈕。

將開啟“<範本名稱>”視窗。“**一般**”標籤顯示範本名稱和有關該範本的其他資訊；“**選項**”標籤列出了儲存於範本中的安全性設定。

套用安全性設定範本

► 為所選節點套用範本中的安全性設定：

1. 在應用程式主控台樹狀目錄中，選擇要對其套用安全性設定範本的工作。
2. 在所選工作的詳細資訊視窗中，點擊“**配置防護範圍**”或“**配置掃描範圍**”連結。
3. 在電腦的網路檔案資源樹狀目錄或清單中，開啟要對其套用範本的節點或項的上下文選單。
4. 選取“**套用範本**”→“<範本名稱>”。
5. 點擊“**儲存**”按鈕。

將對電腦檔案資源樹狀目錄中的所選節點套用該安全性設定範本。選定節點的“**安全等級**”標籤現在具有“**自訂**”值。

套用到電腦檔案資源樹狀目錄中的父節點的範本中的安全性設定將套用到所有子節點中。

如果電腦檔案資源樹狀目錄中的子節點的防護範圍或掃描範圍單獨進行配置，則套用到父節點的範本中的安全性設定不會自動套用到此類子節點。

► 若要為所有選定節點套用範本中的安全性設定，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，選擇要對其套用安全性設定範本的工作。
2. 在所選工作的詳細資訊視窗中，點擊“配置防護範圍”或“配置掃描範圍”連結。
3. 在電腦網路檔案資源樹狀目錄或清單中，選擇一個父節點，以便將範本套用於選定的節點和其所有子節點。
4. 在右鍵選單中，選取“套用範本 → <範本名稱>”。
5. 點擊“儲存”按鈕。

將對電腦檔案資源樹狀目錄中的父節點和所有子節點套用安全性設定範本。選定節點的“安全等級”標籤現在具有“自訂”值。

刪除安全性設定範本

► 若要刪除安全性設定範本，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，選擇不希望再使用安全性設定範本配置其安全性設定的工作。
2. 在選定工作的內容功能表中，選擇“範本設定”。

您可從“自訂掃描”父節點的詳細資訊視窗檢視自訂掃描工作的設定範本。

將開啟“範本”視窗。

3. 在開啟的視窗中的範本清單中，選擇要刪除的範本。
4. 點擊“刪除”按鈕。

將顯示一個視窗，提示您確認刪除。

5. 在開啟的視窗中，點擊“是”。

將刪除所選範本。

如果套用安全性設定範本防護或掃描電腦檔案資源的節點，則在刪除該範本後會保留為此類節點配置的安全性設定。

檢視防護狀態和 Kaspersky Embedded Systems Security 資訊

► 要檢視有關 *Kaspersky Embedded Systems Security* 電腦防護狀態的資訊，

在應用程式主控台樹狀目錄中選擇“**Kaspersky Embedded Systems Security**”節點。

預設情況下，將自動重新整理應用程式主控台的詳細資訊視窗中的資訊：

- 對於本機連線，每 10 秒鐘重新整理一次。
- 對於遠端連線，每 15 秒鐘重新整理一次。

您可以手動重新整理資訊。

► 在“*Kaspersky Embedded Systems Security*”節點中手動重新整理資訊，

在“**Kaspersky Embedded Systems Security**”節點的內容功能表中選擇“**重新整理**”指令。

應用程式主控台的詳細資訊窗格中會顯示以下應用程式資訊：

- “卡巴斯基安全網路使用”狀態。
- 電腦防護狀態。
- 有關資料庫和應用程式模組更新的資訊。
- 實際診斷資料。
- 有關電腦控制工作的資料。
- 產品授權資訊。

- 與卡斯基安全管理中心的整合狀態：已安裝與應用程式連線的卡斯基安全管理中心的電腦的詳細資訊；有關活動政策控制的應用程式工作的資訊。

使用不同的顏色指示防護狀態：

- **綠色**。根據配置的設定執行工作。防護處於活動狀態。
- **黃色**。工作未啟動，已暫停或已停止。可能會發生安全威脅。建議您配置並啟動工作。
- **紅色**。工作完成，但出現錯誤，或工作執行時偵測到安全威脅。建議您啟動工作或採取措施消除偵測到的安全威脅。

此塊中的某些詳細資訊（例如，工作名稱或偵測到的威脅數量）為點擊後將轉至相關工作的節點或開啟工作記錄的連結。

“卡斯基安全網路使用情況”部分顯示目前工作狀態，例如，正在執行、已停止或從未執行。該指示器可以使用的設定值如下：

- 綠色表示“KSN 使用”工作正在執行，並且對狀態的檔案請求正在傳送到 KSN。
- 黃色表示聲明之一已被接受，但工作未執行；或者工作正在執行，但檔案請求未傳送到 KSN。

電腦防護

“電腦防護”部分（請參見下表）顯示有關電腦目前防護狀態的資訊。

表 27. 有關電腦防護狀態的資訊

“防護”部分	資訊
電腦防護狀態指示器	<p>帶有此部分名稱的面板的顏色反映了在該部分中正在執行的工作的狀態。該指示器可以使用的設定值如下：</p> <ul style="list-style-type: none"> • 綠色 – 預設顯示此顏色，指示“即時檔案防護”元件已安裝且工作正在執行。 • 黃色 – “即時檔案防護”元件未安裝，且“關鍵區域掃描”工作已長時間未執行。 • 紅色 – “即時檔案防護”工作未執行。

“防護”部分	資訊
即時檔案防護	<p>工作狀態 – 目前工作狀態，例如，“正在執行”或“已停止”。</p> <p>偵測到 – 由 Kaspersky Embedded Systems Security 偵測到的物件數量。例如，如果 Kaspersky Embedded Systems Security 在五個檔案中偵測到一個惡意軟體程式，該欄位中的值將增加 1。如果偵測到的惡意軟體程式數量超過 0，此值突出顯示為紅色。</p>
關鍵區域掃描	<p>上次掃描日期 – 上次在關鍵區域掃描病毒和其他電腦安全威脅的日期和時間。</p> <p>從未執行 – 在過去 30 天或更長時間(預設值)內沒有執行關鍵區域掃描工作時所發生的一個事件。您可以變更產生此事件的參數值。</p>
弱點利用防禦	<p>狀態 – 弱點利用防禦技術的目前狀態，例如，“已應用”或“未應用”。</p> <p>防禦模式 – 可用的兩個模式之一，在配置處理程序記憶體防護的過程中選擇：</p> <ul style="list-style-type: none"> • 發現弱點利用時終止。 • 僅統計。 <p>防護的處理程序 – 根據選定的模式新增到防護範圍並處理的處理程序總數。</p>
已備份物件	<p>已超過備份區可用空間上限值 – 當備份區可用空間量接近指定限制時會發生該事件。Kaspersky Embedded Systems Security 繼續將物件移至備份區。在這種情況下，“已用空間”欄位高亮顯示為黃色。</p> <p>已超過最大備份容量 – 當備份區大小已達到指定限制時會發生此事件。Kaspersky Embedded Systems Security 繼續將物件移至備份區。在這種情況下，“已用空間”欄位高亮顯示為紅色。</p> <p>已備份物件 – 目前在備份區中的物件數量。</p> <p>已用空間 – 已使用的備份區空間容量。</p>

更新

“更新”部分 (請參見下表) 顯示有關病毒資料庫和應用程式模組的更新程度的資訊。

表 28. 有關 Kaspersky Embedded Systems Security 資料庫和模組狀態的資訊

“更新”部分	資訊
資料庫和軟體 模組狀態指示 器	<p>帶有部分名稱的面板的顏色反映了應用程式資料庫和模組的狀態。該指示器可以使用的設定值如下：</p> <ul style="list-style-type: none"> • 綠色 – 預設顯示此顏色，指示應用程式資料庫處於最新狀態，並且最近的資料庫更新工作已成功完成。 • 黃色 – 資料庫已過期，或上次資料庫更新工作失敗。 • 紅色 – 發生 <i>應用程式資料庫已嚴重過期</i> 或 <i>應用程式資料庫已損壞</i> 事件。
資料庫更新和 軟體模組更新	<p>資料庫狀態 – 資料庫更新狀態的評估。</p> <p>它可能呈現是以下設定值：</p> <ul style="list-style-type: none"> • 應用程式資料庫為最新 – 應用程式資料庫在之前 7 天內進行過更新（預設）。 • 應用程式資料庫已過期 – 應用程式資料庫在之前 7 至 14 天內進行過更新（預設）。 • 應用程式資料庫已嚴重過期 – 應用程式資料庫在超過 14 天前進行過更新（預設）。 <p>您可以變更為用於建立 <i>應用程式資料庫過期</i> 和 <i>應用程式資料庫已長時間未更新</i> 事件上限值。</p> <p>資料庫發佈日期 – 最近資料庫更新的發佈日期和時間。日期和事件指定為 UTC 格式。</p> <p>最新完成的“資料庫更新”工作的狀態 – 最新資料庫更新的日期和時間。日期和時間根據受防護電腦的當地時間指定。如果發生“失敗”事件，則欄位為紅色。</p> <p>可用模組更新數 – 可供下載和安裝的 Kaspersky Embedded Systems Security 模組更新數量。</p> <p>已安裝模組更新數 – 已安裝的 Kaspersky Embedded Systems Security 模組更新數量。</p>

控制

“控制”部分（請參見下表）顯示有關應用程式啟動控制、裝置控制和防火牆工作的資訊。

表 29. 有關電腦控制狀態的資訊

“控制”部分	資訊
電腦控制狀態指示器	<p>帶有此部分名稱的面板的顏色反映了在該部分中正在執行的工作的狀態。該指示器可以使用的設定值如下：</p> <ul style="list-style-type: none"> • 綠色 – 預設顯示此顏色，指示“應用程式啟動控制”元件已安裝，且工作在“活動”模式下執行。 • 黃色 – “應用程式啟動控制”在“僅統計”模式下執行。 • 紅色 – “應用程式啟動控制”工作未執行或失敗。
應用程式啟動控制	<p>工作狀態 – 目前工作狀態，例如，“正在執行”或“已停止”。</p> <p>模式 – 兩種可用的“應用程式啟動控制”工作模式中的一種：</p> <ul style="list-style-type: none"> • 活動 • 僅統計 <p>應用程式啟動被拒絕 – 在“應用程式啟動控制”工作執行期間，嘗試啟動 Kaspersky Embedded Systems Security 已封鎖的應用程式的次數。如果已封鎖的應用程式啟動次數超過 0，則該欄位為紅色。</p> <p>平均處理時間(毫秒) – Kaspersky Embedded Systems Security 處理嘗試在受防護電腦上啟動應用程式所用的時間。</p>
裝置控制	<p>工作狀態 – 目前工作狀態，例如，“正在執行”或“已停止”。</p> <p>模式 – 兩種可用的“裝置控制”工作模式中的一種：</p> <ul style="list-style-type: none"> • 活動 • 僅統計 <p>已封鎖的裝置 – 在執行“裝置控制”工作期間，Kaspersky Embedded Systems Security 封鎖的連接大容量儲存裝置的嘗試次數。如果已封鎖的大容量儲存裝置數量超過 0，則該欄位為紅色。</p>

“控制”部分	資訊
防火牆管理	<p>工作狀態 – 目前工作狀態，例如，“正在執行”或“已停止”。</p> <p>封鎖的連線嘗試次數 – 被指定防火牆規則封鎖的與受防護電腦的連線的數量。</p>

診斷

“診斷”部分（請參見下表）顯示有關“檔案完整性監控”和“記錄審查”工作的資訊。

表 30. 有關系統稽核狀態的資訊

“診斷”部分	資訊
診斷狀態指示器	<p>帶有此部分名稱的面板的顏色反映了在該部分中正在執行的工作的狀態。該指示器可以使用的設定值如下：</p> <ul style="list-style-type: none"> 綠色 – 預設顯示此顏色，指示一個或兩個系統審查元件已安裝，且工作正在執行。 黃色 – 兩個元件均已安裝，但其中一個系統稽核工作未執行；發生“未執行”事件。 紅色 – 其中一個工作失敗。
檔案完整性監控	<p>工作狀態 – 目前工作狀態，例如，“正在執行”或“已停止”。</p> <p>未批准的檔案操作 – 對監控範圍內的檔案的變更次數。這些變更可能表示受防護電腦遭到安全入侵。</p>
記錄審查	<p>工作狀態 – 目前工作狀態，例如，“正在執行”或“已停止”。</p> <p>可能的違規 – 根據來自 Windows 事件記錄的資料，所記錄的違規數量。基於指定的工作規則或使用啟發式分析來確定此數量。</p>

Kaspersky Embedded Systems Security 授權資訊顯示在 **Kaspersky Embedded Systems Security** 節點的詳細資訊窗格左下角的行中。

您可以按照“應用程式內容”連結（請參見第 [171](#) 頁上的“應用程式主控台”中的 Kaspersky Embedded Systems Security 設定”部分）配置 Kaspersky Embedded Systems Security 內容。

可以按照“連線至其他電腦”連結（請參見第 [186](#) 頁上的“透過其他電腦上的應用程式主控台管理 Kaspersky Embedded Systems Security”部分）連線到其他電腦。

小型診斷視窗

本節介紹如何使用小型診斷視窗檢視電腦狀態或目前活動，以及如何配置傾印和偵錯檔案寫入。

本章內容

關於小型診斷視窗	207
透過小型診斷視窗檢視 Kaspersky Embedded Systems Security 狀態.....	208
檢視安全事件統計	209
檢視目前應用程式活動.....	210
配置傾印和偵錯檔案寫入	211

關於小型診斷視窗

“小型診斷視窗”元件 (也稱為“CDI”) 連同“系統欄圖示”元件獨立於應用程式主控台安裝和移除，可在受防護電腦上未安裝應用程式主控台時使用。CDI 透過系統欄圖示啟動，或透過執行電腦上的應用程式資料夾中的 kavfsmui.exe 啟動。

在 CDI 視窗中可執行以下操作：

- 檢視有關一般應用程式狀態的資訊 (請參見第 [208](#) 頁上的“透過小型診斷視窗檢視 Kaspersky Embedded Systems Security 狀態”部分) 。
- 檢視已發生的安全事件 (請參見第 [209](#) 頁上的“檢視安全事件統計”部分) 。
- 檢視受防護電腦上的目前活動 (請參見第 [210](#) 頁上的“檢視目前應用程式活動”部分) 。
- 啟動或停止寫入傾印和偵錯檔案 (請參見第 [211](#) 頁上的“配置傾印和偵錯檔案寫入”部分) 。
- 開啟應用程式主控台。
- 開啟含有已安裝更新和可用修補程式清單的“關於應用程式”視窗。

即使對 Kaspersky Embedded Systems Security 功能的存取受密碼防護，CDI 仍然可用。無需任何密碼。

CDI 元件不能透過卡巴斯基安全管理中心進行配置。

透過小型診斷視窗檢視 Kaspersky Embedded Systems Security 狀態

► 要開啟“小型診斷視窗”視窗，請執行以下操作：

1. 右鍵點擊工具列通知區域中的 Kaspersky Embedded Systems Security 系統欄圖示。
2. 選擇“開啟小型診斷視窗”選項。

“小型診斷視窗”視窗將開啟。

在“防護狀態”標籤上檢視金鑰、即時電腦防護工作和更新工作的目前狀態。使用了不同的顏色來向使用者通知防護狀態（請參見下表）。

表 31. 小型診斷視窗防護狀態。

部分	狀態
即時電腦防護	<p>在以下情況之一中（滿足任意數量的條件），面板呈綠色：</p> <ul style="list-style-type: none"> 建議需求： <ul style="list-style-type: none"> “即時檔案防護”工作以預設設置啟動。 “應用程式啟動控制”工作在“活動”模式下以預設設定啟動。 可接受配置： <ul style="list-style-type: none"> “即時檔案防護”工作由使用者配置。 “應用程式啟動控制”工作設定被修改。
	<p>如果滿足以下一個或多個條件，面板呈黃色：</p> <ul style="list-style-type: none"> “即時檔案防護”工作暫停（使用者暫停或按排程暫停）。 “應用程式啟動控制”工作在“僅統計”模式下啟動。 “弱點利用防禦”和“應用程式啟動控制”在“僅統計”模式下啟動。

部分	狀態
	<p>如果同時滿足以下兩個條件，面板呈紅色：</p> <ul style="list-style-type: none"> “即時檔案防護”元件未安裝或者工作停止或暫停。 “應用程式啟動控制”元件未安裝或工作在“僅統計”模式下啟動。
授權	<p>如果目前產品授權有效，面板呈綠色。</p>
	<p>黃色面板表示發生以下事件之一：</p> <ul style="list-style-type: none"> 檢查產品授權狀態。 產品授權將在 14 天后到期，且未新增備用金鑰或啟動碼。 新增的金鑰已被列入黑名單且將被封鎖。
	<p>紅色面板表示發生以下事件之一：</p> <ul style="list-style-type: none"> 應用程式未啟動。 產品授權已到期。 已違反最終使用者產品授權協議。 金鑰已被列入黑名單。
更新	<p>應用程式資料庫為最新時，面板呈綠色。</p>
	<p>應用程式資料庫已過期時，面板呈黃色。</p>
	<p>應用程式資料庫已嚴重過期時，面板呈紅色。</p>

檢視安全事件統計

“統計”標籤顯示所有安全事件。單獨塊中顯示的每個防護工作統計說明了事件數量和上次發生事件的日期和時間。記錄某個事件後，塊顏色變為紅色。

► 要檢視統計：

1. 右鍵點擊工具列通知區域中的 Kaspersky Embedded Systems Security 系統欄圖示。
2. 選擇“開啟小型診斷視窗”選項。

“小型診斷視窗”視窗將開啟。

3. 開啟“統計”標籤。
4. 檢視防護工作的安全事件。

檢視目前應用程式活動

在該標籤上，您可以檢視目前工作和應用程式處理程序的狀態，並迅速獲得關於所發生的緊急事件的通知。

使用不同的顏色指示應用程式活動狀態：

- 在“工作”部分中：
 - 綠色。沒有對應於黃色或紅色的條件。
 - 黃色。很長時間未掃描關鍵區域。
 - 紅色。符合以下任一條件：
 - 未啟動任何工作和沒有為任何工作設定啟動排程。
 - 應用程式啟動錯誤將記錄為緊急事件。
- 在“卡巴斯基安全網路”部分中：
 - 綠色。“KSN 使用”工作已啟動。
 - 黃色。KSN 聲明被接受，但工作未啟動。

► 要檢視電腦上的目前應用程式活動：

1. 右鍵點擊工具列通知區域中的 Kaspersky Embedded Systems Security 系統欄圖示。
2. 選擇“開啟小型診斷視窗”選項。
“小型診斷視窗”視窗將開啟。
3. 開啟“目前應用程式活動”標籤。
4. 在“工作”部分中檢視以下資訊：
 - 很長時間未掃描關鍵區域

僅當應用程式返回相應的關鍵區域掃描警告時，才會顯示該欄位。

- 現在正在執行
 - 執行失敗
 - 排程定義的下次啟動
5. 在“卡巴斯基安全網路”部分中檢視以下資訊：
- **KSN 開啟。**檔案信譽服務已啟用或防護關閉。
 - **應用程式統計資訊正在傳送到 KSN。**

應用程式將傳送有關在“即時檔案防護”工作和“自訂掃描”工作執行過程中偵測到的惡意軟體（包括欺詐軟體）的資訊，以及有關掃描過程中的錯誤的調試資訊。

如果在“KSN 使用”工作設定中選中“傳送卡巴斯基安全網路統計資訊”核取方塊，將顯示該欄位。

6. 在“與卡巴斯基安全管理中心整合”部分中檢視以下資訊：
- 允許本機管理。
 - 套用政策：<卡巴斯基安全管理中心伺服器名稱>。

配置傾印和偵錯檔案寫入

您可以透過 CDI 配置傾印和偵錯檔案的寫入。

還可以透過應用程式主控台配置故障診斷（請參見第 171 頁上的“應用程式主控台中的 Kaspersky Embedded Systems Security 設定”部分）。

► 要開始寫入傾印和偵錯檔案，請執行以下操作：

1. 右鍵點擊工具列通知區域中的 Kaspersky Embedded Systems Security 系統欄圖示。
2. 選擇“開啟小型診斷視窗”選項。

“小型診斷視窗”視窗將開啟。

3. 開啟“故障排除”標籤。
4. 如果必要，變更以下偵錯設定：
 - a. 選中“將調試資訊寫入此資料夾中的偵錯檔案”核取方塊。
 - b. 點擊“瀏覽”按鈕以指定 Kaspersky Embedded Systems Security 將會儲存偵錯檔案的資料夾。
將對所有元件啟用跟蹤（採用預設參數，使用“調試”等級的詳細資訊，預設最大記錄大小為 50 MB）。
5. 如果必要，變更以下傾印檔案設定：
 - a. 選中“在以下資料夾中建立故障傾印檔案”核取方塊。
 - b. 點擊“瀏覽”按鈕以指定 Kaspersky Embedded Systems Security 將會儲存傾印檔案的資料夾。
6. 點擊“套用”按鈕。
將套用新設定。

更新 Kaspersky Embedded Systems Security 資料庫和軟體模組

本節提供有關 Kaspersky Embedded Systems Security 資料庫和軟體模組更新工作（複製更新和回溯 Kaspersky Embedded Systems Security 資料庫更新）的資訊，以及有關如何設定資料庫和軟體模組更新工作的說明。

本章內容

關於更新工作.....	213
關於 Kaspersky Embedded Systems Security 軟體模組更新.....	214
關於 Kaspersky Embedded Systems Security 資料庫更新.....	215
組織內所使用的病毒防護程式資料庫和模組的更新方案.....	216
設定更新工作.....	219
回溯 Kaspersky Embedded Systems Security 資料庫更新.....	227
回溯應用程式模組更新.....	227
更新工作統計.....	228

關於更新工作

Kaspersky Embedded Systems Security 支援四種系統更新工作：資料庫更新、軟體模組更新、複製更新和資料庫更新回溯。

預設情況下，Kaspersky Embedded Systems Security 每小時連線一次更新來源（Kaspersky Lab 的更新電腦之一）。您可設定所有更新工作（請參見第 219 頁上的“設定更新工作”部分），除“資料庫更新回溯”工作外。修改工作設定後，Kaspersky Embedded Systems Security 會在下次啟動工作時套用新值。

不允許暫停和還原更新工作。

資料庫更新

預設情況下，Kaspersky Embedded Systems Security 會將資料庫從更新來源複製到受防護電腦，並透過執行“即時電腦防護”工作來立即開始使用這些資料庫。“自訂掃描”工作將在下次啟動時開始使用更新的資料庫。

預設情況下，Kaspersky Embedded Systems Security 每小時執行一次“資料庫更新”工作。

軟體模組更新

預設情況下，Kaspersky Embedded Systems Security 檢查更新來源上的軟體模組更新的可用性。為開始使用安裝的軟體模組，可能需要重新啟動電腦和/或重新啟動 Kaspersky Embedded Systems Security。

預設情況下，Kaspersky Embedded Systems Security 將在每週五的下午 04:00 (時間根據受防護電腦的地區設定) 執行“軟體模組更新”工作。在執行工作期間，應用程式會檢查 Kaspersky Embedded Systems Security 模組的重要排程更新的可用性，而不分發這些更新。

複製更新

預設情況下，在執行工作期間，Kaspersky Embedded Systems Security 會下載資料庫更新檔案，並將它們儲存到指定的網路或本機資料夾，不進行應用。

預設情況下，停用“複製更新”工作。

資料庫更新回溯

執行工作期間，Kaspersky Embedded Systems Security 將資料庫還原為使用之前安裝的更新。

預設情況下，停用“資料庫更新回溯”工作。

關於 Kaspersky Embedded Systems Security 軟體模組更新

Kaspersky Lab 會發佈 Kaspersky Embedded Systems Security 模組的更新套件。更新套件可以為緊急 (或重要) 和排程。重要更新套件可修復弱點和錯誤；排程更新可新增新功能或增強現有功能。

緊急 (重要) 更新套件會上傳到 Kaspersky Lab 更新伺服器。您可以使用“軟體模組更新”工作來設定自動安裝這些更新。預設情況下，Kaspersky Embedded Systems Security 將在每週五的下午 04:00 (時間根據受防護電腦的地區設定) 執行“軟體模組更新”工作。

Kaspersky Lab 不會在其用於自動更新的更新伺服器上發佈排程更新；已排程更新可從 Kaspersky Lab 網站進行下載。“軟體模組更新”工作可用於接收有關排程的 Kaspersky Embedded Systems Security 更新發佈的資訊。

您可以從網際網路將重要更新下載至每個受防護電腦，或者將一個電腦用作中間電腦，將所有更新複製給它，然後再將它們分發給網路電腦。若要複製並儲存更新而不進行安裝，請使用“複製更新”工作。

在安裝模組更新之前，Kaspersky Embedded Systems Security 會為之前安裝的模組建立備份副本。如果軟體模組更新過程中斷或產生錯誤，Kaspersky Embedded Systems Security 將自動還原為使用之前安裝的軟體模組。您可以手動將軟體模組回溯到之前安裝的更新。

在安裝下載的更新期間，Kaspersky Security 服務會自動停止，然後重新啟動。

關於 Kaspersky Embedded Systems Security 資料庫更新

儲存於受防護電腦上的 Kaspersky Embedded Systems Security 資料庫將很快過期。Kaspersky Lab 的病毒分析師每天會偵測到幾百個新威脅，他們會為這些威脅建立識別記錄，然後將其新增到應用程式資料庫更新中。資料庫更新是一個檔案或套件，其中包含自上次更新以來發現威脅特徵碼的記錄。若要維持所需等級的電腦防護，建議您定期接收資料庫更新。

預設情況下，如果 Kaspersky Embedded Systems Security 資料庫在其上次更新後一週之內未更新，系統將發生“應用程式資料庫過期”事件。如果資料庫在兩週內沒有更新，則會發生“應用程式資料庫嚴重過期”事件。資料庫目前狀態資訊(請參見第 [201](#) 頁上的“檢視防護狀態和 Kaspersky Embedded Systems Security 資訊”部分)顯示在應用程式主控台樹狀目錄的 **Kaspersky Embedded Systems Security** 節點的詳細資訊窗格中。您可以使用 Kaspersky Embedded Systems Security 一般設定來指定這些事件出現之前的不同天數。您也可以配置關於這些事件的管理員通知(請參見第 [269](#) 頁上的“設定管理員和使用者通知”部分)。

Kaspersky Embedded Systems Security 會從 Kaspersky Lab 的 FTP 或 HTTP 更新伺服器、卡巴斯基安全管理中心管理伺服器或其他更新來源中下載應用程式資料庫和模組更新。

您可以將更新下載至每個受防護電腦，或者將一台電腦用作中間電腦，將所有更新複製給它，然後再將它們分發給其他電腦。如果您使用卡巴斯基安全管理中心來集中管理公司內的電腦防護，則可以使用卡巴斯基安全管理中心管理電腦作為下載更新的中介。

可以手動啟動資料庫更新工作，也可以按排程啟動(請參見第 [189](#) 頁上的“設定工作啟動排程設定”部分)。預設情況下，Kaspersky Embedded Systems Security 每小時執行一次“資料庫更新”工作。

如果更新下載過程中斷或者產生錯誤，Kaspersky Embedded Systems Security 將自動轉換至使用上次更新的資料庫。如果 Kaspersky Embedded Systems Security 資料庫損壞，可以手動回溯(請參見第 227 頁上的“回溯 Kaspersky Embedded Systems Security 資料庫更新”部分)至先前安裝的更新。

組織內所使用的病毒防護程式資料庫和模組的更新方案

在更新工作中對更新來源的選擇取決於公司中使用的資料庫和程式模組更新方案。

您可以使用以下方案在受防護電腦上更新 Kaspersky Embedded Systems Security 資料庫和模組：

- 直接透過網際網路將更新下載到每台受防護電腦 (方案 1)。
- 透過網際網路將更新下載到中間電腦，然後再將更新從該電腦分發到其他電腦。

已安裝以下所列軟體的任何電腦均可用作中間電腦：

- Kaspersky Embedded Systems Security (方案 2)。
- 卡斯基安全管理中心管理伺服器 (方案 3)。

使用中間電腦進行更新不僅可以降低網際網路流量，還可確保其他網路電腦的安全性。

以下提供了對更新方案的敘述。

方案 1. 直接從 Internet 更新資料庫和模組

► 要設定直接透過網際網路進行 Kaspersky Embedded Systems Security 更新：

在每台受防護電腦上，在“資料庫更新”工作和“軟體模組更新”工作的設定中，將 Kaspersky Lab 的更新電腦指定為更新來源。

您可以將擁有更新資料夾的其他 HTTP 或 FTP 伺服器配置為更新來源。

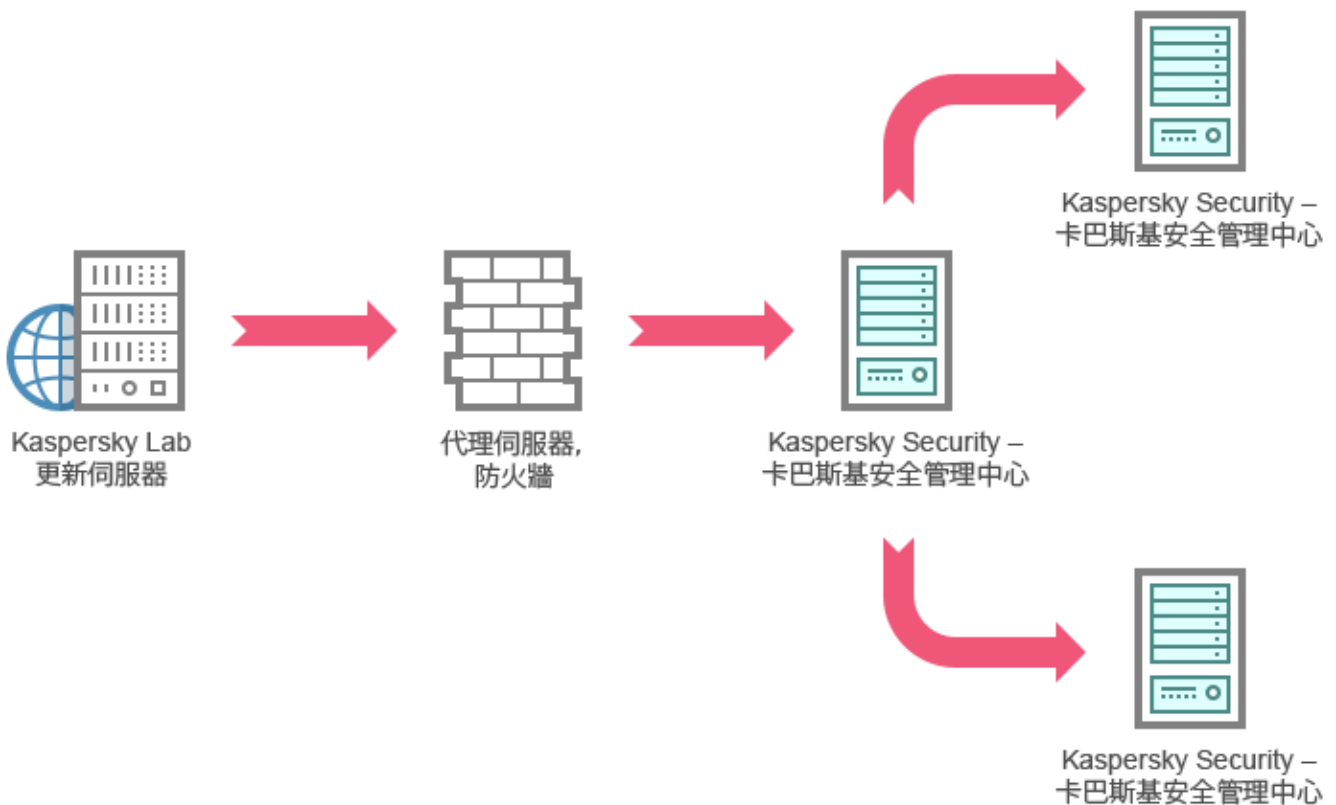


方案 2。透過一台受防護電腦更新資料庫和模組

► 要設定透過一台受防護電腦進行 *Kaspersky Embedded Systems Security* 更新：

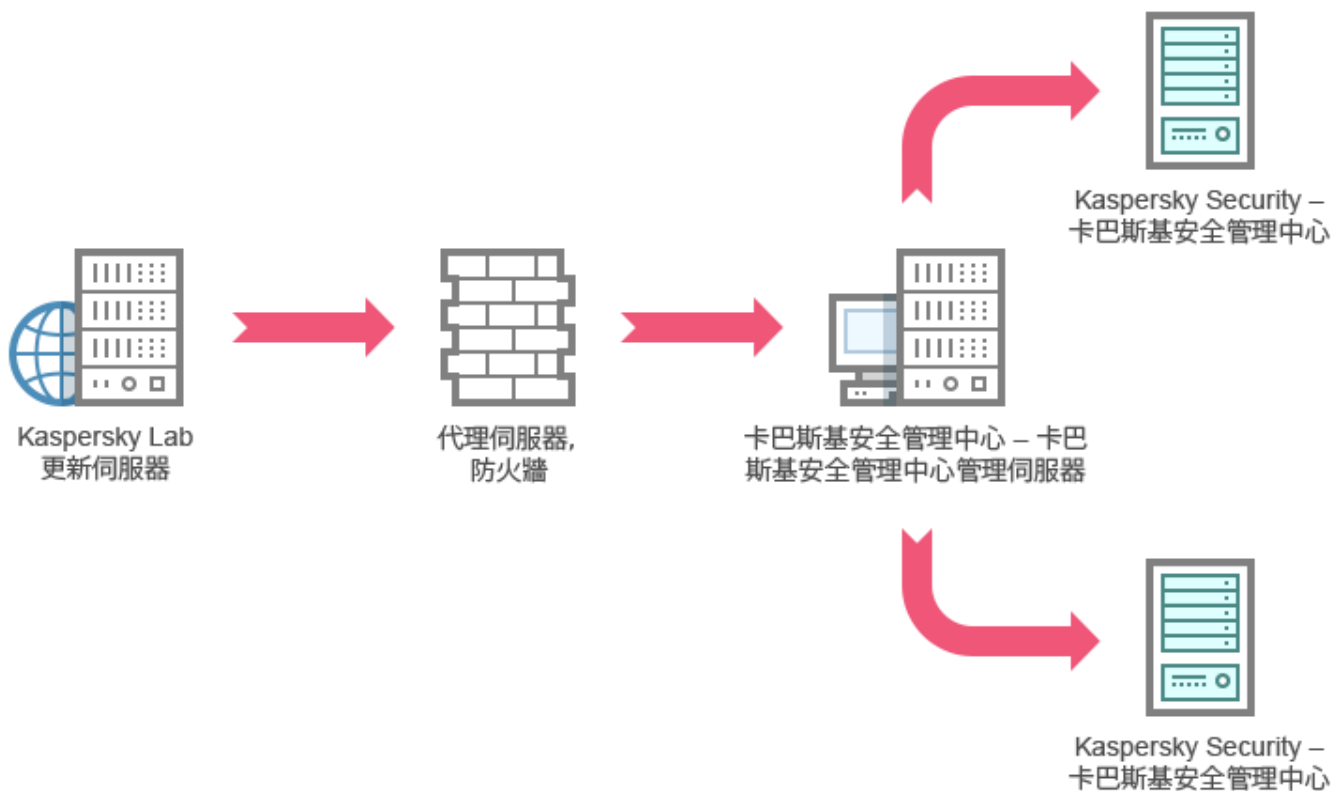
1. 將更新複製到選定的受防護電腦。為此，請執行以下操作：
 - 在選定電腦上設定“複製更新”工作設定：
 - a. 指定 Kaspersky Lab 的更新伺服器作為更新來源。
 - b. 指定用作儲存更新的資料夾的共用資料夾。
2. 將更新發佈到其他受防護電腦。為此，請執行以下操作：
 - 在每台受防護電腦上，配置“資料庫更新”工作和軟體模組更新工作的設定（請參見下圖）。
 - a. 對於更新來源，在中間電腦磁碟機上指定一個用於儲存下載更新的資料夾。

Kaspersky Embedded Systems Security 將透過一台受防護電腦獲取更新。



方案 3。透過卡斯基安全管理中心管理伺服器更新資料庫和模組

如果管理中心的應用程式用於集中管理電腦病毒防護，則可透過在區域網路中安裝的卡斯基安全管理中心管理伺服器下載更新（請參見下圖）。



► 要設定透過卡斯基安全管理中心管理伺服器進行 *Kaspersky Embedded Systems Security* 更新：

1. 將更新從 Kaspersky Lab 的更新伺服器下載到卡斯基安全管理中心管理伺服器。為此，請執行以下操作：
 - 為指定的一組電腦配置“按管理伺服器檢索更新”工作：
 - a. 指定 Kaspersky Lab 的更新伺服器作為更新來源。
2. 將更新發佈到受防護電腦。為此，請執行以下操作之一：
 - 在卡斯基安全管理中心上，設定病毒資料庫（應用程式模組）更新群組工作以將更新發佈到受防護電腦：
 - a. 在工作排程中，指定“管理伺服器擷取更新之後”作為啟動頻率。
管理伺服器將在每次接收到更新時啟動該工作（建議）。

不能在應用程式主控台中指定“管理伺服器擷取更新之後”的啟動頻率。

- 在每台受防護電腦上，設定“資料庫更新”工作和“軟體模組更新”工作：
 - a. 指定卡斯基安全管理中心管理伺服器作為更新來源。
 - b. 若有必要，設定工作排程。

如果 Kaspersky Embedded Systems Security 病毒資料庫很少更新(從每月一次至每年一次)，則能夠偵測到危險的可能性就會降低，且假報警的頻率會隨著應用程式元件的增加而增大。

Kaspersky Embedded Systems Security 將透過卡斯基安全管理中心管理伺服器獲取更新。

如果您計劃使用卡斯基安全管理中心管理電腦發佈更新，請將網路代理 (卡斯基安全管理中心發佈套件中包含的一個應用程式元件) 安裝到每台受防護電腦上。這可確保受防護電腦上的管理電腦與 Kaspersky Embedded Systems Security 進行互動。有關網路代理以及使用卡斯基安全管理中心對其進行配置的詳細資訊，請參見 *卡斯基安全管理中心管理說明*。

配置更新工作

本節提供有關如何設定 Kaspersky Embedded Systems Security 更新工作的說明。

本章節說明項目

配置使用 Kaspersky Embedded Systems Security 更新來源的設定	220
在執行資料庫更新工作時最佳化磁碟 I/O 的使用	223
設定複製更新工作設定	224
設定軟體模組更新工作設定	225

配置使用 Kaspersky Embedded Systems Security 更新來源的設定

對於除“資料庫更新回溯”工作外的每個更新工作，您可指定一個或多個更新來源，新增使用者定義的更新來源，以及設定與指定來源的連線設定。

在修改了更新工作設定後，將不會在正執行的更新工作中立即應用新設定。僅當重新開機工作時才會應用設定的設定。

► *要指定更新來源的類型：*

1. 在應用程式主控台樹狀目錄中，展開“更新”節點。
2. 選擇與要設定的更新工作相應的子節點。
3. 在所選節點的詳細資訊視窗中，點擊“內容”連結。

將開啟“工作設定”視窗的“一般”標籤。

4. 在“更新來源”部分中，選擇 Kaspersky Embedded Systems Security 更新來源的類型：
 - **卡巴斯基安全管理中心管理伺服器**

Kaspersky Embedded Systems Security 使用卡巴斯基安全管理中心管理伺服器作為更新來源。

只有網路中的 Kaspersky Lab 應用程式使用卡巴斯基安全管理中心遠端存取系統進行管理，並且受防護電腦上安裝有網路代理（在電腦與管理電腦之間提供連線的卡巴斯基安全管理中心元件），才能選擇該選項。

- **Kaspersky Lab 更新伺服器**

Kaspersky Embedded Systems Security 將 Kaspersky Lab 網站用作更新來源，為公司所有產品託管資料庫和軟體模組更新。

預設選中該選項。

- **自訂 HTTP 或 FTP 伺服器，或網路資料夾**

Kaspersky Embedded Systems Security 將管理員指定的 HTTP 或 FTP 電腦或區域網路電腦上的資料夾用作更新來源。

您可以點擊“**自訂 HTTP 或 FTP 伺服器，或網路資料夾**”連結，建立包含最新更新的來源清單。

5. 如有需要，為使用者定義的更新來源設定進階設定：

a. 點擊“**自訂 HTTP 或 FTP 伺服器，或網路資料夾**”連結。

i. 在開啟的“**更新伺服器**”視窗中，選中或清除使用者定義的更新來源旁邊的核取方塊，以便開始或終止其使用。

ii. 點擊“**確定**”。

b. 在“**更新來源**”部分的“**一般**”標籤中，選中或清除“**如果指定的伺服器無法使用，則使用 Kaspersky Lab 更新伺服器**”核取方塊。

該核取方塊用於在使用者定義的更新來源不可用時啟用或停用將 Kaspersky Lab 更新伺服器用作更新來源的選項。

如果選中該核取方塊，則啟用該功能。

預設將會選定該核取方塊。

在“**如果指定的伺服器無法使用，則使用 Kaspersky Lab 更新伺服器**”選項啟用時，您可以選中“**自訂 HTTP 或 FTP 伺服器，或網路資料夾**”核取方塊。

6. 在“**工作設定**”視窗中，選擇“**連線設定**”標籤以設定用於連線到更新來源的設定：

• 清除或選中“**使用指定的代理伺服器設定以連線至 Kaspersky Lab 更新伺服器**”核取方塊。

該核取方塊用於在透過 Kaspersky Lab 伺服器接收更新或選中“**如果指定的伺服器不可用，則使用 Kaspersky Lab 更新伺服器**”核取方塊時啟用/停用代理伺服器設定。

如果選中該核取方塊，則使用代理伺服器設定。

如果取消選中該核取方塊，則不使用代理伺服器設定。

預設將會選定該核取方塊。

- 清除或選中“**使用代理伺服器設定連線至其他伺服器**”核取方塊。

該核取方塊用於在選擇選項“**自訂 HTTP 或 FTP 伺服器，或網路資料夾**”作為更新來源時啟用或停用代理伺服器設定。

如果選中該核取方塊，則使用代理伺服器設定。

預設取消選定該核取方塊。

有關配置用於存取代理伺服器的可選代理伺服器設定和身分驗證設定的資訊，請參閱“[啟動和配置 Kaspersky Embedded Systems Security 資料庫更新工作](#)”部分。

7. 點擊“**確定**”。

Kaspersky Embedded Systems Security 更新來源的已配置設定將被儲存並在下次工作啟動時套用。

您可管理使用者定義的 Kaspersky Embedded Systems Security 更新來源清單。

► 編輯使用者定義的應用程式更新來源清單：

1. 在應用程式主控台樹狀目錄中，展開“**更新**”節點。
2. 選擇與要設定的更新工作相應的子節點。
3. 在所選節點的詳細資訊視窗中，點擊“**內容**”連結。

將開啟“**工作設定**”視窗的“**一般**”標籤。

4. 點擊“**自訂 HTTP 或 FTP 伺服器，或網路資料夾**”連結。

將開啟“**更新伺服器**”視窗。

5. 執行以下操作：

- 要新增新的使用者定義的更新來源，在輸入欄位中，定義 FTP 或 HTTP 伺服器上包含更新檔案的資料夾位址；按 UNC (通用命名慣例) 格式指定本機或網路資料夾。點擊 **ENTER** 鍵。
預設情況下，已新增的資料夾用作更新來源。
- 要停用使用者定義的更新來源，則清除清單中的更新來源旁邊的核取方塊。

- 要啟用使用者定義的更新來源，則選中清單中的更新來源旁邊的核取方塊。
- 若要變更 Kaspersky Embedded Systems Security 存取使用者定義更新源的順序，請使用“上移”和“下移”按鈕將選定的源移至清單的開頭或末尾，具體取決於是在其他來源之前還是之後使用該來源。
- 若要變更使用者定義的更新來源的路徑，請在清單中選擇來源，點擊“編輯”按鈕，在輸入欄位中進行所需的變更，然後按 **ENTER** 鍵。
- 若要刪除使用者定義的更新來源，請在清單中選擇該來源，然後點擊“刪除”按鈕。

您無法從清單中刪除剩餘的唯一一個使用者定義的來源。

6. 點擊“確定”。

將儲存使用者定義的應用程式更新來源清單的變更。

在執行資料庫更新工作時最佳化磁碟 I/O 的使用

執行“資料庫更新”工作時，Kaspersky Embedded Systems Security 會將更新檔案儲存在電腦的本機磁碟上。您可以在執行更新工作時將更新檔案儲存在記憶體中虛擬磁碟機上，從而降低電腦的磁碟 I/O 子系統的工作負載。

此功能可用於 Microsoft Windows 7 作業系統及更高版本。

在執行“資料庫更新”工作時使用此功能，會在作業系統中出現一個額外的邏輯磁碟機。工作完成之後，此邏輯磁碟機將從作業系統中刪除。

► 若要減輕資料庫更新工作期間電腦磁碟 I/O 子系統的工作負載，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“更新”節點。
2. 選擇“資料庫更新”子節點。

3. 在“**資料庫更新**”節點的詳細資訊視窗中，點擊“**內容**”連結。
4. 將開啟“**工作設定**”視窗的“**一般**”標籤。
5. 在“**磁碟 I/O 使用情況最佳化**”部分中，定義以下設定：
 - 清除或選中“**降低磁碟 I/O 上的負載**”核取方塊。

使用此核取方塊可以啟用或停用透過將更新檔案儲存在記憶體中的虛擬磁碟機上實現磁碟子系統最佳化的功能。

如果選中該核取方塊，則啟用該功能。

預設取消選定該核取方塊。

- 在“**用於最佳化 RAM**”欄位中，指定記憶體容量（以 MB 為單位）。作業系統臨時分配指定的記憶體容量，用於在執行工作時儲存更新檔案。預設記憶體大小為 512 MB。最小記憶體大小為 400 MB。

6. 點擊“**確定**”。

已設定的設定將被儲存，並在下次工作啟動時應用。

配置複製更新工作設定

► 要設定複製更新工作：

1. 在應用程式主控台樹狀目錄中，展開“**更新**”節點。
2. 選擇“**複製更新**”子節點。
3. 在“**複製更新**”節點的詳細資訊視窗中，點擊“**內容**”連結。

將開啟“**工作設定**”視窗。

4. 在“**一般**”和“**連線設定**”標籤上，配置使用更新來源的設定（請參見第 [220](#) 頁上的“配置使用 Kaspersky Embedded Systems Security 更新來源的設定”部分）。
5. 在“**一般**”標籤上的“**複製更新設定**”部分：
 - 指定複製更新的條件：
 - **複製資料庫更新**。

Kaspersky Embedded Systems Security 僅下載軟體資料庫更新。

預設選中該選項。

- **複製軟體模組的重要更新。**

Kaspersky Embedded Systems Security 僅下載緊急 Kaspersky Embedded Systems Security 軟體模組更新。

- **複製資料庫更新與軟體模組的重要更新。**

Kaspersky Embedded Systems Security 下載 Kaspersky Embedded Systems Security 的軟體資料庫更新和關鍵軟體模組更新。

- 指定 Kaspersky Embedded Systems Security 用來分發下載更新的本機或網路資料夾。
6. 在“**排程**”和“**進階**”標籤上，設定工作啟動排程 (請參見第 [189](#) 頁上的“設定工作啟動排程設定”部分)。
 7. 在“**執行帳戶**”標籤上，將工作設定為使用帳戶權限啟動 (請參見第 [192](#) 頁上的“指定使用者帳戶以執行工作”部分)。
 8. 點擊“**確定**”。

已設定的設定將被儲存，並在下次工作啟動時應用。

配置軟體模組更新工作設定

► 要配置“軟體模組更新”工作：

1. 在應用程式主控台樹狀目錄中，展開“**更新**”節點。
2. 選擇“**軟體模組更新**”子節點。
3. 在“**軟體模組更新**”節點的詳細資訊視窗中，點擊“**內容**”連結。

將開啟“**工作設定**”視窗。

4. 在“**一般**”和“**連線設定**”標籤上，配置使用更新來源的設定 (請參見第 [220](#) 頁上的“配置使用 Kaspersky Embedded Systems Security 更新來源的設定”部分)。

5. 在“一般”標籤上的“應用程式更新設定”標籤上，配置用於更新應用程式模組的設定：
 - **僅檢查關鍵軟體更新是否可用**

Kaspersky Embedded Systems Security 顯示更新來源中可用的軟體模組緊急更新的通知，但不下載更新。如果啟用此類事件通知，將顯示該通知。

預設選中該選項。
 - **複製並安裝軟體模組的重要更新**

Kaspersky Embedded Systems Security 下載並安裝軟體模組的重要更新。
 - **允許作業系統重新啟動**

在安裝需要重新開機的更新後，作業系統會重新開機。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會在安裝需要重新啟動的更新後重新啟動作業系統。

如果選中“**複製並安裝軟體模組的重要更新**”選項，則該核取方塊才可用。

預設取消選定該核取方塊。
 - **接收有關可用的排程軟體模組更新的資訊**

顯示更新來源中所有可用的 Kaspersky Embedded Systems Security 軟體模組排程更新的通知。如果啟用此類事件通知，應用程式會顯示相關通知。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會顯示更新來源中所有可用的軟體模組排程更新的通知。

預設將會選定該核取方塊。
6. 在“排程”和“進階”標籤上，設定工作啟動排程(請參見第 [189](#) 頁上的“設定工作啟動排程設定”部分)。預設情況下，Kaspersky Embedded Systems Security 將在每週五的下午 04:00 (時間根據受防護電腦的地區設定) 執行“軟體模組更新”工作。
7. 在“執行帳戶”標籤上，將工作設定為使用帳戶權限啟動(請參見第 [192](#) 頁上的“指定使用者帳戶以執行工作”部分)。
8. 點擊“確定”。

已設定的設定將被儲存，並在下次工作啟動時應用。

Kaspersky Lab 不會在更新伺服器上發佈排程的軟體更新套件以供自動安裝；您可以手動從 Kaspersky Lab 網站下載這些軟體更新套件。您可以設定有關“*有新的排程軟體模組更新可用事件*”事件的管理員通知；該通知將包含我們網站上可下載排程更新頁面的 URL。

回溯 Kaspersky Embedded Systems Security 資料庫更新

在應用資料庫更新之前，Kaspersky Embedded Systems Security 會建立先前使用資料庫的備份副本。如果更新中斷或發生錯誤，Kaspersky Embedded Systems Security 將自動還原為使用之前安裝的資料庫。

如果在您已更新後出現任何問題，則可透過“資料庫更新回溯”工作將資料庫回溯到之前安裝的更新。

► 若要啟動“資料庫更新回溯”工作，請執行以下操作：

在“**資料庫更新回溯**”節點的詳細資訊視窗中，點擊“**啟動**”連結。

回溯應用程式模組更新

在不同 Windows 作業系統中，設定的名稱可能會有所不同。

在套用軟體模組更新之前，Kaspersky Embedded Systems Security 會為目前使用的模組建立備份副本。如果模組更新過程中斷或發生錯誤，Kaspersky Embedded Systems Security 將自動還原為使用最新安裝更新版本的資料庫。

若要回溯軟體模組，請使用 Microsoft Windows 元件“**安裝和刪除應用程式**”。

更新工作統計

執行更新工作期間，可以檢視有關在啟動工作後到目前時間這一時段內所下載的資料量的即時資訊，以及其他工作執行統計。

工作完成或停止後，您可以在工作記錄中檢視此資訊。

► 若要檢視更新工作統計，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“更新”節點。
2. 選擇與要檢視其統計的工作相應的子節點。

工作統計顯示在選定節點的詳細資訊視窗的“統計”部分中。

如果您正檢視“資料庫更新”工作或“複製更新”工作，則“統計”塊將顯示目前 Kaspersky Embedded Systems Security 已下載的資料量（“已接收資料”）。

如果您正檢視“軟體模組更新”工作，則會看到下表中所述的資訊。

表 32. 有關“軟體模組更新”工作的資訊

欄位	敘述
已接收資料	已下載資料的總量。
可用的重要更新	可進行安裝的重要更新數。
可用的排程更新	可進行安裝的排程更新數。
套用更新時發生錯誤	如果該欄位的值不為零，則表示未應用更新。可在工作記錄中檢視在其套用過程中導致出錯的更新的名稱(請參見第 257 頁上的“在工作記錄中檢視有關 Kaspersky Embedded Systems Security 工作的統計和資訊”部分)。

物件隔離和備份複製

本節提供了有關在清除或刪除之前備份偵測到的惡意物件的資訊，以及有關隔離可疑感染物件的資訊。

本章內容

隔離可疑感染物件。隔離	229
製作物件的備份副本。備份	241

隔離可疑感染物件。隔離

本章節介紹如何隔離可疑感染物件以及配置隔離區設定。

本章節說明項目

關於隔離可疑感染的物件	229
檢視隔離區物件	229
隔離區掃描	232
還原隔離的物件	234
將物件移到隔離	236
從隔離區刪除物件	237
傳送可疑感染物件到 Kaspersky Lab 以供分析	237
配置隔離區設定	239
隔離統計	240

關於隔離可疑感染的物件

Kaspersky Embedded Systems Security 透過將疑似感染的物件從原始位置移動到 **隔離區** 資料夾來進行隔離。出於安全考慮，物件以加密形式儲存在隔離區資料夾中。

檢視隔離物件

您可以從應用程式主控台的“**隔離**”節點檢視已隔離的物件。

► 若要檢視隔離的物件，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“儲存”節點。
2. 選擇“隔離”子節點。

有關已隔離物件的資訊顯示在選定節點的詳細資訊視窗中。

► 在已隔離物件清單中尋找所需的物件：

排序物件（請參見第 [230](#) 頁上的“排序隔離的物件”部分）或篩選物件（請參見第 [231](#) 頁上的“篩選隔離的物件”部分）。

本章節說明項目

排序隔離的物件	230
篩選隔離的物件	231

排序隔離的物件

預設情況下，已隔離物件清單中的物件按照隔離日期從新到舊進行排列。若要尋找所需物件，您可以點擊包含有關物件資訊的欄位排序物件。如果關閉“隔離”節點，然後重新開啟，則將儲存排序結果；如果關閉應用程式主控台，則儲存 msc 檔案，然後從該檔案重新開啟排序結果。

► 若要排序物件，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“儲存”節點。
2. 選擇“隔離”子節點。
3. 在“隔離”節點的詳細資訊視窗中，選擇想要用於對清單中的物件進行排序的欄位標題。

清單中的物件將基於選定設定排序。

篩選隔離的物件

若要檢視所需的已隔離物件，您可以篩選清單中的物件 - 只顯示符合您指定的篩選標準(篩選器)的物件。如果離開再重新開啟“**隔離**”節點，則將儲存篩選結果；如果關閉應用程式主控台，可以儲存 msc 檔案，然後從該檔案重新開啟篩選結果。

► 若要指定一個或多個篩選器，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“**儲存**”節點。
2. 選擇“**隔離**”子節點。
3. 在節點名稱的內容功能表中，選擇“**篩選**”。

將開啟“**篩選設定**”視窗。

4. 若要新增篩選器，請執行以下步驟：

- a. 在“**欄位名稱**”中，選擇將比較篩選值的項。
- b. 在“**運算子**”清單中選擇篩選條件。清單中篩選條件的值可能有所不同，具體取決於您在“**欄位名稱**”清單中選定的值。
- c. 在“**欄位值**”欄位中輸入篩選值，或者從清單中進行選擇。
- d. 點擊“**新增**”按鈕。

已新增的篩選將出現在“**篩選設定**”視窗的篩選清單中。對於要新增的每個篩選重複步驟 a-d。使用篩選器時請遵循以下方式：

- 若要使用邏輯運算子“AND”組合多個篩選，請選擇“**如果符合所有條件**”。
- 若要使用邏輯運算子“OR”組合多個篩選，請選擇“**如果符合任何條件**”。
- 若要刪除篩選，請選擇篩選列表中要刪除的篩選，然後點擊“**刪除**”按鈕。
- 若要編輯篩選，請從“**篩選設定**”視窗的清單中選擇該篩選器。然後在“**欄位名稱**”、“**運算子**”或“**欄位值**”欄位中變更所設定值，並按點擊“**取代**”按鈕。

5. 新增所有篩選後，點擊“**套用**”按鈕。

將儲存已建立的篩選器。

► 若要重新顯示已隔離物件清單中的所有物件，

在“隔離”節點的內容功能表中，選擇“刪除”篩選。

隔離區掃描

預設情況下，每次資料庫更新之後，Kaspersky Embedded Systems Security 都會執行“隔離區掃描”系統工作。工作設定在下表敘述。無法修改“隔離區掃描”工作的設定。

您可以配置工作啟動排程（請參見第 189 頁上的“配置工作啟動排程設定”部分），手動啟動它以及修改用於啟動工作的帳戶權限（請參見第 192 頁上的“指定使用者帳戶以執行工作”部分）。

透過在更新資料庫後掃描隔離物件，Kaspersky Embedded Systems Security 能夠將某些物件重新歸類為未被感染：此類物件的狀態會變更為“誤報”。其他物件可被重新歸類為已感染，在這種情況下，Kaspersky Embedded Systems Security 會根據“隔離區掃描”工作設定（解毒，或解毒失敗則刪除）所指定來處理此類物件。

表 33. 隔離區掃描工作設定

隔離區掃描工作設定	值
掃描範圍	隔離資料夾
安全性設定	適用整個掃描區域；它們的值在下一個清單中提供

表 34. “隔離區掃描”工作中的掃描設定

安全性設定	值
掃描物件	包含在掃描範圍內的所有物件
最佳化	已停用
要對受感染的物件和其他偵測到的物件執行的操作	解毒，如果無法解毒則刪除
對受感染的物件執行的操作	略過
排除物件	否

安全性設定	值
不偵測	否
執行超過以下時間 (秒) 時停止掃描	未設定
不掃描大於以下大小的物件(MB)	未設定
掃描 NTFS 交換資料串流	已啟用
磁碟機的開機磁區和 MBR	已停用
使用 iChecker 技術	已停用
使用 iSwift 技術	已停用
掃描複合檔案	<ul style="list-style-type: none"> • 壓縮檔案* • SFX 壓縮檔案* • 封裝的物件* • 內嵌的 OLE 物件* <p>* “停用僅掃描新檔案和變更的檔案”已停用。</p>
檢查 Microsoft 簽章的檔案	未執行
使用啟發式分析	已啟用深度分析等級
信任區域	未套用

還原隔離的物件

Kaspersky Embedded Systems Security 以加密形式將可疑感染物件放入隔離區資料夾中，以防護受防護電腦免受可能的有害影響。

您可以從隔離區還原任意物件。在以下情況下，可能需要執行以下操作：

- 如果使用更新的資料庫進行隔離區掃描之後，物件的狀態變更為“誤報”或“已解毒”。
- 如果您認為物件對電腦存在危害，而又希望使用該檔案。如果您希望 Kaspersky Embedded Systems Security 在後續掃描期間不將該物件隔離，可以將該物件從“即時檔案防護”工作和“自訂掃描”工作的處理中排除。若要執行該操作，請將物件指定為**排除檔案**（按檔案名稱）的值或在這些工作中指定**不偵測**安全性設定，或者將物件新增到信任區域（請參見第 559 頁）。

在還原物件時，您可以選擇將儲存還原的物件的位置：原始位置（預設）、受防護電腦上針對還原物件的特殊資料夾、安裝應用程式主控台的電腦或者網路中的其他電腦上的自訂資料夾。

“**還原到資料夾**”選項用於在受防護電腦上儲存還原物件。您可以為需要掃描的物件配置特殊的安全性設定。該資料夾的路徑由隔離區設定。

從隔離區中還原物件可能會導致電腦感染病毒。

您可以還原物件，並將其副本儲存到隔離區資料夾中以備稍後使用，例如資料庫更新之後重新掃描物件。

如果已隔離物件包含在複合檔案中（例如壓縮檔案），Kaspersky Embedded Systems Security 還原期間將不會包括此複合檔案，而是單獨儲存到選定的資料夾。

您可以還原一個或多個物件。

► 若要還原已隔離的物件，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“**儲存**”節點。
2. 選擇“**隔離**”子節點。

3. 在“隔離”節點的詳細視窗中執行以下之一操作：
 - 若要還原一個物件，請從要還原的物件的內容功能表中選擇“還原”。
 - 若要還原多個物件，請使用 **CTRL** 或 **SHIFT** 鍵選取想要還原的物件，右鍵點擊其中一個選定的物件，並在上下文功能表中選取“還原”。

“還原物件”視窗開啟。

4. 在“還原物件”視窗中，為每個選定物件指定將儲存還原物件的資料夾。

物件的名稱顯示在視窗上部的“物件”欄位中。如果選定多個物件，系統將顯示選定物件清單中第一個物件的名稱。

5. 執行以下步驟之一：
 - 若要將物件還原到原始位置，請選擇“還原到來源資料夾”。
 - 若要將物件還原到設定中的適用於還原物件位置所指定的資料夾，請選擇“還原到預設還原資料夾”。
 - 若要將物件儲存在安裝應用程式主控台的電腦上的其他資料夾或共用資料夾，請選擇“還原至本機電腦或網路資源上的資料夾”，然後選擇所需資料夾或指定資料夾路徑。
6. 如果希望於還原之後在隔離區資料夾中儲存物件的副本，請清除“還原物件後從儲存區中刪除物件”核取方塊。
7. 若要為其餘選定物件套用指定的還原條件，請選定“套用至所有選擇的物件”核取方塊。

所有選定物件都將還原並儲存到指定資料夾：如果選擇“還原到來源資料夾”，則每個物件都將儲存到其原始位置；如果選擇“還原到預設還原資料夾”或“還原至本機電腦或網路資源上的資料夾”，則所有物件都將儲存到您所指定的資料夾。

8. 點擊“確定”。

Kaspersky Embedded Systems Security 將開始還原選定物件的第一個物件。

9. 如果指定位置已存在擁有該名稱的物件，則系統將開啟“已存在具有此名稱的物件”視窗。
 - a. 選擇以下 Kaspersky Embedded Systems Security 操作之一：
 - “**取代**”，使用還原物件取代現有物件。
 - “**重新命名**”，使用其他名稱儲存還原的物件。在輸入欄位中輸入新物件的檔案名稱和檔案的完整路徑。
 - “**透過新增後置詞重命名**”，透過為物件檔案名稱新增後置詞重新命名物件。在項目欄位中輸入後置詞。
 - b. 如果選定還原多個物件，要將選定的操作（例如透過新增後置詞來“**取代**”或“**重新命名**”）套用到其餘選定物件，請選定“**套用至所有選擇的物件**”核取方塊。（如果已選擇“**重新命名**”，“**套用至所有選擇的物件**”核取方塊將不可用。）
 - c. 點擊“**確定**”。

物件將被還原。有關還原操作的資訊將輸入到系統稽核記錄中。

如果您在“**還原物件**”視窗中沒有選擇“**套用至所有選擇的物件**”，“**還原物件**”視窗將再次開啟。您可以使用該視窗指定儲存下個選定物件的位置（請參閱流程的步驟 4）。

將物件移到隔離

您可以手動隔離檔案。

► 若要隔離檔案，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，開啟“**隔離**”節點的內容功能表。
2. 選擇“**新增**”。
3. 在“**開啟**”視窗中，選擇磁碟上您想要隔離的檔案。
4. 點擊“**確定**”。

Kaspersky Embedded Systems Security 將隔離選定檔案。

從隔離區刪除物件

根據隔離區掃描工作的設定，如果在使用更新的資料庫掃描隔離期間物件狀態變更為 *已感染*，並且 Kaspersky Embedded Systems Security 無法解毒這些物件，Kaspersky Embedded Systems Security 將從隔離區資料夾自動刪除這些物件。Kaspersky Embedded Systems Security 不會從隔離中刪除其他物件。

您可以從隔離區刪除一個或多個物件。

► 若要從隔離區刪除一個或多個物件，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“**儲存**”節點。
2. 選擇“**隔離**”子節點。
3. 執行以下步驟之一：
 - 若要刪除一個物件，請從物件名稱的內容功能表中選擇“**刪除**”。
 - 若要刪除多個物件，請使用 **Ctrl** 或 **Shift** 鍵選擇想要刪除的物件，並在其中任何一個選定物件上開啟內容功能表，然後選擇“**刪除**”。
4. 在確認視窗中點擊“**是**”按鈕以確認操作。

將從隔離區刪除選定物件。

傳送可疑感染物件到 Kaspersky Lab 以供分析

如果某個檔案的行為使您懷疑該檔案可能包含威脅，並且 Kaspersky Embedded Systems Security 認定該檔案需要解毒，則您可能遇到未知威脅，而該威脅的特徵碼尚未新增到資料庫。您可以將此檔案傳送到 Kaspersky Lab 以供分析。Kaspersky Lab 的病毒分析人員將對檔案進行分析，如果偵測到檔案中包含新威脅，則將在資料庫中新增記錄標識該威脅。可能您在資料庫更新之後重新掃描物件時，Kaspersky Embedded Systems Security 將發現此物件並未感染，並能夠將其解毒。您不僅能夠保留物件，而且能夠預防病毒爆發。

僅能傳送已隔離的檔案以供分析。已隔離的檔案會以加密的形式儲存，且在傳輸過程中不會被安裝在郵件伺服器上的病毒防護程式刪除。

產品授權過期之後，您不能將已隔離的物件傳送到 Kaspersky Lab 以供分析。

► 若要傳送檔案到 Kaspersky Lab 以供分析，請執行以下步驟：

1. 如果檔案尚未被隔離，請首先**隔離**。
2. 在“**隔離**”節點中，在想要傳送物件進行分析的檔案上開啟內容功能表並選擇內容功能表中的“**傳送物件進行分析**”。
3. 如果您確定要傳送選定物件以供分析，在開啟的確認視窗中，點擊“**是**”。
4. 如果安裝應用程式主控台的電腦上已設定郵件用戶端，則將新建電子郵件訊息。檢視該訊息並點擊“**傳送**”按鈕。

“**收件者**”欄位包含 Kaspersky Lab 電子郵件信箱 newvirus@kaspersky.com。“**主旨**”欄位將包含“已隔離的物件”文字。

訊息文字將包含以下文字：“此檔案將傳送到 Kaspersky Lab 以供分析。”您可以在訊息文字中包含有關該檔案任何的附加資訊：您為何認為該檔案為可疑感染或存在危險、該檔案的行為如何或該檔案對系統有何影響。

壓縮檔案 <檔案名稱>.cab 將附加到訊息。該壓縮檔案將包含 <uuid>.klq 檔案，其中包含加密形式的物件；<uuid>.txt 檔案，其中包含有關 Kaspersky Embedded Systems Security 提取關於物件的資訊；以及 Sysinfo.txt 檔案，其中包含有關電腦上安裝的 Kaspersky Embedded Systems Security 和作業系統的以下資訊：

- 作業系統的名稱和版本。
- Kaspersky Embedded Systems Security 的名稱和版本。
- 已安裝最新資料庫更新的發佈日期。
- 啟動金鑰。

卡斯基的病毒分析人員需要上述資訊才能更快更有效地分析您的檔案。但是，如果您不想傳輸此資訊，可以刪除壓縮檔案中的 Sysinfo.txt 檔案。

如果具有應用程式主控台的電腦上未安裝郵件用戶端，則應用程式會提示您將選定已加密物件儲存到檔案。手動將該檔案傳送到 Kaspersky Lab。

► 若要將已加密物件儲存到檔案，請執行以下步驟：

1. 在開啟提示儲存物件的視窗中，點擊“**確定**”。
2. 選擇受防護電腦磁碟上的資料夾或網路資料夾，其中將儲存包含物件的檔案。

會將物件儲存到 CAB 檔案。

配置隔離設定

您可設定隔離區設定。儲存後將立即套用新的隔離設定。

► 若要配置隔離區設定，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“**儲存**”節點。
2. 開啟“**隔離**”子節點的內容功能表。
3. 選擇“**內容**”。
4. 在“**隔離內容**”視窗中，根據您的要求配置所需的隔離區設定：

- 在“**隔離設定**”部分中：

- **隔離資料夾**

隔離區資料夾的路徑，路徑格式為 UNC (通用命名慣例)。

預設路徑為 C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Quarantine\。

- **隔離最大容量**

該核取方塊用於啟用或停用監控儲存在隔離區資料夾中的物件的總大小的功能。如果超過指定的值(預設值為 200 MB)，Kaspersky Embedded Systems Security 會記錄“**已超過最大隔離容量**”事件，並根據此事件類型的通知設定發佈通知。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會監控置於隔離區的物件的總大小。

如果清除該核取方塊，Kaspersky Embedded Systems Security 不會監控置於隔離區的物件的總大小。

預設取消選定該核取方塊。

- 可用空間上限值

如果隔離區中的物件大小超過最大隔離區容量或超過可用空間上限值，在您繼續將物件放入隔離區時，Kaspersky Embedded Systems Security 將通知您此情況。

- 在“還原設定”部分中：
 - 還原物件的指定資料夾

5. 點擊“確定”。

將儲存為隔離區新設定的設定。

隔離統計

您可以檢視有關已隔離物件數量的資訊 - 隔離統計。

► 若要檢視隔離統計，

在應用程式主控台樹狀目錄的“隔離”節點的內容功能表中，選擇“統計”。

“統計”視窗將顯示目前儲存在隔離物件數量的相關資訊（請參閱下表）：

欄位	敘述
疑似感染的物件	Kaspersky Embedded Systems Security 發現的疑似被感染的物件數。
已使用的隔離區空間	隔離區資料夾中的資料總大小

欄位	敘述
誤報	因使用更新的資料庫於隔離區掃描期間歸類為未被感染而收到“誤報”狀態的物件數。
物件已解毒	隔離區掃描之後收到“已解毒”狀態的物件數。
物件總數	隔離區中的物件總數。

製作物件的備份副本。備份

本章節提供有關在解毒或刪除之前備份偵測到的惡意物件以及設定備份的說明。

本章節說明項目

關於備份物件之後再解毒或刪除.....	241
檢視備份中儲存的物件.....	242
從備份還原檔案.....	244
從備份刪除檔案.....	247
設定備份設定.....	247
備份統計.....	249

關於備份物件之後再解毒或刪除

對於被歸類為“已感染”的物件，Kaspersky Embedded Systems Security 會在對其進行解毒或刪除之前，在備份中儲存這些物件的加密副本。

如果該物件是複合檔案的一部分（例如壓縮檔案的一部分），Kaspersky Embedded Systems Security 會將此複合檔案整體儲存在備份中。例如，如果 Kaspersky Embedded Systems Security 偵測到郵件資料庫其中一個物件感染病毒，則會備份整個郵件資料庫。

Kaspersky Embedded Systems Security 放入備份中的大型檔案可能會降低系統速度，並減少硬碟上的磁碟空間。

您可以從備份將檔案還原到其原始資料夾或還原到受防護電腦上其他資料夾或者區域網路中的其他電腦。您可以從備份中還原檔案，例如，如果受感染物件包含重要資訊，但是 Kaspersky Embedded Systems Security 對該檔案在解毒期間無法保證檔案的完整性，因此該重要資訊將無法使用。

從備份中還原檔案可能會導致電腦感染病毒。

檢視備份中儲存的檔案

只能使用應用程式主控台中的“備份”節點將物件儲存在備份資料夾中。您無法使用 Microsoft Windows 檔案管理員檢視這些檔案。

► 若要檢視備份中的物件，

1. 在應用程式主控台樹狀目錄中，展開“儲存”節點。
2. 選擇“備份”子節點。

有關置於備份中的物件的資訊顯示在選定節點的詳細資訊視窗中。

► 若要在備份中的物件清單中尋找所需物件，

排序物件或篩選物件。

本章節說明項目

排序備份中的檔案	243
篩選備份中的檔案	243

排序備份中的檔案

設情況下，按儲存日期倒序排序備份中的檔案。預若要尋找所需要的檔案，您可以根據詳細資訊視窗中任意欄的內容排序檔案。

如果離開並重新開啟“備份”節點，則將儲存排序結果；如果關閉應用程式主控台，則儲存 msc 檔案，然後從該檔案重新開啟排序結果。

► 若要排序備份中的檔案，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“儲存”節點。
2. 選擇“備份”子節點。
3. 在備份的檔案清單中，選擇想要用於排序物件的標題列。

將基於選定標準排序備份中的檔案。

篩選備份中的檔案

若要尋找備份中的所需檔案，您可以篩選檔案：在“備份”節點中只顯示符合您指定的篩選標準（篩選器）的檔案。

如果離開再重新開啟“備份”節點，則系統將儲存排序結果；或者如果關閉應用程式主控台，則儲存 msc 檔案，然後從該檔案重新開啟該排序結果。

► 若要篩選備份中的檔案，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，開啟“備份”節點的內容功能表，並選擇“篩選”。

將開啟“篩選設定”視窗。

2. 若要新增篩選器，請執行以下步驟：
 - a. 從“欄位名稱”清單中，指定在選擇期間根據篩選值所對比的欄位。
 - b. 在“運算子”清單中選擇篩選條件。清單中篩選條件的值可能有所不同，具體取決於您在“欄位名稱”欄位中選定的值。
 - c. 在“欄位值”欄位中輸入篩選值或者選擇篩選值。

d. 點擊“新增”按鈕。

已新增的篩選將出現在“篩選設定”視窗的篩選清單中。對於要新增的每個篩選重複這些步驟。使用篩選器時可遵循以下方式：

- 若要使用邏輯運算子“AND”組合多個篩選，請選擇“如果符合所有條件”。
- 若要使用邏輯運算子“OR”組合多個篩選，請選擇“如果符合任何條件”。
- 若要刪除篩選，請選擇篩選列表中要刪除的篩選，然後點擊“刪除”按鈕。
- 若要編輯篩選，請從“篩選設定”視窗的篩選清單中選擇篩選器，修改“欄位名稱”、“運算子”或“欄位值”欄位中的設定值，並點擊“取代”按鈕。

新增所有的篩選之後，點擊“套用”按鈕。只有由您指定篩選選定的檔案將顯示在清單中。

- ▶ 若要顯示備份儲存物件清單中包括的所有檔案，
在“備份”節點的內容功能表，選擇“刪除篩選”。

從備份還原檔案

Kaspersky Embedded Systems Security 以加密形式將檔案儲存在備份資料夾中，以防護受防護電腦免受可能的有害影響。

所有檔案都可以從備份還原。

在下列情況下可能需要還原物件：

- 如果顯示受感染的原始檔案原本包含重要資訊，Kaspersky Embedded Systems Security 將無法保證其完整性，檔案中的資訊可能會變得無法使用。
- 如果您認為檔案對電腦存在危害，而又希望使用該檔案。如果您不希望 Kaspersky Embedded Systems Security 將該檔案視為已感染或可疑感染，則在後續掃描期間，可以將其從“即時檔案防護”工作和自訂掃描工作的處理中排除。為此，請在對應工作中將該檔案指定為“排除檔案”或“不偵測”。

從備份中還原檔案可能會導致電腦感染病毒。

還原檔案時，您可以選擇用於儲存檔案的位置：儲存到原始位置（預設）、儲存到受防護電腦上針對還原物件的專用資料夾、儲存到安裝應用程式主控台電腦上的自訂資料夾或者儲存到網路中的其他電腦。

“還原到資料夾”用於在受防護電腦上儲存還原物件。您可以為需要掃描的物件配置特殊的安全性設定。此資料夾的路徑由“備份設定”指定（請參見第 247 頁上的“設定備份設定”部分）。

預設情況下，Kaspersky Embedded Systems Security 會還原在備份中建立副本的檔案。還原之後，您可以從備份刪除檔案副本。

► 若要從備份還原檔案，請執行下列步驟：

1. 在應用程式主控台樹狀目錄中，展開“儲存”節點。
2. 選擇“備份”子節點。
3. 在“備份”節點的詳細視窗中執行以下之一操作：
 - 若要還原一個物件，請從要還原的物件的內容功能表中選擇“還原”。
 - 若要還原多個物件，請使用 **CTRL** 或 **SHIFT** 鍵選取想要還原的物件，右鍵點擊其中一個選定的物件，並在上下文功能表中選取“還原”。

“還原物件”視窗開啟。

4. 在“還原物件”視窗中，為每個選定物件指定將儲存還原物件的資料夾。

物件的名稱顯示在視窗上部的“物件”欄位中。如果選定多個物件，系統將顯示選定物件清單中第一個物件的名稱。

5. 執行以下步驟之一：
 - 若要將物件還原到原始位置，請選擇“還原到來源資料夾”。
 - 若要將物件還原到設定中的適用於還原物件位置所指定的資料夾，請選擇“還原到預設還原資料夾”。
 - 若要將物件儲存在安裝應用程式主控台的電腦上的其他資料夾或共用資料夾，請選擇“還原至本機電腦或網路資源上的資料夾”，然後選擇所需資料夾或指定資料夾路徑。

6. 如果您不希望於還原之後在備份資料夾中儲存物件的副本，請取消選定“**還原物件後從儲存區中刪除物件**”核取方塊（預設情況下，清除此核取方塊）。
7. 若要為其餘選定物件套用指定的還原條件，請選定“**套用至所有選擇的物件**”核取方塊。

所有選定物件都將還原並儲存到指定資料夾：如果選擇“**還原到來源資料夾**”，則每個物件都將儲存到其原始位置；如果選擇“**還原到預設還原資料夾**”或“**還原至本機電腦或網路資源上的資料夾**”，則所有物件都將儲存到您所指定的資料夾。

8. 點擊“**確定**”。

Kaspersky Embedded Systems Security 將開始還原選定物件的第一個物件。

9. 如果指定位置已存在擁有該名稱的物件，則系統將開啟“**已存在具有此名稱的物件**”視窗。
 - a. 選擇以下 Kaspersky Embedded Systems Security 操作之一：
 - “**取代**”，使用還原物件取代現有物件。
 - “**重新命名**”，使用其他名稱儲存還原的物件。在輸入欄位中輸入新物件的檔案名稱和檔案的完整路徑。
 - “**透過新增後置詞重命名**”，透過為物件檔案名稱新增後置詞重新命名物件。在項目欄位中輸入後置詞。
 - b. 如果選定還原多個物件，要將選定的操作（例如透過新增後置詞來“**取代**”或“**重新命名**”）套用到其餘選定物件，請選定“**套用至所有選擇的物件**”核取方塊。（如果已選擇“**重新命名**”，“**套用至所有選擇的物件**”核取方塊將不可用。）
 - c. 點擊“**確定**”。

物件將被還原。有關還原操作的資訊將輸入到系統稽核記錄中。

如果您在“**還原物件**”視窗中沒有選擇“**套用至所有選擇的物件**”，“**還原物件**”視窗將再次開啟。您可以使用該視窗指定儲存下個選定物件的位置（請參閱流程的步驟 4）。

從備份刪除檔案

► 若要從備份刪除一個或多個檔案，請執行下列步驟：

1. 在應用程式主控台樹狀目錄中，展開“**儲存**”節點。
2. 選擇“**備份**”子節點。
3. 執行以下步驟之一：
 - 若要刪除一個物件，請從物件名稱的內容功能表中選擇“**刪除**”。
 - 若要刪除多個物件，請使用 **Ctrl** 或 **Shift** 鍵選擇想要刪除的物件，並在其中任何一個選定物件上開啟內容功能表，然後選擇“**刪除**”。
4. 在確認視窗中點擊“**是**”按鈕以確認操作。

將從備份中刪除選定檔案。

配置備份設定

► 若要配置備份設定，請執行下列步驟：

1. 在應用程式主控台樹狀目錄中，展開“**儲存**”節點。
2. 開啟“**備份**”子節點的內容功能表。
3. 選擇“**內容**”。
4. 在“**備份內容**”視窗中，根據您的要求設定所需的備份設定：

在“**備份設定**”部分中：

- **備份資料夾**

備份資料夾的路徑，路徑格式為 UNC (通用命名慣例)。

預設路徑為 C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Backup\。

- **最大備份空間(MB)**

該核取方塊用於啟用或停用監控儲存在備份資料夾中的物件的總大小的功能。如果超過指定的值（預設值為 200 MB），Kaspersky Embedded Systems Security 會記錄“已超過最大備份容量”事件，並根據此事件種類的通知設定發佈通知。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會監控置於備份中的物件的總大小。

如果清除該核取方塊，Kaspersky Embedded Systems Security 會監控置於備份中的物件的總大小。

預設取消選定該核取方塊。

- **可用空間上限值(MB)**

該核取方塊用於啟用或停用監控備份中的最小可用空間大小（預設值為 50 MB）的功能。如果可用空間大小下降到低於指定上限值，Kaspersky Embedded Systems Security 會記錄“已超過備份區可用空間上限值”事件，並根據此事件類型的通知設定發佈通知。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會監控備份中的可用空間的大小。

如果選中“最大備份空間(MB)”核取方塊，“可用空間上限值(MB)”核取方塊才可用。

預設將會選定該核取方塊。

如果備份中的物件大小超過最大備份容量或超過可用空間上限值，在您繼續將物件放入備份時，Kaspersky Embedded Systems Security 將通知您此情況。

在“還原設定”部分中：

- **還原物件的指定資料夾**

用於還原物件的資料夾的路徑，路徑格式為 UNC（通用命名慣例）。

預設路徑：C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored\。

5. 點擊“確定”。

將儲存已設定的備份設定。

備份統計

您可以檢視有關目前備份狀態的資訊：備份統計。

► 若要檢視備份統計，

請在應用程式主控台樹狀目錄的“備份”節點上開啟內容功能表並選擇“統計”。將開啟“備份區統計”視窗。

“備份區統計”視窗將顯示有關目前備份狀態的資訊（請參閱下表）。

表 35. 有關目前備份狀態的資訊

欄位	敘述
備份區已使用空間	備份資料夾中的資料大小；程式以加密形式計算檔案大小
物件總數	備份中目前的物件總數

事件註冊。Kaspersky Embedded Systems Security 記錄

本節提供有關使用 Kaspersky Embedded Systems Security 記錄的資訊：系統稽核記錄、工作執行記錄和事件記錄。

本章內容

註冊 Kaspersky Embedded Systems Security 事件的方式	250
系統稽核記錄	251
工作記錄	254
安全記錄	259
在事件檢視器中檢視 Kaspersky Embedded Systems Security 事件記錄	259
在 Kaspersky Embedded Systems Security 主控台中配置記錄設定	260

註冊 Kaspersky Embedded Systems Security 事件的方式

Kaspersky Embedded Systems Security 的事件分為兩組：

- 與 Kaspersky Embedded Systems Security 工作中物件處理相關的事件。
- 與管理 Kaspersky Embedded Systems Security 相關的事件，例如應用程式啟動、建立或刪除工作或者編輯工作設定。

Kaspersky Embedded Systems Security 使用以下方式來記錄事件：

- “**工作記錄**”。工作記錄包含有關目前工作狀態以及執行工作期間發生事件的資訊。
- **系統稽核記錄**。系統稽核記錄包含有關與管理 Kaspersky Embedded Systems Security 相關的事件的資訊。
- **事件記錄**。事件記錄包含有關在 Kaspersky Embedded Systems Security 操作中診斷故障所需的事件資訊。可在 Microsoft Windows 事件檢視器中檢視事件記錄。

- **安全記錄。**安全記錄檢查包含有關事件的資訊，這些事件與受防護電腦上的安全入侵和嘗試進行安全入侵相關。

如果 Kaspersky Embedded Systems Security 執行期間發生問題（例如，Kaspersky Embedded Systems Security 或個別工作異常終止或者無法啟動），您可以建立偵錯檔案和 Kaspersky Embedded Systems Security 程序的記憶體傾印檔案，並將包含該分析資訊的檔案傳送給 Kaspersky Lab 技術支援服務部門，以便對發生的問題予以診斷。

Kaspersky Embedded Systems Security 不會自動傳送任何偵錯或傾印檔案。診斷資料只能由具有相應權限的使用者傳送。

Kaspersky Embedded Systems Security 會以未加密的形式將資訊寫入到偵錯檔案和傾印檔案。儲存檔案的資料夾由使用者選擇，由作業系統配置和 Kaspersky Embedded Systems Security 設定管理。您可以配置存取權限（請參見第 280 頁上的“管理 Kaspersky Embedded Systems Security 功能的存取權限”部分）並僅允許所需使用者存取記錄、偵錯和傾印檔案。

系統稽核記錄

Kaspersky Embedded Systems Security 執行與 Kaspersky Embedded Systems Security 管理有關的事件的系統稽核。例如，應用程式會記錄有關啟動應用程式、啟動和停止 Kaspersky Embedded Systems Security 工作、變更工作設定、建立和刪除自訂掃描工作的資訊。當您在應用程式主控台中選擇“系統稽核記錄”節點時，所有這些事件的記錄都會顯示在詳細資訊視窗中。

預設情況下，Kaspersky Embedded Systems Security 會無限期地儲存系統稽核記錄中的記錄。您可以指定系統稽核記錄中記錄的儲存週期。

您可以指定一個資料夾以供 Kaspersky Embedded Systems Security 用來儲存包含系統稽核記錄的檔案，而不使用預設值。

本章節說明項目

在系統稽核記錄中排序事件	252
在系統稽核記錄中篩選事件	252
刪除系統稽核記錄中的事件	253

在系統稽核記錄中排序事件

預設情況下，系統稽核記錄節點中的事件按時間倒序顯示。

事件可按除“事件”以外的任何欄位內容進行排序。

► *要在系統稽核記錄中排序事件：*

1. 在應用程式主控台樹狀目錄中，展開“記錄和通知”節點。
2. 選擇“系統稽核記錄”子節點。
3. 在詳細資訊視窗中，選擇要用於排序清單中事件的欄位標題。

在系統稽核記錄中執行下一次檢視以前，將一直儲存該排序結果。

在系統稽核記錄中篩選事件

您可以將系統稽核記錄設定僅顯示符合指定篩選條件（篩選器）的事件記錄。

► *若要篩選系統稽核記錄中的事件，請執行下列步驟：*

1. 在應用程式主控台樹狀目錄中，展開“記錄和通知”節點。
2. 開啟“系統稽核記錄”子節點的上下文功能表，然後選擇“篩選”。

將開啟“篩選設定”視窗。

3. 若要新增篩選器，請執行以下步驟：

- a. 在“欄位名稱”清單中，選擇作為事件篩選依據的欄位。
- b. 在“運算子”清單中選擇篩選條件。篩選條件因您在“欄位名稱”清單中選定的項目而有所不同。

- c. 在“欄位值”清單中，選擇篩選值。
- d. 點擊“新增”按鈕。

已新增的篩選將出現在“篩選設定”視窗的篩選清單中。

4. 若有需要，請執行以下操作之一：
 - 如果要使用邏輯運算子“AND”組合多個篩選，請選擇“如果符合所有條件”。
 - 如果要使用邏輯運算子“OR”組合多個篩選，請選擇“如果符合任何條件”。
5. 點擊“套用”按鈕以在系統稽核記錄中儲存篩選條件。

系統稽核記錄的事件清單將僅顯示符合篩選條件的事件。在系統稽核記錄中執行下一次檢視以前，將一直儲存該篩選結果。

► *停用篩選器：*

1. 在應用程式主控台樹狀目錄中，展開“記錄和通知”節點。
2. 開啟“系統稽核記錄”子節點的上下文功能表，然後選擇“刪除篩選”。

系統稽核記錄的事件清單隨後將顯示所有事件。

刪除系統稽核記錄中的事件

預設情況下，Kaspersky Embedded Systems Security 會無限期地儲存系統稽核記錄中的記錄。您可以指定系統稽核記錄中記錄的儲存週期。

可以手動刪除系統稽核記錄中的所有事件。

► *要刪除系統稽核記錄中的事件：*

1. 在應用程式主控台樹狀目錄中，展開“記錄和通知”節點。
2. 開啟“系統稽核記錄”子節點的上下文功能表，然後選擇“清除”。
3. 執行以下步驟之一：
 - 如果要在刪除系統稽核記錄中的事件之前將記錄內容另存為 CSV 或 TXT 格式的檔案，則請點擊刪除確認視窗中的“是”按鈕。在開啟的視窗中，指定檔案名稱和位置。

- 如果不想將記錄內容另存，則點擊刪除確認視窗中的“否”按鈕。

系統稽核記錄將被清除。

工作記錄

本章節提供有關 Kaspersky Embedded Systems Security 工作記錄的資訊，並說明如何管理這些工作記錄。

本章節說明項目

關於工作記錄.....	254
在工作記錄中檢視事件清單.....	255
排序工作記錄中的事件.....	255
在工作記錄中篩選事件.....	256
在工作記錄中檢視有關 Kaspersky Embedded Systems Security 工作的統計和資訊.....	257
匯出工作記錄中的資訊.....	257
刪除工作記錄中的事件.....	258

關於工作記錄

在應用程式主控台中選擇“**工作記錄**”節點後，詳細資訊視窗中會顯示有關 Kaspersky Embedded Systems Security 工作執行情況的資訊。

在每個工作的記錄中，可以檢視工作執行情況的統計、自工作啟動起至目前時刻應用程式已處理每個物件的詳細資訊及工作設定。

預設情況下，Kaspersky Embedded Systems Security 工作記錄中儲存的記錄自工作完成後保留 30 天。您可以變更記錄在工作記錄中的儲存期間。

您可以指定 Kaspersky Embedded Systems Security 儲存包含工作記錄檔案所使用的資料夾，而不使用預設的資料夾。還可以選擇 Kaspersky Embedded Systems Security 將記錄到工作記錄中的事件。

在工作記錄中檢視事件清單

► 若要在工作記錄中檢視事件清單，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“**記錄和通知**”節點。
2. 選擇“**工作記錄**”子節點。

詳細資訊視窗中將顯示 Kaspersky Embedded Systems Security 工作記錄中所儲存事件的清單。

事件可以按任意欄位進行排序，也可以進行篩選。

排序工作記錄中的事件

預設情況下，工作記錄中的事件將按時間倒序顯示。可以按任意欄位進行排序。

► 若要在工作記錄中排序事件，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“**記錄和通知**”節點。
2. 選擇“**工作記錄**”子節點。
3. 在詳細資訊視窗中，選擇要用於排序 Kaspersky Embedded Systems Security 工作記錄中事件的欄位標題。

在工作記錄中執行下一次檢視以前，將一直儲存該排序結果。

在工作記錄中篩選事件

您可以設定工作記錄清單，以僅顯示符合指定篩選條件（篩選器）的事件記錄。

► 若要在工作記錄中篩選事件，請執行以下操作：

1. 在應用程式主控台樹狀目錄中，展開“**記錄和通知**”節點。
2. 開啟“**工作記錄**”子節點的內容功能表，然後選擇“**篩選**”。

將開啟“**篩選設定**”視窗。

3. 若要新增篩選器，請執行以下步驟：

- a. 在“**欄位名稱**”清單中，選擇作為事件篩選依據的欄位。
- b. 在“**運算子**”清單中選擇篩選條件。篩選條件因您在“**欄位名稱**”清單中選定的項目而有所不同。
- c. 在“**欄位值**”清單中，選擇篩選值。
- d. 點擊“**新增**”按鈕。

已新增的篩選將出現在“**篩選設定**”視窗的篩選清單中。

4. 若有需要，請執行以下操作之一：
 - 如果要使用邏輯運算子“AND”組合多個篩選，請選擇“**如果符合所有條件**”。
 - 如果要使用邏輯運算子“OR”組合多個篩選，請選擇“**如果符合任何條件**”。
5. 點擊“**套用**”按鈕以在工作記錄中儲存篩選條件。

工作記錄的事件清單將僅顯示符合篩選條件的事件。在工作記錄中執行下一次檢視以前，將一直儲存該篩選結果。

► 停用篩選器：

1. 在應用程式主控台樹狀目錄中，展開“**記錄和通知**”節點。
2. 開啟“**工作記錄**”子節點的內容功能表，然後選擇“**刪除篩選**”。

工作記錄的事件清單隨後將顯示所有事件。

在工作記錄中檢視有關 Kaspersky Embedded Systems Security 工作的統計和資訊

在工作記錄中，可以檢視有關工作中自工作開始至目前時刻發生所有事件的詳細資訊，以及工作執行統計和工作設定。

▶ 要檢視有關 Kaspersky Embedded Systems Security 工作的統計和資訊：

1. 在應用程式主控台樹狀目錄中，展開“**記錄和通知**”節點。
 2. 選擇“**工作記錄**”子節點。
 3. 在結果視窗中，透過以下某種方法開啟“**記錄**”視窗：
 - 點擊兩下您要檢視其記錄的工作事件。
 - 開啟您要檢視其記錄工作事件的內容功能表，選擇“**檢視記錄**”。
 4. 在開啟的視窗中，將顯示以下詳細資訊：
 - “**統計**”選項顯示工作啟動和完成時間及工作統計。
 - “**事件**”標籤顯示工作執行期間所記錄事件的清單。
 - “**選項**”標籤顯示工作設定。
 5. 如有需要，請點擊“**篩選**”按鈕以在工作記錄中篩選事件。
 6. 如有需要，請點擊“**匯出**”按鈕以將工作記錄中的資料匯出至 CSV 或 TXT 格式的檔案中。
 7. 按“**關閉**”按鈕。
- “**記錄**”視窗將關閉。

匯出工作記錄中的資訊

您可以將工作記錄中的資料匯出至 CSV 或 TXT 格式的檔案中。

▶ 要匯出工作記錄中的資訊：

1. 在應用程式主控台樹狀目錄中，展開“**記錄和通知**”節點。
2. 選擇“**工作記錄**”子節點。

3. 在結果視窗中，透過以下某種方法開啟“記錄”視窗：
 - 點擊兩下您要檢視其記錄的工作事件。
 - 開啟您要檢視其記錄工作事件的內容功能表，選擇“檢視記錄”。
4. 在“記錄”視窗下部，點擊“匯出”按鈕。
將開啟“另存為”視窗。
5. 指定要從工作記錄中將資料匯出到其中的檔案的名稱、位置、類型和編碼。
6. 點擊“儲存”按鈕。
將儲存指定設定。

刪除工作記錄中的事件

預設情況下，Kaspersky Embedded Systems Security 工作記錄中儲存的記錄自工作完成後保留 30 天。您可以變更記錄在工作記錄中的儲存期間。

您可以手動從目前已完成工作的記錄中刪除所有事件。

對於目前正在執行的工作及其他使用者正在使用的工作，不會刪除其記錄中的事件。

► 若要刪除工作記錄中的事件，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“記錄和通知”節點。
2. 選擇“工作記錄”子節點。
3. 執行以下步驟之一：
 - 如果要從目前已完成的所有工作記錄中刪除事件，則開啟“工作記錄”子節點的內容功能表，然後選擇“清除”。
 - 如果要清除單個工作記錄，則在詳細資訊視窗中，開啟要清除記錄的工作事件的內容功能表，然後選擇“刪除”。

- 如果要清除多個工作的記錄：
 - a. 在詳細資訊視窗中，使用 **Ctrl** 或 **Shift** 鍵選擇要清除記錄的工作事件。
 - b. 開啟任何選定事件的內容功能表，然後選擇“刪除”。
- 4. 在刪除確認視窗中點擊“是”按鈕以確認您要刪除這些記錄。

選擇的工作記錄將被清除。從工作記錄中刪除事件的操作將被記錄到系統稽核記錄中。

安全記錄

Kaspersky Embedded Systems Security 保持有與受防護電腦上的安全入侵或嘗試進行安全入侵相關的事件的記錄。本記錄中記錄以下事件：

- 弱點利用防禦事件。
- 關鍵記錄檢查事件。
- 表示嘗試進行安全入侵的緊急事件（對於“即時電腦防護”、“自訂掃描”、“檔案完整性監控”、“應用程式啟動控制”和“裝置控制”工作）。

您可以清除安全記錄以及系統稽核記錄（請參見第 [253](#) 頁上的“刪除系統稽核記錄中的事件”部分）。此外，Kaspersky Embedded Systems Security 記錄與清除安全記錄相關的系統稽核記錄事件。

在事件檢視器中檢視 Kaspersky Embedded Systems Security 事件記錄

您可以使用 Microsoft 管理主控台的 Microsoft Windows 事件檢視器管理元件來檢視 Kaspersky Embedded Systems Security 的事件記錄。該記錄包含由 Kaspersky Embedded Systems Security 記錄且在其操作中診斷故障時所需的事件。

您可以根據以下標準選擇需要將其記錄在事件記錄的事件：

- **按事件類型**

- **按詳細等級。**詳細等級與記錄中的事件重要等級相對應(資訊、重要或緊急事件)。最詳細等級是“資訊事件”等級，它將記錄所有事件，最簡略等級是“緊急事件”等級，它只記錄緊急事件。預設情況下，除“更新”元件之外的所有元件都選定“重要事件”詳細等級(只記錄重要和緊急事件)；對於“更新”元件，則選定“資訊事件”詳細等級。

► *要檢視 Kaspersky Embedded Systems Security 事件記錄:*

1. 點擊“開始”按鈕，在搜尋欄中輸入 mmc 指令，然後按 **ENTER** 鍵。

此時將會開啟 Microsoft 管理主控台的視窗。

2. 選擇“檔案 > 新增或刪除管理單元”。

將開啟“新增或刪除管理單元”視窗。

3. 在可用管理單元清單中，選擇“事件檢視器”管理單元並點擊“新增”按鈕。

將開啟“選擇電腦”視窗。

4. 在“選擇電腦”視窗中，指定已安裝 Kaspersky Embedded Systems Security 的電腦，然後點擊“確定”。

5. 在“新增和刪除管理元件”視窗中，點擊“確定”。

在 Microsoft 管理主控台樹狀目錄中，將出現“事件監視器”節點。

6. 展開“事件監視器”節點，並選擇“應用程式和服務記錄 > Kaspersky Embedded Systems Security”子節點。

將開啟 Kaspersky Embedded Systems Security 事件記錄。

在 Kaspersky Embedded Systems Security 主控台中配置記錄設定

您可以編輯 Kaspersky Embedded Systems Security 的以下記錄設定：

- 事件在工作記錄和系統稽核記錄中儲存的時間長度。
- Kaspersky Embedded Systems Security 在其中儲存工作記錄和系統稽核記錄檔案的資料夾的位置。

- 應用程式資料庫已過期、資料庫已長時間未更新和已很長時間未執行關鍵區域掃描的事件產生上限值。
- Kaspersky Embedded Systems Security 在事件檢視器中將儲存到工作記錄、系統稽核記錄和 Kaspersky Embedded Systems Security 事件記錄中的事件。
- 用於將稽核事件和工作執行事件透過 Syslog 協定發佈到 syslog 伺服器的設定。

► 要設定 Kaspersky Embedded Systems Security 記錄，請執行下列步驟：

1. 在應用程式主控台樹狀目錄中，開啟“記錄和通知”節點的內容功能表，並選擇“內容”。
將開啟“記錄和通知設定”視窗。
2. 在“記錄和通知設定”視窗中，根據需要設定記錄。為此，請執行以下操作：
 - 在“一般”標籤上，如有必要，選擇 Kaspersky Embedded Systems Security 在事件檢視器中將儲存到工作記錄、系統稽核記錄和 Kaspersky Embedded Systems Security 事件記錄中的事件。為此，請執行以下操作：
 - 在“元件”清單中，選擇您要設定其詳細等級的 Kaspersky Embedded Systems Security 元件。

對於“即時檔案防護”、“自訂掃描”和“更新”元件，可透過工作日誌和事件記錄註冊事件。對於這些元件，事件清單表格包含“工作記錄”和“Windows 事件記錄”欄位。“隔離”和“備份”元件的事件記錄在系統稽核記錄和事件記錄中。對於這些元件，事件清單表格包含“稽核”和“Windows 事件記錄”欄位。

- 在“重要性等級”清單中，選擇事件在工作記錄、系統稽核記錄和選定元件的事件記錄中的詳細等級。

在包含事件清單的下表中，使用工作記錄、系統稽核記錄和事件記錄，根據目前詳細等級記錄的事件選取旁邊的核取方塊。

- 如果您想手動為選定的元件啟用記錄特定事件，請執行以下操作：
 - a. 在“重要性等級”清單中選擇“自訂”。

- b. 在包含事件清單的表格中，選定您想要記錄到工作記錄、系統稽核記錄和事件記錄中事件旁邊的核取方塊。
- 在“**進階**”標籤上，配置電腦防護狀態的記錄儲存設定和事件產生上限值：
 - 在“**記錄儲存**”部分中：
 - **記錄資料夾**

採用 UNC (通用命名慣例) 格式的記錄資料夾路徑。

預設路徑：C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\ 2.3\Reports\。

如果變更預設路徑，將建立一個具有相應名稱的資料夾。新記錄將儲存在新資料夾中。舊記錄將保留。
 - **刪除早於該天數的工作記錄**

該核取方塊用於啟用/停用功能，該功能可在指定的一段時間後 (預設值：30 天) 刪除包含已完成工作執行結果的記錄和在正在執行工作的記錄中發佈的事件。

如果選定該核取方塊，Kaspersky Embedded Systems Security 會在指定的時間後刪除部分記錄 (記錄中包含已完成工作的執行結果) 和事件 (發佈在執行工作的記錄中的事件) 。

預設將會選定該核取方塊。
 - **刪除早於該天數的系統稽核記錄事件**

該核取方塊用於啟用/停用一項功能，即在指定的時間段後刪除系統稽核記錄中記錄的事件 (預設時間段：60 天) 。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會在指定的時間段後刪除系統稽核記錄中記錄的事件。

預設取消選定該核取方塊。

- 在“事件產生上限值”部分：
 - 指定在經過多少天後，發生 *應用程式資料庫已過期*、*應用程式資料庫已嚴重過期* 和 *已很長時間未執行關鍵區域掃描* 事件。

表 36. 事件產生上限值

設定	事件產生上限值。
敘述	<p>您可以指定建立以下事件類型的閾值：</p> <p><i>應用程式資料庫過期</i> 和 <i>應用程式資料庫已嚴重過期</i>。從最近安裝的資料庫更新的發佈日期起算，如果未在設定所指定的天數內更新 Kaspersky Embedded Systems Security 資料庫，則會發生此事件。您可以配置關於此事件的管理員通知。</p> <p><i>已很長時間未執行關鍵區域掃描</i>。在指定的天數內，如果沒有標記了“將工作視為關鍵區域掃描”核取方塊的工作被執行，則發生該事件。</p>
可能的值	天數範圍為 1 至 365。
預設值	<p><i>應用程式資料庫已過期</i> – 7 天；</p> <p><i>應用程式資料庫已嚴重過期</i> – 14 天。</p> <p><i>已很長時間未執行關鍵區域掃描</i> – 30 天。</p>

- 在“**SIEM 整合**”標籤上，配置用於將稽核事件和工作執行事件發佈到 syslog 伺服器的設定（請參見第 [265](#) 頁上的“配置 SIEM 整合設定”部分）。

3. 點擊“**確定**”以儲存變更。

本章節說明項目

關於 SIEM 整合	264
配置 SIEM 整合設定	265

關於 SIEM 整合

為了減小低效能裝置上的負載和降低由於應用程式記錄量增大而造成系統效能降級的風險，可以透過 Syslog 協定將稽核事件和工作效能事件的發佈配置到 *syslog 伺服器*。

syslog 伺服器是用於聚合事件 (SIEM) 的外部伺服器。它可以收集和分析接收到的事件，還可以執行管理記錄的其他操作。

可以在兩種模式中使用 SIEM 整合：

- **syslog 伺服器上的重複事件**：此模式指定其發佈在記錄設定中進行配置的所有工作效能事件，以及即使被傳送到 SIEM 後仍繼續儲存到本機電腦上的所有系統系統稽核記錄事件。

建議使用此模式，以便能夠最大限度地減小受防護電腦上的負載。

- **刪除事件的本機副本**：此模式指定將從本機電腦上刪除在應用程式執行過程中註冊和已發佈到 SIEM 的所有事件。

應用程式永遠不會刪除安全記錄的本機版本。

Kaspersky Embedded Systems Security 可以將應用程式記錄中的事件轉換為 syslog 伺服器支援的格式，以便這些事件能夠被傳輸和被 SIEM 成功識別。應用程式支援轉換為結構化資料格式和 JSON 格式。

建議根據使用的 SIEM 的配置來選擇事件的格式。

可靠性設定

透過定義連線到映像 syslog 伺服器的設定，可以降低將事件傳輸到 SIEM 的不成功的風險。

映像 syslog 伺服器是一個額外的 syslog 伺服器，如果與主 syslog 伺服器的連線不可用或不能使用主要伺服器，應用程式會自動轉換到該伺服器。

Kaspersky Embedded Systems Security 還會通知您與 SIEM 連線未成功的嘗試次數，以及使用系統稽核事件傳送事件到 SIEM 的有關錯誤。

配置 SIEM 整合設定

預設情況下，不使用 SIEM 整合。可以啟用和停用 SIEM 整合，並配置功能性設定（請參見以下表格）。

表 37. SIEM 整合設定

設定	預設值	敘述
透過 syslog 協定傳送事件到遠端 syslog 伺服器	未套用	可以分別透過選擇或清除該核取方塊來啟用或停用 SIEM 整合。
刪除已被傳送到遠端 syslog 伺服器的事件本機副本	未套用	可以為儲存記錄的本機副本配置設定（透過選擇或清除該核取方塊將它們傳送到 SIEM 後）。
事件格式	結構化資料	可以選擇以下兩種格式之一，應用程式在將事件傳送到 syslog 伺服器以便 SIEM 能夠更好進行識別之前，將其事件轉換為該格式。
連線協定	TCP	可以使用下拉清單來配置透過 UDP 或 TCP 協定與主 syslog 伺服器和映像 syslog 伺服器的連線。
主 syslog 伺服器連線設定	IP 位址： 127.0.0.1 連接埠：514	可以使用適當的欄位來配置用於連線到主 syslog 伺服器的 IP 位址和連接埠。 可以指定 IP 位址僅為 IPv4 格式。
如果無法存取主伺服器則使用映像 syslog 伺服器	未套用	可以使用核取方塊來啟用或停用映像 syslog 伺服器。
映像 syslog 伺服器連線設定	IP 位址： 127.0.0.1 連接埠：514	可以使用適當的欄位來配置用於連線到映像 syslog 伺服器的 IP 位址和連接埠。 可以指定 IP 位址僅為 IPv4 格式。

► 要配置 SIEM 整合設定：

1. 在應用程式主控台樹狀目錄中，開啟“記錄和通知”節點的內容功能表。

2. 選擇“內容”。

將開啟“記錄和通知設定”視窗。

3. 選擇“SIEM 整合”標籤。

4. 在“整合設定”部分中，選擇“透過 syslog 協定傳送事件到遠端 syslog 伺服器”核取方塊。

該核取方塊可啟用或停用將已發佈的事件傳送到外部 syslog 伺服器的功能。

如果選中該核取方塊，則應用程式將根據配置的 SIEM 整合設定將已發佈的事件傳送到 SIEM。

如果清除該核取方塊，則應用程式不執行 SIEM 整合。如果該核取方塊已被清除，則無法配置 SIEM 整合設定。

預設取消選定該核取方塊。

5. 如果需要，在“整合設定”部分中，選擇“刪除已被傳送到遠端 syslog 伺服器的事件本機副本”核取方塊。

該核取方塊可啟用或停用傳送到 SIEM 後記錄本機副本的刪除。

如果選中該核取方塊，則應用程式在事件被成功發佈到 SIEM 後刪除事件的本機副本。建議在低效能電腦上使用此模式。

如果清除該核取方塊，則應用程式僅將事件傳送到 SIEM。記錄的副本將繼續儲存在本機。

預設取消選定該核取方塊。

“刪除已被傳送到遠端 syslog 伺服器的事件本機副本”核取方塊的狀態不會影響儲存安全記錄檔案事件的設定：應用程式永遠不會自動刪除安全記錄事件。

6. 在“事件格式”部分中，指定您要將應用程式操作事件轉換為該格式的格式，以便能夠將它們傳送到 SIEM。

預設情況下，應用程式將它們轉換為結構化資料格式。

7. 在“連線設定”部分中：

- 指定 SIEM 連線協定。
- 指定用於連線到主 syslog 伺服器的設定。

可以僅指定 IP 位址為 IPv4 格式。

- 當無法傳送事件到主 syslog 伺服器時，如果想讓應用程式使用其他連線設定，請選中“**如果無法存取主伺服器則使用映像 syslog 伺服器**”核取方塊。
- 指定用於連線到映像 syslog 伺服器的設定：“**IP 位址**”和“**埠號**”。

如果已清除“**如果無法存取主伺服器則使用映像 syslog 伺服器**”核取方塊，則無法編輯映像 syslog 伺服器的“**IP 位址**”和“**埠號**”欄位。

可以僅指定 IP 位址為 IPv4 格式。

8. 點擊“確定”。

將套用已配置的 SIEM 整合設定。

通知設定

本章節提供有關如何設定向 Kaspersky Embedded Systems Security 的使用者和管理員通知應用程式事件和電腦防護狀態資訊的方法。

本章內容

管理員和使用者通知方式	268
設定管理員和使用者通知	269

通知管理員和使用者的方式

您可以設定程式通知受防護電腦的管理員和使用者，有關 Kaspersky Embedded Systems Security 操作中的事件和電腦上病毒防護的狀態。

程式將確認執行以下工作：

- 管理員可以收到有關選定類型事件的資訊。
- 存取受防護電腦的區域網路使用者和終端電腦使用者可以收到“即時檔案防護”工作中“偵測到物件”類型事件的資訊。

在應用程式主控台中，使用多種方式啟動管理員或使用者通知：

- 使用者通知方式：
 - a. 終端服務工具。

如果受防護電腦用作終端，則可以應用此方式來通知終端電腦。
 - b. 訊息服務工具。

您可以透過 Microsoft Windows 訊息服務使用此方式來進行通知。
- 管理員通知方式：
 - a. 訊息服務工具。

您可以透過 Microsoft Windows 訊息服務使用此方式來進行通知。
 - b. 執行可執行檔。

當事件發生時，該方式會執行儲存在受防護電腦本機硬碟上的可執行檔。
 - c. 透過電子郵件傳送。

該方式使用電子郵件傳輸訊息。

您可以為單個事件類型建立訊息文字。它可以包括用以說明事件的訊息欄位。預設情況下，應用程式使用預設的文字通知使用者。

設定管理員和使用者通知

事件通知設定使您可以選擇配置和編寫訊息文字的方式。

► 若要配置事件通知設定，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，開啟“**記錄和通知**”節點的內容功能表，並選擇“**內容**”。

將開啟“**記錄和通知設定**”視窗。

2. 在“**通知**”標籤中，選擇通知模式：
 - a. 從“**事件類型**”清單中選擇您希望為其選擇通知方式的事件。
 - b. 在“**通知管理員**”或“**通知使用者**”設定中，選定您希望配置的通知方式旁邊的核取方塊。

只能為“**偵測到物件**”事件、“**偵測到並限制不受信任的大容量儲存**”事件和“**主機已列為不受信任**”事件設定使用者通知。

3. 新增訊息文字：
 - a. 點擊“**訊息文字**”按鈕。
 - b. 在開啟的視窗中輸入要在相應的事件訊息中顯示的文字。

您可以為多種事件類型建立一個訊息文字：在為一種事件類型選擇通知方式後，選擇您希望對其使用相同訊息文字的其他事件類型，方法是使用 **Ctrl** 或 **Shift** 鍵，然後點擊“**訊息文字**”按鈕。

- c. 若要新增有關事件資訊的欄位，請點擊“**巨集**”按鈕，然後從下拉清單中選擇相關欄位。事件資訊欄位在本部分中的清單中有所說明。
- d. 若要還原預設事件訊息文字，請點擊“**使用預設值**”按鈕。

4. 若要配置選定事件指定管理員通知方式，請點擊“通知”標籤，點擊“通知管理員”部分中的“設定”按鈕，並在“進階設定”視窗中配置選定的方式。為此，請執行以下操作：
 - a. 對於電子郵件通知，請開啟“電子郵件”標籤，然後在相應的欄位中指定收件者的電子郵件信箱(位址使用分號隔開)、SMTP 伺服器名稱或網路位址，以及埠號。若有需要，請指定在“主旨”和“寄件者”欄位中顯示的文字。在“主旨”欄位中也可以包括有關事件資訊的變數(請參閱下表)。如果您希望在連線 SMTP 伺服器時應用帳戶身分驗證，請在“身分驗證設定”群組中選擇“需要 SMTP 驗證”，然後指定要身分驗證帳戶的使用者名稱和密碼。
 - b. 對於使用“Windows Messenger 服務”的通知，請在“Windows Messenger 服務”標籤上建立的通知收件者電腦的清單：對於您希望新增的每台電腦，請點擊“新增”按鈕並在輸入欄位中輸入其網路名稱。
 - c. 若要執行可執行檔，請選擇在事件觸發時需要執行的受防護電腦上本機硬碟中的檔案，或在“可執行檔”選項上輸入檔案的絕對路徑。輸入用於執行檔的使用者名稱和密碼。
指定可執行檔的路徑時可使用系統環境變數；不允許使用使用者環境變數。
如果您希望限制一種事件類型在一段時間內的訊息數量，請在“進階”選項上選擇“不要傳送相同的通知超過”，然後指定次數和時間單位。

5. 點擊“確定”。

將儲存設定的通知設定。

表 38. 事件資訊欄位

變數	敘述
%EVENT_TYPE%	事件類型。
%EVENT_TIME%	事件時間。
%EVENT_SEVERITY%	重要性等級。
%OBJECT%	物件名稱 (在“即時電腦防護”和“自訂掃描”工作中)。 “軟體模組更新”工作包括更新的名稱和帶有更新資訊的網頁位址。

變數	敘述
%VIRUS_NAME%	根據病毒百科全書 https://encyclopedia.kaspersky.com/knowledge/classification/ 分類確定的物件名稱。該名稱包含在 Kaspersky Embedded Systems Security 偵測物件時回傳的物件全名中。您可以在工作記錄中檢視偵測到的物件的完整名稱 (請參閱第 257 頁上的“使用工作記錄檢視 Kaspersky Embedded Systems Security 工作的統計和資訊”部分) 。
%VIRUS_TYPE%	根據 Kaspersky Lab 分類的偵測到的物件類型，例如“病毒”或“木馬”。它包含在 Kaspersky Embedded Systems Security 發現被感染的物件或疑似感染的物件時返回的偵測到的物件全名中。您可以在工作記錄中檢視偵測到的物件的全名。
%USER_COMPUTER%	在“即時檔案防護”工作中，存取電腦上的物件的使用者的電腦名稱。
%USER_NAME%	在“即時檔案防護”工作中，存取電腦上的物件的使用者的名稱。
%FROM_COMPUTER%	發出通知的受防護電腦名稱。
%EVENT_REASON%	發生事件的原因 (某些事件沒有該欄位) 。
%ERROR_CODE%	錯誤代碼 (僅用於“內部工作錯誤”事件) 。
%TASK_NAME%	工作名稱 (僅適用於與工作效能相關的事件) 。

啟動和停止 Kaspersky Embedded Systems Security

本節包含有關啟動應用程式主控台的資訊，同時包含有關啟動和停止 Kaspersky Security 服務的資訊。

本章內容

啟動 Kaspersky Embedded Systems Security 管理外掛程式.....	272
從開始功能表啟動 Kaspersky Embedded Systems Security 主控台	272
啟動和停止 Kaspersky Security 服務.....	273
在作業系統安全模式下啟動 Kaspersky Embedded Systems Security	275

啟動 Kaspersky Embedded Systems Security 管理外掛程式

在卡巴斯基安全管理中心中啟動 Kaspersky Embedded Systems Security 管理外掛程式無需執行額外的操作。在管理員的電腦上安裝該外掛程式後，它會隨卡巴斯基安全管理中心同時啟動。有關啟動卡巴斯基安全管理中心的詳細資訊，請參見《卡巴斯基安全管理中心說明》。

從開始功能表啟動 Kaspersky Embedded Systems Security 主控台

在不同 Windows 作業系統中，設定的名稱可能會有所不同。

► 要從“開始”功能表啟動應用程式主控台：

1. 在“開始”選單中，選取“程式 > Kaspersky Embedded Systems Security > 管理工具 > Kaspersky Embedded Systems Security 主控台”。

要向應用程式主控台中新增其他管理單元，請以作者模式啟動應用程式主控台。

► 要以作者模式啟動應用程式主控台，請執行以下步驟：

1. 在“開始”選單中，選取“程式 > Kaspersky Embedded Systems Security > 管理工具”。
2. 在應用程式主控台的內容功能表中，選擇“作者”指令。

將以作者模式啟動應用程式主控台。

如果已在受防護電腦上啟動應用程式主控台，則將開啟應用程式主控台視窗。

如果已在其他電腦（而非受防護電腦）上啟動應用程式主控台，則會連線到受防護電腦。

► 要連線到受防護電腦：

1. 在應用程式主控台樹狀目錄中，開啟 **Kaspersky Embedded Systems Security** 節點的內容功能表。
2. 選擇“連線至其他電腦”指令。

將開啟“選擇電腦”視窗。

3. 在開啟的視窗中選擇“其他電腦”。
4. 在右側的輸入欄位中指定受防護電腦的網路名稱。
5. 點擊“確定”。

應用程式主控台將連線到受防護電腦。

如果用來登入 Microsoft Windows 的使用者帳戶沒有足夠權限來存取電腦上的 Kaspersky Security 管理服務，則選擇“使用以下帳戶身分連線”核取方塊，然後指定具有此權限的使用者帳戶。

啟動和停止 Kaspersky Security 服務

預設情況下，Kaspersky Security 服務會在作業系統啟動後立即自動啟動。Kaspersky Security 服務將管理執行即時防護、電腦控制、自訂掃描和更新工作的工作處理程序。

預設情況下，當 Kaspersky Embedded Systems Security 服務啟動時，將啟動“即時檔案防護”和“在作業系統啟動時掃描”工作以及其他排程在在應用程式啟動時啟動的工作。

如果停止 Kaspersky Security 服務，則會停止所有正在執行的工作。重新啟動 Kaspersky Security 服務之後，應用程式只會自動啟動其排程中已將啟動頻率設定為“在應用程式啟動時”的工作，而其他工作必須手動啟動。

您可以使用 **Kaspersky Embedded Systems Security** 節點的內容功能表或使用 Microsoft Windows 服務管理單元啟動和停止 Kaspersky Security 服務。

如果您是受防護電腦上“管理員”群組的成員，您可以啟動和停止 Kaspersky Embedded Systems Security。

► 要使用應用程式主控台停止或啟動應用程式，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，開啟 **Kaspersky Embedded Systems Security** 節點的內容功能表。
2. 選擇以下之一項目：
 - 停止服務。
 - 啟動服務。

將啟用或停止 Kaspersky Security 服務。

在作業系統安全模式下啟動 Kaspersky Embedded Systems Security

本節提供有關在作業系統安全模式下工作的 Kaspersky Embedded Systems Security 的資訊。

本章內容

關於在作業系統安全模式下工作的 Kaspersky Embedded Systems Security	275
在安全模式下啟動 Kaspersky Embedded Systems Security	276

關於在作業系統安全模式下工作的 Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security 元件可以在作業系統以安全模式載入時啟動。除了 Kaspersky Security 服務 (kavfs.exe)，klam.sys 驅動程式也會載入，它用於在作業系統啟動期間將 Kaspersky Security 服務註冊為受防護服務。有關詳細資訊，請參見“將 Kaspersky Security 服務註冊為受防護服務”部分。

Kaspersky Embedded Systems Security 可以在作業系統的以下安全模式下啟動：

- 最小安全模式 - 選擇作業系統安全模式的標準選項時，將啟動此模式。此時，Kaspersky Embedded Systems Security 可以啟動以下元件：
 - 即時檔案防護。
 - 自訂掃描。
 - 應用程式啟動控制和應用程式啟動控制規則產生器。
 - 記錄審查。
 - 檔案完整性監控。
 - 應用程式完整性控制。

- 網路安全模式 – 在帶有網路驅動程式的安全模式下載入作業系統時，將啟動此模式。除了在最小安全模式下啟動的元件，Kaspersky Embedded Systems Security 還可以啟動以下元件：
 - 資料庫更新。
 - 軟體模組更新。

在安全模式下啟動 Kaspersky Embedded Systems Security

預設情況下，在作業系統以安全模式載入時，不啟動 Kaspersky Embedded Systems Security。

► 要使 *Kaspersky Embedded Systems Security* 在作業系統安全模式下啟動，請執行以下操作：

1. 啟動 Windows 登錄檔編輯程式 (C:\Windowsregedit.exe)。
2. 開啟系統登錄檔的
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] 項。
3. 開啟 LoadInSafeMode 參數。
4. 設定值 1。
5. 點擊“確定”。

► 要取消 *Kaspersky Embedded Systems Security* 在作業系統安全模式下啟動，請執行以下操作：

1. 啟動 Windows 登錄檔編輯程式 (C:\Windowsregedit.exe)。
2. 開啟系統登錄檔的
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] 項。
3. 開啟 LoadInSafeMode 參數。
4. 設定值 0。
5. 點擊“確定”。

Kaspersky Embedded Systems Security 自我防護

有關 Kaspersky Embedded Systems Security 自我防護機制的資訊。

本章內容

關於 Kaspersky Embedded Systems Security 自我防護.....	277
防止包含已安裝的 Kaspersky Embedded Systems Security 元件的資料夾被變更.....	277
防止 Kaspersky Embedded Systems Security 登錄機碼被變更.....	278
將 Kaspersky Security 服務註冊為受防護服務.....	278
管理 Kaspersky Embedded Systems Security 功能的存取權限.....	280

關於 Kaspersky Embedded Systems Security 自我防護

Kaspersky Embedded Systems Security 包含自我防護機制，可防止該應用程式在硬碟磁碟機上的資料夾、記憶體處理程序和系統登錄機碼被修改或刪除。

防止包含已安裝的 Kaspersky Embedded Systems Security 元件的資料夾被變更

Kaspersky Embedded Systems Security 會限制任何使用者帳戶對包含已安裝的應用程式元件的資料夾進行重新命名和刪除。預設情況下，應用程式安裝資料夾的路徑如下：

- 在 32 位元版本的 Microsoft Windows 中：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- 在 64 位元版本的 Microsoft Windows 中：%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

防止 Kaspersky Embedded Systems Security 登錄機碼被變更

Kaspersky Embedded Systems Security 會限制對以下登入分支和登錄機碼的存取權限，這些登錄機碼提供了應用程式驅動程式和服務的載入：

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgrt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfssl]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\CrashDump] (64 位元版本的 Microsoft Windows 上)
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\Trace]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Trace] (64 位元版本的 Microsoft Windows 上)

變更這些登錄分支和登錄機碼的權限僅授予給本機系統 (SYSTEM) 帳戶。使用者和管理員帳戶僅被授予唯讀權限。

將 Kaspersky Security 服務註冊為受防護服務

輕度受防護處理程序 (也稱為“PPL”) 技術確保作業系統只載入受信任的服務和處理程序。對於要作為受防護服務執行的服務，必須在受防護電腦上安裝 *早期啟動惡意軟體防護* 驅動程式。

早期啟動惡意軟體防護 (也稱為“ELAM”) 驅動程式在網路中的電腦啟動時及協力廠商驅動程式初始化之前為這些電腦提供防護。

ELAM 驅動程式在 Kaspersky Embedded Systems Security 安裝期間自動安裝，用於在作業系統啟動時將 Kaspersky Security 服務註冊為 PPL。Kaspersky Security 服務 (KAVFS) 作為系統防護處理程序啟動後，系統中的其他非受防護處理程序將不能注入執行緒、寫入受防護處理程序的虛擬記憶體或停止服務。

當某個處理程序以 PPL 的形式啟動時，使用者無法對其進行管理，不管分配的使用者權限如何。Microsoft Windows 10 及更高版本作業系統支援使用 ELAM 驅動程式將 Kaspersky Security 服務註冊為 PPL。如果在執行支援 PPL 的作業系統的伺服器上安裝 Kaspersky Embedded Systems Security，Kaspersky Security 服務 (KAVFS) 的權限管理將不可用。

- ▶ 要安裝 Kaspersky Embedded Systems Security 作為 PPL，請執行以下指令：

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

管理 Kaspersky Embedded Systems Security 功能的存取權限

本節包含有關 Kaspersky Embedded Systems Security 和應用程式註冊的 Windows 服務的管理權限的資訊，以及如何設定這些權限的說明。

本章內容

關於 Kaspersky Embedded Systems Security 的管理權限	280
關於管理註冊服務的權限	282
關於 Kaspersky Security 服務的管理權限.....	284
關於 Kaspersky Security 管理服務的存取權限.....	286
配置用於管理 Kaspersky Embedded Systems Security 和 Kaspersky Security 服務的存取權限.....	286
對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取	290
在卡巴斯基安全管理中心中設定存取權限.....	291

關於 Kaspersky Embedded Systems Security 的管理權限

預設情況下，為受防護電腦上的管理員組的使用者、在安裝 Kaspersky Embedded Systems Security 的過程中在受防護電腦上建立的 ESS 管理員群組的使用者以及 SYSTEM 群組授予對所有 Kaspersky Embedded Systems Security 功能的存取權限。

有權限存取 Kaspersky Embedded Systems Security 的“編輯”權限功能的使用者可以向其他在受防護電腦上註冊的使用者或者該網域中包含的使用者授予對 Kaspersky Embedded Systems Security 功能的存取權限。

未在 Kaspersky Embedded Systems Security 使用者清單中註冊的使用者無法開啟應用程式主控台。

您可以為使用者或使用者群組選擇以下預設存取權限等級之一：

- **完整控制** – 所有應用程式功能的存取權限：可檢視和編輯 Kaspersky Embedded Systems Security 一般設定、元件設定和 Kaspersky Embedded Systems Security 使用者權限，還可以檢視 Kaspersky Embedded Systems Security 統計。
- **編輯** – 除編輯使用者權限以外的所有應用程式功能的存取權限：可以檢視和編輯 Kaspersky Embedded Systems Security 一般設定和 Kaspersky Embedded Systems Security 元件設定。
- **讀取** – 可以檢視 Kaspersky Embedded Systems Security 一般設定、Kaspersky Embedded Systems Security 元件設定、Kaspersky Embedded Systems Security 統計和 Kaspersky Embedded Systems Security 使用者權限。

您還可以配置進階存取權限：允許或封鎖存取 Kaspersky Embedded Systems Security 的特定功能。

如果您已為某個使用者或群組手動設定存取權限，則為該使用者或群組設定“**特殊權限**”存取層級。

表 39. 關於 Kaspersky Embedded Systems Security 功能的存取權限

使用者權限	敘述
工作管理	可啟動/停止/暫停/還原 Kaspersky Embedded Systems Security 工作。
建立和刪除自訂掃描工作	可建立和刪除自訂掃描工作。
編輯設定	可執行以下操作： <ul style="list-style-type: none"> • 從設定檔匯入 Kaspersky Embedded Systems Security 設定。 • 編輯應用程式設定。
讀取設定	可執行以下操作： <ul style="list-style-type: none"> • 檢視 Kaspersky Embedded Systems Security 一般設定和工作設定。 • 將 Kaspersky Embedded Systems Security 設定匯出到設定檔。 • 檢視工作記錄、系統稽核記錄和通知設定。

使用者權限	敘述
管理儲存區	可執行以下操作： <ul style="list-style-type: none"> 將物件移到隔離。 從隔離和備份中刪除物件。 從隔離和備份中還原物件。
管理記錄	可刪除工作記錄和清除系統稽核記錄。
讀取記錄	可檢視工作記錄和系統稽核記錄中的病毒防護事件。
讀取統計	可檢視每個 Kaspersky Embedded Systems Security 工作的統計。
應用程式授權	可啟動 Kaspersky Embedded Systems Security。
移除應用程式	可移除 Kaspersky Embedded Systems Security。
讀取權限	可檢視 Kaspersky Embedded Systems Security 使用者和使用者存取權限的清單。
編輯權限	可執行以下操作： <ul style="list-style-type: none"> 編輯具有應用程式管理存取權限的使用者清單。 編輯 Kaspersky Embedded Systems Security 功能的使用者存取權限。

關於管理註冊服務的權限

安裝過程中，Kaspersky Embedded Systems Security 會在 Windows 中註冊 Kaspersky Security 服務 (KAVFS) 和 Kaspersky Security 管理服務 (KAVFSGT) 以及 Kaspersky Security 弱點利用防禦 (KAVFSSLP)。

Microsoft Windows 10 及更高版本作業系統支援使用 ELAM 驅動程式將 Kaspersky Security 服務註冊為輕度受防護處理程序。當某個處理程序以 PPL 的形式啟動時，使用者無法對其進行管理，不管分配的使用者權限如何。如果在執行支援 PPL 的作業系統的電腦上安裝 Kaspersky Embedded Systems Security，Kaspersky Security 服務 (KAVFS) 的權限管理將不可用。

Kaspersky Security 服務

預設情況下，將管理 Kaspersky Security 服務的存取權限授予受防護電腦上“管理員”群組中的使用者，以及具有讀取權限的 SERVICE 和 INTERACTIVE 群組，和具有讀取和執行權限的 SYSTEM 群組。

有權存取“編輯權限”等級（請參見第 290 頁上的“對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取”部分）功能的使用者可以向在受防護電腦上註冊的其他使用者或者該網域中包含的其他使用者授予對管理 Kaspersky Security 服務的存取權限。

Kaspersky Security 管理服務

要透過安裝在其他電腦上的應用程式主控台來管理應用程式，使用其權限與 Kaspersky Embedded Systems Security 建立連線的帳戶必須對受防護電腦上的 Kaspersky Security 管理服務具有完全存取權限。

預設情況下，系統向以下兩組使用者授予存取所有 Kaspersky Security 管理服務的權限：受防護電腦上的管理員群組的使用者，以及安裝 Kaspersky Embedded Systems Security 時在受防護電腦上建立的 ESS 管理員群組的使用者。

只能透過 Microsoft Windows 服務管理單元管理 Kaspersky Security 管理服務。

Kaspersky Security 弱點利用防禦

預設情況下，將管理 Kaspersky Security 弱點利用防禦服務的存取權限授予受防護電腦上“管理員”群組中的使用者，以及具有讀取和執行權限的 SYSTEM 群組。

關於 Kaspersky Security 服務的管理權限

在安裝 Kaspersky Embedded Systems Security 的過程中在 Windows 中註冊 Kaspersky Security 服務 (KAVFS)，並在內部啟用在啟動作業系統時啟動的功能元件。為了降低協力廠商透過 Kaspersky Security 服務的管理存取應用程式功能和受防護電腦上安全性設定的風險，可以從應用程式主控台或管理外掛程式限制管理 Kaspersky Security 服務的權限。

預設情況下，將管理 Kaspersky Security 服務的存取權限授予受防護電腦上“管理員”群組中的使用者。將讀取權限授予 SERVICE 和 INTERACTIVE 群組，並將讀取和執行權限授予 SYSTEM 群組。

您無法刪除 SYSTEM 使用者帳戶或編輯此帳戶的權限。如果編輯 SYSTEM 帳戶的權限，則當儲存變更時會還原此帳戶的最大權限。

有權存取需要編輯權限的功能（請參見第 280 頁上的“關於 Kaspersky Embedded Systems Security 的管理權限”部分）的使用者可以向在受防護電腦上註冊的其他使用者或者該網域中包含的其他使用者授予用於管理 Kaspersky Security 服務的存取權限。

您可以為 Kaspersky Embedded Systems Security 使用者或使用者組選擇以下預設權限等級之一以管理 Kaspersky Security 服務：

- **完整控制**：可檢視和編輯 Kaspersky Security 服務的一般設定和使用者權限，以及啟動和停止 Kaspersky Security 服務。
- **讀取**：可檢視 Kaspersky Security 服務一般設定和使用者權限。
- **修改**：可檢視和編輯 Kaspersky Security 服務一般設定和使用者權限。
- **執行**：可啟動和停止 Kaspersky Security 服務。

您還可以設定進階存取權限：允許或拒絕存取指定的 Kaspersky Embedded Systems Security 功能（請參見下表）。

如果您已為某個使用者或群組手動設定存取權限，則為該使用者或群組設定“**特殊權限**”存取層級。

表 40. Kaspersky Security 服務功能的存取權限

功能	敘述
檢視服務設定	可檢視 Kaspersky Security 服務一般設定和使用者權限。
從服務管理員請求服務狀態	可從 Microsoft Windows 服務控制管理員請求 Kaspersky Security 服務的執行狀態。
從服務請求狀態	可從 Kaspersky Security 服務請求服務執行狀態。
讀取依存服務清單	可檢視 Kaspersky Security 服務依存的以及依存於 Kaspersky Security 服務的服務清單。
編輯服務設定	可檢視和編輯 Kaspersky Security 服務一般設定和使用者權限。
啟動服務	可啟動 Kaspersky Security 服務。
停止服務	可停止 Kaspersky Security 服務。
暫停/還原服務	可暫停和還原 Kaspersky Security 服務。
讀取權限	可檢視 Kaspersky Security 服務使用者清單和每個使用者的存取權限。
編輯權限	可執行以下操作： <ul style="list-style-type: none"> • 新增和刪除 Kaspersky Security 服務使用者。 • 編輯 Kaspersky Security 服務的使用者存取權限。
刪除服務	可在 Microsoft Windows 服務控制管理員中取消註冊 Kaspersky Security 服務。
使用者定義的服務請求	可建立和傳送對 Kaspersky Security 服務的使用者請求。

關於 Kaspersky Security 管理服務的存取權限

您可以檢視 [Kaspersky Embedded Systems Security 服務的清單](#)。

在安裝過程中，Kaspersky Embedded Systems Security 會註冊 Kaspersky Security 管理服務 (KAVFSGT)。要透過安裝在其他電腦上的應用程式主控台來管理應用程式，用於連線到 Kaspersky Embedded Systems Security 的帳戶必須對受防護電腦上的 Kaspersky Security 管理服務具有完全存取權限。

預設情況下，系統向以下兩組使用者授予存取所有 Kaspersky Security 管理服務的權限：受防護電腦上的管理員群組的使用者，以及安裝 Kaspersky Embedded Systems Security 時在受防護電腦上建立的 ESS 管理員群組的使用者。

只能透過 Microsoft Windows 服務管理單元管理 Kaspersky Security 管理服務。

您不能透過配置 Kaspersky Embedded Systems Security 來允許或封鎖使用者存取 Kaspersky Security 管理服務。

您可以從本機帳戶連線到 Kaspersky Embedded Systems Security，只要在受防護電腦上註冊具有相同使用者名稱和密碼的帳戶即可。

配置用於管理 Kaspersky Embedded Systems Security 和 Kaspersky Security 服務的存取權限

您可以編輯被允許存取 Kaspersky Embedded Systems Security 功能和管理 Kaspersky Security 服務的使用者和使用者組清單。您還可以編輯這些使用者和使用者群組的存取權限。

► 要從清單中新增或刪除使用者或群組：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其配置應用程式設定的管理群組。

3. 在選定的管理群組的詳細視窗中執行以下之一操作：

- 要為一組電腦配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 [144](#) 頁上的“配置政策”部分）。
- 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 [150](#) 頁上的“在卡斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**選項**”部分，執行以下步驟之一：

- 如果您希望編輯具有 Kaspersky Embedded Systems Security 功能管理存取權限的使用者清單，請點擊“**應用程式管理的使用者存取權限**”子部分中的“**設定**”。
- 如果您希望編輯具有 Kaspersky Security 服務管理存取權限的使用者清單，請點擊“**Kaspersky Security 服務管理的使用者存取權限**”子部分中的“**設定**”。

將開啟“**Kaspersky Embedded Systems Security 權限**”群組視窗。

5. 在開啟的視窗中，執行以下操作：

- 要向清單中新增使用者或群組，請點擊“**新增**”按鈕，然後選擇要授予權限的使用者或群組。
- 要從清單中刪除使用者或群組，請選擇要限制其存取權限的使用者或群組，然後點擊“**刪除**”按鈕。

6. 點擊“**套用**”按鈕。

將新增或刪除所選使用者（群組）。

► 編輯使用者或群組對管理 Kaspersky Embedded Systems Security 或 Kaspersky Security 服務的權限：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 [144](#) 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 [150](#) 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**選項**”部分，執行以下步驟之一：
 - 如果您希望編輯具有用於管理 Kaspersky Embedded Systems Security 功能的存取權限的使用者清單，請點擊“**修改應用程式管理使用者權限**”子部分中的“**設定**”。
 - 如果您希望編輯具有用於透過 Kaspersky Security 服務管理應用程式的存取權限的使用者清單，請點擊“**修改 Kaspersky Security 服務管理使用者權限**”子部分中的“**設定**”。

將開啟“**Kaspersky Embedded Systems Security 權限**”群組視窗。
5. 在開啟的視窗的“**群組或使用者**”清單中，選擇要變更其權限的使用者或使用者群組。

6. 在“<使用者 (群組) > 的權限”部分中，選中與以下存取權限等級對應的“允許”或“拒絕”核取方塊：
 - **完整控制**：可管理 Kaspersky Embedded Systems Security 或 Kaspersky Security 服務的全套權限。
 - **讀取**：
 - 管理 Kaspersky Embedded Systems Security 的以下權限：**檢索統計、讀取設定、讀取記錄和讀取權限。**
 - 用於管理 Kaspersky Security 服務的以下權限：**讀取服務設定、從服務控制管理員請求服務狀態、從服務請求狀態、讀取依存服務清單、讀取權限。**
 - **修改**：
 - 除**編輯權限**之外的所有 Kaspersky Embedded Systems Security 管理權限。
 - 管理 Kaspersky Security 服務的以下權限：**修改服務設定、讀取權限。**
 - **特殊權限**：用於管理 Kaspersky Security 服務的以下權限：**啟動服務、停止服務、暫停/還原服務、讀取權限、使用者定義的服務請求。**
7. 要配置某個使用者或群組的進階權限 (**特殊權限**)，請點擊“**進階**”按鈕。
 - a. 在開啟的“**Kaspersky Embedded Systems Security 進階安全性設定**”視窗中，選擇所需的使用者或群組。
 - b. 點擊“**編輯**”按鈕。
 - c. 在視窗頂部的下拉清單中，選擇存取控制類型 (“**允許**”或“**封鎖**”)。
 - d. 選中與要為所選使用者或群組允許或封鎖的功能旁邊的核取方塊。
 - e. 點擊“**確定**”。
 - f. 在“**Kaspersky Embedded Systems Security 的進階安全性設定**”視窗中，點擊“**確定**”。
8. 在“**Kaspersky Embedded Systems Security 的權限**”群組視窗中，點擊“**套用**”按鈕。
9. 已配置的用於管理 Kaspersky Embedded Systems Security 或 Kaspersky Security 服務的權限將被儲存。

對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取

您可透過配置使用者權限來限制對應用程式管理和已註冊服務的存取（請參見第 280 頁上的“管理 Kaspersky Embedded Systems Security 功能的存取權限”部分）。您也可在 Kaspersky Embedded Systems Security 設定中設定密碼防護，以提供額外防護。密碼防護允許您對存取應用程式主控台管理和執行命令列指令施加額外限制。如果應用密碼防護，Kaspersky Embedded Systems Security 要求所有使用者在啟動應用程式主控台或執行命令列指令時輸入密碼。

► 要防護對 Kaspersky Embedded Systems Security 功能的存取權限：

1. 在應用程式主控台樹狀目錄中，選擇“Kaspersky Embedded Systems Security”節點並執行以下操作之一：
 - 在節點的詳細資訊視窗中，點擊“應用程式內容”連結。
 - 在節點的內容功能表中選擇“內容”。將開啟“應用程式設定”視窗。
2. 在“安全性和可靠性”標籤上的“密碼防護設定”中，點擊“套用密碼防護”核取方塊。
“密碼”和“確認密碼”欄位變為活動狀態。
3. 在“密碼”欄位中，輸入想要用於防護對 Kaspersky Embedded Systems Security 功能進行存取的值。
4. 在“確認密碼”欄位中，再次輸入您的密碼。
5. 點擊“確定”。

此密碼無法還原。遺失密碼會導致完全失去對應用程式的控制。此外，還將無法從受防護電腦移除應用程式。

您可以隨時重設密碼。為此，請清除“套用密碼防護”核取方塊並儲存變更。密碼防護將被停用，舊密碼核對總和將刪除。使用新密碼重複密碼輸入過程。

在卡斯基安全管理中心中設定存取權限

您可在卡斯基安全管理中心中，為一組電腦或單台電腦設定用於管理應用程式和 Kaspersky Security 服務的存取權限。

► *配置用於管理應用程式和 Kaspersky Security 服務的存取權限：*

1. 展開卡斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 [144](#) 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 [150](#) 頁上的“在卡斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 開啟“**選項**”部分，然後執行以下操作：
 - 要為一個使用者或一組使用者設定管理 Kaspersky Embedded Systems Security 的存取權限，在“**應用程式管理的使用者存取權限**”部分中點擊“**設定**”按鈕。
 - 要為一個使用者或一組使用者配置管理 Kaspersky Security 服務的存取權限，在“**Security Service 管理的使用者存取權限**”部分中點擊“**設定**”按鈕。
5. 在開啟的視窗中，根據需要配置存取權限（請參見第 [280](#) 頁上的“管理 Kaspersky Embedded Systems Security 功能的存取權限”部分）。

將儲存指定設定。

即時檔案防護

本節包含有關即時檔案防護工作以及如何設定的資訊。

本章內容

關於“即時檔案防護”工作	292
關於工作防護範圍和安全設定	293
關於虛擬防護範圍	294
預設的防護範圍	295
預設安全等級	296
“即時檔案防護”工作中預設掃描的檔案副檔名	298
“即時檔案防護”工作預設設定	303
透過管理外掛程式管理“即時檔案防護”工作	304
透過應用程式主控台管理“即時檔案防護”工作	323

關於“即時檔案防護”工作

“即時檔案防護”工作執行期間，在存取以下受防護的電腦物件時，Kaspersky Embedded Systems Security 會對這些物件進行掃描：

- 檔案。
- 交換檔案系統執行緒 (NTFS 執行緒)。
- 本機硬碟磁碟機和外部裝置上的主開機紀錄區和啟動磁區。

當任何應用程式將檔案寫入電腦或從電腦上讀取檔案時，Kaspersky Embedded Systems Security 會攔截此檔案進行掃描以偵測其是否存在威脅；如果偵測到威脅，則執行預設操作或您指定的操作：嘗試解毒威脅、將其移至隔離區或將其刪除（如果無法解毒威脅）。在清除或刪除前，Kaspersky Embedded Systems Security 會將原始檔案的加密副本儲存到備份資料夾。如果成功解毒檔案中的威脅，Kaspersky Embedded Systems Security 會將檔案從隔離區還原到原始資料夾。

Kaspersky Embedded Systems Security 還會偵測在 Windows Subsystem for Linux® 下執行的處理程序是否存在惡意軟體。對於此類處理程序，“即時檔案防護”工作將套用目前配置定義的操作。

關於工作防護範圍和安全設定

預設情況下，即時檔案防護工作將防護電腦檔案系統中的所有物件。如果不需要對檔案系統中的所有物件進行安全防護，或者您想從工作範圍中排除任何物件，則可以限制防護範圍。

在應用程式主控台中，防護範圍以 Kaspersky Embedded Systems Security 可以控制的電腦檔案資源樹狀目錄或清單的形式顯示。預設情況下，受防護電腦的網路檔案資源以清單圖示模式顯示。

在管理外掛程式中，只有清單視圖可用。

► 若要在應用程式主控台中以樹狀檢視模式顯示網路檔案資源，

請開啟視窗左上角“設定防護範圍”部分中的下拉清單，然後選擇“樹狀檢視”。

項或節點將顯示在電腦檔案資源的清單檢視或樹狀檢視模式中，如下所示：

節點包含在防護範圍內。

節點排除在防護範圍之外。

該節點至少有一個子節點排除在防護範圍之外，或子節點的安全設定與父節點的安全設定不同（僅限樹狀檢視模式）。

如果選擇所有子節點，但未選擇父節點，則顯示  圖示。在這種情況下，在為所選子節點建立了防護範圍後，如果父節點所包含的檔案和資料夾發生變更，將自動略過這些變更。

使用應用程式主控台，您還可以新增虛擬磁碟機（請參見第 [332](#) 頁上的“建立虛擬防護範圍”部分）。
虛擬節點的名稱以藍色字體顯示。

安全性設定

工作安全設定可以配置為防護範圍中包括的所有節點或項的一般設定，或配置為電腦檔案資源樹狀目錄或清單中各個節點或項的不同設定。

為所選父節點配置的安全設定將自動套用到其所有子節點。父節點的安全設定不會套用到單獨配置的子節點。

可以使用以下方法之一配置選定防護範圍的設定：

- 選擇三個預設安全等級（請參見第 [296](#) 頁）中的一個。
- 手動為檔案資源樹狀目錄或清單中的選定節點或項配置安全設定（請參見第 [313](#) 頁上的“手動配置安全設定”部分）（安全等級變更為“自訂”）。

可以將節點或項的一組設定儲存為範本，以便以後套用至其他節點或項。

關於虛擬防護範圍

Kaspersky Embedded Systems Security 不僅可以掃描硬碟和卸除式磁碟機上的現有資料夾和檔案，還可以掃描由各種應用程式和服務在電腦上動態建立的磁碟機。

若所有電腦物件均包含在防護範圍內，則這些動態節點將自動包含在防護範圍內。但是，如果您要為這些動態節點的安全設定指定特殊值，或者沒有選擇整個電腦進行即時防護，而是選擇電腦中的離散區域，則為了將動態磁碟機、檔案或資料夾包含在防護範圍內，您必須首先在應用程式主控台中建立它們：即指定虛擬防護範圍。建立的磁碟機、檔案和資料夾將僅存在於應用程式主控台中，而非受防護電腦的檔案結構中。

若在建立防護範圍時選擇了所有子資料夾或檔案，但未選擇父資料夾，則其中顯示的所有動態資料夾或檔案將不會自動包含在防護範圍內。應在應用程式主控台中建立這些動態資料夾或檔案的“虛擬複本”並將其新增至防護範圍。

預設的防護範圍

檔案資源樹狀目錄或清單顯示基於 Microsoft Windows 的配置安全設定所擁有的讀取存取權限的節點。

Kaspersky Embedded Systems Security 覆寫以下預定義防護範圍：

- **本機磁碟。** Kaspersky Embedded Systems Security 將防護電腦硬碟磁碟機中的檔案。
- **卸除式磁碟機。** Kaspersky Embedded Systems Security 將防護外部裝置上的檔案，如 CD 或 USB 磁碟機。您可以在防護範圍中包含或排除所有卸除式裝置、單個磁碟、資料夾或檔案。
- **網路。** Kaspersky Embedded Systems Security 將掃描電腦上執行的應用程式寫入到網路資料夾或從網路資料夾讀取的檔案。當其他電腦上的應用程式存取此類檔案時，Kaspersky Embedded Systems Security 不會防護此類檔案。
- **虛擬磁碟機。** 您可以將動態資料夾和檔案以及臨時連線到電腦的硬碟包含在防護範圍內，例如共用叢集硬碟。

預設情況下，您可以在範圍清單中檢視和配置預設防護範圍；還可以在清單形成期間在設定防護範圍中向該清單新增預設範圍。

預設情況下，防護範圍包括除虛擬磁碟機外的所有預定義區域。

使用 SUBST 指令建立的虛擬硬碟將不會顯示在應用程式主控台的電腦檔案資源樹狀目錄中。若要將虛擬硬碟中的物件包含在防護範圍內，請將與此虛擬磁碟機關聯的電腦資料夾包含在防護範圍內。

已連線的網路磁碟也不會顯示在電腦檔案資源清單中。若要將網路磁碟中的物件包含在防護範圍內，請以 UNC 格式指定與該網路磁碟對應的資料夾的路徑。

預設安全等級

可以為電腦檔案資源樹狀目錄或檔案資源清單中所選的節點套用以下一項預設安全設定：“最佳效能”、“建議”和“最佳防護”。這些等級均有各自的安全設定集（請參閱下表）。

最佳效能

如果除了在電腦上使用 Kaspersky Embedded Systems Security 外，還在網路內採取了其他電腦安全措施（例如，防火牆和現有安全政策），則建議使用“最佳效能”安全等級。

建議

“建議”安全等級確保防護與對電腦的效能影響的最佳組合。Kaspersky Lab 專家建議使用該等級，因為它足以防護大多數公司網路上的電腦。預設情況下，將設定“建議”安全等級。

最佳防護

如果組織的網路有更高的電腦安全要求，則建議使用“最佳防護”安全等級。

表 41. 預設安全等級和相應的設定值

選項	安全等級		
	最佳效能	建議	最佳防護
物件防護	依副檔名	依格式	依格式
僅防護新增與變更過的檔案	已啟用	已啟用	已停用

選項	安全等級		
對受感染物件和其他物件執行的操作	封鎖存取並解毒。 解毒失敗則刪除	封鎖存取並執行 建議的操作	封鎖存取並解毒。 解毒失敗則刪除
對可疑物件執行的操作	封鎖存取並隔離	封鎖存取並執行 建議的操作	封鎖存取並隔離
排除檔案	否	否	否
不偵測	否	否	否
超過以下時間則停止掃描(秒)	60 秒	60 秒	60 秒
不掃描超過此值複合檔案(MB)	8 MB	8 MB	未設定
掃描 NTFS 交換資料串流	是	是	是
掃描開機磁區和 MBR	是	是	是
複合物件防護	<ul style="list-style-type: none"> 封裝的物件* <p>*僅新物件和已修改的物件</p>	<ul style="list-style-type: none"> SFX 壓縮檔案* 封裝的物件* 內嵌的 OLE 物件* <p>*僅新物件和已修改的物件</p>	<ul style="list-style-type: none"> SFX 壓縮檔案* 封裝的物件* 內嵌的 OLE 物件* <p>* 所有物件</p>
在偵測到嵌入物件時完全刪除應用程式無法修改的複合檔案	否	否	是

預設安全等級設定中不包含“物件防護”、“使用 iChecker 技術”、“使用 iSwift 技術”和“使用啟發式分析”設定。若變更了“物件防護”、“使用 iChecker 技術”、“使用 iSwift 技術”或“使用啟發式分析”，所選的安全等級不會變更。

“即時檔案防護”工作中預設掃描的檔案副檔名

預設情況下，Kaspersky Embedded Systems Security 將掃描具有以下副檔名的檔案：

- *386* ;
- *acm* ;
- *ade*、*adp* ;
- *asp* ;
- *asx* ;
- *ax* ;
- *bas* ;
- *bat* ;
- *bin* ;
- *chm* ;
- *cla*、*clas** ;
- *cmd* ;
- *com* ;
- *cpl* ;
- *crt* ;
- *dll* ;
- *dpl* ;
- *drv* ;
- *dvb* ;

- *dwg* ;
- *efi* ;
- *emf* ;
- *eml* ;
- *exe* ;
- *fon* ;
- *fpm* ;
- *hlp* ;
- *hta* ;
- *htm*、*html** ;
- *htt* ;
- *ico* ;
- *inf* ;
- *ini* ;
- *ins* ;
- *isp* ;
- *jpg*、*jpe* ;
- *js*、*jse* ;
- *lnk* ;
- *mbx* ;
- *msc* ;
- *msg* ;
- *msi* ;

- *msp* ;
- *mst* ;
- *nws* ;
- *ocx* ;
- *oft* ;
- *otm* ;
- *pcd* ;
- *pdf* ;
- *php* ;
- *pht* ;
- *phtm** ;
- *pif* ;
- *plg* ;
- *png* ;
- *pot* ;
- *prf* ;
- *prg* ;
- *reg* ;
- *rsc* ;
- *rtf* ;
- *scf* ;
- *scr* ;
- *sct* ;

- *shb* ;
- *shs* ;
- *sht* ;
- *shtm** ;
- *swf* ;
- *sys* ;
- *the* ;
- *them** ;
- *tsp* ;
- *url* ;
- *vb* ;
- *vbe* ;
- *vbs* ;
- *vxd* ;
- *wma* ;
- *wmf* ;
- *wmv* ;
- *wsc* ;
- *wsf* ;
- *wsh* ;
- *do?* ;
- *md?* ;
- *mp?* ;

- *ov?* ;
- *pp?* ;
- *vs?* ;
- *xl?* 。

“即時檔案防護”工作預設值

預設情況下，“即時檔案防護”工作將使用下表敘述的設定。您可以變更這些設定值。

表 42. “即時檔案防護”工作預設值

設定	預設值	敘述
防護範圍	整個電腦，虛擬磁碟機除外。	您可以限制防護範圍。
物件防護模式	存取及修改時	您可以選擇防護模式，即定義 Kaspersky Embedded Systems Security 掃描物件所採用的存取類型。
啟發式分析	套用“中度”安全等級。	您可以啟用或停用“啟發式分析”並設定分析等級。
套用信任區域	已套用。	可用於所選工作中的一般排除清單。
在防護中使用 KSN	已套用。	您可以使用卡斯基安全網路雲端服務的基礎架構提高您的伺服器防護能力(接受 KSN 聲明後可用)。
工作啟動排程	程式啟動時。	您可以配置排程的工作啟動。
封鎖對顯示惡意活動的主機的網路共用資源的存取	未套用。	可以將出現惡意活動的主機新增到封鎖的主機清單中。

透過管理外掛程式管理“即時檔案防護”工作

在本節中，學習如何導航管理外掛程式介面，以及如何為網路中的一台或所有電腦配置工作設定。

本章節說明項目

導航	304
配置“即時檔案防護”工作	306
建立和配置工作防護範圍	312
手動配置安全性設定	313

導航

學習如何透過介面導航到所需工作設定。

本章節說明項目

開啟“即時檔案防護”工作的政策設定	304
關於“即時檔案防護”工作內容	305

開啟“即時檔案防護”工作的政策設定

► 要透過卡巴斯基安全管理中心政策開啟“即時檔案防護”工作設定：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“**政策**”標籤。
4. 點擊要設定的政策名稱。

5. 在開啟的“內容：<政策名稱>”視窗中，選擇“即時電腦防護”部分。
6. 點擊“即時檔案防護”子部分中的“設定”按鈕。

將開啟“即時檔案防護”視窗。

如果某台電腦受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過應用程式主控台編輯這些設定。

開啟“即時檔案防護”工作內容

► 要開啟單台網路電腦的“即時檔案防護”工作設定視窗：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“裝置”標籤。
4. 採用以下方法之一開啟“內容：<電腦名稱>”視窗：
 - 點擊受防護電腦的名稱。
 - 在受防護電腦的上下文功能表中選擇“內容”項。

將開啟“內容：<電腦名稱>”視窗。

5. 在“工作”部分中，選擇“即時檔案防護”工作。
6. 點擊“內容”按鈕。

將開啟“內容：即時檔案防護”視窗。

配置“即時檔案防護”工作

► 要配置“即時檔案防護”工作設定：

1. 開啟“即時檔案防護”視窗（請參見第 [304](#) 頁上的“開啟‘即時檔案防護’工作的政策設定”部分）。
2. 配置以下工作設定：
 - 在“一般”標籤上：
 - 物件防護模式（請參見第 [307](#) 頁上的“選擇防護模式”部分）
 - 啟發式分析
 - 與其他元件整合（請參見第 [308](#) 頁上的“配置啟發式分析以及與其他應用程式元件的整合”部分）
 - 在“工作管理”標籤上：
 - 排程工作啟動配置（請參見第 [164](#) 頁上的“配置工作啟動排程設定”部分）。
3. 選擇“防護範圍”標籤，然後執行以下操作：
 - 點擊“新增”或“編輯”按鈕編輯防護範圍（請參見第 [329](#) 頁上的“建立防護範圍”部分）。
 - 在開啟的視窗中，選擇要包含到工作防護範圍的內容：
 - 預設的範圍
 - 磁碟、資料夾或網路資料夾
 - 檔案
 - 選擇一項預設安全等級（請參見第 [296](#) 頁）或手動配置防護（請參見第 [313](#) 頁上的“手動配置安全設定”部分）設定。
4. 在“即時檔案防護”視窗中點擊“確定”。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在系統稽核記錄中。

本章節說明項目

選擇防護模式.....	307
配置啟發式分析以及與其他應用程式元件的整合.....	308
配置工作啟動排程設定.....	310

選擇防護模式

在“即時檔案防護”工作中，可以選擇防護模式。在“**物件防護模式**”部分中，您可以指定 Kaspersky Embedded Systems Security 在掃描物件時所採用的存取類型。

“**物件防護模式**”設定中的值套用於在工作中指定的整個防護範圍。無法為防護範圍內的單個節點指定不同的設定值。

► 要選擇防護模式：

1. 開啟“**即時檔案防護**”視窗（請參見第 [304](#) 頁上的“開啟‘即時檔案防護’工作的政策設定”部分）。
2. 在開啟的視窗中，開啟“**一般**”標籤，然後選擇要設定的防護模式：

- **智慧模式**

Kaspersky Embedded Systems Security 自行選擇要掃描的物件。在物件開啟時掃描該物件，如果物件進行了修改，則在物件儲存後重新掃描該物件。在處理程序執行過程中，如果多次調用物件或對該物件進行了修改，則 Kaspersky Embedded Systems Security 僅在處理程序最後一次儲存物件之後重新掃描該物件。

- **存取及修改時**

Kaspersky Embedded Systems Security 在物件開啟時掃描該物件，如果物件進行了修改，則在物件儲存後重新掃描該物件。

預設選中該選項。

- **存取時**

Kaspersky Embedded Systems Security 在物件開啟以進行讀取、執行或修改時掃描所有物件。

- **執行時**

僅在存取檔案以執行該檔案時 Kaspersky Embedded Systems Security 才掃描該檔案。

3. 點擊“確定”。

選中防護模式將生效。

配置啟發式分析以及與其他應用程式元件的整合

要啟動“KSN 使用”工作，您必須接受卡巴斯基安全網路聲明。

► *要配置啟發式分析以及與其他元件的整合：*

1. 開啟“即時檔案防護”視窗（請參見第 [304](#) 頁上的“開啟‘即時檔案防護’工作的政策設定”部分）。
2. 在“一般”標籤上，清除或選中“使用啟發式分析”核取方塊。

此核取方塊可在物件掃描過程中啟用/停用啟發式分析。

如果選中該核取方塊，則啟用啟發式分析。

如果取消選中該核取方塊，則停用啟發式分析。

預設將會選定該核取方塊。

3. 如有必要，使用滑塊調整分析等級。

使用滑塊可以調整啟發式分析等級。掃描強度等級用於在威脅搜尋的徹底程度、作業系統資源負荷和掃描所需時間之間建立平衡。

以下掃描強度等級可用：

- **輕度**。啟發式分析在可執行檔中執行較少的操作。在該模式下偵測出威脅的可能性較小。掃描速度較快，而且佔用資源較少。
- **中度**。啟發式分析在可執行檔中執行 Kaspersky Lab 專家建議的多條指令。預設選中該等級。
- **深度**。啟發式分析在可執行檔中執行較多的操作。在該模式下偵測出威脅的可能性較大。掃描使用更多的系統資源、花費更多時間且可導致更多的誤報。

如果選中“**使用啟發式分析**”核取方塊，則滑塊才可用。

4. 在“**與其他元件整合**”部分中，配置以下設定：

- 選中或清除“**套用信任區域**”核取方塊。

使用此核取方塊可啟用/停用工作的信任區域。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會將受信任處理程序的檔案操作新增到工作設定中配置的掃描排除中。

如果清除該核取方塊，Kaspersky Embedded Systems Security 會在建立工作的防護範圍時略過受信任處理程序的檔案操作。

預設將會選定該核取方塊。

- 選中或清除“**在防護中使用 KSN**”核取方塊。

該核取方塊可啟用或停用 KSN 服務的使用。

如果選中該核取方塊，應用程式將使用卡斯基安全網路資料確保應用程式更快速地對新威脅做出回應，並降低誤報的可能性。

如果清除該核取方塊，則工作將不使用 KSN 服務。

預設將會選定該核取方塊。

在“KSN 使用”工作設定中必須選中“傳送關於已掃描檔案的資料”核取方塊。

- 選中或清除“封鎖對顯示惡意活動的主機的網路共用資源的存取”核取方塊。

5. 點擊“確定”。

配置的工作設定將立即套用到正在執行的工作。如果工作未執行，則將在下次啟動時套用修改後的設定。

配置工作啟動排程設定

您可以在應用程式主控台中配置本機系統和自訂工作的啟動排程。您不能為群組工作配置啟動排程。

► 要配置群組工作啟動排程設定，請執行以下操作：

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開“受管理裝置”節點。
2. 選取受防護伺服器所屬的群組。
3. 在詳細資訊窗格中，選取“工作”標籤。
4. 採用以下方法之一開啟“內容：<工作名稱>”視窗：
 - 點擊工作的名稱。
 - 開啟工作名稱的上下文功能表，然後選取“內容”項。
5. 選取“排程”部分。
6. 在“排程設定”設定塊中，選中“依排程執行”核取方塊。

如果卡巴斯基安全管理中心政策封鎖按排程啟動自訂掃描工作和更新工作，則這些工作的排程設定的欄位不可用。

7. 根據需要配置排程設定。為此，請執行以下操作：
 - a. 在“週期”清單中，選擇以下值之一：
 - **每小時**，如果您希望該工作在指定的小時數內間隔執行，請在“每 <數量> 小時”欄位中指定小時數。
 - **每天**，如果您希望該工作在指定的天數內間隔執行，請在“每 <數量> 天”欄位中指定天數。

- **每週**，如果您希望該工作在指定的週數內間隔執行，請在“每 <數量> 週”欄位中指定週數。指定工作啟動的星期中的日期（預設在星期一啟動工作）。
 - **在應用程式啟動時**，如果您希望在每次啟動 Kaspersky Embedded Systems Security 時執行該工作。
 - **應用程式資料庫更新後**，如果您希望在每次更新應用程式資料庫後執行該工作。
- b. 在“**開始時間**”欄位中指定首次啟動工作的時間。
- c. 在“**開始日期**”欄位中，指定套用排程的開始日期。

指定了工作啟動頻率之後，將在視窗頂部的“**下次開始**”欄位中顯示工作的首次啟動時間、排程的開始套用日期以及預計下一個工作啟動時間的相關資訊。每次開啟“**工作設定**”視窗的“**排程**”標籤時，將顯示有關工作的下一次預計啟動時間的最新資訊。

如果 卡巴斯基安全管理中心的活動政策設定禁止活動排程的系統工作，則將在“**下次開始**”欄位中顯示值“**政策不允許**”（請參見第 [123](#) 頁上的“**配置本機預設工作的排程啟動**”一節）。

8. 根據需要使用“**進階**”標籤來配置以下排程設定。
- 在“**工作停止設定**”部分中：
 - a. 選中“**持續時間**”核取方塊，並輸入右側欄位中輸入所需的小時數和分鐘數以指定工作執行的最大持續時間。
 - b. 選中“**暫停開始於**”核取方塊，並在右側欄位中輸入時間間隔的開始和結束值，以指定在工作執行的 24 小時中將暫停執行工作的時間間隔。
 - 在“**進階設定**”部分中：
 - a. 選中“**取消排程開始於**”核取方塊，並指定停止執行排程的日期。
 - b. 選定“**執行錯過的工作**”核取方塊以允許啟動略過的工作。
 - c. 選中“**在該時間間隔內隨機化工作開始時間**”核取方塊，並按分鐘指定該值。
9. 點擊“**確定**”。
10. 點擊“**套用**”按鈕儲存工作啟動設定。

如果要使用卡巴斯基安全管理中心配置單個工作的應用程式設定，請執行第 [150](#) 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分中介紹的步驟。

建立和配置工作防護範圍

► 要透過卡巴斯基安全管理中心建立和配置工作防護範圍：

1. 開啟“即時檔案防護”視窗（請參見第 [304](#) 頁上的“開啟‘即時檔案防護’工作的政策設定”部分）。
2. 選擇“防護範圍”標籤。
3. 已經受工作防護的所有項目都列在“防護範圍”表中。
4. 點擊“新增”按鈕向清單中新增新項目。

將開啟“新增物件至防護範圍”視窗。

5. 選擇物件類型以將其新增到防護範圍中：
 - 預設的範圍，以便將一個預設範圍包含在伺服器的防護範圍中。然後在下拉清單中，選擇必需的防護範圍。
 - 磁碟、資料夾或網路資料夾，以便在防護範圍中包括單個磁碟機、資料夾或網路物件。然後透過點擊“瀏覽”按鈕選擇必需的防護範圍。
 - 檔案，以便在防護範圍中包括單個檔案。然後透過點擊“瀏覽”按鈕選擇必需的防護範圍。

如果某個物件已經作為防護範圍的排除新增，則不能再將其新增到防護範圍中。

6. 要從防護範圍中排除單個項目，請清除這些項目名稱旁邊的核取方塊，或者執行以下步驟：
 - a. 右鍵點擊防護範圍開啟其內容功能表。
 - b. 在內容功能表中，選擇“新增排除項目”選項。
 - c. 在“新增排除項目”視窗中，選擇要作為防護範圍的排除項新增的物件類型，並遵循將物件新增到防護範圍中的過程的邏輯。

7. 要修改新增的防護範圍或排除，請選擇所需防護範圍內容功能表中的“**編輯範圍**”選項。
8. 若要在網路檔案資源清單中隱藏之前新增的防護範圍或排除，請在所需防護範圍的內容功能表中選擇“**刪除範圍**”選項。

該防護範圍將從網路檔案資源清單中刪除，同時從“即時檔案防護”工作範圍中排除。

9. 點擊“**儲存**”按鈕。

防護範圍設定視窗將關閉。將儲存新配置的設定。

僅在至少有一個電腦檔案資源節點包含在防護範圍內時，才可啟動“即時檔案防護”工作。

手動配置安全性設定

預設情況下，“即時檔案防護”工作對整個防護範圍使用通用安全設定。這些設定對應于“**建議**”預設安全等級（請參見第 [296](#) 頁上的“預設安全等級”部分）。

若要修改安全性設定的預設值，可透過將它們配置為用於整個防護範圍的一般設定，或為電腦檔案資源清單中的不同項目或樹狀目錄中的節點配置不同設定。

► 要手動設定所選節點的安全性設定：

1. 開啟“**即時檔案防護**”視窗（請參見第 [304](#) 頁上的“開啟‘即時檔案防護’工作的政策設定”部分）。
2. 在“**防護範圍**”標籤上，選擇您要配置其安全設定的節點，然後點擊“**配置**”。
將開啟“**即時檔案防護設定**”視窗。
3. 在“**安全等級**”標籤上，點擊“**設定**”按鈕以設定自訂設定。
4. 您可以根據需求配置選定節點的自訂安全設定：
 - 一般設定（請參見第 [314](#) 頁上的“配置一般工作設定”部分）
 - 操作（請參見第 [318](#) 頁上的“設定操作”部分）

- 效能 (請參見第 [320](#) 頁上的“設定效能”部分)

5. 在“即時檔案防護”視窗中點擊“確定”。

將儲存新的防護範圍設定。

本章節說明項目

配置一般工作設定	314
配置操作	318
配置效能	320

配置一般工作設定

► 要配置“即時檔案防護”工作的一般安全設定：

1. 開啟“即時檔案防護設定”視窗 (請參見第 [304](#) 頁上的“開啟‘即時檔案防護’工作的政策設定”部分) 。
2. 選擇“一般”標籤。
3. 在“物件防護”部分中，指定要包含在防護範圍內的物件類型：

- **所有物件**

Kaspersky Embedded Systems Security 掃描所有物件。

- **按格式掃描物件**

Kaspersky Embedded Systems Security 僅根據檔案格式掃描感染物件。

Kaspersky Lab 編制了該格式清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。

- **按病毒資料庫中指定的副檔名清單掃描物件**

Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。

Kaspersky Lab 編制了該副檔名清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。

- **按指定的副檔名清單掃描物件**

Kaspersky Embedded Systems Security 根據檔案副檔名掃描檔案。可在“**副檔名清單**”視窗（透過點擊“**編輯**”按鈕開啟）中手動自訂檔案副檔名清單。

- **掃描開機磁區和 MBR**

啟用對開機磁區和主引導記錄的防護。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描電腦的硬碟磁碟機和卸除式磁碟機上的開機磁區和主引導記錄。

預設將會選定該核取方塊。

- **掃描 NTFS 交換資料串流**

掃描 NTFS 檔案系統磁碟機上的替代檔案和資料夾執行緒。

如果選中該核取方塊，應用程式將掃描疑似感染物件以及與該物件關聯的所有 NTFS 執行緒。

如果清除該核取方塊，應用程式將只掃描偵測到並被視為疑似感染的物件。

預設將會選定該核取方塊。

4. 在“**效能**”部分中，選中或清除“**僅防護新增與變更過的檔案**”核取方塊。

使用此核取方塊可啟用/停用對自上次掃描以來 Kaspersky Embedded Systems Security 識別為新檔案或已修改的檔案的掃描和防護。

如果選中該核取方塊，Kaspersky Embedded Systems Security 僅掃描和防護自上次掃描以來被識別為新檔案或已修改的檔案。

如果清除該核取方塊，您可以選擇希望僅掃描和防護新檔案，還是掃描和防護所有檔案而略過檔案的修改狀態。

對於“**最佳效能**”安全等級，預設選定該核取方塊。如果設定“**最佳防護**”或“**建議**”安全等級，則取消選中該核取方塊。

如果清除該核取方塊，要在可用選項之間轉換，請點擊每個複合物件類型對應的“全部/僅新建”連結。

5. 在“複合物件防護”部分中，指定要包含在防護範圍內的複合物件：

- **全部/僅新的壓縮檔案**

掃描 ZIP、CAB、RAR、ARJ 壓縮檔案及其他壓縮檔案格式。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描壓縮檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過壓縮檔案。

預設值取決於所選的防護等級。

- **全部/僅新的 SFX 壓縮檔案**

掃描自解壓壓縮檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描 SFX 壓縮檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過 SFX 壓縮檔案。

預設值取決於所選的防護等級。

如果取消選中“**壓縮檔案**”核取方塊，則該選項處於活動狀態。

- **全部/僅新的電子郵件資料庫**

掃描 Microsoft Outlook 和 Microsoft Outlook Express 郵件資料庫檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描郵件資料庫檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過郵件資料庫檔案。

預設值取決於所選的安全等級。

- **全部/僅新的封裝的物件**

掃描由二進位代碼封裝程式 (例如 UPX 或 ASPack) 封裝的可執行檔。

如果選中該核取方塊 , Kaspersky Embedded Systems Security 將掃描由封裝程式封裝的可執行檔。

如果取消選中該核取方塊 , Kaspersky Embedded Systems Security 將在掃描期間略過由封裝程式封裝的可執行檔。

預設值取決於所選的防護等級。

- **全部/僅新的純文字電子郵件**

掃描郵件格式檔案 , 例如 Microsoft Office Outlook 和 Microsoft Outlook Express 郵件。

如果選中該核取方塊 , Kaspersky Embedded Systems Security 將掃描郵件格式檔案。

如果取消選中該核取方塊 , Kaspersky Embedded Systems Security 將在掃描期間略過郵件格式檔案。

預設值取決於所選的安全等級。

- **全部/僅新嵌入的 OLE 物件**

掃描嵌入到檔案中的物件 (如 Microsoft Word 巨集或電子郵件附件) 。

如果選中該核取方塊 , Kaspersky Embedded Systems Security 將掃描嵌入到檔案中的物件。

如果取消選中該核取方塊 , Kaspersky Embedded Systems Security 將在掃描期間略過嵌入到檔案中的物件。

預設值取決於所選的防護等級。

6. 點擊“儲存”。

將儲存新的工作配置。

配置操作

► 要為“即時檔案防護”工作配置對受感染的物件和其他偵測到的物件的操作：

1. 開啟“即時檔案防護設定”視窗（請參見第 [304](#) 頁上的“開啟‘即時檔案防護’工作的政策設定”部分）。
2. 選擇“操作”標籤。
3. 選擇要對受感染的物件和其他偵測到的物件執行的操作：

- **僅通知。**

選擇此模式時，Kaspersky Embedded Systems Security 不封鎖存取受感染的物件和其他偵測到的物件，也不對它們執行任何操作。以下事件在工作記錄中註冊：*物件未解毒。原因：由於使用者定義的設定，未執行任何操作使偵測到的物件無效。*該事件指定有關偵測到的物件的所有可用資訊。

應該為每個防護或掃描區域單獨配置“僅通知”模式。預設情況下，任何安全等級都不使用此模式。如果選擇此模式，Kaspersky Embedded Systems Security 會自動將安全等級變更為“自訂”。

- **封鎖存取。**

選擇此選項時，Kaspersky Embedded Systems Security 會封鎖對偵測到或疑似感染的物件的存取。您可以在下拉清單中選擇對已封鎖物件的其他操作。

- **執行附加操作。**

從下拉清單中選擇操作：

- **解毒。**
- **解毒，無法解毒時刪除。**
- **刪除。**
- **建議。**

4. 選擇要對可疑的物件執行的操作：

- **僅通知。**

選擇此模式時，Kaspersky Embedded Systems Security 不封鎖存取受感染的物件和其他偵測到的物件，也不對它們執行任何操作。以下事件在工作記錄中註冊：*物件未解毒。原因：由於使用者定義的設定，未執行任何操作使偵測到的物件無效。*該事件指定有關偵測到的物件的所有可用資訊。

應該為每個防護或掃描區域單獨配置“**僅通知**”模式。預設情況下，任何安全等級都不使用此模式。如果選擇此模式，Kaspersky Embedded Systems Security 會自動將安全等級變更為“**自訂**”。

- **封鎖存取。**

選擇此選項時，Kaspersky Embedded Systems Security 會封鎖對偵測到或疑似感染的物件的存取。您可以在下拉清單中選擇對已封鎖物件的其他操作。

- **執行附加操作。**

從下拉清單中選擇操作：

- **隔離。**
- **刪除。**
- **建議。**

5. 選擇依威脅類型對物件執行的操作：

- a. 清除或選中“**根據偵測到的物件的類型執行操作**”核取方塊。

如果選中該核取方塊，可以透過點擊該核取方塊旁邊的“**設定**”按鈕來獨立設定針對每種偵測到的物件類型的主要和次要操作。此時，Kaspersky Embedded Systems Security 將不允許開啟或執行受感染的物件，無論您的選擇如何。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將對指定的物件類型分別執行在“**對受感染物件和其他物件執行的操作**”和“**對可疑物件執行的操作**”部分中選擇的操作。

預設取消選定該核取方塊。

- b. 點擊“設定”按鈕。
 - c. 在開啟的視窗中，選擇針對每種偵測到的物件類型的主要和次要操作（如果主要操作失敗）。
 - d. 點擊“確定”。
6. 選擇要對不可修改的複合物件執行的操作：選擇或清除“在偵測到嵌入物件時完全刪除應用程式無法修改的複合檔案”核取方塊。

此核取方塊用於啟用或停用當偵測到惡意、疑似感染或其他偵測到的子內嵌物件時強制刪除父複合檔案。

如果選中該核取方塊並且工作設定為刪除受感染和疑似感染的物件，Kaspersky Embedded Systems Security 會在偵測到惡意或其他內嵌物件時強制刪除整個父複合物件。如果應用程式無法只刪除偵測到的子物件（例如，如果父物件不可修改），將強制刪除父物件及其所有內容。

如果清除該核取方塊並且工作設定為刪除受感染和疑似感染的物件，當父物件不可修改時，Kaspersky Embedded Systems Security 不會執行所選操作。

7. 點擊“儲存”。

將儲存新的工作配置。

配置效能

► 要配置“即時檔案防護”工作的效能：

1. 開啟“即時檔案防護設定”視窗（請參見第 [304](#) 頁上的“開啟‘即時檔案防護’工作的政策設定”部分）視窗。
2. 選擇“效能”標籤。
3. 在“排除”部分中：
 - 清除或選中“排除檔案”核取方塊。

按檔案名或檔案名遮罩從掃描中排除檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過指定的物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將掃描所有物件。

預設取消選定該核取方塊。

- 清除或選中“**不偵測**”核取方塊。

按可偵測物件的名稱或名稱遮罩從掃描中排除物件。病毒百科全書

<https://encyclopedia.kaspersky.com/knowledge/classification/> 網站上提供了可偵測物件的名稱清單。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過指定的可偵測物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 預設將偵測程式中指定的所有物件。

預設取消選定該核取方塊。

- 針對每個設定點擊“**編輯**”按鈕以新增排除項目。

4. 在“**進階設定**”部分中：

- **超過以下時間則停止掃描(秒)**

限制物件掃描的持續時間。預設值為 60 秒。

如果選中該核取方塊，則掃描持續時間將限制為指定的值。

如果取消選中該核取方塊，則對掃描持續時間沒有限制。

對於“**最佳效能**”安全等級，預設選定該核取方塊。

- **不掃描超過此值複合檔案(MB)**

將超過指定大小的物件排除在掃描之外。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在病毒掃描期間略過大小超過指定限制值的複合物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將掃描任意大小的複合物件。

對於“最佳效能”安全等級，預設選定該核取方塊。

- **使用 iSwift 技術**

iSwift 將資料庫中儲存的檔案 NTFS 識別碼與目前識別碼進行比較。只對識別碼發生變化的檔案（新檔案和自上次掃描 NTFS 系統物件以來修改過的檔案）執行掃描。

如果選中該核取方塊，Kaspersky Embedded Systems Security 僅掃描自上次掃描 NTFS 系統物件以來新建或修改的檔案。

如果清除該核取方塊，Kaspersky Embedded Systems Security 在掃描 NTFS 系統檔案時將不考慮檔案建立或修改的日期（網路資料夾中的檔案除外）。

預設將會選定該核取方塊。

- **使用 iChecker 技術**

iChecker 會計算並記住掃描的檔案的核對總和。如果物件被修改，核對總和會發生變化。應用程式在掃描工作中比較所有核對總和，並且僅掃描新檔案和自上次掃描檔案以來修改過的檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 僅掃描新檔案和修改的檔案。

如果清除該核取方塊，Kaspersky Embedded Systems Security 在掃描檔案時將不考慮檔案建立或修改的日期。

預設將會選定該核取方塊。

透過應用程式主控台管理“即時檔案防護”工作

在本節中，學習如何導航應用程式主控台介面以及如何在本地電腦上配置工作設定。

本章節說明項目

導航	323
開啟“即時檔案防護”範圍設定	323
開啟“即時檔案防護”工作設定	324
配置“即時檔案防護”工作	324
建立防護範圍	329
手動配置安全性設定	333
即時檔案防護工作統計	343

導航

學習如何透過介面導航到所需工作設定。

開啟“即時檔案防護”範圍設定

► 要開啟“即時檔案防護”工作的防護範圍設定視窗：

1. 在應用程式主控台樹狀目錄中展開“**即時電腦防護**”節點。
2. 選擇“**即時檔案防護**”子節點。
3. 在詳細資訊窗格中點擊“**配置防護範圍**”連結。

開啟“**設定防護範圍**”視窗。

開啟“即時檔案防護”工作設定

► 要開啟一般工作設定視窗：

1. 在應用程式主控台樹狀目錄中展開“**即時電腦防護**”節點。
2. 選擇“**即時檔案防護**”子節點。
3. 在詳細資訊視窗中點擊“**內容**”連結。

將開啟“**工作設定**”視窗。

配置“即時檔案防護”工作

► 要配置“即時檔案防護”工作設定：

1. 開啟“**工作設定**”視窗（請參見第 [324](#) 頁上的“開啟‘即時檔案防護’工作設定”部分）。
2. 在“**一般**”標籤上，配置以下工作設定：
 - **物件防護模式**（請參見第 [325](#) 頁上的“選擇防護模式”部分）
 - **啟發式分析**
 - **與其他元件整合**（請參見第 [326](#) 頁上的“配置啟發式分析以及與其他應用程式元件的整合”部分）
3. 在“**排程**”和“**進階**”標籤上，指定排程的啟動設定（請參見第 [189](#) 頁上的“配置工作啟動排程設定”部分）。
4. 在“**工作設定**”視窗中點擊“**確定**”。

將儲存修改的設定。

5. 在“**即時檔案防護**”節點的詳細資訊窗格中，點擊“**配置防護範圍**”連結。
6. 執行以下操作：
 - 在電腦檔案資源樹狀目錄或清單中，選擇要包含在工作防護範圍內的節點或項目。
 - 選擇其中一個預設安全等級或手動配置物件防護設定（請參見第 [546](#) 頁上的“手動配置安全設定”部分）。
7. 在“**設定防護範圍**”視窗中，點擊“**儲存**”按鈕。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在系統稽核記錄中。

本章節說明項目

選擇防護模式	325
配置啟發式分析以及與其他應用程式元件的整合	326
配置工作啟動排程設定	328

選擇防護模式

在“即時檔案防護”工作中，可以選擇防護模式。在“**物件防護模式**”部分中，您可以指定 Kaspersky Embedded Systems Security 在掃描物件時所採用的存取類型。

“**物件防護模式**”設定中的值套用於在工作中指定的整個防護範圍。無法為防護範圍內的單個節點指定不同的設定值。

► 若要選擇防護模式，請執行以下步驟：

1. 開啟“**工作設定**”視窗（請參見第 [324](#) 頁上的“開啟‘即時檔案防護’工作設定”部分）。
2. 在開啟的視窗中，開啟“**一般**”標籤，然後選擇要設定的防護模式：

- **智慧模式**

Kaspersky Embedded Systems Security 自行選擇要掃描的物件。在物件開啟時掃描該物件，如果物件進行了修改，則在物件儲存後重新掃描該物件。在處理程序執行過程中，如果多次調用物件或對該物件進行了修改，則 Kaspersky Embedded Systems Security 僅在處理程序最後一次儲存物件之後重新掃描該物件。

- **存取及修改時**

Kaspersky Embedded Systems Security 在物件開啟時掃描該物件，如果物件進行了修改，則在物件儲存後重新掃描該物件。

預設選中該選項。

- **存取時**

Kaspersky Embedded Systems Security 在物件開啟以進行讀取、執行或修改時掃描所有物件。

- **執行時**

僅在存取檔案以執行該檔案時 Kaspersky Embedded Systems Security 才掃描該檔案。

3. 點擊“確定”。

選中防護模式將生效。

配置啟發式分析以及與其他應用程式元件的整合

要啟動“KSN 使用”工作，您必須接受卡巴斯基安全網路聲明。

► *要配置啟發式分析以及與其他元件的整合：*

1. 開啟“工作設定”視窗（請參見第 [324](#) 頁上的“開啟‘即時檔案防護’工作設定”部分）。

2. 在“一般”標籤上，清除或選中“使用啟發式分析”核取方塊。

此核取方塊可在物件掃描過程中啟用/停用啟發式分析。

如果選中該核取方塊，則啟用啟發式分析。

如果取消選中該核取方塊，則停用啟發式分析。

預設將會選定該核取方塊。

3. 如有必要，使用滑塊調整分析等級。

使用滑塊可以調整啟發式分析等級。掃描強度等級用於在威脅搜尋的徹底程度、作業系統資源負荷和掃描所需時間之間建立平衡。

以下掃描強度等級可用：

- **輕度**。啟發式分析在可執行檔中執行較少的操作。在該模式下偵測出威脅的可能性較小。掃描速度較快，而且佔用資源較少。
- **中度**。啟發式分析在可執行檔中執行 Kaspersky Lab 專家建議的多條指令。預設選中該等級。
- **深度**。啟發式分析在可執行檔中執行較多的操作。在該模式下偵測出威脅的可能性較大。掃描使用更多的系統資源、花費更多時間且可導致更多的誤報。

如果選中“**使用啟發式分析**”核取方塊，則滑塊才可用。

4. 在“**與其他元件整合**”部分中，配置以下設定：

- 選中或清除“**套用信任區域**”核取方塊。

使用此核取方塊可啟用/停用工作的信任區域。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會將受信任處理程序的檔案操作新增到工作設定中配置的掃描排除中。

如果清除該核取方塊，Kaspersky Embedded Systems Security 會在建立工作的防護範圍時略過受信任處理程序的檔案操作。

預設將會選定該核取方塊。

點擊“**信任區域**”連結開啟“信任區域”設定。

- 選中或清除“**在防護中使用 KSN**”核取方塊。

該核取方塊可啟用或停用 KSN 服務的使用。

如果選中該核取方塊，應用程式將使用卡斯基安全網路資料確保應用程式更快速地對新威脅做出回應，並降低誤報的可能性。

如果清除該核取方塊，則工作將不使用 KSN 服務。

預設將會選定該核取方塊。

在“KSN 使用”工作設定中必須選中“**傳送關於已掃描檔案的資料**”核取方塊。

- 選中或清除“封鎖對顯示惡意活動的主機的網路共用資源的存取”核取方塊。

5. 點擊“確定”。

將套用新設定的設定。

配置工作啟動排程設定

您可以在應用程式主控台中配置本機系統和自訂工作的啟動排程。您不能為群組工作配置啟動排程。

► 要配置工作啟動排程設定：

1. 開啟要配置啟動排程工作的內容功能表。

2. 選擇“內容”。

將開啟“工作設定”視窗。

3. 在開啟的視窗中的“排程”標籤上，選中“依排程執行”核取方塊。

4. 根據需要配置排程設定。為此，請執行以下操作：

a. 在“週期”中，選擇以下值之一：

- **每小時**，如果您希望該工作在指定的小時數內間隔執行，請在“每 <數量> 小時”欄位中指定小時數。
- **每天**，如果您希望該工作在指定的天數內間隔執行，請在“每 <數量> 天”欄位中指定天數。
- **每週**，如果您希望該工作在指定的週數內間隔執行，請在“每 <數量> 週”欄位中指定週數。指定工作啟動的星期中的日期（預設在星期一啟動工作）。
- **在應用程式啟動時**，如果您希望在每次啟動 Kaspersky Embedded Systems Security 時執行該工作。
- **應用程式資料庫更新後**，如果您希望在每次更新應用程式資料庫後執行該工作。

b. 在“開始時間”欄位中指定首次啟動工作的時間。

c. 在“開始日期”欄位中，指定套用排程的開始日期。

指定了工作啟動頻率之後，將在視窗頂部的“下次開始”欄位中顯示工作的首次啟動時間、排程的開始套用日期以及預計下一個工作啟動時間的相關資訊。每次開啟“工作設定”視窗的“排程”標籤時，將顯示有關工作的下一次預計啟動時間的最新資訊。

在卡斯基安全管理中心政策設定中設定了按排程啟動系統工作，則“政策不允許”顯示在“下次開始”欄位中。

5. 根據需要使用“進階”標籤來配置以下排程設定。

- 在“工作停止設定”部分中：
 - a. 選中“持續時間”核取方塊，並輸入右側欄位中輸入所需的小時數和分鐘數以指定工作執行的最大持續時間。
 - b. 選中“暫停開始於”核取方塊，並在右側欄位中輸入時間間隔的開始和結束值，以指定在工作執行的 24 小時中將暫停執行工作的時間間隔。
- 在“進階設定”部分中：
 - a. 選中“取消排程開始於”核取方塊，並指定停止執行排程的日期。
 - b. 選定“執行錯過的工作”核取方塊以允許啟動略過的工作。
 - c. 選中“在該時間間隔內隨機啟動工作”核取方塊，並按分鐘指定該值。

6. 點擊“確定”。

將儲存已配置的工作啟動設定。

建立防護範圍

本節提供有關在即時檔案防護工作中建立和管理防護範圍的說明。

本章節說明項目

建立防護範圍.....	330
建立虛擬防護範圍.....	332

建立防護範圍

建立即時檔案防護工作範圍的過程取決於網路檔案資源視圖模式(請參見第 293 頁上的“關於工作防護範圍和安全設定”部分)。可以將網路檔案資源檢視模式配置為樹狀目錄或清單(設定為預設值)。

要對工作應用新的設定防護範圍，必須重新啟動“即時檔案防護”工作。

► 要使用網路檔案資源樹狀目錄建立防護範圍：

1. 開啟“設定防護範圍”視窗(請參見第 323 頁上的“開啟‘即時檔案防護’範圍設定”部分)。
2. 在視窗的左側部分中，開啟網路檔案資源樹狀目錄以顯示所有節點和子節點。
3. 執行以下操作：
 - 要從防護範圍中排除單個節點，請清除這些節點名稱旁邊的核取方塊。
 - 要從防護範圍中包含單個節點，請清除“我的電腦”核取方塊，然後執行以下步驟：
 - 如果要將某一類型的所有磁碟機均包含在防護範圍內，請核取所需磁碟類型名稱旁的方塊(例如，若要新增電腦上的所有卸除式硬碟，則啟用“卸除式磁碟機”核取方塊)。
 - 如果要將特定類型的單個磁碟包含在防護範圍內，請展開包含此類型磁碟清單的節點，並核取所需磁碟名稱旁的方塊。例如，若要選擇卸除式磁碟機 F:，則展開“卸除式磁碟機”節點，並核取磁碟機 F: 對應的方塊。
 - 如果您想要僅包含磁碟機上的單個資料夾或檔案，請選中該資料夾或檔案名稱旁邊的核取方塊。
4. 點擊“儲存”按鈕。

“防護範圍設定”視窗將關閉。已儲存新配置的設定。

► 要使用網路檔案資源清單建立防護範圍：

1. 開啟“設定防護範圍”視窗（請參見第 323 頁上的“開啟‘即時檔案防護’範圍設定”部分）。
2. 要從防護範圍中包含單個節點，請清除“我的電腦”核取方塊，然後執行以下步驟：
 - a. 右鍵點擊防護範圍開啟其內容功能表。
 - b. 在按鈕的內容功能表中，選擇“新增防護範圍”。
 - c. 在“新增防護範圍”視窗中，選擇一個物件類型以將其新增到防護範圍中：
 - 預設的範圍，以便將一個預設範圍包含在電腦的防護範圍中。然後在下拉清單中，選擇必需的防護範圍。
 - 磁碟、資料夾或網路資料夾，以便在防護範圍中包括單個磁碟機、資料夾或網路物件。然後透過點擊“瀏覽”按鈕選擇所需的範圍。
 - 檔案，以便在防護範圍中包括單個檔案。然後透過點擊“瀏覽”按鈕選擇所需的範圍。

如果某個物件已經作為防護範圍的排除新增，則不能再將其新增到防護範圍中。

3. 要從防護範圍中排除單個節點，請清除這些節點名稱旁邊的核取方塊，或者執行以下步驟：
 - a. 右鍵點擊防護範圍開啟其內容功能表。
 - b. 在內容功能表中，選擇“新增排除項目”選項。
 - c. 在“新增排除項目”視窗中，選擇要作為防護範圍的排除項新增的物件類型，並遵循將物件新增到防護範圍中的過程的邏輯。
4. 要修改新增的防護範圍或排除，請選擇所需防護範圍內容功能表中的“編輯範圍”選項。
5. 若要在網路檔案資源清單中隱藏之前新增的防護範圍或排除，請在所需範圍的內容功能表中選擇“從清單刪除”選項。

該防護範圍將從網路檔案資源清單中刪除，同時從“即時檔案防護”工作範圍中排除。

6. 點擊“儲存”按鈕。

“防護範圍設定”視窗將關閉。已儲存新配置的設定。

僅在至少有一個電腦檔案資源節點包含在防護範圍內時，才可啟動“即時檔案防護”工作。

若指定了複雜防護範圍，例如，為電腦檔案資源樹狀目錄中的多個節點指定了不同的安全性設定值，則將可能導致掃描遭存取物件的速度緩慢。

建立虛擬防護範圍

僅當防護/掃描範圍以檔案資源樹狀目錄的形式顯示時，您才可透過新增單個虛擬磁碟機、資料夾或檔案來延伸防護/掃描範圍（請參見第 540 頁上的“配置網路檔案資源的視圖模式”部分）。

► 要新增虛擬磁碟機至防護範圍：

1. 開啟“設定防護範圍”視窗（請參見第 323 頁上的“開啟‘即時檔案防護’範圍設定”部分）。
2. 開啟視窗左上角的下拉清單部分，然後選擇**樹狀檢視**。
3. 開啟**虛擬磁碟機**的內容功能表。
4. 選擇“**新增虛擬磁碟機**”選項。
5. 在可用名稱清單中，為所建立的虛擬磁碟機選擇名稱。
6. 啟用所新增的磁碟機旁的核取方塊以將磁碟機包含在防護範圍內。
7. 在“設定防護範圍”視窗中，點擊“儲存”按鈕。

已儲存新配置的設定。

► *要新增虛擬資料夾或虛擬檔案至防護範圍：*

1. 開啟“**設定防護範圍**”視窗（請參見第 [323](#) 頁上的“開啟‘即時檔案防護’範圍設定”部分）。
2. 開啟視窗左上角的下拉清單部分，然後選擇**樹狀檢視**。
3. 開啟要新增資料夾或檔案的虛擬磁碟機的內容功能表，然後選擇以下選項之一：
 - **新增虛擬資料夾**，如果您想要向防護範圍中新增虛擬資料夾。
 - **新增虛擬檔案**，如果您想要向防護範圍中新增虛擬檔案。
4. 在輸入欄位中指定資料夾或檔案的名稱。
5. 在已建立資料夾或已建立檔案的名稱列中，選擇核取方塊，以將此資料夾檔案包含在防護範圍內。
6. 在“**設定防護範圍**”視窗中，點擊“**儲存**”按鈕。

將儲存修改的工作設定。

手動配置安全性設定

預設情況下，即時電腦防護工作對整個防護範圍使用通用安全設定。這些設定對應于“**建議**”預設安全等級（請參見第 [296](#) 頁上的“預設安全等級”部分）。

若要修改安全性設定的預設值，可透過將它們配置為用於整個防護範圍的一般設定，或為電腦檔案資源清單中的不同項目或樹狀目錄中的節點配置不同設定。

在使用伺服器檔案資源樹狀目錄時，為所選父節點配置的安全性設定將自動套用於所有子節點。父節點的安全設定不會套用到單獨配置的子節點。

► *要手動配置安全設定：*

1. 開啟“**設定防護範圍**”視窗（請參見第 [323](#) 頁上的“開啟‘即時檔案防護’範圍設定”部分）。
2. 在左側視窗部分中，選擇用於配置安全設定的節點。

可以為防護範圍內的選定節點或項目套用包含安全設定的預設範本（請參見第 197 頁上的“關於安全設定範本”部分）。

3. 根據需求配置選定節點或項目的所需安全設定：
 - 一般（請參見第 334 頁上“配置一般工作設定”部分）
 - 操作（請參見第 338 頁上的“設定操作”部分）
 - 效能（請參見第 341 頁上的“設定效能”部分）
4. 在“設定防護範圍”視窗中，點擊“儲存”按鈕。

將儲存新的防護範圍設定。

本章節說明項目

配置一般工作設定	334
配置操作	338
配置效能	341

配置一般工作設定

► 要配置“即時檔案防護”工作的一般安全設定：

1. 開啟“設定防護範圍”視窗（請參見第 323 頁上的“開啟‘即時檔案防護’範圍設定”部分）。
2. 選擇“一般”標籤。
3. 在“物件防護”部分中，指定要包含在防護範圍內的物件：
 - 所有物件

Kaspersky Embedded Systems Security 掃描所有物件。
 - 按格式掃描物件

Kaspersky Embedded Systems Security 僅根據檔案格式掃描感染物件。

Kaspersky Lab 編制了該格式清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。

- **按病毒資料庫中指定的副檔名清單掃描物件**

Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。

Kaspersky Lab 編制了該副檔名清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。

- **按指定的副檔名清單掃描物件**

Kaspersky Embedded Systems Security 根據檔案副檔名掃描檔案。可在“**副檔名清單**”視窗（透過點擊“**編輯**”按鈕開啟）中手動自訂檔案副檔名清單。

- **掃描開機磁區和 MBR**

啟用對開機磁區和主引導記錄的防護。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描電腦的硬碟磁碟機和卸除式磁碟機上的開機磁區和主引導記錄。

預設將會選定該核取方塊。

- **掃描 NTFS 交換資料串流**

掃描 NTFS 檔案系統磁碟機上的替代檔案和資料夾執行緒。

如果選中該核取方塊，應用程式將掃描疑似感染物件以及與該物件關聯的所有 NTFS 執行緒。

如果清除該核取方塊，應用程式將只掃描偵測到並被視為疑似感染的物件。

預設將會選定該核取方塊。

4. 在“效能”部分中，選中或清除“**僅防護新增與變更過的檔案**”核取方塊。

使用此核取方塊可啟用/停用對自上次掃描以來 Kaspersky Embedded Systems Security 識別為新檔案或已修改的檔案的掃描和防護。

如果選中該核取方塊，Kaspersky Embedded Systems Security 僅掃描和防護自上次掃描以來被識別為新檔案或已修改的檔案。

如果清除該核取方塊，您可以選擇希望僅掃描和防護新檔案，還是掃描和防護所有檔案而略過檔案的修改狀態。

對於“最佳效能”安全等級，預設選定該核取方塊。如果設定“最佳防護”或“建議”安全等級，則取消選中該核取方塊。

如果清除該核取方塊，要在可用選項之間轉換，請點擊每個複合物件類型對應的“全部/僅新建”連結。

5. 在“複合物件防護”部分中，指定要包含在防護範圍內的複合物件：

- **全部/僅新的壓縮檔案**

掃描 ZIP、CAB、RAR、ARJ 壓縮檔案及其他壓縮檔案格式。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描壓縮檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過壓縮檔案。

預設值取決於所選的防護等級。

- **全部/僅新的 SFX 壓縮檔案**

掃描自解壓壓縮檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描 SFX 壓縮檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過 SFX 壓縮檔案。

預設值取決於所選的防護等級。

如果取消選中“壓縮檔案”核取方塊，則該選項處於活動狀態。

- **全部/僅新的電子郵件資料庫**

掃描 Microsoft Outlook 和 Microsoft Outlook Express 郵件資料庫檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描郵件資料庫檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過郵件資料庫檔案。

預設值取決於所選的安全等級。

- **全部/僅新的封裝的物件**

掃描由二進位代碼封裝程式 (例如 UPX 或 ASPack) 封裝的可執行檔。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描由封裝程式封裝的可執行檔。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過由封裝程式封裝的可執行檔。

預設值取決於所選的防護等級。

- **全部/僅新的純文字電子郵件**

掃描郵件格式檔案，例如 Microsoft Office Outlook 和 Microsoft Outlook Express 郵件。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描郵件格式檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過郵件格式檔案。

預設值取決於所選的安全等級。

- **全部/僅新嵌入的 OLE 物件**

掃描嵌入到檔案中的物件 (如 Microsoft Word 巨集或電子郵件附件) 。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描嵌入到檔案中的物件。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過嵌入到檔案中的物件。

預設值取決於所選的防護等級。

6. 點擊“儲存”。

將儲存新的工作配置。

配置操作

► 要為“即時檔案防護”工作配置對受感染的物件和其他偵測到的物件的操作：

1. 開啟“設定防護範圍”視窗（請參見第 [323](#) 頁上的“開啟‘即時檔案防護’範圍設定”部分）。
2. 選擇“操作”標籤。
3. 選擇要對受感染的物件和其他偵測到的物件執行的操作：

- **僅通知。**

選擇此模式時，Kaspersky Embedded Systems Security 不封鎖存取受感染的物件和其他偵測到的物件，也不對它們執行任何操作。以下事件在工作記錄中註冊：*物件未解毒。原因：由於使用者定義的設定，未執行任何操作使偵測到的物件無效。*該事件指定有關偵測到的物件的所有可用資訊。

應該為每個防護或掃描區域單獨配置“僅通知”模式。預設情況下，任何安全等級都不使用此模式。如果選擇此模式，Kaspersky Embedded Systems Security 會自動將安全等級變更為“自訂”。

- **封鎖存取。**

選擇此選項時，Kaspersky Embedded Systems Security 會封鎖對偵測到或疑似感染的物件的存取。您可以在下拉清單中選擇對已封鎖物件的其他操作。

- **執行附加操作。**

從下拉清單中選擇操作：

- **解毒。**

- 解毒，無法解毒時刪除。
- 刪除。
- 建議。

4. 選擇要對可疑的物件執行的操作：

- 僅通知。

選擇此模式時，Kaspersky Embedded Systems Security 不封鎖存取受感染的物件和其他偵測到的物件，也不對它們執行任何操作。以下事件在工作記錄中註冊：*物件未解毒。原因：由於使用者定義的設定，未執行任何操作使偵測到的物件無效。*該事件指定有關偵測到的物件的所有可用資訊。

應該為每個防護或掃描區域單獨配置“僅通知”模式。預設情況下，任何安全等級都不使用此模式。如果選擇此模式，Kaspersky Embedded Systems Security 會自動將安全等級變更為“自訂”。

- 封鎖存取。

選擇此選項時，Kaspersky Embedded Systems Security 會封鎖對偵測到或疑似感染的物件的存取。您可以在下拉清單中選擇對已封鎖物件的其他操作。

- 執行附加操作。

從下拉清單中選擇操作：

- 隔離。
- 刪除。
- 建議。

5. 選擇依威脅類型對物件執行的操作：

- a. 清除或選中“根據偵測到的物件的類型執行操作”核取方塊。

如果選中該核取方塊，可以透過點擊該核取方塊旁邊的“設定”按鈕來獨立設定針對每種偵測到的物件類型的主要和次要操作。此時，Kaspersky Embedded Systems Security 將不允許開啟或執行受感染的物件，無論您的選擇如何。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將對指定的物件類型分別執行在“對受感染物件和其他物件執行的操作”和“對可疑物件執行的操作”部分中選擇的操作。

預設取消選定該核取方塊。

- b. 點擊“設定”按鈕。
 - c. 在開啟的視窗中，選擇針對每種偵測到的物件類型的主要和次要操作（如果主要操作失敗）。
 - d. 點擊“確定”。
6. 選擇要對不可修改的複合物件執行的操作：選擇或清除“在偵測到嵌入物件時完全刪除應用程式無法修改的複合檔案”核取方塊。

此核取方塊用於啟用或停用當偵測到惡意、疑似感染或其他偵測到的子內嵌物件時強制刪除父複合檔案。

如果選中該核取方塊並且工作設定為刪除受感染和疑似感染的物件，Kaspersky Embedded Systems Security 會在偵測到惡意或其他內嵌物件時強制刪除整個父複合物件。如果應用程式無法只刪除偵測到的子物件（例如，如果父物件不可修改），將強制刪除父物件及其所有內容。

如果清除該核取方塊並且工作設定為刪除受感染和疑似感染的物件，當父物件不可修改時，Kaspersky Embedded Systems Security 不會執行所選操作。

7. 點擊“儲存”。

將儲存新的工作配置。

配置效能

► 要配置“即時檔案防護”工作的效能：

1. 開啟“設定防護範圍”視窗（請參見第 [323](#) 頁上的“開啟‘即時檔案防護’範圍設定”部分）。
2. 選擇“效能”標籤。
3. 在“排除”部分中：

- 清除或選中“排除檔案”核取方塊。

按檔案名或檔案名遮罩從掃描中排除檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過指定的物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將掃描所有物件。

預設取消選定該核取方塊。

- 清除或選中“不偵測”核取方塊。

按可偵測物件的名稱或名稱遮罩從掃描中排除物件。病毒百科全書

<https://encyclopedia.kaspersky.com/knowledge/classification/> 網站上提供了可偵測物件的名稱清單。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過指定的可偵測物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 預設將偵測程式中指定的所有物件。

預設取消選定該核取方塊。

- 針對每個設定點擊“編輯”按鈕以新增排除項目。

4. 在“進階設定”部分中：

- 超過以下時間則停止掃描(秒)

限制物件掃描的持續時間。預設值為 60 秒。

如果選中該核取方塊，則掃描持續時間將限制為指定的值。

如果取消選中該核取方塊，則對掃描持續時間沒有限制。

對於“最佳效能”安全等級，預設選定該核取方塊。

- **不掃描超過此值複合檔案(MB)**

將超過指定大小的物件排除在掃描之外。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在病毒掃描期間略過大小超過指定限制值的複合物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將掃描任意大小的複合物件。

對於“最佳效能”安全等級，預設選定該核取方塊。

- **使用 iSwift 技術**

iSwift 將資料庫中儲存的檔案 NTFS 識別碼與目前識別碼進行比較。只對識別碼發生變化的檔案（新檔案和自上次掃描 NTFS 系統物件以來修改過的檔案）執行掃描。

如果選中該核取方塊，Kaspersky Embedded Systems Security 僅掃描自上次掃描 NTFS 系統物件以來新建或修改的檔案。

如果清除該核取方塊，Kaspersky Embedded Systems Security 在掃描 NTFS 系統檔案時將不考慮檔案建立或修改的日期（網路資料夾中的檔案除外）。

預設將會選定該核取方塊。

- **使用 iChecker 技術**

iChecker 會計算並記住掃描的檔案的核對總和。如果物件被修改，核對總和會發生變化。應用程式在掃描工作中比較所有核對總和，並且僅掃描新檔案和自上次掃描檔案以來修改過的檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 僅掃描新檔案和修改的檔案。

如果清除該核取方塊，Kaspersky Embedded Systems Security 在掃描檔案時將不考慮檔案建立或修改的日期。

預設將會選定該核取方塊。

即時檔案防護工作統計

執行即時檔案防護工作時，您可以檢視有關 Kaspersky Embedded Systems Security 自工作啟動以來已處理的物件數量的詳細即時資訊。

► 若要檢視“即時檔案防護”工作統計資料，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中展開“即時電腦防護”節點。
2. 選擇“即時檔案防護”子節點。

工作統計顯示在選定節點的詳細資訊視窗的“統計”部分中。

您可以檢視 Kaspersky Embedded Systems Security 自啟動以來已處理的物件的資訊（請參見下表）：

表 43. 即時檔案防護工作統計

欄位	敘述
偵測到	Kaspersky Embedded Systems Security 偵測到的物件數量。例如，如果 Kaspersky Embedded Systems Security 在五個檔案中偵測到一個惡意軟體，該欄位中的值將增加 1。
偵測到受感染物件和其他物件	Kaspersky Embedded Systems Security 發現並歸類為“已感染”的物件數量，或者發現的可被入侵者用來破壞電腦或個人資料的合法軟體檔案數量。
偵測到可能存在的威脅	Kaspersky Embedded Systems Security 發現的疑似被感染的物件數。

欄位	敘述
物件未解毒	Kaspersky Embedded Systems Security 因以下原因未解毒的物件數： <ul style="list-style-type: none"> • 無法對偵測到的物件類型進行解毒。 • 解毒時發生錯誤。
物件未移至隔離區	Kaspersky Embedded Systems Security 本應隔離但因磁碟空間不足等錯誤，而無法隔離的物件數目。
物件未刪除	Kaspersky Embedded Systems Security 嘗試刪除但因某些原因（例如，另一程式封鎖存取物件）而無法刪除的物件數目。
物件未掃描	Kaspersky Embedded Systems Security 因某些原因（例如，另一程式封鎖存取物件）而未能掃描的防護範圍內物件數目。
物件未備份	Kaspersky Embedded Systems Security 嘗試將其副本儲存至備份但因出錯而無法執行此操作的物件數目。
處理錯誤	處理中導致錯誤的物件數目。
物件已解毒	Kaspersky Embedded Systems Security 已解毒的物件的數量。
已移至隔離區	Kaspersky Embedded Systems Security 已隔離的物件的數量。
已移至備份區	Kaspersky Embedded Systems Security 儲存至備份的檔案數目。
物件已刪除	Kaspersky Embedded Systems Security 已刪除的物件的數量。
受密碼防護的物件	由於受密碼防護而導致 Kaspersky Embedded Systems Security 錯過的物件（如壓縮檔案）數目。
已損壞的物件	由於格式遭損壞而導致 Kaspersky Embedded Systems Security 錯過的物件數目。
物件已處理	Kaspersky Embedded Systems Security 已刪除的物件的總數。

透過點擊詳細資訊窗格中“管理”部分的“開啟工作記錄”，可以在工作記錄中檢視即時檔案防護工作統計。

如果“即時防護工作記錄”視窗中的“總計事件:”欄位的值大於 0，則建議手動處理“事件”標籤的工作記錄中出現的事件。

KSN 使用

本節包含有關“KSN 使用”工作以及如何設定的資訊。

本章內容

關於“KSN 使用”工作.....	346
“KSN 使用”工作預設設定.....	348
透過管理外掛程式管理“KSN 使用”.....	349
透過應用程式主控台管理“KSN 使用”.....	354
設定其他資料傳輸.....	358
“KSN 使用”工作統計.....	360

關於“KSN 使用”工作

卡巴斯基安全網路(也稱為“KSN”)是一個線上服務的基礎架構，提供存取 Kaspersky Lab 有效的知識庫。該知識庫中包含了檔案信譽、網頁資源和程式的相關資訊。卡巴斯基安全網路允許 Kaspersky Embedded Systems Security 十分迅速地對新威脅作出反應，提高許多防護元件的效能，以降低誤報可能性。

要啟動“KSN 使用”工作，您必須接受卡巴斯基安全網路聲明。

Kaspersky Embedded Systems Security 從卡巴斯基安全網路接收的資訊僅與程式的信譽有關。

加入 KSN 使 Kaspersky Lab 能夠接收有關新威脅類型和來源的資訊，研發出使其失效的方法，並減少應用程式元件中的誤報數量。

有關傳輸、處理、儲存和銷毀有關應用程式使用情況的更多詳細資訊在“KSN 使用”工作的“資料處理”視窗中和 Kaspersky Lab 網站上的隱私政策中提供。

加入卡巴斯基安全網路完全出於自願。在安裝 Kaspersky Embedded Systems Security 後，做出關參加卡巴斯基安全網路的決定。您可以隨時變更有關參加卡巴斯基安全網路的決定。

可在以下 Kaspersky Embedded Systems Security 工作中使用卡巴斯基安全網路：

- 即時檔案防護。
- 自訂掃描。
- 應用程式啟動控制。

卡巴斯基專屬安全網路

有關如何配置卡巴斯基專屬安全網路（以下稱“私有 KSN”）的詳細資訊，請參見《卡巴斯基安全管理中心說明》。

如果在受防護電腦上使用專屬 KSN，則在“KSN 使用”工作的“資料處理”視窗（參見第 352 頁的“透過管理外掛程式配置資料處理”部分）中，可以透過選擇“我接受卡巴斯基私有安全網路聲明”核取方塊來閱讀 KSN 聲明和啟用該工作。接受該條款，即表示您同意將 KSN 聲明中提到的各類資料（安全請求、統計資料）傳送到 KSN 服務。

接受私有 KSN 條款後，用於調整全球 KSN 使用的核取方塊將不可用。

如果在“KSN 使用”工作執行時停用私有 KSN，則將出現 *產品授權衝突* 錯誤且工作將停止。要繼續防護電腦，您需要接受“資料處理”視窗中的 KSN 聲明並重新啟動該工作。

撤銷接受 KSN 聲明

您可以隨時撤銷接受聲明並停止與卡巴斯基安全網路的任何資料交換。以下操作被視為完全或部分撤銷 KSN 聲明：

- 清除“傳送關於已掃描檔案的資料”核取方塊：應用程式停止將掃描的檔案的核對總和傳送到 KSN 服務進行分析。
- 清除“傳送卡巴斯基安全網路統計資訊”核取方塊：應用程式停止處理附加 KSN 統計的資料。
- 清除“我接受卡巴斯基安全網路聲明的條款”核取方塊：應用程式停止所有與 KSN 相關的資料處理，“KSN 使用”工作停止。
- 移除“KSN 使用”元件：所有與 KSN 相關的資料處理都將停止。
- 移除 Kaspersky Embedded Systems Security：所有與 KSN 相關的資料處理都將停止。

“KSN 使用”工作預設設定

您可以變更“KSN 使用”工作的預設設定（請參見下表）。

表 44. “KSN 使用”工作預設設定

設定	預設值	敘述
對 KSN 不信任的物件執行的操作	刪除	您可以指定 Kaspersky Embedded Systems Security 對 KSN 標識為不受信任的物件執行的操作。
資料傳輸	為大小不超過 2 MB 的檔案計算檔案核對總和（MD5 雜湊）。	您可以指定要使用 MD5 演算法為其計算核對總和以提交給 KSN 的檔案的最大大小。如果清除該核取方塊，Kaspersky Embedded Systems Security 將為任意大小的檔案計算 MD5 雜湊。
工作啟動排程	不設定工作的初次啟動排程。	您可以手動啟動該工作或設定排程啟動。

設定	預設值	敘述
使用卡巴斯基安全管理中心作為 KSN 代理	選中	預設情況下，資料透過卡巴斯基安全管理中心傳送到 KSN。 您只能透過管理外掛程式變更此設定。
我接受卡巴斯基安全網路聲明的條款	已解毒	如果選中，即接受安裝後加入 KSN。您可以隨時變更決定。
傳送卡巴斯基安全網路統計資訊	選中（僅當接受 KSN 聲明時應用）	如果接受 KSN 聲明，將自動傳送 KSN 統計，除非清除相應核取方塊。
傳送關於已掃描檔案的資料	選中（僅當接受 KSN 聲明時應用）	如果接受 KSN 聲明，將傳送自工作啟動以來掃描和分析的檔案的資料。您可以隨時清除該核取方塊。
傳送關於掃描的 URL 的資料	選中（僅當接受 KSN 聲明時應用）	如果接受 KSN 聲明，應用程式會將有關存取的 URL 的資訊傳送到 Kaspersky Lab。
接受 Kaspersky Managed Protection 聲明的條款	已解毒	您可以啟用或停用 KMP 服務。僅當在應用程式購買過程中簽訂了附加協議時，該服務才可用。

透過管理外掛程式管理“KSN 使用”

在本節中，學習如何透過管理外掛程式配置“KSN 使用”工作和資料處理。

本章節說明項目

透過管理外掛程式配置“KSN 使用”工作	350
透過管理外掛程式配置資料處理	352

透過管理外掛程式配置“KSN 使用”工作

► 要設定“KSN 使用”工作，請執行以下步驟：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“政策”標籤，然後開啟“內容：<政策名稱>”視窗（請參見第 144 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“裝置”標籤，然後開啟“應用程式設定”視窗（請參見第 150 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“應用程式設定”視窗中編輯這些設定。

4. 在“即時電腦防護”部分中，點擊“KSN 使用”設定塊中的“設定”按鈕。
將開啟“KSN 使用”視窗。
5. 在“一般”標籤上，配置以下工作設定：
 - 在“對 KSN 不信任的物件執行的操作”部分中，指定 Kaspersky Embedded Systems Security 在偵測到 KSN 確定為不受信任的物件時將執行的操作：

- **刪除**

Kaspersky Embedded Systems Security 將刪除具有 KSN 不信任狀態的物件，並在備份中放置副本。

預設選中該選項。

- **記錄資訊**

Kaspersky Embedded Systems Security 將在工作記錄中記錄有關具有 KSN 不信任狀態的物件的資訊。Kaspersky Embedded Systems Security 不會刪除不受信任的物件。

- 在“**資料傳輸**”部分中，限制要為其計算核對總和的檔案的大小：
- 清除或選中“**如果檔案大小超過以下大小，則在傳送到 KSN 之前不計算核對總和 (MB)**”核取方塊。

此核取方塊可啟用或停用為指定大小的檔案計算核對總和，以將此資訊提交至 KSN 服務。

核對總和計算的持續時間取決於檔案大小。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 不會為超過指定大小（以 MB 為單位）的檔案計算核對總和。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將為任意大小的檔案計算核對總和。

預設將會選定該核取方塊。

- 如果需要，在右側欄位中指定 Kaspersky Embedded Systems Security 要為其計算核對總和的最大檔案大小。
- 在“**KSN 代理**”部分中，清除或選中“**使用卡巴斯基安全管理中心作為 KSN 代理**”核取方塊。

該核取方塊允許管理受防護電腦與 KSN 之間的資料傳輸。

如果清除該核取方塊，管理電腦和受防護電腦的資料將直接傳送到 KSN（不透過卡巴斯基安全管理中心）。活動政策定義了哪種類型的資料可以直接傳送到 KSN。

如果選中該核取方塊，所有資料都透過卡巴斯基安全管理中心傳送到 KSN。

預設將會選定該核取方塊。

要啟用 KSN 代理，必須接受 KSN 聲明並正確配置卡巴斯基安全管理中心。有關詳細資訊，請參閱 [卡巴斯基安全管理中心說明](#)。

6. 如果需要，在“**工作管理**”標籤上配置工作啟動排程。例如，如果您希望在重新啟動伺服器時自動執行該工作，可以按排程啟動工作並指定“**在應用程式啟動時**”頻率。

應用程式將按排程自動啟動“KSN 使用”工作。

7. 在啟動工作前配置資料處理（請參見第 [352](#) 頁上的“透過管理外掛程式配置資料處理”部分）。
8. 點擊“確定”。

將套用修改的設定。修改設定的日期和時間以及有關修改前後的工作設定的資訊均儲存在系統稽核記錄中。

透過管理外掛程式配置資料處理

► 要設定哪些資料將被 KSN 服務處理並接受 KSN 聲明：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 [144](#) 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 [150](#) 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**即時電腦防護**”部分中，點擊“**KSN 使用**”設定塊中的“**資料處理**”按鈕。
將開啟“**資料處理**”視窗。
5. 在“**統計和服務**”標籤上，閱讀聲明並選中“**我接受卡巴斯基安全網路聲明的條款**”核取方塊。

6. 為提高防護等級，以下核取方塊會自動選中：

- **傳送關於已掃描檔案的資料。**

如果選中該核取方塊，Kaspersky Embedded Systems Security 會將掃描的檔案的核對總和傳送到 Kaspersky Lab。關於每個檔案的安全性的結論基於從 KSN 收到的信譽。

如果清除該核取方塊，Kaspersky Embedded Systems Security 不會將檔案的核對總和傳送到 KSN。

請注意，檔案信譽請求可能在受限制模式下傳送。限制用於防護 Kaspersky Lab 信譽伺服器免受 DDoS 攻擊。在這種情況下，所傳送的檔案信譽請求的參數由 Kaspersky Lab 專家建立的規則和方法定義，使用者無法在受防護電腦上進行設定。這些規則和方法的更新與應用程式資料庫更新一起接收。如果應用限制，“KSN 使用”工作統計中將顯示“由 Kaspersky Lab 啟用以防護 KSN 伺服器免受 DDoS 攻擊”狀態。

預設將會選定該核取方塊。

- **傳送卡巴斯基安全網路統計資訊。**

如果選中該核取方塊，Kaspersky Embedded Systems Security 會傳送附加統計，其中可能包括個人資料。作為 KSN 統計傳送的所有資料的清單在 KSN 聲明中有所說明。Kaspersky Lab 收到的資料用於改善應用程式質量和提高威脅偵測速率等級。

如果清除該核取方塊，Kaspersky Embedded Systems Security 不會傳送其他統計。

預設將會選定該核取方塊。

您可以隨時清除這些核取方塊並停止傳送附加資料。

7. 在“Kaspersky Managed Protection”標籤上，閱讀聲明並選中“我接受 Kaspersky Managed Protection 聲明的條款”核取方塊。

如果選中該核取方塊，表示您同意將有關受防護電腦活動的統計傳送給 Kaspersky Lab 專家。接收的資料用於持續不停的分析和報告，是防止安全弱點事件所必需的。

預設取消選定該核取方塊。

變更“我接受 Kaspersky Managed Protection 聲明的條款”核取方塊狀態不會立即啟動或停止資料處理。要套用變更，必須重新啟動 Kaspersky Embedded Systems Security。

要使用 KMP 服務，您需要簽訂服務協議並在受防護電腦上執行設定檔。

要使用 KMP 服務，必須接受“統計和服務”標籤上的 KSN 聲明的資料處理條款。

8. 點擊“確定”。

將儲存資料處理配置。

透過應用程式主控台管理“KSN 使用”

在本節中，學習如何透過應用程式主控台配置“KSN 使用”工作和資料處理。

本章節說明項目

透過應用程式主控台配置“KSN 使用”工作	354
透過應用程式主控台配置資料處理	356

透過應用程式主控台配置“KSN 使用”工作

► 要設定“KSN 使用”工作，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中展開“即時電腦防護”節點。
2. 選擇“KSN 使用”子節點。
3. 在詳細資訊視窗中點擊“內容”連結。

將開啟“工作設定”視窗的“一般”標籤。

4. 設定工作：

- 在“對 KSN 不信任的物件執行的操作”部分中，指定 Kaspersky Embedded Systems Security 在偵測到 KSN 確定為不受信任的物件時將執行的操作：

- **刪除**

Kaspersky Embedded Systems Security 將刪除具有 KSN 不信任狀態的物件，並在備份中放置副本。

預設選中該選項。

- **記錄資訊**

Kaspersky Embedded Systems Security 將在工作記錄中記錄有關具有 KSN 不信任狀態的物件的資訊。Kaspersky Embedded Systems Security 不會刪除不受信任的物件。

- 在“資料傳輸”部分中，限制要為其計算核對總和的檔案的大小：

- 清除或選中“如果檔案大小超過以下大小，則在傳送到 KSN 之前不計算核對總和 (MB)”核取方塊。

此核取方塊可啟用或停用為指定大小的檔案計算核對總和，以將此資訊提交至 KSN 服務。

核對總和計算的持續時間取決於檔案大小。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 不會為超過指定大小（以 MB 為單位）的檔案計算核對總和。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將為任意大小的檔案計算核對總和。

預設將會選定該核取方塊。

- 如果需要，在右側欄位中指定 Kaspersky Embedded Systems Security 要為其計算核對總和的最大檔案大小。

5. 如果需要，在“**排程**”和“**進階**”標籤上設定工作啟動排程。例如，如果您希望在重新啟動電腦時自動執行該工作，可以啟用按排程啟動工作並指定“**在應用程式啟動時**”的啟動頻率。

應用程式將按排程自動啟動“KSN 使用”工作。

6. 在啟動工作前配置資料處理（請參見第 [356](#) 頁上的“透過應用程式主控台配置資料處理”部分）。
7. 點擊“**確定**”。

將套用修改的設定。修改設定的日期和時間以及有關修改前後的工作設定的資訊均儲存在系統稽核記錄中。

透過應用程式主控台配置資料處理

► 要設定哪些資料將被 KSN 服務處理並接受 KSN 聲明：

1. 在應用程式主控台樹狀目錄中展開“**即時電腦防護**”節點。
2. 選擇“**KSN 使用**”子節點。
3. 在詳細資訊視窗中點擊“**資料處理**”連結。
將開啟“**資料處理**”視窗。
4. 在“**統計和服務**”標籤上，閱讀聲明並選中“**我接受卡斯基安全網路聲明的條款**”核取方塊。
5. 為提高防護等級，以下核取方塊會自動選中：

- **傳送關於已掃描檔案的資料。**

如果選中該核取方塊，Kaspersky Embedded Systems Security 會將掃描的檔案的核對總和傳送到 Kaspersky Lab。關於每個檔案的安全性的結論基於從 KSN 收到的信譽。

如果清除該核取方塊，Kaspersky Embedded Systems Security 不會將檔案的核對總和傳送到 KSN。

請注意，檔案信譽請求可能在受限制模式下傳送。限制用於防護 Kaspersky Lab 信譽伺服器免受 DDoS 攻擊。在這種情況下，所傳送的檔案信譽請求的參數由 Kaspersky Lab 專家建立的規則和方法定義，使用者無法在受防護電腦上進行設定。這些規則和方法的更新與應用程式資料庫更新一起接收。如果應用限制，“KSN 使用”工作統計中將顯示“由 Kaspersky Lab 啟用以防護 KSN 伺服器免受 DDoS 攻擊”狀態。

預設將會選定該核取方塊。

- **傳送卡巴斯基安全網路統計資訊。**

如果選中該核取方塊，Kaspersky Embedded Systems Security 會傳送附加統計，其中可能包括個人資料。作為 KSN 統計傳送的所有資料的清單在 KSN 聲明中有所說明。Kaspersky Lab 收到的資料用於改善應用程式質量和提高威脅偵測速率等級。

如果清除該核取方塊，Kaspersky Embedded Systems Security 不會傳送其他統計。

預設將會選定該核取方塊。

您可以隨時清除這些核取方塊並停止傳送附加資料。

6. 在“Kaspersky Managed Protection”標籤上，閱讀聲明並選中“**我接受 Kaspersky Managed Protection 聲明的條款**”核取方塊。

如果選中該核取方塊，表示您同意將有關受防護電腦活動的統計傳送給 Kaspersky Lab 專家。接收的資料用於持續不停的分析和報告，是防止安全弱點事件所必需的。

預設取消選定該核取方塊。

變更“我接受 Kaspersky Managed Protection 聲明的條款”核取方塊狀態不會立即啟動或停止資料處理。要套用變更，必須重新啟動 Kaspersky Embedded Systems Security。

要使用 KMP 服務，您需要簽訂服務協議並在受防護電腦上執行設定檔。

要使用 KMP 服務，必須接受“統計和服務”標籤上的 KSN 聲明的資料處理條款。

7. 點擊“確定”。

將儲存資料處理配置。

設定其他資料傳輸

Kaspersky Embedded Systems Security 可以設定為將以下資料傳送到 Kaspersky Lab：

- 掃描的檔案的核對總和（“傳送關於已掃描檔案的資料”核取方塊）。
- 附加統計資訊，包括個人資料（“傳送卡巴斯基安全網路統計資訊”核取方塊）。

有關傳送到 Kaspersky Lab 的資料的詳細資訊，請參見本手冊的“本機資料處理”部分。

只有選中“我接受卡巴斯基安全網路聲明的條款”核取方塊，才能選中或清除相應的核取方塊（請參見第 [356](#) 頁上的“透過應用程式主控台配置資料處理”部分）。

預設情況下，當您接受 KSN 聲明後，Kaspersky Embedded Systems Security 將傳送檔案的核對總和和附加統計。

表 45. 可能的核取方塊狀態和相應條件

核取方塊狀態	“傳送關於已掃描檔案的資料”核取方塊狀態的條件	“傳送卡巴斯基安全網路統計資訊”核取方塊狀態的條件	“傳送關於掃描的 URL 的資料”核取方塊狀態的條件	“我接受 Kaspersky Managed Protection 聲明的條款”核取方塊狀態的條件	“我接受卡巴斯基安全網路聲明的條款”核取方塊狀態的條件

核取方塊狀態	“傳送關於已掃描檔案的資料”核取方塊狀態的條件	“傳送卡巴斯基安全網路統計資訊”核取方塊狀態的條件	“傳送關於掃描的 URL 的資料”核取方塊狀態的條件	“我接受 Kaspersky Managed Protection 聲明的條款”核取方塊狀態的條件	“我接受卡巴斯基安全網路聲明的條款”核取方塊狀態的條件
<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> 已傳送信譽請求 核取方塊可編輯 	<ul style="list-style-type: none"> 已傳送附加統計 核取方塊可編輯 	<ul style="list-style-type: none"> 已傳送關於掃描的 URL 的資料 核取方塊可編輯 	<ul style="list-style-type: none"> 已接受 Kaspersky Managed Protection 聲明的條款 核取方塊可編輯 	<ul style="list-style-type: none"> 已接受卡巴斯基安全網路聲明的條款 核取方塊可編輯
<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> 已傳送信譽請求 核取方塊不可編輯 	<ul style="list-style-type: none"> 已傳送附加統計 核取方塊不可編輯 	<ul style="list-style-type: none"> 已傳送關於掃描的 URL 的資料 核取方塊不可編輯 	<ul style="list-style-type: none"> 已接受 Kaspersky Managed Protection 聲明的條款 核取方塊不可編輯 	<ul style="list-style-type: none"> 已接受卡巴斯基安全網路聲明的條款 核取方塊不可編輯
<input type="checkbox"/>	<ul style="list-style-type: none"> 未傳送信譽請求 核取方塊可編輯 	<ul style="list-style-type: none"> 未傳送附加統計 核取方塊可編輯 	<ul style="list-style-type: none"> 未傳送關於掃描的 URL 的資料 核取方塊可編輯 	<ul style="list-style-type: none"> 未接受 Kaspersky Managed Protection 聲明的條款 核取方塊可編輯 	<ul style="list-style-type: none"> 未接受卡巴斯基安全網路聲明的條款 核取方塊可編輯

核取方塊狀態	“傳送關於已掃描檔案的資料”核取方塊狀態的條件	“傳送卡巴斯基安全網路統計資訊”核取方塊狀態的條件	“傳送關於掃描的 URL 的資料”核取方塊狀態的條件	“我接受 Kaspersky Managed Protection 聲明”核取方塊狀態的條件	“我接受卡巴斯基安全網路聲明的條款”核取方塊狀態的條件
<input type="checkbox"/>	<ul style="list-style-type: none"> 未傳送信譽請求 核取方塊不可編輯 	<ul style="list-style-type: none"> 未傳送附加統計 核取方塊不可編輯 	<ul style="list-style-type: none"> 未傳送關於掃描的 URL 的資料 核取方塊不可編輯 	<ul style="list-style-type: none"> 未接受 Kaspersky Managed Protection 聲明的條款 核取方塊不可編輯 	<ul style="list-style-type: none"> 未接受卡巴斯基安全網路聲明的條款 核取方塊不可編輯

“KSN 使用”工作統計

在執行“KSN 使用”工作期間，可以即時檢視 Kaspersky Embedded Systems Security 自啟動以來已處理的物件數量的相關詳細資訊。有關工作執行期間發生的所有事件的資訊記錄在工作記錄中（請參見第 [254](#) 頁上的“關於工作記錄”部分）。

► 若要檢視“KSN 使用”工作統計，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中展開“即時電腦防護”節點。
2. 選擇“KSN 使用”子節點。

工作統計顯示在選定節點的詳細資訊視窗的“統計”部分中。

您可以檢視自工作啟動以來 Kaspersky Embedded Systems Security 已處理物件的相關資訊（請參見下表）。

表 46. “KSN 使用”工作統計

欄位	敘述
----	----

欄位	敘述
請求傳送錯誤	對其處理產生工作錯誤的 KSN 請求數。
統計資訊已形成	傳送到 KSN 的產生的統計封包數量。
物件已刪除	Kaspersky Embedded Systems Security 在執行“KSN 使用”工作時刪除的物件數。
已移至備份區	Kaspersky Embedded Systems Security 儲存至備份的檔案數目。
物件未刪除	Kaspersky Embedded Systems Security 嘗試刪除但因某些原因 (例如 , 另一程式封鎖存取物件) 而無法刪除的物件數目。有關此類物件的資訊記錄在工作記錄中。
物件未備份	Kaspersky Embedded Systems Security 嘗試將其副本儲存至備份但因出錯而無法執行此操作的物件數目。程式不會解毒或刪除無法移動到備份中的檔案。有關此類物件的資訊記錄在工作記錄中。
受限制模式	該狀態表示應用程式是否在受限制模式下傳送檔案信譽請求。

應用程式啟動控制

本節包含有關“應用程式啟動控制”工作以及如何設定的資訊。

本章內容

關於“應用程式啟動控制”工作	362
關於應用程式啟動控制規則	364
關於軟體分發控制	366
關於“應用程式啟動控制”工作的 KSN 使用	369
產生應用程式啟動控制規則	370
“應用程式啟動控制”工作預設設定	372
透過管理外掛程式管理應用程式啟動控制	376
透過應用程式主控台管理應用程式啟動控制	405

關於“應用程式啟動控制”工作

在執行“應用程式啟動控制”工作時，Kaspersky Embedded Systems Security 會監控使用者啟動應用程式的嘗試，並允許或拒絕這些應用程式啟動。“應用程式啟動控制”工作依賴於“預設拒絕”原則，這意味著工作設定中不允許的任何應用程式都會被自動封鎖。

您可以使用以下方法之一允許應用程式啟動：

- 設定受信任的應用程式的允許規則。
- 啟動時在 KSN 中檢查受信任應用程式的聲譽。

該工作為拒絕應用程式啟動賦予最高優先順序。例如，如果某個應用程式被封鎖規則之一封鎖啟動，該應用程式將被拒絕啟動，不管 KSN 的信任結論如何。此時，如果應用程式不受 KSN 服務信任，但包括在允許規則範圍中，此應用程式會被拒絕啟動。

所有啟動應用程式的嘗試將記錄在工作記錄 (請參見第 [254](#) 頁上的“關於工作記錄”部分) 中。

“應用程式啟動控制”工作可以執行在以下兩種模式之一：

- **活動。** Kaspersky Embedded Systems Security 使用一組規則來控制處於應用程式啟動控制規則範圍內的應用程式的啟動。應用程式啟動控制規則的範圍在該工作的設定中指定。如果應用程式處於應用程式啟動控制規則範圍內，並且工作設定不滿足任何指定規則，此應用程式會被拒絕啟動。

不在“應用程式啟動控制”工作設定中指定的任何規則範圍內的應用程式會被允許啟動，不管“應用程式啟動控制”工作設定如何。

如果未建立任何規則或為一台電腦建了超過 65,535 條規則，則“應用程式啟動控制”工作無法在活動模式下啟動。

- **僅統計。** Kaspersky Embedded Systems Security 不使用應用程式啟動控制規則來允許或拒絕應用程式啟動。相反，它只記錄有關應用程式啟動、正在執行的應用程式所滿足的規則以及如果工作在“活動”模式下執行已執行的操作的資訊。所有應用程式均允許啟動。預設設定此模式。

您可以使用此模式基於工作記錄中記錄的資訊建立應用程式啟動控制規則 (請參見第 [420](#) 頁上的“根據“應用程式啟動控制”工作事件建立允許規則”部分) 。

您可根據以下方案之一配置“應用程式啟動控制”工作：

- 進階規則配置 (請參見第 [364](#) 頁上的“關於應用程式啟動控制規則”部分) 及其在應用程式啟動控制中的使用。
- 基本規則配置和應用程式啟動控制的 KSN 使用 (請參見第 [411](#) 頁上的“配置 KSN 使用”部分) 。

如果作業系統檔案在“應用程式啟動控制”工作的範圍內，建議在建立應用程式啟動控制規則時確保新建立的規則允許此類應用程式。否則，作業系統可能無法啟動。

Kaspersky Embedded Systems Security 還會攔截在 Linux 的 Windows 子系統下啟動的處理程序（從 UNIX™ shell 或命令列解釋器執行的指令碼除外）。對於此類別處理程序，“應用程式啟動控制”工作將套用目前配置定義的操作。“應用程式啟動控制規則產生器”工作會偵測應用程式啟動，並為在 Linux 的 Windows 子系統下執行的應用程式產生相應規則。

關於應用程式啟動控制規則

應用程式啟動控制規則的工作原理

應用程式啟動控制規則的操作基於以下元件：

- 規則類型。

應用程式啟動控制規則可以允許或拒絕應用程式啟動。相應地，它們被稱為 *允許* 或 *拒絕* 規則。要為“應用程式啟動控制”建立允許規則清單，可以使用規則產生器允許規則或在“**僅統計**”模式下使用“應用程式啟動控制”工作。您也可以手動新增允許規則。

- 使用者和/或使用者群組。

應用程式啟動控制規則可以按使用者或使用者群組控制指定應用程式的啟動。

- 規則使用範圍。

應用程式啟動控制規則可套用於 *可執行檔*、*指令碼* 和 *MSI 安裝套件*。

- 規則觸發條件。

應用程式啟動控制規則會控制滿足規則設定中指定的其中一個標準的檔案的啟動：由指定數位憑證簽章、比對指定 SHA256 雜湊或位於指定路徑。

如果將“數位憑證”設定為規則觸發條件，則建立的規則會控制作業系統中所有受信任應用程式的啟動。您可透過選中以下核取方塊為此條件設定更加嚴格的條件：

- **使用主旨**

該核取方塊可啟用或停用使用數位憑證的主旨作為規則觸發條件。

如果選中該核取方塊，則使用指定的數位憑證主旨作為規則觸發條件。建立的規則將僅控制主旨中指定的供應商的應用程式的啟動。

如果清除該核取方塊，應用程式將不會使用數位憑證的主旨作為規則觸發條件。如果選擇“數位憑證”條件，建立的規則將控制使用包含任何主旨的數位憑證簽章的應用程式的啟動。

只能使用位於“規則觸發條件”部分上方的“從檔案內容設定規則觸發條件”按鈕透過所選檔案的內容指定用於對檔案進行簽章的數位憑證的主旨。

預設取消選定該核取方塊。

- **使用指紋**

該核取方塊可啟用/停用使用數位憑證的指紋作為規則觸發條件。

如果選中該核取方塊，則使用指定的數位憑證指紋作為規則觸發條件。建立的規則將控制使用帶指定指紋的數位憑證簽章的應用程式的啟動。

如果清除該核取方塊，應用程式將不會使用數位憑證的指紋作為規則觸發條件。如果選擇“數位憑證”條件，應用程式將控制使用具有任何指紋的數位憑證簽章的應用程式的啟動。

只能使用位於“規則觸發條件”部分上方的“從檔案內容設定規則觸發條件”按鈕透過所選檔案的內容指定用於對檔案進行簽章的數位憑證的指紋。

預設取消選定該核取方塊。

指紋最嚴格地限制了基於數位憑證的應用程式啟動規則的觸發，因為指紋唯一標識了數位憑證且無法偽造，這一點與數位憑證的主題不同。

您可以指定應用程式啟動控制規則的排除。應用程式啟動控制規則的排除基於用於觸發規則的相同條件：數位憑證、SHA256 雜湊和檔案路徑。對於某些允許規則時，可能需要指定應用程式啟動控制規則的排除：例如，如果您希望允許使用者從 C:\Windows 路徑啟動應用程式，同時封鎖啟動檔案 Regedit.exe。

如果作業系統檔案在“應用程式啟動控制”工作的範圍內，建議在建立應用程式啟動控制規則時確保新建立的規則允許此類應用程式。否則，作業系統可能無法啟動。

管理應用程式啟動控制規則

您可以對應用程式啟動控制規則執行以下操作：

- 手動新增規則。
- 自動建立和新增規則。
- 刪除規則。
- 將規則匯出到檔案。
- 檢查所選檔案是否存在允許執行這些檔案的規則。
- 根據指定的條件篩選清單中的規則。

關於軟體分發控制

如果您還需要控制受防護電腦（例如，所安裝軟體會定期自動更新的電腦）上的軟體分發，則建立應用程式啟動控制規則可能很複雜。在這種情況下，必須在每次軟體更新後更新允許規則的清單，以便在“應用程式啟動控制”工作設定中考慮新建立的檔案。為了簡化軟體分發方案中的啟動控制，可以使用“軟體分發控制”子系統。

軟體分發套件 (下文稱為“軟體套件”) 表示要在電腦上安裝的軟體應用程式。每個軟體套件都包含至少一個應用程式，除了應用程式外，可能還包含單個檔案、更新，甚至單個指令，尤其是在您安裝軟體應用程式或更新時。

“軟體分發控制”子系統作為附加排除清單實施。將軟體分發套件新增到此清單時，應用程式允許解壓縮這些受信任套件，並允許受信任套件所安裝或修改的軟體自動啟動。提取的檔案可以繼承主分發套件的受信任內容。**主分發套件**是由使用者新增到軟體分發控制排除清單並成為受信任套件的軟體套件。

Kaspersky Embedded Systems Security 僅控制完整軟體分發週期。如果第一次啟動受信任套件時軟體分發控制關閉，或者“應用程式啟動控制”元件未安裝，應用程式將無法正確處理由受信任套件修改的檔案的啟動。

如果在“應用程式啟動控制”工作設定中清除“將規則套用於可執行檔”核取方塊，軟體分發控制將不可用。

軟體分發快取

Kaspersky Embedded Systems Security 使用動態建立的軟體分發快取 (“分發快取”) 在受信任套件與軟體分發期間建立的檔案之間建立關係。第一次啟動軟體套件時，Kaspersky Embedded Systems Security 將偵測該軟體套件在軟體分發過程中建立的所有檔案，並將檔案核對總和及路徑儲存在分發快取中。然後預設允許分發快取中的所有檔案啟動。

您不能透過使用者介面檢視、清除或手動修改分發快取。快取由 Kaspersky Embedded Systems Security 填充和控制。

您可以將分發快取匯出到設定檔 (XML 格式)，同時使用命令列選項清除快取。

► 要將分發快取匯出到設定檔，請執行以下指令：

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

► 要清除分發快取，請執行以下指令：

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security 每 24 小時更新一次分發快取。如果先前允許的檔案的核對總和發生變化，應用程式將從分發快取中刪除此檔案的記錄。如果“應用程式啟動控制”工作在活動模式下啟動，後續啟動該檔案的嘗試將被封鎖。如果先前允許的檔案的完整路徑發生變化，後續啟動該檔案的嘗試不會被封鎖，因為核對總和儲存在分發快取內。

處理提取檔案

第一次啟動軟體套件時，從受信任軟體套件提取的所有檔案都會繼承受信任的內容。如果在第一次啟動後清除該核取方塊，從軟體套件提取的所有檔案都將保留繼承的內容。要重設所有提取檔案中的繼承內容，您需要在再次啟動受信任分發套件之前清除分發快取並清除“允許從該分發套件提取鏈中啟動到所有檔案”核取方塊。

在第一次開啟排除清單中的軟體分發套件時，受信任的主分發套件所建立的提取檔案和套件會在它們的核對總和被新增到分發快取時繼承受信任內容。因此，分發套件本身和從該分發套件提取的所有檔案也將被信任。預設情況下，受信任內容的繼承等級數是無限的。

作業系統重新啟動後，所提取檔案將保留受信任內容。

檔案處理在軟體分發控制設定（請參見第 [383](#) 頁上的“設定軟體分發控制”部分）中透過選中或清除“允許從該分發套件提取鏈中啟動到所有檔案”核取方塊來進行配置。

例如，假設您將包含幾個其他套件和應用程式的 test.msi 套件新增到排除清單中並選中該核取方塊。在這種情況下，將允許執行或提取 test.msi 套件中包含的所有套件和應用程式（如果它們包含其他檔案）。此方案適用於所有嵌套等級上的提取檔案。

如果將 test.msi 套件新增到排除清單中並清除“允許從該分發套件提取鏈中啟動到所有檔案”核取方塊，應用程式只會將受信任內容分配到直接從主受信任套件提取的套件和可執行檔（在第一個嵌套等級上）。此類檔案的核對總和儲存在分發快取中。在第二個和更後面的嵌套等級上的所有檔案都將被“預設拒絕”原則封鎖。

使用應用程式啟動控制規則清單

軟體分發控制子系統的受信任套件清單是一個排除項目清單，該清單擴大了但未更換應用程式啟動控制規則清單。

拒絕應用程式啟動控制規則具有最高優先順序：受信任套件的解壓縮和新檔案或已修改檔案的啟動將被封鎖（如果這些套件和檔案受應用程式啟動控制拒絕規則影響）。

軟體分發控制排除項適用於受信任套件和這些套件建立或修改的檔案（如果應用程式啟動控制清單中沒有拒絕規則適用於這些套件和檔案）。

使用 KSN 結論

KSN 的檔案不受信任的結論具有比軟體分發控制排除項目更高的優先順序：如果 KSN 報告受信任套件建立過修改的檔案不受信任，則受信任套件的解壓縮和這些檔案的啟動都將被封鎖。

從受信任套件解壓縮後，所有子檔案都將被允許執行，不管是否在“應用程式啟動控制”範圍內使用 KSN。此時，“拒絕 KSN 不信任的應用程式”和“允許 KSN 信任的應用程式”核取方塊的狀態不影響“允許從該分發套件提取鍵中啟動到所有檔案”核取方塊的操作。

關於“應用程式啟動控制”工作的 KSN 使用

要啟動“KSN 使用”工作，您必須接受 KSN 聲明。

如果有關某個應用程式聲譽的 KSN 資料被“應用程式啟動控制”工作使用，則 KSN 應用程式聲譽將被視為允許或拒絕該應用程式啟動的條件。如果 KSN 在使用者嘗試啟動某個應用程式時向 Kaspersky Embedded Systems Security 報告該應用程式不受信任，應用程式啟動將被拒絕。如果 KSN 在使用者嘗試啟動某個應用程式時向 Kaspersky Embedded Systems Security 報告該應用程式受信任，應用程式啟動將被允許。KSN 可與應用程式啟動控制規則一起使用，或作為拒絕應用程式啟動的獨立條件。

使用 KSN 結論作為拒絕應用程式啟動的獨立條件

此方案允許在受防護電腦上安全地控制應用程式啟動，而無需對規則清單進行進階配置。

您可以將 KSN 結論連同唯一指定的規則一起套用於 Kaspersky Embedded Systems Security。該應用程式將僅允許啟動 KSN 中信任的或指定規則允許的應用程式。

對於此類方案，建議設定一條根據數位憑證允許應用程式啟動的規則。

按照“預設拒絕”政策，將拒絕所有其他應用程式。當沒有應用任何規則時，使用 KSN 來防護電腦免受 KSN 認為會造成威脅的應用程式的侵害。

與應用程式啟動控制規則一起套用 KSN 結論

將 KSN 結論與應用程式啟動控制規則同時使用時，以下條件適用：

- 如果某個應用程式包括在至少一條拒絕規則的範圍內，Kaspersky Embedded Systems Security 將始終拒絕該應用程式的啟動。如果應用程式被視為受 KSN 信任，則相應結論具有較低優先順序且不被考慮；仍將拒絕應用程式啟動。這允許您延伸不需要的應用程式清單。
- 如果禁止啟動在 KSN 中不受信任的應用程式並且某個應用程式在 KSN 中不受信任，則 Kaspersky Embedded Systems Security 將始終拒絕該應用程式啟動。如果為應用程式設定了允許規則，則此規則具有較低優先順序且不被考慮；仍將拒絕應用程式啟動。這樣可以防護電腦免受被 KSN 視為威脅（但在首次配置規則時未被考慮）的應用程式的侵害。

產生應用程式啟動控制規則

您可使用卡巴斯基安全管理中心工作和政策立同時為公司網路上的所有電腦和電腦群組建立應用程式啟動控制規則清單。如果公司網路沒有參考電腦且您無法根據參考電腦上安裝的應用程式建立允許規則清單，則建議使用此方案。您還可以透過應用程式主控台在本機執行“應用程式啟動控制規則產生器”工作來根據單台電腦上執行的應用程式建立規則清單。

“應用程式啟動控制”元件安裝後具有兩條預設的允許規則：

- 針對作業系統信任的指令碼和帶憑證的 MSI 檔案的允許規則。
- 針對作業系統信任的帶憑證的可執行檔的允許規則。

您可以使用以下方式之一在卡巴斯基安全管理中心一側建立應用程式啟動控制規則清單：

- 使用“應用程式啟動控制規則產生器”群組工作。

在此方案下，一個群組工作會為網路上的每個電腦建立其自己的應用程式啟動控制規則清單，並將這些清單儲存到指定共用資料夾中的 XML 檔案。“應用程式啟動控制規則產生器”工作建立的 XML 檔案包含工作啟動前工作設定中指定的允許規則。不會為指定工作設定中不允許啟動的應用程式建立任何規則。預設情況下將拒絕此類應用程式啟動。然後，您可將建立的規則清單手動匯入卡巴斯基安全管理中心政策的“應用程式啟動控制”工作。您可以將卡巴斯基安全管理中心政策設定為在“應用程式啟動控制規則產生器”群組工作完成後，自動將已建立的規則新增到“應用程式啟動控制”規則清單中。

您可將建立的規則配置為自動匯入“應用程式啟動控制”工作的規則清單。

當您需要快速建立應用程式啟動控制規則清單時，建議使用此方案。建議僅當套用的允許規則包含您知道安全的資料夾和檔案時，才配置“應用程式啟動控制規則產生器”工作的排程啟動。

在網路中使用“應用程式啟動控制”工作之前，請確保所有受防護電腦都能夠存取共用網路資料夾。如果組織的政策未規定使用網路中的共用資料夾，建議在測試電腦群組中的電腦或參考電腦上啟動“應用程式啟動控制規則產生器”工作。

- 基於在“**僅統計**”模式下執行的“應用程式啟動控制”工作在卡巴斯基安全管理中心中建立的工作事件報告。

在此方案下，Kaspersky Embedded Systems Security 不拒絕應用程式啟動。相反，當“應用程式啟動控制”在“**僅統計**”模式下執行時，它會在卡巴斯基安全管理中心中的“管理伺服器”節點的工作區的“**事件**”標籤中報告所有網路電腦中所有已允許和已拒絕的應用程式啟動。卡巴斯基安全管理中心使用工作記錄來建立一個拒絕了應用程式啟動的事件清單。

您需要設定工作執行期限，以便可在指定時間期限內執行所有可能的受防護電腦和電腦群組操作方案以及至少一次電腦重新啟動。將規則新增到“應用程式啟動控制”工作後，您可從儲存的卡巴斯基安全管理中心事件報告 (TXT 格式) 匯入應用程式啟動資料，並基於此資料為此類應用程式建立應用程式啟動控制允許規則。

如果公司網路包含大量不同類型的電腦 (安裝了不同的軟體) ，則建議使用此方案。

- 根據透過卡巴斯基安全管理中心接收到的拒絕應用程式啟動事件，無需建立和匯入設定檔。

要使用此功能，必須在有效的卡巴斯基安全管理中心政策下執行本機電腦上的應用程式啟動控制工作。在本例中，本機電腦上的所有事件均被傳送到管理伺服器。

建議當網路電腦上安裝的應用程式集合變更時（例如，安裝更新或重新安裝作業系統時）更新規則清單。建議透過在測試管理群組中的伺服器上以“**僅統計**”模式執行“應用程式啟動控制規則產生器”工作或“應用程式啟動控制”工作來建立更新的規則清單。測試管理群組包含在網路電腦上安裝新的應用程式之前對這些應用程式的啟動進行測試所需的電腦。

包含允許規則清單的 XML 檔案基於在受防護電腦上啟動的工作分析建立。為了在建立規則清單時將網路上利用的所有應用程式考慮在內，建議在參考電腦上以“**僅統計**”模式啟動“應用程式啟動控制規則產生器”工作和“應用程式啟動控制”工作。

在基於參考電腦上啟動的應用程式建立允許規則之前，確保參考電腦是安全的，並且不包含任何惡意軟體。

新增允許規則之前，請選擇其中一個可用的規則套用模式。卡巴斯基安全管理中心政策規則清單將僅顯示由政策指定的那些規則，與規則應用模式無關。本機規則清單包括所有已套用的規則 — 本機規則和透過政策新增的規則。

“應用程式啟動控制”工作預設設定

預設情況下，“應用程式啟動控制”工作具有下表所述的設定。您可以變更這些設定值。

表 47. “應用程式啟動控制”工作預設設定

設定	預設值	敘述
----	-----	----

設定	預設值	敘述
工作模式	僅統計。該工作根據設定的規則記錄拒絕的啟動事件和允許的啟動事件。應用程式啟動實際不會被拒絕。	在建立最終規則清單後，您可以選擇“活動”模式。
為檔案隨後的所有啟動重複執行該檔案第一次啟動時的動作	已套用	您可以為檔案隨後的所有啟動重複執行該檔案第一次啟動時的動作。
在沒有可執行的指令時拒絕指令解釋器啟動	未套用。	您可以在沒有可執行的指令時拒絕指令解釋器啟動。
規則管理	使用政策規則取代本機規則	可以選擇將政策中指定的規則與本機電腦上的規則一起套用的模式。
規則使用範圍	工作控制可執行檔、指令碼和 MSI 資料套件的啟動。它還監控 DLL 模組的載入。	您可以指定要使用規則控制其啟動的檔案類型。
KSN 使用	不使用 KSN 應用程式聲譽資料。	在執行“應用程式啟動控制”工作時，您可以使用 KSN 應用程式聲譽資料。
自動允許為所列應用程式和資料套件分發軟體	未套用。	可以使用安裝程式和設定中指定的應用程式允許軟體分發。預設情況下，僅允許使用 Windows Installer 進行軟體分發。
始終允許透過 Windows Installer 進行軟體分發	已套用（僅當“自動允許為所列應用程式和資料套件分發軟體”設定啟用時可以變更）。	如果透過 Windows Installer 執行操作，您可允許任何軟體安裝或更新。

設定	預設值	敘述
始終允許使用背景智慧傳輸服務透過 SCCM 進行軟體分發	未套用 (僅當“自動允許為所列應用程式和資料套件分發軟體”設定啟用時可以變更) 。	可以使用 System Center Configuration Manager 開啟或關閉軟體分發。
啟動工作	不設定工作的初次啟動排程。	“應用程式啟動控制”工作不會在 Kaspersky Embedded Systems Security 啟動時自動啟動。您可以手動啟動該工作或設定排程啟動。

表 48. “應用程式啟動控制規則產生器”工作的預設設定

設定	預設值	敘述
允許規則名稱的前置詞	與安裝了 Kaspersky Embedded Systems Security 的電腦的名稱相同。	您可以變更允許規則的名稱前置詞。
允許規則的使用範圍	<p>預設情況下，允許規則的範圍包括以下檔案類別：</p> <ul style="list-style-type: none"> 位於以下資料夾中的具有 EXE 副檔名的檔案：C:\Windows、C:\Program Files (x86) 和 C:\Program Files 儲存在 C:\Windows 資料夾中的 MSI 安裝套件 儲存在 C:\Windows 資料夾中的指令碼 <p>該工作還會為所有正在執行的應用程式建立規則，而不管其位置和格式。</p>	您可以透過新增或刪除資料夾路徑並指定將被自動建立的規則允許啟動的檔案類型來變更防護範圍。您還可以在建立允許規則時略過正在執行的應用程式。

設定	預設值	敘述
建立允許規則的條件	使用數位憑證主旨和指紋；為所有使用者和使用者群組建立規則。	在建立允許規則時，可以使用 SHA256 雜湊。 您可以選擇需要為其自動建立允許規則的使用者和使用者群組。
工作完成時的 操作	允許規則新增到應用程式啟動控制規則清單；新規則與現有規則合併；重複規則被刪除。	您可以將規則新增到現有規則，而不進行合併和刪除重複規則，或將現有規則替換為新的允許規則，或設定將允許規則匯出到檔案。
工作啟動設定 及權限	在系統帳戶下啟動工作。	您可以允許“應用程式啟動控制規則產生器”工作在系統帳戶下或使用指定使用者的權限啟動。
工作啟動排程	不設定工作的初次啟動排程。	“應用程式啟動控制規則產生器”工作不會在 Kaspersky Embedded Systems Security 啟動時自動啟動。您可以手動啟動該工作或設定排程啟動。

透過管理外掛程式管理應用程式啟動控制

在本節中，學習如何導航管理外掛程式介面，以及如何為網路中的一台或所有電腦配置工作設定。

本章節說明項目

導航	376
配置“應用程式啟動控制”工作設定	378
配置軟體分發控制	383
配置“應用程式啟動控制規則產生器”工作	386
透過卡斯基安全管理中心配置應用程式啟動控制規則	389
建立“應用程式啟動控制規則產生器”工作	399

導航

學習如何透過介面導航到所需工作設定。

本章節說明項目

開啟“應用程式啟動控制”工作的政策設定	376
開啟應用程式啟動控制規則清單	377
開啟“應用程式啟動控制規則產生器”工作精靈和內容	377

開啟“應用程式啟動控制”工作的政策設定

► 要透過卡斯基安全管理中心政策開啟“應用程式啟動控制”工作設定：

1. 展開卡斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“**政策**”標籤。

4. 點擊要設定的政策名稱。
5. 在開啟的“內容：<政策名稱>”視窗中，選擇“本機行為控制”部分。
6. 點擊“應用程式啟動控制”子部分中的“設定”按鈕。

將開啟“應用程式啟動控制”視窗。

根據需要設定政策。

開啟應用程式啟動控制規則清單

► 要透過卡巴斯基安全管理中心開啟應用程式啟動控制規則清單：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“政策”標籤。
4. 點擊要設定的政策名稱。
5. 在開啟的“內容：<政策名稱>”視窗中，選擇“本機行為控制”部分。
6. 點擊“應用程式啟動控制”子部分中的“設定”按鈕。

將開啟“應用程式啟動控制”視窗。

7. 在“一般”標籤上，點擊“規則清單”按鈕。

將開啟“應用程式啟動控制規則”視窗。

根據需要設定規則清單。

開啟“應用程式啟動控制規則產生器”工作精靈和內容

► 要開始建立“應用程式啟動控制規則產生器”工作：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。

2. 選擇要為其設定工作的管理群組。
3. 選擇“工作”標籤。
4. 點擊“建立工作”按鈕。

將開啟“新建工作精靈”視窗。

5. 選擇“應用程式啟動控制規則產生器”工作。
6. 點擊“下一步”。

將開啟“設定”視窗。

► 要配置現有“應用程式啟動控制規則產生器”工作：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“工作”標籤。
4. 點擊卡巴斯基安全管理中心工作清單中的工作名稱。

將開啟“內容：應用程式啟動控制規則產生器”視窗。

有關配置該工作的詳細資訊，請參見“配置‘應用程式啟動控制規則產生器’工作”部分。

配置“應用程式啟動控制”工作設定

► 要配置一般“應用程式啟動控制”工作設定：

1. 開啟“應用程式啟動控制”視窗(請參見第 [376](#) 頁上的“開啟“應用程式啟動控制”工作的政策設定”部分)視窗。
2. 在“一般”標籤上，選擇“工作模式”部分的以下設定：
 - 在“工作模式”下拉清單中，指定工作模式。

在此下拉清單中，可選擇“應用程式啟動控制”工作的模式：

- **活動。** Kaspersky Embedded Systems Security 使用指定的規則控制任何應用程式的啟動。
- **僅統計。** Kaspersky Embedded Systems Security 不使用指定的規則控制應用程式啟動。相反，它僅在工作記錄中記錄有關啟動事件的資訊。所有應用程式均允許啟動。您可以使用此模式根據工作記錄中記錄的有關拒絕的應用程式啟動的資訊產生應用程式啟動控制規則清單。

預設情況下，“應用程式啟動控制”工作在“僅統計”模式下執行。

- 清除或選中“**為檔案隨後的所有啟動重複執行該檔案第一次啟動時的操作**”核取方塊。

此核取方塊用於啟用或停用根據快取中儲存的事件資訊對第二次和後續應用程式啟動嘗試的啟動控制。

如果選中此核取方塊，Kaspersky Embedded Systems Security 將根據工作針對應用程式第一次啟動的結論允許或拒絕應用程式的後續啟動。例如，如果規則允許了第一次應用程式啟動，則有關此操作的資訊將儲存在快取中，第二次和所有後續啟動也將被允許，而不進行重複檢查。

如果清除該核取方塊，Kaspersky Embedded Systems Security 會在每次嘗試啟動應用程式時進行分析該應用程式。

預設將會選定該核取方塊。

- 清除或選中“**在沒有可執行的指令時拒絕指令解釋器啟動**”核取方塊。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將拒絕命令列編譯器啟動，即使允許編譯器啟動。只有同時滿足以下兩個條件時，才能在沒有指令的情況下啟動命令列編譯器：

- 允許命令列解釋器啟動。
- 要執行的指令獲得允許。

如果清除該核取方塊，Kaspersky Embedded Systems Security 在啟動命令列編譯器時只考慮允許規則。如果未套用任何允許規則或可執行處理程序不受 KSN 信任，啟動將被拒絕。如果套用了允許規則或處理程序受 KSN 信任，則無論是否有要執行的指令，都可以啟動命令列編譯器。

Kaspersky Embedded Systems Security 可辨識以下命令列解釋器：

- cmd.exe
- powershell.exe
- python.exe
- perl.exe

預設取消選定該核取方塊。

3. 在“規則管理”部分中，配置應用規則的設定：

a. 點擊“規則清單”按鈕以新增“應用程式啟動控制”工作的允許規則。

Kaspersky Embedded Systems Security 無法辨識包含斜線“/”的路徑。請使用反斜線“\”來正確輸入路徑。

b. 選擇套用規則的模式：

- 使用政策規則取代本機規則。

應用程式將針對電腦群組上的應用程式啟動控制套用政策中指定的規則清單。不能建立、編輯或套用本機規則清單。

- 將政策規則新增到本機規則。

應用程式將與本機規則清單一起套用政策中指定的規則清單。可以使用“應用程式啟動控制規則產生器”工作編輯本機規則清單。

預設情況下，Kaspersky Embedded Systems Security 套用兩條預設規則，這兩條規則允許一系列指令碼、MSI 套裝軟體和可執行檔，只要這些物件具有受信任數位簽章。

4. 在“規則使用範圍”部分中，指定以下設定：

- **將規則套用於可執行檔。**

該核取方塊用於啟用或停用可執行檔的啟動控制。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用指定的規則（其設定指定**可執行檔**為範圍）允許或封鎖程式可執行檔的啟動。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不使用指定的規則控制程式可執行檔的啟動。將允許可執行檔啟動。

預設將會選定該核取方塊。

- **監控 DLL 模組的載入。**

該核取方塊用於啟用或停用 DLL 模組的載入控制。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用指定的規則（其設定將**可執行檔**指定為範圍）允許或封鎖 DLL 模組的載入。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不使用指定的規則控制 DLL 模組的載入。將允許 DLL 模組載入。

如果選中“**將規則套用於可執行檔**”核取方塊，則此核取方塊處於活動狀態。

預設取消選定該核取方塊。

控制 DLL 模組的載入可能影響作業系統的效能。

- **將規則套用於指令碼和 MSI 資料套件。**

此核取方塊用於啟用或停用指令碼和 MSI 資料套件的啟動。

如果選中此核取方塊，Kaspersky Embedded Systems Security 將使用指定的規則（其設定將指令碼和 MSI 資料套件指定為範圍）允許或封鎖指令碼和 MSI 資料套件啟動。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不使用指定的規則控制指令碼和 MSI 資料套件的啟動。將允許指令碼和 MSI 資料套件的啟動。

預設將會選定該核取方塊。

5. 在“**KSN 使用**”方塊中，配置以下應用程式啟動設定：

- **拒絕 KSN 不信任的應用程式。**

此核取方塊用於啟用或停用根據 KSN 中的應用程式聲譽資料進行應用程式啟動控制。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將封鎖任何在 KSN 中不受信任的應用程式執行。適用於在 KSN 中不受信任的應用程式的應用程式啟動控制允許規則不會被觸發。選中此核取方塊將會提供額外的惡意軟體防護。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 將不考慮 KSN 中不受信任的應用程式的聲譽，並根據適用於此類應用程式的規則允許或封鎖啟動。

預設取消選定該核取方塊。

- **允許 KSN 信任的應用程式。**

此核取方塊用於啟用或停用根據 KSN 中的應用程式聲譽資料進行應用程式啟動控制。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將允許在 KSN 中受到信任的應用程式執行。適用於 KSN 信任的應用程式的拒絕應用程式啟動控制規則具有更高優先順序：如果某個應用程式受到 KSN 服務信任，應用程式啟動將被拒絕。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 將不考慮 KSN 信任的應用程式的聲譽，並根據適用於此類應用程式的規則允許或封鎖啟動。

預設取消選定該核取方塊。

- 允許啟動 KSN 中信任的應用程式的使用者和/或使用群組。
6. 在“軟體分發控制”標籤上，配置軟體分發控制的設定（請參見第 [383](#) 頁上的“配置軟體分發控制”部分）。
 7. 在“工作管理”標籤上，配置排程的工作啟動設定（請參見第 [164](#) 頁上的“配置工作啟動排程設定”部分）。
 8. 在“工作設定”視窗中點擊“確定”。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在系統稽核記錄中。

配置軟體分發控制

► 要新增受信任分發套件：

1. 開啟“應用程式啟動控制”視窗（請參見第 [376](#) 頁上的“開啟“應用程式啟動控制”工作的政策設定”部分）。
2. 在“軟體分發控制”標籤上，選中“自動允許為所列應用程式和資料套件分發軟體”核取方塊。

使用此核取方塊可啟用和停用自動建立使用清單中指定的安裝套件啟動的所有檔案的排除項目。

如果選中此核取方塊，應用程式會自動允許受信任安裝套件中的檔案啟動。可以編輯允許啟動的應用程式和分發套件清單。

如果清除此核取方塊，應用程式不會應用清單中指定的排除項目。

預設取消選定該核取方塊。

如果在“應用程式啟動控制”工作設定中選中“一般”標籤中的“將規則套用於可執行檔”核取方塊，則您可選中“自動允許為所列應用程式和資料套件分發軟體”。

3. 根據需要清除“始終允許透過 Windows Installer 進行軟體分發”核取方塊。

此核取方塊用於啟用和停用自動建立透過 Windows Installer 執行的所有檔案的排除項目。

如果選中此核取方塊，透過 Windows Installer 安裝的檔案將始終被允許啟動。

如果清除該核取方塊，檔案將不被允許無條件啟動，即使透過 Windows Installer 啟動它們。

預設將會選定該核取方塊。

如果未選中“自動允許為所列應用程式和資料套件分發軟體”核取方塊，則此核取方塊不可編輯。

僅當在絕對必要時才建議清除“始終允許透過 Windows Installer 進行軟體分發”核取方塊。關閉此功能可能導致更新作業系統檔案出問題，還可能封鎖從分發套件提取的檔案啟動。

4. 如果需要，請選擇“始終允許使用背景智慧傳輸服務透過 SCCM 進行軟體分發”核取方塊。

透過使用 System Center Configuration Manager，該核取方塊可以自動開啟或關閉軟體分發。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 自動允許使用 System Center Configuration Manager 進行 Microsoft Windows 佈署。應用程式僅允許透過背景智慧傳輸服務進行軟體分發。

應用程式可控制具有以下副檔名的物件的啟動：

- .exe
- .msi

預設取消選定該核取方塊。

應用程式控制電腦上從套裝軟體傳送到安裝或更新的軟體分發週期。如果在電腦上安裝應用程式之前已執行分發的任何階段，則應用程式不會控制過程。

5. 要編輯受信任安裝套件的清單，請點擊“**變更分發套件清單**”，然後在開啟的視窗中選擇以下方法之一：

- **新增一個分發套件。**
 - a. 點擊“**瀏覽**”按鈕，然後選擇可執行檔或分發套件。

“**信任條件**”部分會使用有關選定檔案的資料自動進行填充。
 - b. 清除或選中“**允許從該分發套件提取鍵中啟動到所有檔案**”核取方塊。
 - c. 選擇兩個可用條件選項中的一個，用於決定檔案或安裝套件是否受信任：
 - **使用數位憑證**
 - **使用 SHA256 雜湊**
- **按雜湊新增多個分發套件。**

您可以選擇無限數量的可執行檔和分發套件，並同時將它們新增到清單。Kaspersky Embedded Systems Security 將檢查雜湊並允許作業系統啟動指定的檔案。

- 變更選定的分發套件。

使用此選項可以選擇不同的可執行檔或分發套件，或變更信任條件。

- 從檔案匯入分發套件清單。

可以從設定檔匯入受信任安裝套件的清單。要使檔案被 Kaspersky Embedded Systems Security 識別，檔案必須滿足以下參數：

- 檔案副檔名為 TXT。
- 檔案包含結構化成行清單的資訊，其中每一行包含的資料用於一個受信任的檔案。
- 檔案必須包含以下格式之一的清單：
 - <檔案名稱> : <SHA256 雜湊>。
 - <SHA256 雜湊>* <檔案名稱>。

在“開啟”視窗中，指定包含受信任安裝套件清單的設定檔。

6. 如果要刪除受信任清單中以前新增的應用程式或分發套件，請點擊“刪除分發套件”按鈕。將允許執行提取檔案。

要封鎖提取檔案啟動，請在受防護電腦上移除應用程式，或在應用程式啟動控制工作設定中建立拒絕規則。

7. 點擊“確定”。

將儲存新配置的設定。

配置“應用程式啟動控制規則產生器”工作

► 要配置“應用程式啟動控制規則產生器”工作，請執行以下操作：

1. 開啟“內容：應用程式啟動控制規則產生器”（請參見第 [377](#) 頁上的“開啟“應用程式啟動控制規則產生器”工作精靈和內容”部分）視窗。
2. 在“通知”部分中，配置工作事件通知設定。

關於此節中配置設定的詳細資訊，請參見 [卡巴斯基安全管理中心說明](#)。

3. 在“**設定**”部分中，您可配置以下設定：
 - 為規則名稱的前置詞。
 - 配置允許規則的使用範圍：
 - 基於正在執行的應用程式建立允許規則；
 - 為以下資料夾中的應用程式建立允許規則；
4. 在“**選項**”部分中，可以指定在建立應用程式啟動控制允許規則時執行的操作：
 - **使用數位憑證**

如果選擇此選項，則會在新建立的應用程式啟動控制允許規則設定中將存在數位憑證指定為規則觸發條件。此時，應用程式將允許啟動使用帶數位憑證的檔案啟動的程式。如果希望允許作業系統中信任的任何應用程式啟動，建議使用此選項。

預設選中該選項。

- **使用數位憑證主旨和指紋**

此核取方塊用於啟用或停用將檔案數位憑證的主旨和指紋用作觸發應用程式啟動控制允許規則的條件。選中此核取方塊可指定更嚴格的數位憑證驗證條件。

如果選中此核取方塊，為其建立規則的檔案的數位憑證主旨和指紋值設定為觸發允許應用程式啟動控制規則的條件。Kaspersky Embedded Systems Security 將允許使用具有指定指紋和數位憑證的檔案啟動的應用程式。

由於指紋是數位憑證的唯一識別碼且無法偽造，選中此核取方塊會高度限制基於數位憑證觸發允許規則。

如果清除此核取方塊，則在作業系統中任何受信任數位憑證的存在被設定為觸發應用程式啟動控制允許規則的條件。

如果選擇了“**使用數位憑證**”選項，該核取方塊處於活動狀態。

預設將會選定該核取方塊。

- **憑證遺失則使用**

這是一個下拉清單，如果用於建立規則的檔案沒有數位憑證，則可使用此下拉清單選擇用於觸發應用程式啟動控制允許規則的條件。

- **SHA256 雜湊**。將用於建立規則的檔案的核對總和設定為觸發應用程式啟動控制允許規則的條件。應用程式將允許啟動使用帶指定核對總和的檔案啟動的程式。
- **檔案路徑**。將用於建立規則的檔案的路徑設定為觸發應用程式啟動控制允許規則的條件。此時，應用程式將允許啟動使用位於“設定”部分的“為以下資料夾中的應用程式建立允許規則”表中指定的資料夾中的檔案啟動的程式。
- **使用 SHA256 雜湊**

如果選擇此選項，則會在新建立的應用程式啟動控制允許規則的設定中，將用於建立規則的檔案的核對總和指定為規則觸發條件。應用程式將允許啟動使用帶指定核對總和的檔案啟動的程式。

當產生的規則必須達到最高安全等級（SHA256 核對總和可能用作唯一檔案 ID）時，建議使用此選項。使用 SHA256 核對總和作為規則觸發條件會將規則使用範圍限制為一個檔案。

預設清除該選項。

- **為使用者或使用者群組產生規則。**

這是顯示使用者或使用者群組的欄位。應用程式將控制由指定使用者或使用者群組執行的任何應用程式。

預設選擇為“每個人”。

您可以使用 Kaspersky Embedded Systems Security 在工作完成時建立的允許規則清單為設定檔配置設定。

1. 在“**排程**”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。
2. 在“**帳戶**”部分中，指定將使用其權限執行工作的帳戶。
3. 如有需要，在“**工作範圍的排除項目**”部分中指定要從工作範圍中排除的物件。

有關此節中配置設定的詳細資訊，請參見 [卡巴斯基安全管理中心說明](#)。

4. 在“內容：<工作名稱>”視窗中，點擊“確定”。

將儲存新配置的群組工作設定。

透過卡斯基安全管理中心配置應用程式啟動控制規則

瞭解如何使用“應用程式啟動控制”工作根據各種條件建立規則清單，或手動建立允許或拒絕規則。

本章節說明項目

新增應用程式啟動控制規則	389
啟用預設允許模式	393
從卡斯基安全管理中心事件建立允許規則	393
從有關受封鎖應用程式的卡斯基安全管理中心報告中匯入規則	395
從 XML 設定檔匯入應用程式啟動控制規則	397
檢查應用程式啟動	399

新增應用程式啟動控制規則

► 要新增應用程式啟動控制規則：

1. 開啟“應用程式啟動控制規則”視窗(請參見第 [377](#) 頁上的“開啟應用程式啟動控制規則清單”部分)。
2. 點擊“新增”按鈕。
3. 在按鈕的內容功能表中，選擇“新增一項規則”。

將開啟“規則設定”視窗。

4. 指定以下設定：
 - a. 在“名稱”欄位中，輸入規則的名稱。
 - b. 在“類型”下拉清單中，選擇規則類型：
 - 允許，如果您希望規則根據規則設定中指定的條件允許應用程式啟動。

- **拒絕**，如果您希望規則根據規則設定中指定的條件封鎖應用程式啟動。
- c. 在“**範圍**”下拉清單中，選擇將由規則控制執行的檔案類型：
- **可執行檔**，如果您希望規則控制可執行檔的啟動。
 - **指令碼和 MSI 資料套件**，如果希望規則控制指令碼和 MSI 資料套件的啟動。
- d. 在“**使用者或群組**”欄位中，指定根據規則類型將允許或不允許啟動程式的使用者。為此，請執行以下操作：
- i. 點擊“**瀏覽**”按鈕。
 - ii. 將開啟標準 Microsoft Windows“**選擇使用者或群組**”視窗。
 - iii. 指定使用者和/或使用者群組清單。
 - iv. 點擊“**確定**”。
- e. 如果您希望從特定檔案獲取“**規則觸發條件**”部分中列出的規則觸發條件的值：
- i. 點擊“**從檔案內容設定規則觸發條件**”按鈕。
將開啟標準 Microsoft Windows“**開啟**”視窗。
 - ii. 選擇檔案。
 - iii. 點擊“**開啟**”按鈕。
檔案中的條件值顯示在“**規則觸發條件**”部分的欄位中。預設選擇檔案內容中提供有其資料的條件。
- f. 在“**規則觸發條件**”部分中，選擇以下選項之一：
- **數位憑證**，如果您希望規則控制使用數位憑證簽章的檔案啟動的應用程式的啟動：
 - 如果您希望規則控制由僅具有指定標題的數位憑證簽章的檔案的啟動，請選中“**使用主旨**”核取方塊。
 - 如果您希望規則僅控制使用具有指定指紋的數位憑證簽章的檔案的啟動，請選中“**使用指紋**”核取方塊。
 - **SHA256 雜湊**，如果您希望規則控制使用其核對總和與指定值比對的檔案啟動的程式的啟動。

- **檔案路徑**，如果您希望規則控制使用位於指定路徑的檔案啟動的程式的啟動。

Kaspersky Embedded Systems Security 無法辨識包含斜線“/”的路徑。請使用反斜線“\”來正確輸入路徑。

g. 如果希望新增規則排除：

- i. 在“**從規則排除**”部分中，點擊“**新增**”按鈕。

將開啟“**從規則排除**”視窗。

- ii. 在“**名稱**”欄位中，輸入排除項目的名稱。

- iii. 指定從應用程式啟動控制規則中排除應用程式檔案的設定。可點擊“**基於檔案內容設定排除**”按鈕從檔案內容填充設定欄位。

- **數位憑證**

如果選擇此選項，則會在新建立的應用程式啟動控制允許規則設定中將存在數位憑證指定為規則觸發條件。此時，應用程式將允許啟動使用帶數位憑證的檔案啟動的程式。如果希望允許作業系統中信任的任何應用程式啟動，建議使用此選項。

預設選中該選項。

- **使用主旨**

該核取方塊可啟用或停用使用數位憑證的主旨作為規則觸發條件。

如果選中該核取方塊，則使用指定的數位憑證主旨作為規則觸發條件。建立的規則將僅控制主旨中指定的供應商的應用程式的啟動。

如果清除該核取方塊，應用程式將不會使用數位憑證的主旨作為規則觸發條件。如果選擇“**數位憑證**”條件，建立的規則將控制使用包含任何主旨的數位憑證簽章的應用程式的啟動。

只能使用位於“**規則觸發條件**”部分上方的“**從檔案內容設定規則觸發條件**”按鈕透過所選檔案的內容指定用於對檔案進行簽章的數位憑證的主旨。

預設取消選定該核取方塊。

- **使用指紋**

該核取方塊可啟用/停用使用數位憑證的指紋作為規則觸發條件。

如果選中該核取方塊，則使用指定的數位憑證指紋作為規則觸發條件。建立的規則將控制使用帶指定指紋的數位憑證簽章的應用程式的啟動。

如果清除該核取方塊，應用程式將不會使用數位憑證的指紋作為規則觸發條件。如果選擇“**數位憑證**”條件，應用程式將控制使用具有任何指紋的數位憑證簽章的應用程式的啟動。

只能使用位於“**規則觸發條件**”部分上方的“**從檔案內容設定規則觸發條件**”按鈕透過所選檔案的內容指定用於對檔案進行簽章的數位憑證的指紋。

預設取消選定該核取方塊。

- **SHA256 雜湊**

如果選擇此選項，則會在新建立的應用程式啟動控制允許規則的設定中，將用於建立規則的檔案的核對總和指定為規則觸發條件。應用程式將允許啟動使用帶指定核對總和的檔案啟動的程式。

當產生的規則必須達到最高安全等級 (SHA256 核對總和可能用作唯一檔案 ID) 時，建議使用此選項。使用 SHA256 核對總和作為規則觸發條件會將規則使用範圍限制為一個檔案。

預設清除該選項。

- **檔案路徑**

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用檔案的完整路徑來確定處理程序是否受信任。

如果清除該核取方塊，則不使用檔案的路徑來確定處理程序是否受信任。

預設取消選定該核取方塊。

- i. 點擊“**確定**”。
- ii. 如有必要，重複步驟 (i)-(iv) 以新增更多排除。

1. 在“**規則設定**”視窗中點擊“**確定**”。

建立的規則顯示在“應用程式啟動控制規則”視窗中的清單中。

啟用預設允許模式

預設允許模式允許所有應用程式啟動，只要它們未被規則或被 KSN 的不受信任結論封鎖。可以透過新增特定允許規則來啟用預設允許模式。您可以僅為指令碼或為所有可執行檔啟用“預設允許”模式。

► 要新增預設允許規則：

1. 開啟“應用程式啟動控制規則”(請參見第 [377](#) 頁上的“開啟應用程式啟動控制規則清單”部分)視窗。
2. 點擊“新增”按鈕，然後在該按鈕的內容功能表中選擇“新增一項規則”。
將開啟“規則設定”視窗。
3. 在“名稱”欄位中，輸入規則的名稱。
4. 在“類型”下拉清單中，選擇“允許”規則類型。
5. 在“範圍”下拉清單中，選擇將由規則控制執行的檔案類型：
 - 可執行檔，如果希望規則控制可執行檔的啟動。
 - 指令碼和 MSI 資料套件，如果希望規則控制指令碼和 MSI 資料套件的啟動。
6. 在“規則觸發條件”部分中，選擇“檔案路徑”選項。
7. 輸入以下遮罩：?
:\
8. 在“規則設定”視窗中點擊“確定”。

Kaspersky Embedded Systems Security 將套用預設允許模式。

從卡巴斯基安全管理中心事件建立允許規則

► 要在“應用程式啟動控制”中從卡巴斯基安全管理中心事件為應用程式建立允許規則：

1. 開啟“應用程式啟動控制規則”(請參見第 [377](#) 頁上的“開啟應用程式啟動控制規則清單”部分)視窗。
2. 點擊“新增”按鈕，然後在該按鈕的內容功能表中選擇“從卡巴斯基安全管理中心事件為應用程式建立允許規則”。

3. 選擇將規則新增到先前建立的應用程式啟動控制規則清單中的政策：

- **新增到現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
- **取代現有規則**，如果您希望將現有規則取代為匯入的規則。
- **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。

將開啟“產生應用程式啟動控制規則”視窗。

4. 配置以下請求設定：

- **管理伺服器位址**
- **埠號**
- **使用者**
- **密碼**

5. 選擇您希望規則建立工作使用的事件類型：

- **僅統計模式：應用程式啟動被拒絕。**
- **應用程式啟動被拒絕。**

6. 從“請求在以下期間內產生的事件”下拉清單中選擇時間段。

7. 點擊“產生規則”按鈕。

8. 點擊“應用程式啟動控制規則”視窗中的“儲存”按鈕。

將使用基於安裝了卡斯基安全管理中心管理主控台的電腦的系統資料建立的新規則填充“應用程式啟動控制”工作中的規則清單。

如果政策中已指定應用程式啟動控制規則清單，則 Kaspersky Embedded Systems Security 將從封鎖事件中新增選定的規則到已指定的規則。不新增具有相同雜湊的規則，因為清單中的所有規則都必須是唯一的。

從有關受封鎖應用程式的卡斯基安全管理中心報告中匯入規則

您可從在“**僅統計**”模式下執行“應用程式啟動控制”工作後卡斯基安全管理中心中建立的報告匯入有關受封鎖應用程式啟動的資料，並使用此資料在所設定政策中建立應用程式啟動控制允許規則清單。

建立有關“應用程式啟動控制”工作期間發生的事件的事件的報告後，您可以跟蹤被封鎖啟動的應用程式。

將資料從有關受封鎖應用程式的報告匯入到政策設定時，確保您所使用的清單僅包含您希望允許啟動的應用程式。

► 要根據卡斯基安全管理中心中的受封鎖應用程式報告為一組電腦指定應用程式啟動控制允許規則：

1. 開啟“**應用程式啟動控制**”視窗（請參見第 [376](#) 頁上的“開啟‘應用程式啟動控制’工作的政策設定”部分）。
2. 在“**工作模式**”部分中，選擇“**僅統計**”模式。
3. 在“**事件通知**”部分中的政策內容中，確保：
 - 對於**緊急事件**，**應用程式啟動被拒絕**事件的工作記錄保留期超過以“**僅統計**”模式執行工作的排程期（預設值為 30 天）。
 - 對於重要性等級為“**警告**”的事件，**僅統計模式：應用程式啟動被拒絕**事件的工作記錄保留期超過以“**僅統計**”模式執行工作的排程期（預設值為 30 天）。

當事件保留期過後，有關記錄的事件的資訊會被刪除且不會反映在報告檔案中。在“**僅統計**”模式下執行應用程式啟動控制工作之前，確保工作執行時間不超過為指定事件設定的時間段。

4. 當工作完成後，將記錄的事件匯出到 TXT 檔案：
 - a. 在卡斯基安全管理中心中的“**管理伺服器**”節點的工作區中，選擇“**事件**”標籤。
 - b. 點擊“**建立選擇**”按鈕以基於“**封鎖**”條件建立一系列事件，以檢視“應用程式啟動控制”工作將封鎖啟動的應用程式。

- c. 在所選項的詳細資訊視窗中，點擊“**將事件匯出到檔案**”清單以將受封鎖應用程式啟動報告儲存到 TXT 檔案。

在政策中匯入和應用建立的報告之前，確保報告僅包含有關您希望允許啟動的應用程式的資料。

5. 將有關受封鎖應用程式啟動的資料匯入到應用程式啟動控制工作。為此，在政策內容的“應用程式啟動控制”工作設定中：
 - a. 在“**一般**”標籤上，點擊“**規則清單**”按鈕。
將開啟“**應用程式啟動控制規則**”視窗。
 - b. 點擊“**新增**”按鈕，然後在該按鈕的內容功能表中選擇“**從卡巴斯基安全管理中心報告匯入封鎖的應用程式的資料**”。
 - c. 選擇將來自根據卡巴斯基安全管理中心報告建立的清單的規則新增到先前設定的應用程式啟動控制規則清單的政策：
 - **新增到現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
 - **取代現有規則**，如果您希望將現有規則取代為匯入的規則。
 - **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。
 - d. 在開啟的標準 Microsoft Windows 視窗中，選擇已將來自受封鎖應用程式啟動報告的事件匯出到的 TXT 檔案。
 - e. 在“應用程式啟動控制規則”和“**工作設定**”視窗中點擊“**確定**”。

根據有關受封鎖應用程式的卡巴斯基安全管理中心報告建立的規則將被新增到應用程式啟動控制規則清單。

從 XML 設定檔匯入應用程式啟動控制規則

您可匯入由“應用程式啟動控制規則產生器”群組工作建立的報告，並將它們作為允許規則清單套用於所設定的政策中。

當“應用程式啟動控制規則產生器”群組工作完成後，應用程式會將建立的允許規則匯入指定的共用資料夾中儲存的 XML 檔案。包含規則清單的每個檔案透過對公司網路中每台單獨電腦上執行的檔案和啟動的應用程式進行分析所建立。這些清單包含類型與“應用程式啟動控制規則產生器”群組工作中指定的類型比對的檔案和應用程式的允許規則。

► 要根據自動建立的允許規則清單為一組電腦指定應用程式啟動控制允許規則：

1. 在所設定電腦群組的主控台內的“工作”標籤上，建立一個“應用程式啟動控制規則產生器”群組工作或選擇一個現有工作（請參見第 [377](#) 頁上的“開啟“應用程式啟動控制規則產生器”工作精靈和內容”部分）。
2. 在建立的“應用程式啟動控制規則產生器”群組工作的內容中或在工作精靈中，指定以下設定：
 - 在“通知”部分中，設定用於儲存工作執行報告的設定。

有關此節中配置設定的詳細說明，請參見 [卡巴斯基安全管理中心說明](#)。

- 在“設定”部分中，指定所建立規則將允許啟動的應用程式類型。您可編輯包含允許的應用程式的資料夾集合：從工作範圍排除預設資料夾或手動新增新資料夾。
- 在“選項”部分中，指定工作在執行時及完成後執行的操作。指定規則建立條件和建立的規則將匯出到的檔案的名稱。
- 在“排程”部分中設定工作啟動排程設定。
- 在“帳戶”部分中，指定將用於執行工作的使用者帳戶。
- 在“工作範圍的排除項目”部分中，指定要從工作範圍排除的電腦群組。

Kaspersky Embedded Systems Security 不會為在排除的電腦上啟動的應用程式建立允許規則。

3. 在所設定電腦群組的控制台上的“工作”標籤上，從群組工作清單中選擇您已建立的“應用程式啟動控制規則產生器”工作，然後點擊“**啟動**”按鈕啟動工作。

工作完成後，自動建立的允許規則清單將儲存在共用資料夾中的 XML 檔案中。

在網路中使用“應用程式啟動控制”工作之前，請確保所有受防護電腦都能夠存取共用網路資料夾。如果組織的政策未規定使用網路中的共用資料夾，建議在測試電腦群組中的電腦或參考電腦上啟動“應用程式啟動控制規則產生器”工作。

4. 要將建立的允許規則清單新增到“應用程式啟動控制”工作：
 - a. 開啟“**應用程式啟動控制規則**”視窗（請參見第 [377](#) 頁上的“開啟應用程式啟動控制規則清單”部分）。
 - b. 點擊“**新增**”按鈕，然後在開啟的清單中選擇“**從 XML 檔案匯入規則**”。
 - c. 選擇將自動建立的允許規則新增到先前建立的“應用程式啟動控制”規則清單中的政策：
 - **新增到現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
 - **取代現有規則**，如果您希望將現有規則取代為匯入的規則。
 - **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。
 - d. 在開啟的標準 Microsoft Windows 視窗中，選擇“**應用程式啟動控制規則產生器**”群組工作完成後建立的 XML 檔案。
 - e. 在“**應用程式啟動控制規則**”和“**工作設定**”視窗點擊“**確定**”。
5. 如果您希望將建立的規則套用於控制應用程式啟動，則在政策中的“應用程式啟動控制”工作內容中，為工作選擇“**活動**”模式。

基於每台單獨的電腦上的工作執行自動建立的允許規則將被套用於所設定政策涵蓋的所有網路電腦。在這些電腦上，應用程式將允許僅啟動已為其建立允許規則的這些應用程式。

檢查應用程式啟動

在套用所配置的應用程式啟動控制規則前，您可以測試任何應用程式以確定該應用程式會觸發哪些應用程式啟動控制規則。

預設情況下，Kaspersky Embedded Systems Security 將拒絕啟動不被單個規則允許啟動的應用程式。為避免拒絕啟動重要的應用程式，您需要為它們建立允許規則。

如果某個應用程式的啟動受多條不同類型的規則控制，拒絕規則將優先：即使應用程式只在一條拒絕規則下，也將拒絕該應用程式啟動。

► 要測試應用程式啟動控制規則：

1. 開啟“**應用程式啟動控制規則**”視窗(請參見第 [377](#) 頁上的“開啟應用程式啟動控制規則清單”部分)。
2. 在開啟的視窗中，點擊“**顯示檔案規則**”按鈕。

將開啟標準的 Microsoft Windows 視窗。

3. 選擇要測試其啟動控制的檔案。

指定檔案的路徑顯示在搜尋欄位中。清單包含在啟動所選檔案時將觸發的所有規則。

建立“應用程式啟動控制規則產生器”工作

► 要建立和配置“應用程式啟動控制規則產生器”工作設定：

1. 開啟“新建工作精靈”中的“**設定**”視窗(請參見第 [377](#) 頁上的“開啟“應用程式啟動控制規則產生器”工作精靈和內容”部分)。
2. 進行以下設定：
 - 指定規則名稱前置詞。

這是規則名稱的第一部分。規則名稱的第二部分由允許啟動的物件的名稱構成。

預設前置詞是安裝 Kaspersky Embedded Systems Security 的電腦的名稱。您可以變更允許規則的名稱前置詞。

- 配置允許規則使用範圍 (請參見第 [424](#) 頁上的“限制工作使用範圍”部分)。

3. 點擊“下一步”。
4. 指定 Kaspersky Embedded Systems Security 必須執行的操作：
 - 產生允許規則時（請參見第 [425](#) 頁上的“自動規則建立期間要執行的操作”部分）。
 - 工作完成後（請參見第 [427](#) 頁上的“自動規則建立過程完成後要執行的操作”部分）。
5. 在“排程”視窗中，設定排程的工作啟動設定。
6. 點擊“下一步”。
7. 在“選擇帳戶以執行工作”視窗中，指定要使用的帳戶。
8. 點擊“下一步”。
9. 自訂工作名稱。
10. 點擊“下一步”。

工作名稱不應超過 100 個字元，並且不能包含以下符號：
" * < > & \ : |

將開啟“完成工作建立”視窗。

11. 您可以透過選中“精靈完成後執行工作”核取方塊來在精靈完成後執行工作。
12. 點擊“完成”完成建立工作。

► 要在卡斯基安全管理中心中設定現有規則，

開啟“內容：應用程式啟動控制規則產生器”視窗並調整上述設定。

有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在系統稽核記錄中。

本章節說明項目

限制工作使用範圍	401
自動規則產生期間要執行的操作	402
自動規則產生完成後要執行的操作	404

限制工作使用範圍

► 要限制“應用程式啟動控制規則產生器”工作的範圍：

1. 開啟“內容：應用程式啟動控制規則產生器”視窗（請參見第 [377](#) 頁上的“開啟“應用程式啟動控制規則產生器”工作精靈和內容”部分）。
2. 配置以下工作設定：

- **基於正在執行的應用程式建立允許規則。**

此核取方塊用於啟用或停用為已經執行的應用程式建立應用程式啟動控制規則。如果電腦有一組您想要據其建立允許規則的範本應用程式，則建議使用此選項。

如果選中此核取方塊，則將根據正在執行的應用程式建立應用程式啟動控制允許規則。

如果清除此核取方塊，則在建立允許規則時，不考慮正在執行的應用程式。

預設將會選定該核取方塊。

如果在“為以下資料夾中的應用程式建立允許規則”表中未選擇任何資料夾，則無法清除此核取方塊。

- **為以下資料夾中的應用程式建立允許規則。**

您可以使用該表選擇或指定建立應用程式啟動控制規則時要考慮的工作資料夾和可執行檔的類型。該工作將針對位於指定資料夾中的所選類型檔案建立允許規則。

3. 點擊“確定”。

將儲存指定設定。

自動規則產生期間要執行的操作

► 要配置在“應用程式啟動控制規則產生器”工作執行期間 Kaspersky Embedded Systems Security 要執行的操作：

1. 開啟“內容：應用程式啟動控制規則產生器”（請參見第 [377](#) 頁上的“開啟“應用程式啟動控制規則產生器”工作精靈和內容”部分）視窗。
2. 開啟“選項”標籤。
3. 在“產生允許規則時”部分中，配置以下設定：
 - 使用數位憑證

如果選擇此選項，則會在新建立的應用程式啟動控制允許規則設定中將存在數位憑證指定為規則觸發條件。此時，應用程式將允許啟動使用帶數位憑證的檔案啟動的程式。如果希望允許作業系統中信任的任何應用程式啟動，建議使用此選項。

預設選中該選項。

- 使用數位憑證主旨和指紋

此核取方塊用於啟用或停用將檔案數位憑證的主旨和指紋用作觸發應用程式啟動控制允許規則的條件。選中此核取方塊可指定更嚴格的數位憑證驗證條件。

如果選中此核取方塊，為其建立規則的檔案的數位憑證主旨和指紋值設定為觸發允許應用程式啟動控制規則的條件。Kaspersky Embedded Systems Security 將允許使用具有指定指紋和數位憑證的檔案啟動的應用程式。

由於指紋是數位憑證的唯一識別碼且無法偽造，選中此核取方塊會高度限制基於數位憑證觸發允許規則。

如果清除此核取方塊，則在作業系統中任何受信任數位憑證的存在被設定為觸發應用程式啟動控制允許規則的條件。

如果選擇了“使用數位憑證”選項，該核取方塊處於活動狀態。

預設將會選定該核取方塊。

- **憑證遺失則使用**

這是一個下拉清單，如果用於建立規則的檔案沒有數位憑證，則可使用此下拉清單選擇用於觸發應用程式啟動控制允許規則的條件。

- **SHA256 雜湊**。將用於建立規則的檔案的核對總和設定為觸發應用程式啟動控制允許規則的條件。應用程式將允許啟動使用帶指定核對總和的檔案啟動的程式。
- **檔案路徑**。將用於建立規則的檔案的路徑設定為觸發應用程式啟動控制允許規則的條件。此時，應用程式將允許啟動使用位於“設定”部分的“為以下資料夾中的應用程式建立允許規則”表中指定的資料夾中的檔案啟動的程式。

- **使用 SHA256 雜湊**

如果選擇此選項，則會在新建立的應用程式啟動控制允許規則的設定中，將用於建立規則的檔案的核對總和指定為規則觸發條件。應用程式將允許啟動使用帶指定核對總和的檔案啟動的程式。

當產生的規則必須達到最高安全等級 (SHA256 核對總和可能用作唯一檔案 ID) 時，建議使用此選項。使用 SHA256 核對總和作為規則觸發條件會將規則使用範圍限制為一個檔案。

預設清除該選項。

- **為使用者或使用者群組產生規則。**

這是顯示使用者或使用者群組的欄位。應用程式將控制由指定使用者或使用者群組執行的任何應用程式。

預設選擇為“每個人”。

4. 點擊“確定”。

將儲存指定設定。

自動規則產生完成後要執行的操作

► 要配置在“應用程式啟動控制規則產生器”工作完成後 Kaspersky Embedded Systems Security 要執行的操作：

1. 開啟“內容：應用程式啟動控制規則產生器”視窗（請參見第 [377](#) 頁上的“開啟“應用程式啟動控制規則產生器”工作精靈和內容”部分）。
2. 開啟“選項”標籤。
3. 在“工作完成後”部分中，配置以下設定：
 - 將允許規則新增到應用程式啟動控制規則清單。

此核取方塊用於啟用或停用將新建立的允許規則新增到應用程式啟動控制規則清單。當點擊“應用程式啟動控制”節點的詳細資訊視窗中的“應用程式啟動控制規則”連結時，應用程式啟動控制規則清單顯示。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將依據所選的規則新增政策，將“應用程式啟動控制規則產生器”工作建立的規則新增到應用程式啟動控制規則清單中。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不會將新建立的允許規則新增到應用程式啟動控制規則清單中。建立的規則僅匯出至檔案。

預設將會選定該核取方塊。

- **新增原則。**

此下拉清單用於指定用來將新建立的允許規則新增到應用程式啟動控制規則清單的方法。

- **新增到現有規則。** 將規則新增到現有規則清單。將複製具有相同設定的規則。
- **取代現有規則。** 規則會替換清單中的現有規則。
- **與現有規則合併。** 將規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。

預設選中“與現有規則合併”方法。

- 將允許規則匯出到檔案。
- 將電腦詳細資訊新增到檔案名稱。

該核取方塊用於啟用或停用將有關受防護電腦的資訊新增到允許規則將匯出到的檔案的名稱中。

如果選中該核取方塊，應用程式會將受防護電腦名稱以及檔案建立日期和時間新增到匯出檔案的名稱中。

如果清除該核取方塊，應用程式不會將有關受防護電腦的資訊新增到匯出檔案的名稱中。

預設將會選定該核取方塊。

4. 點擊“確定”。

將儲存指定設定。

透過應用程式主控台管理應用程式啟動控制

在本節中，學習如何導航應用程式主控台介面以及如何在本地電腦上配置工作設定。

本章節說明項目

導航	406
配置“應用程式啟動控制”工作設定	407
配置應用程式啟動控制規則	416
配置“應用程式啟動控制規則產生器”工作	423

導航

學習如何透過介面導航到所需工作設定。

本章節說明項目

開啟“應用程式啟動控制”工作設定	406
開啟應用程式啟動控制規則視窗	406
開啟“應用程式啟動控制規則產生器”工作設定	407

開啟“應用程式啟動控制”工作設定

► 要透過應用程式主控台開啟“應用程式啟動控制”一般工作設定：

1. 在應用程式主控台樹狀目錄中，展開“**電腦控制**”節點。
2. 選擇“**應用程式啟動控制**”子節點。
3. 在“**應用程式啟動控制**”子節點的詳細資訊視窗中，點擊“**內容**”連結。

將開啟“**工作設定**”視窗。

開啟應用程式啟動控制規則視窗

► 要透過應用程式主控台開啟應用程式啟動控制規則清單：

1. 在應用程式主控台樹狀目錄中，展開“**電腦控制**”節點。
2. 選擇“**應用程式啟動控制**”子節點。
3. 在“**應用程式啟動控制**”節點的詳細資訊視窗中，點擊“**應用程式啟動控制規則**”連結。

將開啟“**應用程式啟動控制規則**”視窗。

4. 根據需要設定規則清單。

開啟“應用程式啟動控制規則產生器”工作設定

► 要配置“應用程式啟動控制規則產生器”工作：

1. 在應用程式主控台樹狀目錄中，展開“自動規則產生器”節點。
2. 選擇“應用程式啟動控制規則產生器”子節點。
3. 在“應用程式啟動控制規則產生器”子節點的詳細資訊視窗中，點擊“內容”連結。
將開啟“工作設定”視窗。
4. 根據需要配置工作。

伺服器配置“應用程式啟動控制”工作設定

► 要配置一般“應用程式啟動控制”工作設定：

1. 開啟“工作設定”視窗（請參見第 [406](#) 頁上的“開啟‘應用程式啟動控制’工作設定”部分）。
2. 配置以下工作設定：
 - 在“一般”標籤上：
 - “應用程式啟動控制”工作模式（請參見第 [408](#) 頁上的“選擇‘應用程式啟動控制’工作的模式”部分）。
 - 工作中的規則使用範圍（請參見第 [410](#) 頁上的“配置‘應用程式啟動控制’工作的範圍”部分）。
 - KSN 使用（請參見第 [411](#) 頁上的“配置 KSN 使用”部分）。
 - “軟體分發控制”標籤上的軟體分發控制設定（請參見第 [413](#) 頁上的“軟體分發控制”部分）。
 - “排程”和“進階”標籤上的工作啟動排程設定（請參見第 [189](#) 頁上的“配置工作啟動排程設定”部分）。
3. 在“工作設定”視窗中點擊“確定”。
將儲存修改的設定。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在系統稽核記錄中。

本章節說明項目

選擇“應用程式啟動控制”工作的模式	408
配置“應用程式啟動控制”工作的範圍	410
配置 KSN 使用	411
軟體分發控制	413

選擇“應用程式啟動控制”工作的模式

► 要配置“應用程式啟動控制”工作的模式：

1. 開啟“工作設定”（請參見第 [406](#) 頁上的“開啟“應用程式啟動控制”工作設定”部分）視窗。
2. 在“一般”標籤上的“工作模式”下拉清單中，指定工作模式。

在此下拉清單中，可選擇應用程式啟動控制工作的模式：

- **活動。** Kaspersky Embedded Systems Security 使用指定的規則控制已啟動的任何應用程式。
- **僅統計。** Kaspersky Embedded Systems Security 不使用指定的規則控制應用程式啟動。相反，它僅在工作記錄中記錄有關這些啟動的資訊。所有程式均允許啟動。您可以使用此模式根據工作記錄中記錄的封鎖的相關資訊建立應用程式啟動控制規則清單。

預設情況下，“應用程式啟動控制”工作在“僅統計”模式下執行。

3. 清除或選中“為檔案隨後的所有啟動重複執行該檔案第一次啟動時的操作”核取方塊。

此核取方塊用於啟用或停用根據快取中儲存的事件資訊對第二次和後續應用程式啟動嘗試的啟動控制。

如果選中此核取方塊，Kaspersky Embedded Systems Security 將根據工作針對應用程式第一次啟動的結論允許或拒絕應用程式的後續啟動。例如，如果規則允許了第一次應用程式啟動，則有關此操作的資訊將儲存在快取中，第二次和所有後續啟動也將被允許，而不進行重複檢查。

如果清除該核取方塊，Kaspersky Embedded Systems Security 會在每次嘗試啟動應用程式時進行分析該應用程式。

預設將會選定該核取方塊。

每次修改“應用程式啟動控制”工作設定後，Kaspersky Embedded Systems Security 都會建立一個新的快取事件清單。這意味著“應用程式啟動控制”按照目前安全設定執行。

4. 清除或選中“在沒有可執行的指令時拒絕指令解釋器啟動”。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將拒絕命令列編譯器啟動，即使允許編譯器啟動。只有同時滿足以下兩個條件時，才能在沒有指令的情況下啟動命令列編譯器：

- 允許命令列解釋器啟動。
- 要執行的指令獲得允許。

如果清除該核取方塊，Kaspersky Embedded Systems Security 在啟動命令列編譯器時只考慮允許規則。如果未套用任何允許規則或可執行處理程序不受 KSN 信任，啟動將被拒絕。如果套用了允許規則或處理程序受 KSN 信任，則無論是否有要執行的指令，都可以啟動命令列編譯器。

Kaspersky Embedded Systems Security 可辨識以下命令列解釋器：

- cmd.exe
- powershell.exe
- python.exe
- perl.exe

預設取消選定該核取方塊。

5. 點擊“確定”。

將儲存指定設定。

所有啟動程式的嘗試都將被記錄在工作記錄中。

配置“應用程式啟動控制”工作的範圍

► 要定義“應用程式啟動控制”工作的範圍：

1. 開啟“工作設定”（請參見第 [406](#) 頁上的“開啟“應用程式啟動控制”工作設定”部分）視窗。
2. 在“一般”標籤上的“規則使用範圍”部分中，指定以下設定：

- **將規則套用於可執行檔**

該核取方塊用於啟用或停用可執行檔的啟動控制。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用指定的規則（其設定指定可執行檔為範圍）允許或封鎖程式可執行檔的啟動。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不使用指定的規則控制程式可執行檔的啟動。將允許可執行檔啟動。

預設將會選定該核取方塊。

- **監控 DLL 模組的載入**

該核取方塊用於啟用或停用 DLL 模組的載入控制。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用指定的規則（其設定將可執行檔指定為範圍）允許或封鎖 DLL 模組的載入。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不使用指定的規則控制 DLL 模組的載入。將允許 DLL 模組載入。

如果選中“將規則套用於可執行檔”核取方塊，則此核取方塊處於活動狀態。

預設取消選定該核取方塊。

控制 DLL 模組的載入可能影響作業系統的效能。

- **將規則套用於指令碼和 MSI 資料套件**

此核取方塊用於啟用或停用指令碼和 MSI 資料套件的啟動。

如果選中此核取方塊，Kaspersky Embedded Systems Security 將使用指定的規則（其設定將指令碼和 MSI 資料套件指定為範圍）允許或封鎖指令碼和 MSI 資料套件啟動。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不使用指定的規則控制指令碼和 MSI 資料套件的啟動。將允許指令碼和 MSI 資料套件的啟動。預設將會選定該核取方塊。

3. 點擊“確定”。

將儲存指定設定。

配置 KSN 使用

► 要配置“應用程式啟動控制”工作的 KSN 服務的使用：

1. 開啟“工作設定”（請參見第 406 頁上的“開啟“應用程式啟動控制”工作設定”部分）視窗。
2. 在“一般”標籤上的“KSN 使用”部分中，指定 KSN 服務的使用設定：
 - 如果必要，請選擇“拒絕 KSN 不信任的應用程式”核取方塊。

此核取方塊用於啟用或停用根據 KSN 中的應用程式聲譽資料進行應用程式啟動控制。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將封鎖任何在 KSN 中不受信任的應用程式執行。適用於在 KSN 中不受信任的應用程式的應用程式啟動控制允許規則不會被觸發。選中此核取方塊將會提供額外的惡意軟體防護。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 將不考慮 KSN 中不受信任的應用程式的聲譽，並根據適用於此類應用程式的規則允許或封鎖啟動。

預設取消選定該核取方塊。

- 如果必要，請選擇“**允許 KSN 信任的應用程式**”核取方塊。

此核取方塊用於啟用或停用根據 KSN 中的應用程式聲譽資料進行應用程式啟動控制。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將允許在 KSN 中受到信任的應用程式執行。適用於 KSN 信任的應用程式的拒絕應用程式啟動控制規則具有更高優先順序：如果某個應用程式受到 KSN 服務信任，應用程式啟動將被拒絕。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 將不考慮 KSN 信任的應用程式的聲譽，並根據適用於此類應用程式的規則允許或封鎖啟動。

預設取消選定該核取方塊。

- 如果選擇了“**允許 KSN 信任的應用程式**”核取方塊，則請指定可以在 KSN 中啟動應用程式的使用者和/或使用者群組。為此，請執行以下操作：
 - a. 點擊“**編輯**”按鈕。

將開啟標準的 Microsoft Windows“**選擇使用者或群組**”視窗。
 - b. 指定使用者和/或使用者群組清單。
 - c. 點擊“**確定**”。

3. 在“**工作設定**”視窗中點擊“**確定**”。

將儲存指定設定。

軟體分發控制

► 要新增受信任分發套件：

1. 開啟“工作設定”（請參見第 406 頁上的“開啟‘應用程式啟動控制’工作設定”部分）視窗。
2. 在“軟體分發控制”標籤上，選中“自動允許為所列應用程式和資料套件分發軟體”核取方塊。

使用此核取方塊可啟用和停用自動建立使用清單中指定的安裝套件啟動的所有檔案的排除項目。

如果選中此核取方塊，應用程式會自動允許受信任安裝套件中的檔案啟動。可以編輯允許啟動的應用程式和分發套件清單。

如果清除此核取方塊，應用程式不會應用清單中指定的排除項目。

預設取消選定該核取方塊。

如果在“應用程式啟動控制”工作設定中選中“一般”標籤中的“將規則套用於可執行檔”核取方塊，則您可選中“自動允許為所列應用程式和資料套件分發軟體”。

3. 根據需要清除“始終允許透過 Windows Installer 進行軟體分發”核取方塊。

此核取方塊用於啟用和停用自動建立透過 Windows Installer 執行的所有檔案的排除項目。

如果選中此核取方塊，透過 Windows Installer 安裝的檔案將始終被允許啟動。

如果清除該核取方塊，檔案將不被允許無條件啟動，即使透過 Windows Installer 啟動它們。

預設將會選定該核取方塊。

如果未選中“自動允許為所列應用程式和資料套件分發軟體”核取方塊，則此核取方塊不可編輯。

僅當在絕對必要時才建議清除“始終允許透過 Windows Installer 進行軟體分發”核取方塊。關閉此功能可能導致更新作業系統檔案出問題，還可能封鎖從分發套件提取的檔案啟動。

4. 如果需要，請選擇“始終允許使用背景智慧傳輸服務透過 SCCM 進行軟體分發”核取方塊。

透過使用 System Center Configuration Manager，該核取方塊可以自動開啟或關閉軟體分發。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 自動允許使用 System Center Configuration Manager 進行 Microsoft Windows 佈署。應用程式僅允許透過背景智慧傳輸服務進行軟體分發。

應用程式可控制具有以下副檔名的物件的啟動：

- .exe
- .msi

預設取消選定該核取方塊。

應用程式控制電腦上從套裝軟體傳送到安裝或更新的軟體分發週期。如果在電腦上安裝應用程式之前已執行分發的任何階段，則應用程式不會控制過程。

5. 要編輯受信任安裝套件的清單，請點擊“變更分發套件清單”，然後在開啟的視窗中選擇以下方法之一：

- **新增一個分發套件。**
 - a. 點擊“瀏覽”按鈕，然後選擇可執行檔或分發套件。

“信任條件”部分會使用有關選定檔案的資料自動進行填充。
 - b. 清除或選中“允許從該分發套件提取鍵中啟動到所有檔案”核取方塊。
 - c. 選擇兩個可用條件選項中的一個，用於決定檔案或安裝套件是否受信任：
 - 使用數位憑證
 - 使用 SHA256 雜湊
- **按雜湊新增多個分發套件。**

您可以選擇無限數量的可執行檔和分發套件，並同時將它們新增到清單。Kaspersky Embedded Systems Security 將檢查雜湊並允許作業系統啟動指定的檔案。

- 變更選定的分發套件。

使用此選項可以選擇不同的可執行檔或分發套件，或變更信任條件。

- 從檔案匯入分發套件清單。

可以從設定檔匯入受信任安裝套件的清單。要使檔案被 Kaspersky Embedded Systems Security 識別，檔案必須滿足以下參數：

- 檔案副檔名為 TXT。
- 檔案包含結構化成行清單的資訊，其中每一行包含的資料用於一個受信任的檔案。
- 檔案必須包含以下格式之一的清單：
 - <檔案名稱> : <SHA256 雜湊>。
 - <SHA256 雜湊> * <檔案名稱>。

在“開啟”視窗中，指定包含受信任安裝套件清單的設定檔。

6. 如果要刪除受信任清單中以前新增的應用程式或分發套件，請點擊“刪除分發套件”按鈕。將允許執行提取檔案。

要封鎖提取檔案啟動，請在受防護電腦上移除應用程式，或在應用程式啟動控制工作設定中建立拒絕規則。

7. 點擊“確定”。

將儲存新配置的設定。

配置應用程式啟動控制規則

瞭解如何使用“應用程式啟動控制”工作建立、匯入和匯出規則清單，或手動建立允許或拒絕規則。

本章節說明項目

新增應用程式啟動控制規則.....	416
啟用預設允許模式.....	420
根據“應用程式啟動控制”工作事件建立允許規則.....	420
匯出應用程式啟動控制規則.....	421
從 XML 設定檔匯入應用程式啟動控制規則.....	421
刪除應用程式啟動控制規則.....	422

新增應用程式啟動控制規則

► 要新增應用程式啟動控制規則，請執行以下步驟：

1. 開啟“應用程式啟動控制規則”視窗。
2. 點擊“新增”按鈕。
3. 在按鈕的內容功能表中，選擇“新增一項規則”。

將開啟“規則設定”視窗。

4. 指定以下設定：
 - a. 在“名稱”欄位中，輸入規則的名稱。
 - b. 在“類型”下拉清單中，選擇規則類型：
 - **允許**，如果您希望規則根據規則設定中指定的條件允許應用程式啟動。
 - **拒絕**，如果您希望規則根據規則設定中指定的條件封鎖應用程式啟動。

- c. 在“**範圍**”下拉清單中，選擇將由規則控制執行的檔案類型：
- **可執行檔**，如果您希望規則控制可執行檔的啟動。
 - **指令碼和 MSI 資料套件**，如果希望規則控制指令碼和 MSI 資料套件的啟動。
- d. 在“**使用者或群組**”欄位中，指定根據規則類型將允許或不允許啟動程式的使用者。為此，請執行以下操作：
- i. 點擊“**瀏覽**”按鈕。
 - ii. 將開啟標準 Microsoft Windows“**選擇使用者或群組**”視窗。
 - iii. 指定使用者和/或使用者群組清單。
 - iv. 點擊“**確定**”。
- e. 如果您希望從特定檔案獲取“**規則觸發條件**”部分中列出的規則觸發條件的值：
- i. 點擊“**從檔案內容設定規則觸發條件**”按鈕。
將開啟標準 Microsoft Windows“**開啟**”視窗。
 - ii. 選擇檔案。
 - iii. 點擊“**開啟**”按鈕。
檔案中的條件值顯示在“**規則觸發條件**”部分的欄位中。預設選擇檔案內容中提供有其資料的條件。
- f. 在“**規則觸發條件**”部分中，選擇以下選項之一：
- **數位憑證**，如果您希望規則控制使用數位憑證簽章的檔案啟動的應用程式的啟動：
 - 如果您希望規則控制由僅具有指定標題的數位憑證簽章的檔案的啟動，請選中“**使用主旨**”核取方塊。
 - 如果您希望規則僅控制使用具有指定指紋的數位憑證簽章的檔案的啟動，請選中“**使用指紋**”核取方塊。
 - **SHA256 雜湊**，如果您希望規則控制使用其核對總和與指定值比對的檔案啟動的程式的啟動。
 - **檔案路徑**，如果您希望規則控制使用位於指定路徑的檔案啟動的程式的啟動。

Kaspersky Embedded Systems Security 無法辨識包含斜線“/”的路徑。請使用反斜線“\”來正確輸入路徑。

- g. 如果希望新增規則排除：
- i. 在“**從規則排除**”部分中，點擊“**新增**”按鈕。
將開啟“**從規則排除**”視窗。
 - ii. 在“**名稱**”欄位中，輸入排除項目的名稱。
 - iii. 指定從應用程式啟動控制規則中排除應用程式檔案的設定。可點擊“**基於檔案內容設定排除**”按鈕從檔案內容填充設定欄位。

- **數位憑證**

如果選擇此選項，則會在新建立的應用程式啟動控制允許規則設定中將存在數位憑證指定為規則觸發條件。此時，應用程式將允許啟動使用帶數位憑證的檔案啟動的程式。如果希望允許作業系統中信任的任何應用程式啟動，建議使用此選項。

預設選中該選項。

- **使用主旨**

該核取方塊可啟用或停用使用數位憑證的主旨作為規則觸發條件。

如果選中該核取方塊，則使用指定的數位憑證主旨作為規則觸發條件。建立的規則將僅控制主旨中指定的供應商的應用程式的啟動。

如果清除該核取方塊，應用程式將不會使用數位憑證的主旨作為規則觸發條件。如果選擇“**數位憑證**”條件，建立的規則將控制使用包含任何主旨的數位憑證簽章的應用程式的啟動。

只能使用位於“**規則觸發條件**”部分上方的“**從檔案內容設定規則觸發條件**”按鈕透過所選檔案的內容指定用於對檔案進行簽章的數位憑證的主旨。

預設取消選定該核取方塊。

- **使用指紋**

該核取方塊可啟用/停用使用數位憑證的指紋作為規則觸發條件。

如果選中該核取方塊，則使用指定的數位憑證指紋作為規則觸發條件。建立的規則將控制使用帶指定指紋的數位憑證簽章的應用程式的啟動。

如果清除該核取方塊，應用程式將不會使用數位憑證的指紋作為規則觸發條件。如果選擇“**數位憑證**”條件，應用程式將控制使用具有任何指紋的數位憑證簽章的應用程式的啟動。

只能使用位於“**規則觸發條件**”部分上方的“**從檔案內容設定規則觸發條件**”按鈕透過所選檔案的內容指定用於對檔案進行簽章的數位憑證的指紋。

預設取消選定該核取方塊。

- **SHA256 雜湊**

如果選擇此選項，則會在新建立的應用程式啟動控制允許規則的設定中，將用於建立規則的檔案的核對總和指定為規則觸發條件。應用程式將允許啟動使用帶指定核對總和的檔案啟動的程式。

當產生的規則必須達到最高安全等級（SHA256 核對總和可能用作唯一檔案 ID）時，建議使用此選項。使用 SHA256 核對總和作為規則觸發條件會將規則使用範圍限制為一個檔案。

預設清除該選項。

- **檔案路徑**

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用檔案的完整路徑來確定處理程序是否受信任。

如果清除該核取方塊，則不使用檔案的路徑來確定處理程序是否受信任。

預設取消選定該核取方塊。

- i. 點擊“**確定**”。
- ii. 如有必要，重複步驟 (i)-(iv) 以新增更多排除。

5. 在“**規則設定**”視窗中點擊“**確定**”。

建立的規則顯示在“**應用程式啟動控制規則**”視窗中的清單中。

啟用預設允許模式

預設允許模式允許所有應用程式啟動，只要它們未被規則或被 KSN 的不受信任結論封鎖。可以透過新增特定允許規則來啟用預設允許模式。您可以僅為指令碼或為所有可執行檔啟用“預設允許”模式。

► 要新增預設允許規則：

1. 開啟“應用程式啟動控制規則”視窗。
2. 點擊“新增”按鈕。
3. 在按鈕的內容功能表中，選擇“新增一項規則”。
將開啟“規則設定”視窗。
4. 在“名稱”欄位中，輸入規則的名稱。
5. 在“類型”下拉清單中，選擇“允許”規則類型。
6. 在“範圍”下拉清單中，選擇將由規則控制執行的檔案類型：
 - 可執行檔，如果希望規則控制可執行檔的啟動。
 - 指令碼和 MSI 資料套件，如果希望規則控制指令碼和 MSI 資料套件的啟動。
7. 在“規則觸發條件”部分中，選擇“檔案路徑”選項。
8. 輸入以下遮罩：?:\
9. 在“規則設定”視窗中點擊“確定”。

Kaspersky Embedded Systems Security 將套用預設允許模式。

根據“應用程式啟動控制”工作事件建立允許規則

► 要建立包含根據“應用程式啟動控制”工作事件建立的允許規則的設定檔：

1. 以“僅統計”模式啟動“應用程式啟動控制”工作(請參見第 408 頁上的“選擇‘應用程式啟動控制’工作的執行模式”部分)，以便在工作記錄中記錄有關受防護電腦上的所有應用程式啟動的資訊。
2. 當工作在“僅統計”模式下執行完成後，透過點擊“應用程式啟動控制”節點詳細資訊窗格的“管理”部分中的“開啟工作記錄”按鈕，開啟工作記錄。

3. 在“記錄”視窗中，點擊“基於事件建立規則”。

Kaspersky Embedded Systems Security 將會建立一個 XML 設定檔，其中包含基於“僅統計”模式下的“應用程式啟動控制”工作事件的規則清單。您可以在“應用程式啟動控制”工作中套用此規則清單（請參見第 [421](#) 頁上的“從 XML 檔案匯入應用程式啟動控制規則”部分）。

在應用根據記錄的工作事件建立的規則清單前，建議檢視並手動處理清單，以確定指定規則允許關鍵檔案（例如系統檔案）啟動。

無論工作模式如何，所有工作事件都將記錄在工作記錄中。您可以根據當工作在“活動”模式下執行時所建立的記錄來建立包含規則清單的設定檔。除了緊急情況外，不建議使用此方案，因為在“活動”模式下執行工作前必須建立最終規則清單才能使其生效。

匯出應用程式啟動控制規則

► 要將應用程式啟動控制規則匯出到設定檔：

1. 開啟“應用程式啟動控制規則”視窗。
2. 點擊“匯出至檔案”按鈕。

將開啟標準的 Microsoft Windows 視窗。

3. 在開啟的視窗中，指定想要將規則匯出到其中的檔案。如果不存在此類檔案，則將建立它。如果具有指定名稱的檔案已存在，其內容在規則匯出後將被覆蓋。

4. 點擊“儲存”按鈕。

規則設定將匯出到指定檔案。

從 XML 設定檔匯入應用程式啟動控制規則

► 要匯入應用程式啟動控制規則：

1. 開啟“應用程式啟動控制規則”視窗。
2. 點擊“新增”按鈕。

3. 在按鈕的內容功能表中，選擇“從 XML 檔案匯入規則”。
4. 指定新增匯入規則的方法。要執行此操作，請從“從 XML 檔案匯入規則”按鈕的內容功能表中選擇一個選項：
 - **新增到現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
 - **取代現有規則**，如果您希望將現有規則取代為匯入的規則。
 - **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。

將開啟標準 Microsoft Windows“開啟”視窗。

5. 在“開啟”視窗中，選擇包含應用程式啟動控制規則的 XML 檔案。
6. 點擊“開啟”按鈕。

匯入的規則將顯示在“應用程式啟動控制規則”視窗中的清單中。

刪除應用程式啟動控制規則

► *要刪除應用程式啟動控制規則：*

1. 開啟“應用程式啟動控制規則”視窗。
2. 在清單中，選擇要刪除的一項或多項規則。
3. 點擊“刪除選取的項目”按鈕。
4. 點擊“儲存”按鈕。

將刪除所選應用程式啟動控制規則。

配置“應用程式啟動控制規則產生器”工作

► 要配置“應用程式啟動控制規則產生器”工作設定：

1. 開啟“應用程式啟動控制規則產生器”工作的“工作設定”視窗(請參見第 [407](#) 頁上的“開啟‘應用程式啟動控制規則產生器’工作設定”部分)。

2. 配置以下設定：

- 在“一般”標籤上：
 - 指定規則名稱前置詞。

這是規則名稱的第一部分。規則名稱的第二部分由允許啟動的物件的名稱構成。

預設前置詞是安裝 Kaspersky Embedded Systems Security 的電腦的名稱。您可以變更允許規則的名稱前置詞。

- 配置允許規則使用範圍(請參見第 [424](#) 頁上的“限制工作使用範圍”部分)。
- 在“操作”標籤上，指定 Kaspersky Embedded Systems Security 必須執行的操作：
 - 產生允許規則時(請參見第 [425](#) 頁上的“自動規則建立期間要執行的操作”部分)。
 - 工作完成後(請參見第 [427](#) 頁上的“自動規則建立過程完成後要執行的操作”部分)。
- 在“排程”和“進階”標籤上，配置排程的工作啟動設定(請參見第 [189](#) 頁上的“配置工作啟動排程設定”部分)。
- 在“執行帳戶”標籤上，配置工作啟動設定及帳戶權限(請參見第 [192](#) 頁上的“指定使用者帳戶以啟動工作”部分)。

3. 點擊“確定”。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊。

本章節說明項目

限制工作使用範圍	424
自動規則產生期間要執行的操作	425
自動規則產生完成後要執行的操作	427

限制工作使用範圍

► 要限制“應用程式啟動控制規則產生器”工作的範圍：

1. 開啟“應用程式啟動控制規則產生器”工作的“工作設定”視窗(請參見第 [407](#) 頁上的“開啟‘應用程式啟動控制規則產生器’工作設定”部分)。

2. 配置以下工作設定：

- **基於正在執行的應用程式建立允許規則。**

此核取方塊用於啟用或停用為已經執行的應用程式建立應用程式啟動控制規則。如果電腦有一組您想要據其建立允許規則的範本應用程式，則建議使用此選項。

如果選中此核取方塊，則將根據正在執行的應用程式建立應用程式啟動控制允許規則。

如果清除此核取方塊，則在建立允許規則時，不考慮正在執行的應用程式。

預設將會選定該核取方塊。

如果在“為以下資料夾中的應用程式建立允許規則”表中未選擇任何資料夾，則無法清除此核取方塊。

- **為以下資料夾中的應用程式建立允許規則。**

您可以使用該表選擇或指定建立應用程式啟動控制規則時要考慮的工作資料夾和可執行檔的類型。該工作將針對位於指定資料夾中的所選類型檔案建立允許規則。

3. 點擊“確定”。

將儲存指定設定。

自動規則產生期間要執行的操作

► 要配置在“應用程式啟動控制規則產生器”工作執行期間 Kaspersky Embedded Systems Security 要執行的操作：

1. 開啟“應用程式啟動控制規則產生器”工作的“工作設定”視窗(請參見第 407 頁上的“開啟‘應用程式啟動控制規則產生器’工作設定”部分)。
2. 開啟“選項”標籤。
3. 在“產生允許規則時”部分中，配置以下設定：
 - 使用數位憑證

如果選擇此選項，則會在新建立的應用程式啟動控制允許規則設定中將存在數位憑證指定為規則觸發條件。此時，應用程式將允許啟動使用帶數位憑證的檔案啟動的程式。如果希望允許作業系統中信任的任何應用程式啟動，建議使用此選項。

預設選中該選項。

- 使用數位憑證主旨和指紋

此核取方塊用於啟用或停用將檔案數位憑證的主旨和指紋用作觸發應用程式啟動控制允許規則的條件。選中此核取方塊可指定更嚴格的數位憑證驗證條件。

如果選中此核取方塊，為其建立規則的檔案的數位憑證主旨和指紋值設定為觸發允許應用程式啟動控制規則的條件。Kaspersky Embedded Systems Security 將允許使用具有指定指紋和數位憑證的檔案啟動的應用程式。

由於指紋是數位憑證的唯一識別碼且無法偽造，選中此核取方塊會高度限制基於數位憑證觸發允許規則。

如果清除此核取方塊，則在作業系統中任何受信任數位憑證的存在被設定為觸發應用程式啟動控制允許規則的條件。

如果選擇了“使用數位憑證”選項，該核取方塊處於活動狀態。

預設將會選定該核取方塊。

- **憑證遺失則使用**

這是一個下拉清單，如果用於建立規則的檔案沒有數位憑證，則可使用此下拉清單選擇用於觸發應用程式啟動控制允許規則的條件。

- **SHA256 雜湊**。將用於建立規則的檔案的核對總和設定為觸發應用程式啟動控制允許規則的條件。應用程式將允許啟動使用帶指定核對總和的檔案啟動的程式。
- **檔案路徑**。將用於建立規則的檔案的路徑設定為觸發應用程式啟動控制允許規則的條件。此時，應用程式將允許啟動使用位於“設定”部分的“為以下資料夾中的應用程式建立允許規則”表中指定的資料夾中的檔案啟動的程式。

- **使用 SHA256 雜湊**

如果選擇此選項，則會在新建立的應用程式啟動控制允許規則的設定中，將用於建立規則的檔案的核對總和指定為規則觸發條件。應用程式將允許啟動使用帶指定核對總和的檔案啟動的程式。

當產生的規則必須達到最高安全等級 (SHA256 核對總和可能用作唯一檔案 ID) 時，建議使用此選項。使用 SHA256 核對總和作為規則觸發條件會將規則使用範圍限制為一個檔案。

預設清除該選項。

- **為使用者或使用者群組產生規則。**

這是顯示使用者或使用者群組的欄位。應用程式將控制由指定使用者或使用者群組執行的任何應用程式。

預設選擇為“每個人”。

4. 點擊“確定”。

將儲存指定設定。

自動規則產生完成後要執行的操作

► 要配置在“應用程式啟動控制規則產生器”工作完成後 Kaspersky Embedded Systems Security 要執行的操作：

1. 開啟“應用程式啟動控制規則產生器”工作的“工作設定”視窗(請參見第 407 頁上的“開啟‘應用程式啟動控制規則產生器’工作設定”部分)。
2. 開啟“選項”標籤。
3. 在“工作完成後”部分中，配置以下設定：
 - 將允許規則新增到應用程式啟動控制規則清單。

此核取方塊用於啟用或停用將新建立的允許規則新增到應用程式啟動控制規則清單。當點擊“應用程式啟動控制”節點的詳細資訊視窗中的“應用程式啟動控制規則”連結時，應用程式啟動控制規則清單顯示。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將依據所選的規則新增政策，將“應用程式啟動控制規則產生器”工作建立的規則新增到應用程式啟動控制規則清單中。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不會將新建立的允許規則新增到應用程式啟動控制規則清單中。建立的規則僅匯出至檔案。

預設將會選定該核取方塊。

- **新增原則。**

此下拉清單用於指定用來將新建立的允許規則新增到應用程式啟動控制規則清單的方法。

- **新增到現有規則。** 將規則新增到現有規則清單。將複製具有相同設定的規則。
- **取代現有規則。** 規則會替換清單中的現有規則。
- **與現有規則合併。** 將規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。

預設選中“與現有規則合併”方法。

- 將允許規則匯出到檔案。
- 將電腦詳細資訊新增到檔案名稱。

該核取方塊用於啟用或停用將有關受防護電腦的資訊新增到允許規則將匯出到的檔案的名稱中。

如果選中該核取方塊，應用程式會將受防護電腦名稱以及檔案建立日期和時間新增到匯出檔案的名稱中。

如果清除該核取方塊，應用程式不會將有關受防護電腦的資訊新增到匯出檔案的名稱中。

預設將會選定該核取方塊。

4. 點擊“確定”。

將儲存指定設定。

裝置控制

本節包含有關裝置控制工作的資訊以及配置工作設定的說明。

本章內容

關於裝置控制工作	429
關於裝置控制規則	431
關於裝置控制規則清單填充	433
關於裝置控制規則產生器工作	435
裝置控制規則建立方案	435
“裝置控制”工作預設設定	436
透過管理外掛程式管理裝置控制	437
透過應用程式主控台管理裝置控制	450

關於裝置控制工作

Kaspersky Embedded Systems Security 控制大容量儲存裝置和 CD/DVD 磁碟機的註冊和使用，以防護電腦免受電腦安全性威脅的侵害，與快閃記憶體磁碟機或透過 USB 連線的其他類型的外部裝置進行檔案交換的過程中可能出現這些威脅。大容量儲存是可連線到電腦以複製或儲存檔案的外部裝置。

Kaspersky Embedded Systems Security 控制以下 USB 外部裝置連線：

- USB 連線的快閃記憶體磁碟機
- CD/DVD ROM 磁碟機
- USB 連線的軟碟磁碟機
- USB 連線的 MTP 行動裝置

Kaspersky Embedded Systems Security 會通知您透過 USB 連線的所有裝置，並在工作和事件記錄中記錄相應事件。事件詳細資訊包括裝置類型和連線路徑。“裝置控制”工作啟動後，Kaspersky Embedded Systems Security 將檢查並列出透過 USB 連線的所有裝置。您可以在卡巴斯基安全管理中心通知設定部分中配置通知。

“裝置控制”工作監控外部裝置透過 USB 連線到受防護電腦的所有連線嘗試，如果沒有此類裝置的允許規則，則封鎖連線。封鎖連線後，裝置將不可用。

應用程式為每個連線的大容量儲存裝置規定了以下狀態之一：

- **受信任。** 您想允許其進行檔案交換的裝置。產生規則清單後，**裝置實例路徑**值將包含在至少一個規則的使用範圍中。
- **不受信任。** 您想限制其進行檔案交換的裝置。裝置實例路徑不會包含在任何允許規則的使用範圍中。

您可以使用“裝置控制規則產生器”工作為外部裝置建立允許規則，以允許資料交換。您還可以延伸已指定規則的使用範圍。不能手動建立允許規則。

Kaspersky Embedded Systems Security 使用裝置實例路徑值標識在系統中註冊的大容量儲存裝置。裝置實例路徑是專門為每個外部裝置指定的預設功能。將在每個外部裝置的 Windows 內容中為其指定“裝置實例路徑”值，並且該值將在產生規則期間由 Kaspersky Embedded Systems Security 自動確定。

裝置控制工作可在兩種模式下執行：

- **活動。** Kaspersky Embedded Systems Security 會將規則套用於控制快閃記憶體磁碟機和其他外部裝置的連線，並根據預設拒絕政策和指定允許規則允許或封鎖使用所有裝置。允許使用受信任外部裝置。預設情況下，封鎖使用不受信任的外部裝置。

如果當“裝置控制”工作在**活動**模式下執行前您認為不受信任的外部裝置連線到受防護電腦，應用程式不會封鎖該裝置。建議您手動斷開不信任裝置或重新啟動電腦。否則，不會將“預設拒絕”原則套用於裝置。

- **僅統計.**Kaspersky Embedded Systems Security 不會控制快閃記憶體磁碟機和其他外部裝置的連線，但僅記錄有關外部裝置在受防護電腦上的連接和註冊，以及有關相連裝置觸發的裝置控制允許規則的資訊。允許使用所有外部裝置。預設設定此模式。

您可以基於工作執行期間記錄的有關封鎖的資訊對規則建立套用此模式（請參見第 [455](#) 頁上的“基於裝置控制工作事件填寫規則清單”部分）。

關於裝置控制規則

如果目前連線到或曾經連線到受防護電腦的每台裝置的資訊儲存在系統登錄檔中，將為每台裝置建立具有唯一性的規則。

要為裝置控制建立允許規則，可以執行以下操作：

- 套用“裝置控制規則產生器”工作（請參見第 [435](#) 頁上的“關於裝置控制規則產生器工作”部分）。
- 以“僅統計”模式執行裝置控制工作（請參見第 [455](#) 頁上的“基於裝置控制工作事件填寫規則清單”部分）。
- 應用有關之前連線的裝置的系統資訊（請參見第 [456](#) 頁上的“為一個或多個外部裝置新增允許規則”部分）。
- 延伸已指定規則的使用範圍（請參見第 [458](#) 頁上的“延伸裝置控制規則使用範圍”部分）。

Kaspersky Embedded Systems Security 支援的裝置控制規則的最大數量為 3072。

下文介紹了裝置控制規則。

規則類型

規則類型允許為 *允許*。如果快閃記憶體磁碟機和其他外部裝置不包含在任何允許規則的使用範圍內，預設情況下，裝置控制工作會封鎖所有這些裝置連線。

觸發條件和規則使用範圍

裝置控制規則基於 *裝置實例路徑* 識別快閃記憶體磁碟機和其他外部裝置。裝置實例路徑是裝置建立連接並註冊為大容量儲存裝置或 CD/DVD 光碟機（例如，IDE 或 SCSI）時系統分配給裝置的唯一條件。

無論用於連線的匯流排如何，Kaspersky Embedded Systems Security 都控制 CD/DVD 磁碟機的連線。當透過 USB 安裝此類裝置時，作業系統會註冊兩個裝置實例路徑值：針對大容量儲存裝置和針對 CD/DVD 光碟機（例如，IDE 或 SCSI）。要直接連接此類裝置，必須設定每個實例路徑值的允許規則。

Kaspersky Embedded Systems Security 自動定義裝置實例路徑並將獲取的值解析為以下元素：

- 裝置製造商 (VID)
- 裝置控制器類型 (PID)
- 裝置序號

您不能手動設定裝置實例路徑。允許規則觸發條件定義規則使用範圍。預設情況下，新建立的規則使用範圍包括一台初始裝置，具體是哪台裝置取決於 Kaspersky Embedded Systems Security 基於哪台裝置的內容建立該規則。您可以配置建立的規則設定中的值並使用遮罩延伸規則使用範圍（請參見第 [458](#) 頁上的“延伸裝置控制規則使用範圍”部分）。

初始裝置值

Kaspersky Embedded Systems Security 用於建立允許規則以及在 Windows 裝置管理器中為每台連線的裝置顯示的裝置內容。

初始裝置值包含以下資訊：

- **裝置實例路徑。** Kaspersky Embedded Systems Security 根據此內容定義規則觸發條件並填寫以下欄位：“規則內容”視窗的“規則使用範圍”部分中的“製造商 (VID)”、“控制器類型 (PID)”和“序號”。
- **易記名稱。** 裝置製造商在裝置內容中設定的明確名稱。

Kaspersky Embedded Systems Security 會在建立規則時自動定義初始裝置值。以後您可以使用這些值識別產生規則時所依據的裝置。初始裝置值無法編輯。

敘述

您可以在“敘述”欄位中為建立的每個裝置控制規則新增更多資訊，例如，您可以記錄所連線的快閃記憶體磁碟機的名稱或定義其擁有者。敘述顯示在“裝置控制規則”視窗內的相應圖表中。

敘述和初始設定值不用於觸發規則，只為了說明使用者識別裝置。

關於裝置控制規則清單填充

您可以從在“裝置控制”或“裝置控制規則產生器”工作執行期間自動建立的 XML 檔案匯入裝置控制允許規則。

預設情況下，如果任何快閃記憶體磁碟機或其他外部裝置不包含在指定的裝置控制規則的使用範圍內，Kaspersky Embedded Systems Security 會限制這些裝置的連線。

表 49. 裝置控制規則清單建立的目標和方案

規則建立方案	目標
裝置控制規則產生器工作	<ul style="list-style-type: none"> 在裝置控制工作第一次啟動之前，為之前連接受信任裝置新增允許規則。 為受防護電腦網路中的受信任裝置產生規則清單。
基於系統資料的規則產生	為一個或多個新連線的裝置新增允許規則。
“僅統計”模式中的裝置控制工作	為大量受信任裝置建立允許規則。

裝置控制規則產生器工作使用

在“裝置控制規則產生器”工作完成時建立的 XML 檔案包含其資料曾儲存在系統登錄檔中的那些快閃記憶體磁碟機和其他外部裝置的允許規則。

在工作執行期間，Kaspersky Embedded Systems Security 會收到有關之前曾連線過或目前連接到受防護電腦的所有大容量儲存裝置的系統資料，並基於偵測到的裝置的系統資料建立允許規則清單。在工作完成時，應用程式會在資料夾中建立 XML 檔案，該資料夾位於工作設定中指定的路徑。您可設定將建立的規則自動匯入“裝置控制”工作的規則清單。

建議在裝置控制工作第一次啟動之前使用此方案建立允許規則清單，以便建立的允許規則涵蓋受防護電腦上使用的所有受信任外部裝置。

使用有關所有連線的裝置的系統資料

在工作執行期間，Kaspersky Embedded Systems Security 會收到有關曾經或目前連線到受防護電腦的所有外部裝置的系統資料，並在“基於系統資訊產生規則”視窗的清單中顯示偵測到的裝置。

對於偵測到的每個裝置，Kaspersky Embedded Systems Security 會分析製造商 (VID)、控制器類型 (PID)、易記名稱、序號和裝置實例路徑的值。您可以為其資料儲存在系統中的任何大容量儲存裝置建立允許規則，並直接將新建立的規則新增到裝置控制規則清單中。

如果必須信任少量新大容量儲存裝置，建議使用此方案更新已經指定的規則清單。

Kaspersky Embedded Systems Security 無法存取透過 MTP 連線的行動裝置的系統資料。無法為 MTP 連線的行動裝置建立允許規則。

“僅統計”模式中的裝置控制工作的使用

將基於工作記錄建立在“僅統計”模式的裝置控制工作完成時收到的 XML 檔案。

在工作執行期間，Kaspersky Embedded Systems Security 會記錄有關與受防護電腦連線的快閃記憶體磁碟機和其他大容量儲存裝置的資訊。您可以基於工作事件建立允許規則並將它們匯出到 XML 檔案。以“僅統計”模式啟動工作之前，建議您配置工作執行時段，以便在該時段內，將執行與受防護電腦的所有可能的外部裝置連線。

如果需要允許大量新的外部裝置，建議使用此方案更新已經建立的規則清單。

如果根據此方案在範本機上產生規則清單，您可以在透過卡斯基安全管理中心配置“裝置控制”工作時應用建立的允許規則清單。這樣，您可以允許在納入受防護網路中的所有電腦上使用連接到範本機的外部裝置。

關於裝置控制規則產生器工作

“裝置控制規則產生器”工作可以基於有關曾連線到受防護電腦的所有外部裝置的系統資料，自動為連線的快閃記憶體磁碟機和其他大容量儲存裝置建立允許規則清單。

Kaspersky Embedded Systems Security 無法存取透過 MTP 連線的行動裝置的系統資料。無法為 MTP 連線的行動裝置建立允許規則。

在工作完成後，Kaspersky Embedded Systems Security 會建立一個 XML 設定檔，其中包含所有偵測到的外部裝置的允許規則清單，或者直接在“裝置控制”清單中新增建立的規則，具體取決於“裝置控制規則產生器”設定。隨後，應用程式將允許自動為其建立允許規則的裝置。

建立的規則和新增到工作中的規則顯示在“**裝置控制規則**”視窗中。

裝置控制規則建立方案

您可以使用三個方案，基於有關曾經或目前連線的所有大容量儲存的 Windows 資料建立規則（請參見第 441 頁上的“透過卡巴斯基安全管理中心建立所有電腦的裝置控制規則”部分）：

- 使用“裝置控制規則產生器”群組工作。可在規則建立過程中使用此方案，以便將所有曾經連接過的、由所有網路電腦上的系統註冊的大容量儲存裝置考慮在內。
- 使用“基於系統資料產生規則”選項。可在規則建立過程中使用此方案，以便將所有曾經連接過的、由安裝卡巴斯基安全管理中心管理主控台的電腦上的系統註冊的大容量儲存裝置考慮在內。
- 使用“裝置控制規則”視窗和“裝置控制規則產生器”工作設定中的“基於連接的裝置產生規則”。產生允許規則時，如果想要僅考慮目前已連線到受防護電腦上的裝置的有關資料，請使用此方法。

Kaspersky Embedded Systems Security 無法存取透過 MTP 連線的行動裝置的系統資料。您不能使用基於有關所有連線的裝置的系統資料的規則清單填寫方案，為透過 MTP 連線的行動裝置建立允許規則。

“裝置控制”工作預設設定

預設情況下，“裝置控制”工作具有下表所述的設定。您可以變更這些設定值。

表 50. 預設裝置控制工作設定

設定	預設值	敘述
工作模式	僅統計	該工作記錄有關根據指定的規則封鎖或允許的外部裝置的資訊。實際上，不會封鎖外部裝置。 您可以為電腦防護選擇“活動”模式以實際封鎖使用外部裝置。
當未執行裝置控制工作時允許使用所有大容量儲存裝置	未套用	無論裝置控制工作狀態如何，Kaspersky Embedded Systems Security 都封鎖使用外部裝置。這會以最大限度防護您的電腦在與外部裝置交換檔案時免受安全威脅。 您可以調整設定，以便 Kaspersky Embedded Systems Security 在裝置控制工作未執行時允許使用所有外部裝置。
工作啟動排程	不設定工作的初次啟動排程。	“裝置控制”工作不會在 Kaspersky Embedded Systems Security 啟動時自動啟動。 您可以配置工作啟動排程。

表 51. “裝置控制規則產生器”工作的預設設定

設定	預設值	敘述
----	-----	----

設定	預設值	敘述
工作模式	考慮曾經連接過的所有大容量記憶體的系統資料	工作執行模式。 您可以選擇“僅考慮目前連線的大容量儲存”工作模式。
工作完成時的操作	將允許規則新增到裝置控制規則清單；新規則與現有規則合併；刪除重複的規則。	您可以將規則新增到現有規則，而不進行合併並刪除重複的規則，或將現有規則替換為新的允許規則，或設定將允許規則匯出到檔案。
工作啟動排程	不設定工作的初次啟動排程。	“裝置控制規則產生器”工作不會在 Kaspersky Embedded Systems Security 啟動時自動啟動。您可以手動啟動該工作或設定排程啟動。

透過管理外掛程式管理裝置控制

在本節中，學習如何透過管理外掛程式介面進行導航，以及如何透過卡巴斯基安全管理中心為電腦群組建立規則清單來管理任意大容量儲存裝置與網路上所有電腦的連線。

本章節說明項目

導航	438
配置“裝置控制”工作	440
透過卡巴斯基安全管理中心建立所有電腦的裝置控制規則	441
配置“裝置控制規則產生器”工作	443
透過卡巴斯基安全管理中心配置裝置控制規則	444

導航

學習如何透過介面導航到所需工作設定。

本章節說明項目

開啟“裝置控制”工作的政策設定.....	438
開啟裝置控制規則清單.....	438
開啟“裝置控制規則產生器”工作精靈和內容.....	439

開啟“裝置控制”工作的政策設定

► 要透過卡巴斯基安全管理中心政策開啟“裝置控制”工作設定：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“**政策**”標籤。
4. 點擊要設定的政策名稱。
5. 在開啟的“內容：<政策名稱>”視窗中，選擇“**本機行為控制**”部分。
6. 在“**裝置控制**”子部分中點擊“**設定**”按鈕。

將開啟“**裝置控制**”視窗。

7. 根據需要設定政策。

開啟裝置控制規則清單

► 要透過卡巴斯基安全管理中心開啟裝置控制規則清單：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“**政策**”標籤。

4. 點擊要設定的政策名稱。
5. 在開啟的“內容：<政策名稱>”視窗中，選擇“本機行為控制”部分。
6. 在“裝置控制”子部分中點擊“設定”按鈕。
將開啟“裝置控制”視窗。
7. 在“一般”標籤上，點擊“規則清單”按鈕。
將開啟“裝置控制規則”視窗。
8. 根據需要設定政策。

開啟“裝置控制規則產生器”工作精靈和內容

► 要初始化“裝置控制規則產生器”工作的建立：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“工作”標籤。
4. 點擊“建立工作”按鈕。
將開啟“新建工作精靈”視窗。
5. 選擇“裝置控制規則產生器”工作。
6. 點擊“下一步”。
將開啟“設定”視窗。

► 要配置現有“裝置控制規則產生器”工作：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其設定工作的管理群組。

3. 選擇“工作”標籤。
4. 點擊卡巴斯基安全管理中心工作清單中的工作名稱。

將開啟“內容：裝置控制規則產生器”視窗。

有關配置該工作的詳細資訊，請參見“配置‘裝置控制規則產生器’工作”部分。

配置“裝置控制”工作

► 要配置“裝置控制”工作設定：

1. 開啟“裝置控制”視窗（請參見第 [438](#) 頁上的“開啟“裝置控制”工作的政策設定”部分）。
2. 在“一般”標籤上，配置以下工作設定：
 - 在“工作模式”部分中，選擇以下工作模式之一：

- 活動。

Kaspersky Embedded Systems Security 會將規則套用於控制快閃記憶體磁碟機和其他外部裝置的連線，並根據預設拒絕政策和指定允許規則允許或封鎖使用所有裝置。允許使用受信任外部裝置。預設情況下，封鎖使用不受信任的外部裝置。

如果當“裝置控制”工作在活動模式下執行前您認為不受信任的外部裝置連線到受防護電腦，應用程式不會封鎖該裝置。建議您手動斷開不信任裝置或重新啟動電腦。否則，不會將“預設拒絕”原則套用於裝置。

- 僅統計。

Kaspersky Embedded Systems Security 不會控制快閃記憶體磁碟機和其他外部裝置的連線，但僅記錄有關外部裝置在受防護電腦上的連接和註冊，以及有關相連裝置觸發的裝置控制允許規則的資訊。允許使用所有外部裝置。預設設定此模式。

- 選中或清除“當未執行裝置控制工作時允許使用所有大容量儲存裝置”核取方塊。

使用此核取方塊可允許或封鎖在裝置控制工作未執行時使用大容量儲存裝置。

如果選擇該核取方塊且裝置控制工作未執行，則 Kaspersky Embedded Systems Security 允許在受防護的電腦上使用任何大容量儲存裝置。

如果清除此核取方塊，應用程式在以下情況下將封鎖在受防護電腦上使用不受信任的大容量儲存裝置：“裝置控制”工作未執行或 Kaspersky Security 服務已關閉。建議使用該選項以最大限度防護您的電腦在與外部裝置交換檔案時免受安全威脅。

預設取消選定該核取方塊。

3. 點擊“規則清單”按鈕以編輯裝置控制規則清單(請參見第 444 頁上的“透過卡巴斯基安全管理中心設定裝置控制規則”部分)。
4. 如有必要，在“工作管理”標籤上配置排程的工作啟動設定。
5. 點擊“確定”。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在工作記錄中。

透過卡巴斯基安全管理中心建立所有電腦的裝置控制規則

您可使用卡巴斯基安全管理中心工作立即為公司網路上的所有電腦和電腦群組建立裝置控制規則清單。

您可採用以下方式透過卡巴斯基安全管理中心建立裝置控制規則清單：

- 使用“裝置控制規則產生器”群組工作。

根據此方案，群組工作會基於有關所有曾經連線到受防護電腦的大容量儲存器的各個電腦系統資料產生規則清單。該工作還會考慮在工作執行的那一刻處於連接狀態的所有大容量儲存器。群組工作完成時，Kaspersky Embedded Systems Security 會為在網路中註冊的所有大容量儲存裝置建立允許規則清單，並將這些清單儲存在指定資料夾內的 XML 檔案中。然後，您可以在裝置控制工作設定中手動匯入建立的規則。與本機電腦上的工作不同的是，政策不允許設定在“裝置控制規則產生器”群組工作完成時將建立的規則自動新增到裝置啟動控制規則清單。

建議使用該方案在裝置控制工作首次以應用活動規則模式啟動之前建立允許規則清單。

在網路中使用裝置控制政策之前，請確保所有受防護電腦都能夠存取共用網路資料夾。如果不提供組織的政策用於網路中的共用網路資料夾，則建議為測試電腦群組或範本機上的電腦控制規則啟動“裝置規則產生器”工作。

- 對於在“**僅統計**”模式下執行的“裝置控制”工作，基於卡斯基安全管理中心中建立的工作事件報告。

根據此方案，Kaspersky Embedded Systems Security 不會限制大容量儲存裝置連線，但會記錄當“裝置控制”工作以“**僅統計**”模式執行時所有網路電腦上發生的所有裝置連線和大容量儲存裝置註冊的相關資訊。記錄的資訊可在卡斯基安全管理中心中的“**管理伺服器**”節點的工作區中，選擇“**事件**”標籤中找到。卡斯基安全管理中心會基於工作記錄建立大容量儲存裝置限制和允許事件的統一清單。

您應該配置工作執行時段，在該時段內將允許所有大容量儲存裝置連線。然後，隨著將規則新增到“裝置控制”工作中，您可從儲存的卡斯基安全管理中心事件報告檔案（採用 TXT 格式）匯入有關裝置連線的資料，並基於此資料為此類裝置建立裝置控制允許規則。匯入的記錄所依據的事件種類不會影響建立的規則類型；只建立允許規則。

若要為大量新的大容量儲存裝置新增允許規則以及為透過 MTP 連線的受信任行動裝置產生規則，則建議使用此方案。

- 基於有關所連線的大容量儲存裝置的系統資料（使用裝置控制工作設定中的“**基於系統資料產生規則**”選項）。

根據此方案，Kaspersky Embedded Systems Security 會為曾經或目前連線到安裝有卡斯基安全管理中心的電腦的大容量儲存裝置建立允許規則。

若要為少量您希望在網路中的所有電腦上信任的新的大容量儲存器產生規則，則建議使用此方案。

- 基於目前已連線裝置的有關資料（使用“**基於連接的裝置產生規則**”）。

在本方案中，Kaspersky Embedded Systems Security 僅為目前已連線的裝置建立允許規則。可以選擇要為其產生允許規則的一個或多個裝置。

Kaspersky Embedded Systems Security 無法存取透過 MTP 連線的行動裝置的系統資料。您不能使用基於有關所有連線的裝置的系統資料的規則清單填寫方案，為透過 MTP 連線的行動裝置建立允許規則。

配置“裝置控制規則產生器”工作

► 要配置“裝置控制規則產生器”工作，請執行以下操作：

1. 開啟“內容：裝置控制規則產生器”(請參見第 439 頁上的“開啟‘裝置控制規則產生器’工作精靈”部分) 視窗。
2. 在“通知”部分中，配置工作事件通知設定。

關於此節中配置設定的詳細資訊，請參見卡巴斯基安全管理中心說明。

3. 在“設定”部分中，您可配置以下設定：
 - 選擇執行模式：考慮有關之前曾連線過的所有大容量儲存的系統資料，或僅考慮目前連線的大容量儲存。
 - 使用 Kaspersky Embedded Systems Security 在工作完成時建立的允許規則清單為設定檔配置設定。
4. 在“排程”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。
5. 在“帳戶”部分中，指定將使用其權限執行工作的帳戶。
6. 如有需要，在“工作範圍的排除項目”部分中指定要從工作範圍中排除的物件。

有關此節中配置設定的詳細資訊，請參見卡巴斯基安全管理中心說明。

7. 在“內容：<工作名稱>”視窗中，點擊“確定”。

將儲存新配置的群組工作設定。

透過卡巴斯基安全管理中心配置裝置控制規則

學習如何使用裝置控制工作根據各種條件建立規則清單，或手動建立允許或拒絕規則。

本章節說明項目

基於卡巴斯基安全管理中心政策中的系統資料建立允許規則	444
為已連線的裝置建立規則	445
從有關被封鎖裝置的卡巴斯基安全管理中心報告中匯入規則	445
使用“裝置控制規則產生器”工作建立規則	447
將建立的規則新增到裝置控制規則清單	449

基於卡巴斯基安全管理中心政策中的系統資料建立允許規則

► 要使用裝置控制工作中的“基於系統資料產生規則”選項指定允許規則：

1. 如有必要，將您希望信任的新的大容量儲存裝置連線到安裝了卡巴斯基安全管理中心管理主控台的電腦。
2. 開啟“裝置控制規則”視窗（請參見第 [438](#) 頁上的“開啟裝置控制規則清單”部分）。
3. 點擊“新增”按鈕，在開啟的內容功能表中，選擇“基於系統資料產生規則”選項。
4. 選擇將允許規則新增到先前建立的“裝置控制”規則清單中的政策。
 - 在“基於系統資訊產生規則”視窗中，選擇一個裝置。
 - 點擊“為所選裝置新增規則”按鈕。
5. 在“裝置控制規則”視窗中點擊“儲存”按鈕。

“裝置控制”工作中的規則清單將使用基於安裝了卡巴斯基安全管理中心管理主控台的電腦的系統資料建立的新規則填充。

為已連線的裝置建立規則

► 要使用裝置控制工作中的“基於連接的裝置產生規則”選項指定允許規則：

1. 開啟“裝置控制規則”（請參見第 [438](#) 頁上的“開啟裝置控制規則清單”部分）。

2. 點擊“新增”按鈕，然後在內容功能表中，選擇“基於連接的裝置產生規則”。

將開啟“基於系統資訊產生規則”視窗。

3. 在偵測到的已連線到受防護電腦的裝置清單中，選擇您要為其建立允許規則的裝置。

4. 點擊“為所選裝置新增規則”按鈕。

5. 在“裝置控制規則”視窗中點擊“儲存”按鈕。

“裝置控制”工作中的規則清單將使用基於安裝了卡斯基安全管理中心管理主控台的電腦的系統資料建立的新規則填充。

從有關被封鎖裝置的卡斯基安全管理中心報告中匯入規則

您可從在“僅統計”模式下完成“裝置控制”工作（請參見第 [440](#) 頁上的“配置“裝置控制”工作”部分）後卡斯基安全管理中心產生的報告匯入有關被封鎖裝置連線的資料，並使用此資料在所配置政策中產生裝置控制允許規則清單。

建立裝置控制工作期間發生的附隨報告時，您可跟蹤其連接受限制的裝置。

► 要基於有關被封鎖裝置的卡斯基安全管理中心報告為一組電腦指定裝置連線允許規則：

1. 在“事件通知”部分中的政策內容中，確保：

- 對於“關鍵事件”重要性等級，“已限制大容量儲存”事件的工作記錄的儲存時間段超過在“僅統計”模式下的執行排程時間段（預設值為 30 天）。

- 對於“警告”重要性等級，“僅統計：已偵測到不受信任的大容量儲存”事件的工作記錄的儲存時間段超過在“僅統計”模式下的工作執行排程時間段（預設值為 30 天）。

當事件的儲存時間段過後，有關記錄的事件的資訊會被刪除且不會反映在報告檔案中。在“僅統計”模式下執行裝置控制工作之前，確保工作執行時間不超過為指定事件配置的儲存時間。

2. 以“僅統計”模式啟動“裝置控制”工作。在卡巴斯基安全管理中心中的“管理伺服器”節點的工作區中，選擇“事件”標籤。點擊“建立選擇”按鈕並基於“已偵測到不受信任的大容量儲存”條件建立一系列事件，以檢視“裝置控制”工作將限制其連線的裝置。在選擇的詳細資訊視窗中，點擊“將事件匯出到檔案”連結以將有關限制的連線的報告儲存到 TXT 檔案。

在政策中匯入和應用建立的報告之前，確保報告僅包含有關您希望允許其連線的裝置的資料。

3. 將有關受限制裝置連線的資料匯入裝置控制工作：
 - a. 開啟“裝置控制規則”視窗（請參見第 438 頁上的“開啟裝置控制規則清單”部分）。
 - b. 點擊“新增”按鈕，然後在該按鈕的內容功能表中選擇“從卡巴斯基安全管理中心報告匯入封鎖的裝置的資料”。
 - c. 選擇將來自根據卡巴斯基安全管理中心報告建立的清單的規則新增到先前設定的裝置啟動控制規則清單的政策：
 - 新增到現有規則，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
 - 取代現有規則，如果您希望將現有規則取代為匯入的規則。
 - 與現有規則合併，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。
 - d. 在開啟的 Microsoft Windows 標準視窗中，選擇已將來自受限制裝置報告的事件匯出到的 TXT 檔案。
 - e. 在“裝置控制規則”視窗中點擊“儲存”按鈕。

4. 在“裝置控制”視窗中點擊“確定”。

根據有關受限制裝置的卡巴斯基安全管理中心報告建立的規則將被新增到裝置控制規則清單。

使用“裝置控制規則產生器”工作建立規則

► 要使用“裝置控制規則產生器”工作為一組電腦指定裝置控制規則：

1. 開啟“新建工作精靈”中的“設定”視窗（請參見第 [439](#) 頁上的“開啟‘裝置控制規則產生器’工作精靈”部分）。
2. 進行以下設定：
 - 在“模式”部分中：
 - 考慮曾經連接過的所有大容量記憶體的系統資料。
 - 僅考慮目前連接的大容量記憶體。
 - 在“工作完成後”部分中：
 - 將允許規則新增到裝置控制規則清單。

此核取方塊用於啟用/停用將新建立的允許規則新增到裝置啟動控制規則清單。點擊“裝置控制”節點的詳細資訊視窗中的“裝置控制規則”連結時，將顯示裝置控制規則清單。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將根據所選的規則新增原則，將“裝置控制規則產生器”工作建立的規則新增到裝置控制規則清單中。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不會將新建立的允許規則新增到裝置控制規則清單中。建立的規則僅匯出至檔案。

預設將會選定該核取方塊。

如果未選中“將允許規則匯出到檔案”核取方塊，則無法選中該核取方塊。

- 新增原則。

此下拉清單用於指定用來將新建立的允許規則新增到應用程式啟動控制規則清單的方法。

- **新增到現有規則。** 將規則新增到現有規則清單。將複製具有相同設定的規則。
- **取代現有規則。** 規則會替換清單中的現有規則。
- **與現有規則合併。** 將規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。

預設選中“**與現有規則合併**”方法。

- **將允許規則匯出到檔案。**

使用此核取方塊可啟用/停用將裝置控制的允許規則匯出至檔案。

如果選中此核取方塊，Kaspersky Embedded Systems Security 會在“裝置控制規則產生器”工作完成後將允許規則匯出到下面的欄位中指定的檔案。

如果選中此核取方塊，應用程式不會在“裝置控制規則產生器”工作完成後將建立的允許規則匯出檔案。而只將它們新增到裝置控制規則清單。

預設取消選定該核取方塊。

如果未選中“**將允許規則新增到裝置控制規則清單**”核取方塊，則無法選中該核取方塊。

- **將電腦詳細資訊新增到檔案名稱。**

該核取方塊用於啟用或停用將有關受防護電腦的資訊新增到允許規則將匯出到的檔案的名稱中。

如果選中該核取方塊，應用程式會將受防護電腦名稱以及檔案建立日期和時間新增到匯出檔案的名稱中。

如果清除該核取方塊，應用程式不會將有關受防護電腦的資訊新增到匯出檔案的名稱中。

預設將會選定該核取方塊。

3. 點擊“下一步”。

4. 在“排程”視窗中，設定排程的工作啟動設定。
5. 點擊“下一步”。
6. 在“選擇帳戶以執行工作”視窗中，指定要使用的帳戶。
7. 點擊“下一步”。
8. 自訂工作名稱。
9. 點擊“下一步”。

工作名稱不應超過 100 個字元，並且不能包含以下符號：

" * < > & \ : |

將開啟“完成工作建立”視窗。

10. 您可以透過選中“精靈完成後執行工作”核取方塊來在精靈完成後執行工作。
11. 點擊“完成”完成建立工作。
12. 在所配置電腦群組的工作區上的“工作”標籤上，從群組工作清單中選擇您已建立的“裝置控制規則產生器”。
13. 點擊“啟動”按鈕啟動工作。

工作完成後，自動建立的允許規則清單將儲存在共用資料夾中的 XML 檔案中。

在網路中使用裝置控制政策之前，請確保所有受防護電腦都能夠存取共用網路資料夾。如果不提供組織的政策用於網路中的共用網路資料夾，則建議為測試電腦群組或範本機上的電腦控制規則啟動“裝置規則產生器”工作。

將建立的規則新增到裝置控制規則清單

► 要將建立的允許規則清單新增到“裝置控制”工作：

1. 開啟“裝置控制規則”視窗（請參見第 [438](#) 頁上的“開啟裝置控制規則清單”部分）。

2. 點擊“新增”按鈕。
 3. 在“新增”按鈕的內容功能表中選擇“從 XML 檔案匯入規則”選項。
 4. 選擇將自動建立的允許規則新增到先前建立的“裝置控制”規則清單中的政策。
 - **新增到現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
 - **取代現有規則**，如果您希望將現有規則取代為匯入的規則。
 - **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。
 5. 在開啟的 Microsoft Windows 標準視窗中，選擇“裝置控制規則產生器”群組工作完成後建立的 XML 檔案。
 6. 點擊“開啟”。
- XML 檔案中所有建立的規則將按照所選原則新增到清單中。
7. 在“裝置控制規則”視窗中點擊“儲存”按鈕。
 8. 如果想要應用建立的裝置控制規則，請在“裝置控制”政策設定中選擇“活動”工作模式。

基於每台單獨的電腦上的系統資料自動建立的允許規則將被套用於所設定政策涵蓋的所有網路電腦。在這些電腦上，應用程式將僅允許已為其建立允許規則的那些裝置進行連接。

透過應用程式主控台管理裝置控制

在本節中，學習如何導航應用程式主控台介面以及如何在本地電腦上配置工作設定。

本章節說明項目

導航	451
配置裝置控制工作設定	453
配置裝置控制規則	454
配置裝置控制規則產生器工作	459

導航

學習如何透過介面導航到所需工作設定。

本章節說明項目

開啟“裝置控制”工作設定	451
開啟“裝置控制規則”視窗	452
開啟“裝置控制規則產生器”工作設定	452

開啟“裝置控制”工作設定

► 要透過應用程式主控台開啟“裝置控制”工作設定：

1. 在應用程式主控台樹狀目錄中，展開“**電腦控制**”節點。
2. 選擇“**裝置控制**”子節點。
3. 在“**裝置控制**”子節點的詳細資訊視窗中，點擊“**內容**”連結。

將開啟“**工作設定**”視窗。

4. 根據需要配置工作。

開啟“裝置控制規則”視窗

► 要透過應用程式主控台開啟裝置控制規則清單：

1. 在應用程式主控台樹狀目錄中，展開“**電腦控制**”節點。
2. 選擇“**裝置控制**”子節點。
3. 在“**裝置控制**”節點的詳細資訊視窗中，點擊“**裝置控制規則**”連結。

將開啟“**裝置控制規則**”視窗。

4. 根據需要設定規則清單。

開啟“裝置控制規則產生器”工作設定

► 要配置“裝置控制規則產生器”工作：

1. 在應用程式主控台樹狀目錄中，展開“**自動規則產生器**”節點。
2. 選擇“**裝置控制規則產生器**”子節點。
3. 在“**裝置控制規則產生器**”子節點的詳細資訊視窗中，點擊“**內容**”連結。

將開啟“**工作設定**”視窗。

4. 根據需要配置工作。

配置裝置控制工作設定

► 要配置“裝置控制”工作設定：

1. 開啟“工作設定”視窗（請參見第 [451](#) 頁上的“開啟‘裝置控制’工作設定”部分）。
2. 在“一般”標籤上，配置以下工作設定：
 - 在“工作模式”部分中，選擇以下工作模式之一：

- **活動。**

Kaspersky Embedded Systems Security 會將規則套用於控制快閃記憶體磁碟機和其他外部裝置的連線，並根據預設拒絕政策和指定允許規則允許或封鎖使用所有裝置。允許使用受信任外部裝置。預設情況下，封鎖使用不受信任的外部裝置。

如果當“裝置控制”工作在活動模式下執行前您認為不受信任的外部裝置連線到受防護電腦，應用程式不會封鎖該裝置。建議您手動斷開不信任裝置或重新啟動電腦。否則，不會將“預設拒絕”原則套用於裝置。

- **僅統計。**

Kaspersky Embedded Systems Security 不會控制快閃記憶體磁碟機和其他外部裝置的連線，但僅記錄有關外部裝置在受防護電腦上的連接和註冊，以及有關相連裝置觸發的裝置控制允許規則的資訊。允許使用所有外部裝置。預設設定此模式。

- 選中或清除“當未執行裝置控制工作時允許使用所有大容量儲存裝置”核取方塊。

使用此核取方塊可允許或封鎖在裝置控制工作未執行時使用大容量儲存裝置。

如果選擇該核取方塊且裝置控制工作未執行，則 Kaspersky Embedded Systems Security 允許在受防護的電腦上使用任何大容量儲存裝置。

如果清除此核取方塊，應用程式在以下情況下將封鎖在受防護電腦上使用不受信任的大容量儲存裝置：“裝置控制”工作未執行或 Kaspersky Security 服務已關閉。建議使用該選項以最大限度防護您的電腦在與外部裝置交換檔案時免受安全威脅。

預設取消選定該核取方塊。

3. 如有必要，在“**排程**”和“**進階**”標籤上，配置排程的工作啟動設定（請參見第 [189](#) 頁上的“配置工作啟動排程設定”部分）。
4. 要編輯裝置控制規則清單（請參見第 [433](#) 頁上的“關於裝置控制規則清單填充”部分），請在“**裝置控制**”節點的詳細資訊視窗的下部，點擊“**裝置控制規則**”連結。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在系統稽核記錄中。

配置裝置控制規則

瞭解如何使用“裝置控制”工作建立、匯入和匯出規則清單，或手動建立允許或拒絕規則。

本章節說明項目

從 XML 檔案匯入裝置控制規則.....	454
基於裝置控制工作事件填寫規則清單.....	455
為一個或多個外部裝置新增允許規則.....	456
刪除裝置控制規則.....	456
匯出裝置控制規則.....	457
啟動和停用裝置控制規則.....	457
延伸裝置控制規則使用範圍.....	458

從 XML 檔案匯入裝置控制規則

► 要匯入裝置控制規則，請執行以下步驟：

1. 開啟“**裝置控制規則**”（請參見第 [452](#) 頁上的“開啟裝置控制規則視窗”部分）視窗。
2. 點擊“**新增**”按鈕。
3. 在按鈕的內容功能表中，選擇“**從 XML 檔案匯入規則**”。

4. 指定新增匯入規則的方法。要執行此操作，請從“從 XML 檔案匯入規則”按鈕的內容功能表中選擇一個選項：
 - **新增到現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
 - **取代現有規則**，如果您希望將現有規則取代為匯入的規則。
 - **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。

將開啟標準 Microsoft Windows“開啟”視窗。

5. 在“開啟”視窗中，選擇包含裝置控制規則的設定的 XML 檔案。
6. 點擊“開啟”按鈕。

匯入的規則將顯示在“裝置控制規則”視窗中的清單中。

基於裝置控制工作事件填寫規則清單

► 要基於“裝置控制”工作事件建立包含裝置控制規則清單的設定檔：

1. 以“僅統計”模式啟動裝置控制工作（請參見第 [453](#) 頁上的“配置裝置控制工作設定”部分），以記錄與受防護電腦連線的快閃記憶體磁碟機和其他外部裝置的所有事件。
2. “僅統計”模式中的工作完成後，透過點擊“裝置控制”節點詳細資訊窗格的“管理”部分中的“開啟工作記錄”按鈕，開啟工作記錄。
3. 在“記錄”視窗中，點擊“基於事件建立規則”。

Kaspersky Embedded Systems Security 將會建立一個 XML 設定檔，其中包含基於“僅統計”模式中的“裝置控制”工作事件建立的規則清單。您可以在“裝置控制”工作中套用此清單（請參見第 [454](#) 頁上的“從 XML 檔案匯入裝置控制規則”部分）。

在套用基於工作事件建立的規則清單之前，建議您仔細檢查，然後手動處理規則清單，以確保指定的規則沒有允許不信任裝置。

在將包含工作事件 XML 檔案轉換為規則清單期間，應用程式將為所有註冊的事件建立允許規則，包括裝置限制。

無論工作模式如何，所有工作事件都將記錄在工作記錄中。您可以基於處於“活動”模式的工作事件建立包含規則清單的設定檔。除非出現緊急情況，例如工作效率要求在工作以活動模式執行之前建立最終規則清單版本，否則不建議使用此方案。

為一個或多個外部裝置新增允許規則

裝置控制工作中支援手動逐個新增規則的功能。但是，如果您需要為一個或多個新外部裝置新增規則，可以使用“基於系統資料產生規則”選項。如果應用此方案，應用程式將使用有關所有曾經連接過的外部裝置的 Windows 資料，並且還允許目前連線的裝置，以填寫允許規則清單。

Kaspersky Embedded Systems Security 無法存取透過 MTP 連線的行動裝置的系統資料。無法為 MTP 連線的行動裝置建立允許規則。

► 要為目前連線的一個或多個外部裝置新增允許規則：

1. 開啟“裝置控制規則”視窗（請參見第 [452](#) 頁上的“開啟裝置控制規則視窗”部分）。
2. 點擊“新增”按鈕。
3. 在開啟的內容功能表中，選擇“基於系統資料產生規則”選項。
4. 在開啟的視窗中，檢視偵測到的裝置清單並選擇要在受防護電腦上信任的一個或多個裝置。
5. 點擊“為所選裝置新增規則”按鈕。

將會建立新規則並新增到裝置控制規則清單中。

刪除裝置控制規則

► 要刪除裝置控制規則：

1. 開啟“裝置控制規則”（請參見第 [452](#) 頁上的“開啟裝置控制規則視窗”部分）視窗。

2. 在清單中，選擇要刪除的一項或多項規則。
3. 點擊“刪除選取的項目”按鈕。
4. 點擊“儲存”按鈕。

將刪除所選裝置控制規則。

匯出裝置控制規則

► 要將裝置控制規則匯出到設定檔：

1. 開啟“裝置控制規則”（請參見第 [452](#) 頁上的“開啟裝置控制規則視窗”部分）視窗。
2. 點擊“匯出至檔案”按鈕。

將開啟標準的 Microsoft Windows 視窗。

3. 在開啟的視窗中，指定想要將規則匯出到其中的檔案。如果不存在此類檔案，則將建立它。如果具有指定名稱的檔案已存在，則將在匯出規則後重寫其內容。
4. 點擊“儲存”按鈕。

規則及其設定將匯出到指定檔案中。

啟動和停用裝置控制規則

您可以啟動和停用已建立的裝置控制規則，而不必刪除它們。

► 若要啟動或停用已建立的裝置控制規則，請執行以下步驟：

1. 開啟“裝置控制規則”（請參見第 [452](#) 頁上的“開啟裝置控制規則視窗”部分）視窗。
2. 在指定規則清單中，透過點擊要配置其內容的規則，開啟“規則內容”視窗。
3. 在開啟的視窗中，選中或清除“套用規則”核取方塊。

此核取方塊可啟用或停用裝置控制規則。

如果選中某個規則的此核取方塊，該規則將被啟動。將允許包含在規則使用範圍中的外部裝置的連線。

如果在規則內容中取消選中此核取方塊，該規則將被停用。將封鎖包含在規則使用範圍中的外部裝置的連線。

預設情況下，在每個已建立規則的設定中選中此核取方塊。

4. 點擊“確定”。

將為指定規則儲存和顯示規則應用狀態。

延伸裝置控制規則使用範圍

每個自動建立的裝置控制規則都只涵蓋一個外部裝置。您可以透過在任何指定規則的內容中設定裝置實例路徑遮罩，來手動延伸規則使用範圍。

應用裝置實例路徑可減少指定的總規則數並簡化規則處理。但是延伸規則使用範圍可能會降低大容量儲存裝置控制效率。

► 要在裝置控制規則內容中應用裝置實例路徑遮罩：

1. 開啟“裝置控制規則”（請參見第 [452](#) 頁上的“開啟裝置控制規則視窗”部分）視窗。
2. 在開啟的視窗中，選擇一個規則以使用其內容來套用遮罩。
3. 透過點擊選定的裝置控制規則，開啟“規則內容”視窗。
4. 在開啟的視窗中，執行以下操作：
 - 如果您希望某選定規則允許所有符合指定的裝置製造商和裝置序號資訊的大容量儲存裝置的連線，請選中“**控制器類型 (PID)**”欄位旁邊的“**使用遮罩**”核取方塊。
 - 如果您希望某選定規則允許所有符合指定的裝置製造商和控制器類型資訊的大容量儲存裝置的連線，請選中“**序號**”欄位旁邊的“**使用遮罩**”核取方塊。
 - 如果您希望某選定規則允許所有符合指定的裝置製造商資訊的大容量儲存裝置的連線，請選中“**控制器類型 (PID)**”欄位和“**序號**”欄位旁邊的“**使用遮罩**”核取方塊。

如果在至少一個欄位中選中了“**使用遮罩**”核取方塊，則將使用 * 符號代替核取方塊被選中的欄位的資料，並且在套用規則時不會考慮這些資料。

5. 如有必要，請在“敘述”欄位中指定有關規則的附加資訊。例如，指定受規則影響的裝置。
6. 點擊“確定”。

將儲存新配置的規則內容。規則使用範圍將根據指定的裝置實例路徑遮罩進行延伸。

配置裝置控制規則產生器工作

► 要配置“裝置控制規則產生器”工作：

1. 在應用程式主控台樹狀目錄中，展開“自動規則產生器”節點。
2. 選擇“裝置控制規則產生器”子節點。
3. 在“裝置控制規則產生器”節點的詳細資訊視窗中，點擊“內容”連結。
將開啟“工作設定”視窗。
4. 在“一般”標籤上的“工作模式”部分中選擇工作執行模式：
 - 考慮曾經連接過的所有大容量記憶體的系统資料。
 - 僅考慮目前連接的大容量記憶體。
5. 在“工作完成後”部分中，指定 Kaspersky Embedded Systems Security 在工作完成後必須執行的操作：
 - 將允許規則新增到裝置控制規則清單。

此核取方塊用於啟用/停用將新建立的允許規則新增到裝置啟動控制規則清單。點擊“裝置控制”節點的詳細資訊視窗中的“裝置控制規則”連結時，將顯示裝置控制規則清單。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將根據所選的規則新增原則，將“裝置控制規則產生器”工作建立的規則新增到裝置控制規則清單中。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不會將新建立的允許規則新增到裝置控制規則清單中。建立的規則僅匯出至檔案。

預設將會選定該核取方塊。

如果未選中“將允許規則匯出到檔案”核取方塊，則無法選中該核取方塊。

- **新增原則。**

此下拉清單用於指定用來將新建立的允許規則新增到應用程式啟動控制規則清單的方法。

- **新增到現有規則。** 將規則新增到現有規則清單。將複製具有相同設定的規則。
- **取代現有規則。** 規則會替換清單中的現有規則。
- **與現有規則合併。** 將規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。

預設選中“與現有規則合併”方法。

- **將允許規則匯出到檔案。**

使用此核取方塊可啟用/停用將裝置控制的允許規則匯出至檔案。

如果選中此核取方塊，Kaspersky Embedded Systems Security 會在“裝置控制規則產生器”工作完成後將允許規則匯出到下面的欄位中指定的檔案。

如果選中此核取方塊，應用程式不會在“裝置控制規則產生器”工作完成後將建立的允許規則匯出檔案。而只將它們新增到裝置控制規則清單。

預設取消選定該核取方塊。

如果未選中“將允許規則新增到裝置控制規則清單”核取方塊，則無法選中該核取方塊。

- **將電腦詳細資訊新增到檔案名稱。**

該核取方塊用於啟用或停用將有關受防護電腦的資訊新增到允許規則將匯出到的檔案的名稱中。

如果選中該核取方塊，應用程式會將受防護電腦名稱以及檔案建立日期和時間新增到匯出檔案的名稱中。

如果清除該核取方塊，應用程式不會將有關受防護電腦的資訊新增到匯出檔案的名稱中。

預設將會選定該核取方塊。

6. 在“排程”和“進階”標籤上，配置排程的工作啟動設定(請參見第 [189](#) 頁上的“配置工作啟動排程設定”部分)。
7. 點擊“確定”。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在系統稽核記錄中。

防火牆管理

本節包含有關防火牆管理工作以及如何設定的資訊。

本章內容

關於防火牆管理工作	462
關於防火牆規則	463
防火牆管理工作預設設定	465
透過管理外掛程式管理防火牆規則	466
透過應用程式主控台管理防火牆規則	471

關於防火牆管理工作

Kaspersky Embedded Systems Security 會提供一個可靠且符合人體工程學的解決方案，以便使用防火牆管理工作防護網路連線。

防火牆管理工作不會執行獨立的網路流量篩選，但它允許您透過 Kaspersky Embedded Systems Security 圖形介面管理 Windows 防火牆。在防火牆管理工作期間，Kaspersky Embedded Systems Security 接管對作業系統防火牆的設定和政策的管理，並封鎖進行任何外部防火牆配置。

在應用程式安裝期間，防火牆管理元件會讀取並複製 Windows 防火牆狀態及所有指定規則。此後，只能變更規則集和規則參數，且防火牆只能在 Kaspersky Embedded Systems Security 中開啟或關閉。

如果在安裝 Kaspersky Embedded Systems Security 期間 Windows 防火牆關閉，則在安裝完成後將不會執行防火牆管理工作。如果在安裝應用程式期間 Windows 防火牆開啟，則會在安裝完成後執行防火牆管理工作，從而封鎖指定規則不允許的所有網路連線。

預設情況下，不會安裝防火牆管理元件，因為其未包括在建議安裝元件集中。

防火牆管理工作強制封鎖工作的指定規則不允許的所有傳入和傳出連接。

該工作會定期輪詢 Windows 防火牆並監控其狀態。預設情況下，輪詢間隔設定為 1 分鐘且無法變更。如果在輪詢期間 Kaspersky Embedded Systems Security 偵測到 Windows 防火牆設定和防火牆管理工作設定之間存在不匹配，應用程式會強制應用作業系統防火牆上的工作設定。

使用 Windows 防火牆的逐分鐘輪詢，Kaspersky Embedded Systems Security 可以監控：

- Windows 防火牆的執行狀態。
- 安裝 Kaspersky Embedded Systems Security 後其他應用程式或工具新增的規則的狀態（例如，使用 wf.msc 的某個連接埠/應用程式新增的新應用程式規則）。

當向 Windows 防火牆套用新規則時，Kaspersky Embedded Systems Security 會在 **Windows 防火牆** 管理單元中建立 Kaspersky Security 群組規則集。此規則集可統一 Kaspersky Embedded Systems Security 使用防火牆管理工作建立的所有規則。在輪詢期間，應用程式不會每分鐘監控 Kaspersky Embedded Systems Security 群組中的規則，且該規則不會自動與防火牆管理工作設定中指定的規則清單同步。

► *要手動更新 Kaspersky Embedded Systems Security 群組規則，*

請重新啟動 Kaspersky Embedded Systems Security 防火牆管理工作。

您還可使用 **Windows 防火牆** 管理單元手動編輯 Kaspersky Security 群組規則。

如果按卡巴斯基安全管理中心群組政策管理 Windows 防火牆，則防火牆管理工作無法啟動。

關於防火牆規則

防火牆管理工作使用工作執行期間強制套用於 Windows 防火牆的允許規則控制傳入和傳出網路流量的篩選。

初次啟動工作時，Kaspersky Embedded Systems Security 會讀取 Windows 防火牆設定中指定的所有傳入網路流量規則，並將其複製到防火牆管理工作設定。然後，應用程式根據以下規則執行：

- 如果在 Windows 防火牆設定中建立新規則 (在安裝新應用程式期間手動或自動建立)，Kaspersky Embedded Systems Security 會刪除該規則。
- 如果從 Windows 防火牆設定中刪除現有規則，則重新啟動工作後 Kaspersky Embedded Systems Security 會還原該規則。
- 如果在 Windows 防火牆設定中變更現有規則的參數，Kaspersky Embedded Systems Security 會回溯變更。
- 如果在防火牆管理設定中建立新規則，Kaspersky Embedded Systems Security 會將該規則強制套用於 Windows 防火牆。
- 如果從防火牆管理設定中刪除現有規則，Kaspersky Embedded Systems Security 會從 Windows 防火牆設定中強制刪除該規則。

Kaspersky Embedded Systems Security 不會使用封鎖規則或控制傳出網路流量的規則。在防火牆管理工作啟動後，Kaspersky Embedded Systems Security 會從 Windows 防火牆設定中刪除所有此類規則。

您可為傳入網路流量設定、刪除和編輯篩選規則。

您無法在防火牆管理工作設定中指定新規則以控制傳出網路流量。Kaspersky Embedded Systems Security 中指定的所有防火牆規則僅控制傳入網路流量。

您可管理以下類型的防火牆規則：

- 應用程式規則。
- 連接埠規則。

應用程式規則

此類型的規則允許指定應用程式的目的網路連線。這些規則的觸發條件基於可執行檔的路徑。

您可管理應用程式規則：

- 新增新規則。
- 刪除現有規則。
- 啟用或停用指定規則。
- 編輯指定規則的參數：指定規則名稱、可執行檔的路徑以及規則使用範圍。

連接埠規則

此類型的規則允許指定連接埠和協定 (TCP/UDP) 的網路連線。這些規則的觸發條件基於埠號和協定類型。

您可管理連接埠規則：

- 新增新規則。
- 刪除現有規則。
- 啟用或停用指定規則。
- 編輯指定規則的參數：設定規則名稱、埠號、協定類型以及規則的應用範圍。

連接埠規則的範圍比應用程式規則的範圍要廣。透過基於連接埠規則允許連線，會下降受防護電腦的安全等級。

防火牆管理工作預設設定

防火牆管理工作使用下表描述的預設設定。您可以變更這些設定值。

表 52. 防火牆管理工作預設設定

設定	預設值	敘述
----	-----	----

設定	預設值	敘述
針對應用程式的防火牆規則	已啟用兩條針對應用程式的預設規則	您可以停用預設規則或新增新規則。
針對連接埠的防火牆規則	已啟用六條針對連接埠的預設規則	您可以停用預設規則或新增新規則。
工作啟動排程	不設定工作的初次啟動排程。	“防火牆管理”工作不會在 Kaspersky Embedded Systems Security 啟動時自動啟動。 您可以配置工作啟動排程。

透過管理外掛程式管理防火牆規則

在本節中，學習如何透過應用程式主控台介面管理防火牆規則。

本章節說明項目

啟用和停用防火牆規則.....	466
手動新增防火牆規則.....	468
刪除防火牆規則.....	469

啟用和停用防火牆規則

► 要啟用或停用篩選傳入網路流量的現有規則，請執行以下操作：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其配置應用程式設定的管理群組。

3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 [144](#) 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 [150](#) 頁上的“在卡斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**網路行為控制**”部分中，點擊“**防火牆管理**”子部分中的“**設定**”按鈕。
5. 點擊開啟的視窗中的“**規則清單**”按鈕。

將開啟“**防火牆規則**”視窗。

6. 根據想要修改其狀態的規則類型，選擇“**應用程式**”或“**埠號**”。
7. 在規則清單中，選擇要修改其狀態的規則，然後執行以下操作之一：
 - 如果您想要啟用已停用的規則，選中規則名稱左側的核取方塊。
將啟用所選規則。
 - 如果您想要停用已啟用的規則，清除規則名稱左側的核取方塊。
將停用所選規則。

8. 在“**防火牆規則**”視窗中，點擊“**確定**”。
9. 在“**防火牆管理**”視窗中，點擊“**確定**”。
10. 在“**內容：<政策名稱>**”視窗中，點擊“**確定**”。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

手動新增防火牆規則

您只能新增和編輯應用程式和連接埠的規則。不能新增或編輯現有群組規則。

► 要新增篩選傳入網路流量的新規則或編輯現有規則，請執行以下操作：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 [144](#) 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 [150](#) 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**網路行為控制**”部分中，點擊“**防火牆管理**”子部分中的“**設定**”按鈕。
5. 點擊開啟的視窗中的“**規則清單**”按鈕。
將開啟“**防火牆規則**”視窗。
6. 根據您要新增的規則類型，選擇“**應用程式**”或“**埠號**”標籤，然後執行以下操作之一：
 - 要編輯現有規則，在規則清單中選擇要編輯的規則，然後點擊“**編輯**”。
 - 要新增新規則，點擊“**新增**”。

根據配置的規則類型，將開啟“**連接埠規則**”視窗或“**應用程式規則**”視窗。

7. 在開啟的視窗中，執行以下操作：

- 如果您使用的是應用程式規則，請執行以下操作：
 - a. 輸入已編輯規則的“規則名稱”。
 - b. 指定您透過修改此規則允許其連線的應用程式的可執行檔的“應用程式路徑”。
您可手動或透過使用“瀏覽”按鈕設定路徑。
 - c. 在“規則套用範圍”欄位中，指定將為其套用已修改規則的網路位址。

您只能使用 IPv4 IP 位址。

- 如果您使用的是連接埠規則，請執行以下操作：
 - a. 輸入已編輯規則的“規則名稱”。
 - b. 指定應用程式將允許連線的“埠號”。
 - c. 選擇應用程式將允許連線的協定類型 (TCP/UDP)。
 - d. 在“規則套用範圍”欄位中，指定將為其套用已修改規則的網路位址。

您只能使用 IPv4 IP 位址。

8. 在“應用程式規則”或“連接埠規則”視窗中，點擊“確定”。
9. 在“防火牆管理”視窗中，點擊“確定”。
10. 在“內容：<政策名稱>”視窗中，點擊“確定”。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

刪除防火牆規則

您只能刪除應用程式和連接埠規則。您無法刪除現有群組規則。

► 要刪除篩選傳入網路流量的現有規則，請執行以下操作：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 [144](#) 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 [150](#) 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**網路行為控制**”部分中，點擊“**防火牆管理**”子部分中的“**設定**”按鈕。
5. 點擊開啟的視窗中的“**規則清單**”按鈕。

將開啟“**防火牆規則**”視窗。

6. 根據想要修改器狀態的規則類型，選擇“**應用程式**”或“**埠號**”標籤。
7. 在規則清單中，選擇要刪除的規則。
8. 點擊“**刪除**”按鈕。

將刪除所選規則。

9. 在“**防火牆規則**”視窗中，點擊“**確定**”。
10. 在“**防火牆管理**”視窗中，點擊“**確定**”。
11. 在“**內容：<政策名稱>**”視窗中，點擊“**確定**”。

將儲存指定防火牆管理工作設定。新規則參數將傳送到 Windows 防火牆。

透過應用程式主控台管理防火牆規則

在本節中，學習如何透過應用程式主控台介面管理防火牆規則。

本章節說明項目

啟用和停用防火牆規則	471
手動新增防火牆規則	472
刪除防火牆規則	473

啟用和停用防火牆規則

► 要啟用或停用篩選傳入網路流量的現有規則，請執行以下操作：

1. 在應用程式主控台樹狀目錄中，展開“**電腦控制**”節點。
2. 選擇“**防火牆管理**”子節點。
3. 在“**防火牆管理**”節點的詳細資訊窗格中，點擊“**防火牆規則**”連結。

將開啟“**防火牆規則**”視窗。

4. 根據想要修改其狀態的規則類型，選擇“**應用程式**”或“**埠號**”。
5. 在規則清單中，選擇要修改其狀態的規則，然後執行以下操作之一：
 - 如果您想要啟用已停用的規則，選中規則名稱左側的核取方塊。
將啟用所選規則。
 - 如果您想要停用已啟用的規則，清除規則名稱左側的核取方塊。
將停用所選規則。
6. 在“**防火牆規則**”視窗中，點擊“**儲存**”。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

手動新增防火牆規則

► 要新增篩選傳入網路流量的新規則或編輯現有規則，請執行以下操作：

1. 在應用程式主控台樹狀目錄中，展開“**電腦控制**”節點。
2. 選擇“**防火牆管理**”子節點。
3. 在“**防火牆管理**”節點的詳細資訊窗格中，點擊“**防火牆規則**”連結。

將開啟“**防火牆規則**”視窗。

4. 根據您要新增的規則類型，選擇“**應用程式**”或“**埠號**”標籤，然後執行以下操作之一：
 - 要編輯現有規則，在規則清單中選擇要編輯的規則，然後點擊“**編輯**”。
 - 要新增新規則，點擊“**新增**”。

根據配置的規則類型，將開啟“**連接埠規則**”視窗或“**應用程式規則**”視窗。

5. 在開啟的視窗中，執行以下操作：
 - 如果您使用的是應用程式規則，請執行以下操作：
 - a. 輸入已編輯規則的“**規則名稱**”。
 - b. 指定您透過修改此規則允許其連線的應用程式的可執行檔的“**應用程式路徑**”。
您可手動或透過使用“**瀏覽**”按鈕設定路徑。
 - c. 在“**規則套用範圍**”欄位中，指定將為其套用已修改規則的網路位址。

您只能使用 IPv4 IP 位址。

- 如果您使用的是連接埠規則，請執行以下操作：
 - a. 輸入已編輯規則的“**規則名稱**”。
 - b. 指定應用程式將允許連線的“**埠號**”。
 - c. 選擇應用程式將允許連線的協定類型 (TCP/UDP)。
 - d. 在“**規則套用範圍**”欄位中，指定將為其套用已修改規則的網路位址。

您只能使用 IPv4 IP 位址。

6. 在“應用程式規則”或“連接埠規則”視窗中，點擊“確定”。
7. 在“防火牆規則”視窗中，點擊“儲存”。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

刪除防火牆規則

您只能刪除應用程式和連接埠規則。您無法刪除現有群組規則。

► 要刪除篩選傳入網路流量的現有規則，請執行以下操作：

1. 在應用程式主控台樹狀目錄中，展開“電腦控制”節點。
2. 選擇“防火牆管理”子節點。
3. 在“防火牆管理”節點的詳細資訊窗格中，點擊“防火牆規則”連結。

將開啟“防火牆規則”視窗。

4. 根據想要修改器狀態的規則類型，選擇“應用程式”或“埠號”標籤。
5. 在規則清單中，選擇要刪除的規則。
6. 點擊“刪除”按鈕。

將刪除所選規則。

7. 在“防火牆規則”視窗中，點擊“儲存”。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

檔案完整性監控

本節包含有關啟動和設定“檔案完整性監控”工作的資訊。

本章內容

關於“檔案完整性監控”工作	474
關於檔案操作監控規則	475
“檔案完整性監控”工作預設設定	478
透過管理外掛程式管理“檔案完整性監控”	479
透過應用程式主控台管理“檔案完整性監控”	484

關於“檔案完整性監控”工作

“檔案完整性監控”工作的設計目的是為了跟蹤針對工作設定中指定的監控範圍內的特定檔案和資料夾執行的操作。可以使用該工作來刪除可能對受防護電腦造成安全入侵的檔案變更。還可以配置監控被中斷期間要對其進行跟蹤的檔案變更。

當監控範圍暫時位於工作範圍之外時（例如，如果工作停止或如果受防護電腦上沒有物理顯示大容量儲存裝置），會出現 *監控中斷*。一旦重新連線大容量儲存裝置，Kaspersky Embedded Systems Security 將報告監控範圍內偵測到的檔案操作。

如果由於重新安裝“檔案完整性監控”元件造成指定監控範圍內的工作停止執行，則不構成監控中斷。這種情況下，“檔案完整性監控”工作並未執行。

環境要求

要啟動“檔案完整性監控”工作，必須滿足以下條件：

- 受防護電腦上必須安裝有支援 ReFS 和 NTFS 檔案系統的大容量儲存裝置。
- 必須啟用 Windows USN 記錄。元件查詢此記錄來獲取有關檔案操作的資訊。

如果為某個磁區建立規則後啟用了 USN 記錄且已啟動“檔案完整性監控”工作，則必須重新啟動該工作。如果不重新啟動，則監控過程中不會套用該規則。

排除監控範圍

您可以建立排除監控範圍（請參見第 480 頁上的“配置監控規則”部分）。排除針對每個單獨的規則進行指定，並且僅對指定的監控範圍產生作用。可以為每個規則指定無限數量的排除。

排除比監控範圍具有更高的優先順序，且即使指定的資料夾或檔案位於監控範圍內，也不受工作的監控。如果其中一個規則的設定指定的監控範圍比排除中指定的資料夾具有更低的等級，則當工作執行時將不會考慮監控範圍。

要指定排除，可以使用與用於指定監控範圍相同的遮罩。

關於檔案操作監控規則

“檔案完整性監控”根據檔案操作監控規則執行。可以使用規則觸發條件來配置觸發工作的條件，以及調整工作記錄中記錄的已刪除檔案操作的事件的重要性等級。

針對每個監控範圍指定了檔案操作監控規則。

可以配置以下規則觸發條件：

- 受信任使用者。
- 檔案操作標記。

受信任使用者

預設情況下，應用程式將所有操作視為潛在安全入侵。受信任使用者清單為空。可以透過在檔案操作監控規則設定中建立受信任使用者清單來配置事件重要性等級。

不受信任使用者 – 監控範圍規則設定中的受信任使用者清單中未指定的任何使用者。如果 Kaspersky Embedded Systems Security 偵測到不受信任使用者執行的檔案操作，則“檔案完整性監控”工作將在工作記錄中記錄一個緊急事件。

受信任使用者 – 經過授權可在指定的監控範圍內執行檔案操作的使用者或使用者群組。如果 Kaspersky Embedded Systems Security 偵測到受信任使用者執行的檔案操作，則“檔案完整性監控”工作將在工作記錄中記錄一個“資訊事件”。

Kaspersky Embedded Systems Security 在監控中斷時間內，無法確定啟動操作的使用者。在此情況下，使用者狀態被確定為未知。

未知使用者 – 如果由於工作中斷或者資料同步驅動程式或 USN 記錄失敗導致 Kaspersky Embedded Systems Security 無法獲取有關使用者的資料，則將此狀態分配給使用者。如果 Kaspersky Embedded Systems Security 偵測到未知使用者執行的檔案操作，則“檔案完整性監控”工作將在工作記錄中記錄一個“警告事件”。

檔案操作標記

當“檔案完整性監控”工作執行時，Kaspersky Embedded Systems Security 使用檔案操作標記來確定已對檔案執行了操作。

檔案操作標記是可以對檔案操作進行特徵化的獨特敘述符。

每個檔案操作可以是針對檔案進行的單個操作或系列操作。每個此類操作等同於一個檔案操作標記。如果您指定作為規則觸發條件的標記在檔案操作鏈中被刪除，則應用程式將記錄一個事件，表示已執行指定的檔案操作。

已記錄事件的重要性等級不取決於選定的檔案操作標記或事件的數量。

預設情況下，Kaspersky Embedded Systems Security 考慮所有可用的檔案操作標記。可以在工作規則設定中手動選擇檔案操作標記。

表 53. 檔案操作標記

檔案操作 ID	檔案操作標記	支援的檔案系統
BASIC_INFO_CHANGE	已變更檔案或資料夾的內容或時間標記	NTFS、ReFS
COMPRESSION_CHANGE	已變更檔案或資料夾的壓縮	NTFS、ReFS
DATA_EXTEND	已變更檔案或資料夾的大小	NTFS、ReFS
DATA_OVERWRITE	已覆蓋檔案或資料夾中的資料	NTFS、ReFS
DATA_TRUNCATION	已截斷檔案或資料夾	NTFS、ReFS
EA_CHANGE	已變更延伸的檔案或資料夾內容	僅限 NTFS
ENCRYPTION_CHANGE	已變更檔案或資料夾的加密狀態	NTFS、ReFS
FILE_CREATE	首次建立檔案或資料夾	NTFS、ReFS
FILE_DELETE	使用 SHIFT+DEL 組合鍵永久刪除的檔案或資料夾	NTFS、ReFS
HARD_LINK_CHANGE	已為建立或刪除檔案或資料夾的硬連結	僅限 NTFS
INDEXABLE_CHANGE	已變更檔案或資料夾的索引狀態	NTFS、ReFS
INTEGRITY_CHANGE	已變更命名的檔案流的完整性內容	僅限 ReFS
NAMED_DATA_EXTEND	已增大命名的檔案流的大小	NTFS、ReFS
NAMED_DATA_OVERWRITE	已覆蓋命名的檔案流	NTFS、ReFS
NAMED_DATA_TRUNCATION	已截斷命名的檔案流	NTFS、ReFS
OBJECT_ID_CHANGE	已變更檔案或資料夾識別碼	NTFS、ReFS
RENAME_NEW_NAME	已為檔案或資料夾分配新名稱	NTFS、ReFS

檔案操作 ID	檔案操作標記	支援的檔案系統
REPARSE_POINT_CHANGE	已為檔案或資料夾建立新的重分析點或變更其現有重分析點	NTFS、ReFS
SECURITY_CHANGE	已變更檔案或資料夾存取權限	NTFS、ReFS
STREAM_CHANGE	已建立新的命名的檔案流或變更現有命名的檔案流	NTFS、ReFS
TRANSACTIONED_CHANGE	TxF 事務已變更命名的檔案流	僅限 ReFS

“檔案完整性監控”工作設定

預設情況下，“檔案完整性監控”工作具有下表所述的設定。您可以變更這些設定值。

表 54. “檔案完整性監控”工作設定

設定	預設值	敘述
監控範圍	未設定	可以指定操作將監控的資料夾和檔案。將針對指定監控範圍內的資料夾和檔案建立監控事件。
受信任使用者清單	未設定	可以指定使用者和/或使用者群組，其在指定資料夾中的操作將被元件視為安全。
工作未執行時監控檔案操作	已使用	可以啟用或停用工作未執行期間在指定監控範圍內執行的檔案操作的記錄。
將以下資料夾從控制範圍中排除	未套用	可以針對無需監控檔案操作的資料夾檢查排除的使用情況。當“檔案完整性監控”執行時，Kaspersky Embedded Systems Security 將略過指定為排除的監控範圍。
核對總和計算	未套用	可以配置在對檔案做出變更後進行檔案核對總和計算。

設定	預設值	敘述
考慮檔案操作標記	考慮所有可用的檔案操作標記	可以指定一組檔案操作標記。如果在監控範圍內執行的檔案操作被一個或多個指定標記進行過特徵化，則 Kaspersky Embedded Systems Security 會產生一個稽核事件。
工作啟動排程	不設定工作的初次啟動排程	您可以配置排程的工作啟動設定。

透過管理外掛程式管理“檔案完整性監控”

在本節中，學習如何透過管理外掛程式配置“檔案完整性監控”工作。

本章節說明項目

配置“檔案完整性監控”工作設定.....	479
配置監控規則.....	480

配置“檔案完整性監控”工作設定

要配置一般“檔案完整性監控”工作設定，請執行以下步驟：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“**政策**”標籤，然後開啟“**內容：<政策名稱>**”視窗（請參見第 [144](#) 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗（請參見第 [150](#) 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“應用程式設定”視窗中編輯這些設定。

4. 在“系統稽核”部分的“檔案完整性監控”部分中，點擊“設定”按鈕。

將開啟“檔案完整性監控”視窗。

5. 在開啟的視窗的“檔案操作監控設定”標籤中，配置監控範圍設定：

- a. 清除或選中“記錄監控中斷期間發生的檔案操作資訊”核取方塊。

當由於任何原因（拆除硬碟磁碟機、使用者停止工作、軟體錯誤）工作未執行時，該核取方塊可以啟用或停用“檔案完整性監控”設定中指定的檔案操作的監控。

如果選中該核取方塊，則當“檔案完整性監控”工作未執行時，Kaspersky Embedded Systems Security 將記錄所有監控範圍內的事件。

如果清除該核取方塊，則當工作未執行時，應用程式將不記錄監控範圍內的檔案操作。

預設將會選定該核取方塊。

- b. 新增工作要監控的監控範圍（請參見第 [480](#) 頁上的“配置監控規則”部分）。

6. 在“工作管理”標籤上的，根據排程配置工作啟動參數（請參見第 [164](#) 頁上的“管理工作排程”部分）。

7. 點擊“確定”以儲存變更。

配置監控規則

可以變更檔案完整性監控的預設設定（請參見下表）。

表 55. “檔案完整性監控”工作設定

設定	預設值	敘述
監控範圍	未設定	可以指定操作將監控的資料夾和檔案。將針對指定監控範圍內的資料夾和檔案建立監控事件。

設定	預設值	敘述
受信任使用者清單	未設定	可以指定使用者和/或使用者群組，其在指定資料夾中的操作將被元件視為安全。
工作未執行時監控檔案操作	已使用	可以啟用或停用工作未執行期間在指定監控範圍內執行的檔案操作的記錄。
將以下資料夾從控制範圍中排除	未套用	可以針對無需監控檔案操作的資料夾檢查排除的使用情況。當“檔案完整性監控”執行時，Kaspersky Embedded Systems Security 將略過指定為排除的監控範圍。
核對總和計算	未套用	可以配置在對檔案做出變更後進行檔案核對總和計算。
考慮檔案操作標記	考慮所有可用的檔案操作標記	可以指定一組檔案操作標記。如果在監控範圍內執行的檔案操作被一個或多個指定標記進行過特徵化，則 Kaspersky Embedded Systems Security 會產生一個稽核事件。
工作啟動排程	不設定工作的初次啟動排程	您可以配置排程的工作啟動設定。

► 要新增監控範圍，請執行以下步驟：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“政策”標籤，然後開啟“內容：<政策名稱>”視窗（請參見第 144 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“裝置”標籤，然後開啟“應用程式設定”視窗（請參見第 150 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“應用程式設定”視窗中編輯這些設定。

4. 在“系統稽核”部分的“檔案完整性監控”部分中，點擊“設定”按鈕。

將開啟“內容：檔案完整性監控”視窗。

5. 在“監控範圍”部分中，點擊“新增”按鈕。

將開啟“監控範圍”視窗。

6. 透過以下方式之一新增監控範圍：

- 如果要透過標準的 Microsoft Windows 對話方塊來選擇資料夾：

- a. 點擊“瀏覽”按鈕。

將開啟標準的 Microsoft Windows“瀏覽資料夾”視窗。

- b. 在開啟的視窗中，選擇要監控操作的資料夾，然後點擊“確定”按鈕。

- 如果想要手動指定監控範圍，請使用支援的遮罩新增路徑：

- `<*.ext>` - 帶有 `<ext>` 副檔名的所有檔案，與其位置無關；
- `<*\name.ext>` - 帶有 `<name>` 名稱和 `<ext>` 副檔名的所有檔案，與其位置無關；
- `<\dir*>` - 位於 `<dir>` 資料夾中的所有檔案；
- `<\dir*\name.ext>` - `<dir>` 資料夾及其所有子資料夾中帶有 `<name>` 名稱和 `<ext>` 副檔名的所有檔案。

當手動指定監控範圍時，請確保路徑為以下格式：`<卷字母>:\<遮罩>`。如果缺少磁區字母，則 Kaspersky Embedded Systems Security 將不會新增指定的監控範圍。

7. 在“受信任使用者”標籤中，點擊“新增”按鈕。

將開啟標準的 Microsoft Windows“選擇使用者或群組”視窗。

8. 選擇在選定監控範圍中允許其檔案操作的使用者或使用者群組，然後點擊“確定”按鈕。

預設情況下，Kaspersky Embedded Systems Security 將未列入受信任使用者清單的所有使用者視為不受信任（請參見第 475 頁上的“關於檔案操作監控規則”部分），並為他們產生緊急事件。

9. 選擇“**檔案操作標記**”標籤。
10. 如果需要，請執行以下操作來選擇一定數量的標記：
 - a. 選擇“**基於以下標記偵測檔案操作**”選項。
 - b. 在可用檔案操作清單中（請參見第 475 頁上的“關於檔案操作監控規則”部分），選中要監控的操作旁邊的核取方塊。

預設情況下，Kaspersky Embedded Systems Security 將偵測所有檔案操作標記，已選擇“**基於所有可辨識的標記偵測檔案操作**”選項。

11. 如果執行操作後，您想要 Kaspersky Embedded Systems Security 計算檔案核對總和，請執行以下操作：

- a. 選中“**如果可能，計算檔案的核對總和。核對總和將可在工作報告中檢視**”核取方塊。

如果選中該核取方塊，則 Kaspersky Embedded Systems Security 將計算修改後的檔案的核對總和，其中偵測到至少帶有一個選定標記的檔案操作。

如果透過許多標記偵測到檔案操作，則將僅計算進行所有修改後的最終檔案核對總和。

如果清除該核取方塊，則 Kaspersky Embedded Systems Security 將為經過修改的檔案計算核對總和。

以下情況不會執行任何核對總和計算：

- 如果檔案變為不可用（例如，由於存取權限的變更造成）。
- 如果此後在已被刪除的檔案中偵測到檔案操作。

預設取消選定該核取方塊。

b. 在“使用算法計算核對總和”下拉清單中，選擇以下選項之一：

- MD5 雜湊
- SHA256 雜湊

12. 如果您不想監控“可用檔案操作清單”中的所有檔案操作(請參見第 [475](#) 頁上的“關於檔案操作監控規則”部分)，並選中要監控的操作旁邊的核取方塊。

13. 如果必要，透過執行以下步驟新增排除的監控範圍：

- 選擇“排除”標籤。
- 選中“將以下資料夾從控制範圍中排除”核取方塊。

該核取方塊可以針對無需監控檔案操作的資料夾停用排除。

如果選中該核取方塊，則當“檔案完整性監控”工作執行時，Kaspersky Embedded Systems Security 將略過排除清單中指定的監控範圍。

如果取消選中該核取方塊，則 Kaspersky Embedded Systems Security 將記錄所有指定監控範圍內的事件。

預設情況下，未選中該核取方塊且排除清單為空。

- 點擊“新增”按鈕。

將開啟“選擇要新增的資料夾”視窗。

- 在開啟的視窗中，指定要從監控範圍中排除的資料夾。

- 點擊“確定”。

指定的資料夾被新增到排除範圍清單。

14. 在“檔案操作監控規則”視窗中點擊“確定”。

指定的規則設定將套用於“檔案完整性監控”工作的選定監控範圍。

透過應用程式主控台管理“檔案完整性監控”

在本節中，學習如何透過應用程式主控台配置“檔案完整性監控”工作。

本章節說明項目

配置“檔案完整性監控”工作設定.....	485
配置監控規則.....	486

配置“檔案完整性監控”工作設定

► 要配置一般“檔案完整性監控”工作設定，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“**系統稽核**”節點。
2. 選擇“**檔案完整性監控**”子節點。
3. 在“**檔案完整性監控**”節點的詳細資訊視窗中，點擊“**內容**”連結。

將開啟“**工作設定**”視窗。

4. 在開啟的視窗中，在“**一般**”標籤上，清除或選中“**記錄監控中斷時間發生的檔案操作資訊**”核取方塊。

當由於任何原因（拆除硬碟磁碟機、使用者停止工作、軟體錯誤）工作未執行時，該核取方塊可以啟用或停用“檔案完整性監控”設定中指定的檔案操作的監控。

如果選中該核取方塊，則當“檔案完整性監控”工作未執行時，Kaspersky Embedded Systems Security 將記錄所有監控範圍內的事件。

如果清除該核取方塊，則當工作未執行時，應用程式將不記錄監控範圍內的檔案操作。

預設將會選定該核取方塊。

5. 在“**排程**”和“**進階**”標籤上，設定工作啟動排程（請參見第 [164](#) 頁上的“管理工作排程”部分）。
6. 點擊“**確定**”以儲存變更。

配置監控規則

可以變更檔案完整性監控的預設設定（請參見下表）。

表 56. “檔案完整性監控”工作設定

設定	預設值	敘述
監控範圍	未設定	可以指定操作將監控的資料夾和檔案。將針對指定監控範圍內的資料夾和檔案建立監控事件。
受信任使用者清單	未設定	可以指定使用者和/或使用者群組，其在指定資料夾中的操作將被元件視為安全。
工作未執行時監控檔案操作	已使用	可以啟用或停用工作未執行期間在指定監控範圍內執行的檔案操作的記錄。
將以下資料夾從控制範圍中排除	未套用	可以針對無需監控檔案操作的資料夾檢查排除的使用情況。當“檔案完整性監控”執行時，Kaspersky Embedded Systems Security 將略過指定為排除的監控範圍。
核對總和計算	未套用	可以配置在對檔案做出變更後進行檔案核對總和計算。
考慮檔案操作標記	考慮所有可用的檔案操作標記	可以指定一組檔案操作標記。如果在監控範圍內執行的檔案操作被一個或多個指定標記進行過特徵化，則 Kaspersky Embedded Systems Security 會產生一個稽核事件。
工作啟動排程	不設定工作的初次啟動排程	您可以配置排程的工作啟動設定。

► 要新增監控範圍，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開“系統稽核”節點。
2. 選擇“檔案完整性監控”子節點。
3. 在“檔案完整性監控”節點的詳細資訊視窗中，點擊“檔案操作監控規則”連結。

將開啟“檔案操作監控”視窗。

4. 透過以下方式之一新增監控範圍：

- 如果要透過標準的 Microsoft Windows 對話方塊來選擇資料夾：

- a. 在視窗的左側，點擊“瀏覽”按鈕。

將開啟標準的 Microsoft Windows“瀏覽資料夾”視窗。

- b. 在開啟的視窗中，選擇要監控操作的資料夾，然後點擊“確定”按鈕。
- c. 點擊“新增”按鈕可讓 Kaspersky Embedded Systems Security 開始監控指定監控範圍內的檔案操作。

- 如果想要手動指定監控範圍，請使用支援的遮罩新增路徑：

- <*.ext> - 帶有 <ext> 副檔名的所有檔案，與其位置無關；
- <*\name.ext> - 帶有 <name> 名稱和 <ext> 副檔名的所有檔案，與其位置無關；
- <\dir*> - 位於 <dir> 資料夾中的所有檔案；
- <\dir*\name.ext> - <dir> 資料夾及其所有子資料夾中帶有 <name> 名稱和 <ext> 副檔名的所有檔案。

當手動指定監控範圍時，請確保路徑為以下格式：<卷字母>:\<遮罩>。如果缺少磁區字母，則 Kaspersky Embedded Systems Security 將不會新增指定的監控範圍。

在螢幕的右側，“規則敘述”標籤將顯示受信任使用者和為此監控範圍選定的檔案操作標記。

5. 在新增的監控範圍清單中，選擇您要配置其設定的範圍。
6. 選擇“受信任使用者”標籤。
7. 點擊“新增”按鈕。

將開啟標準的 Microsoft Windows“選擇使用者或群組”視窗。

8. 選擇針對選定的監控範圍 Kaspersky Embedded Systems Security 將視為受信任的使用者或使用群組。

9. 點擊“確定”。

預設情況下，Kaspersky Embedded Systems Security 將未列入受信任使用者清單的所有使用者視為不受信任（請參見第 475 頁上的“關於檔案操作監控規則”部分），並為他們產生緊急事件。

10. 選擇“設定檔案操作標記”標籤。

11. 如果需要，請執行以下操作來選擇一定數量的標記：

- a. 選擇“基於以下標記偵測檔案操作”選項。
- b. 在可用檔案操作清單中（請參見第 475 頁上的“關於檔案操作監控規則”部分），選擇您要監控的操作旁邊的核取方塊。

預設情況下，Kaspersky Embedded Systems Security 將偵測所有檔案操作標記，已選擇“基於所有可辨識的標記偵測檔案操作”選項。

12. 如果執行操作後，您想要 Kaspersky Embedded Systems Security 計算檔案核對總和，請執行以下操作：

- a. 在“核對總和計算”部分中，選擇“如果可能，在檔案變更後計算檔案最終版本的核對總和”核取方塊。

如果選中該核取方塊，則 Kaspersky Embedded Systems Security 將計算修改後的檔案的核對總和，其中偵測到至少帶有一個選定標記的檔案操作。

如果透過許多標記偵測到檔案操作，則將僅計算進行所有修改後的最終檔案核對總和。

如果清除該核取方塊，則 Kaspersky Embedded Systems Security 將為經過修改的檔案計算核對總和。

以下情況不會執行任何核對總和計算：

- 如果檔案變為不可用（例如，由於存取權限的變更造成）。
- 如果此後在已被刪除的檔案中偵測到檔案操作。

預設取消選定該核取方塊。

- b. 在“使用算法計算核對總和”下拉清單中，選擇以下選項之一：

- MD5 雜湊。
- SHA256 雜湊。

13. 如果必要，透過執行以下步驟新增排除的監控範圍：

- a. 選擇“設定排除”標籤。
- b. 選中“考慮排除的監控範圍”核取方塊。

該核取方塊可以針對無需監控檔案操作的資料夾停用排除。

如果選中該核取方塊，則當“檔案完整性監控”工作執行時，Kaspersky Embedded Systems Security 將略過排除清單中指定的監控範圍。

如果取消選中該核取方塊，則 Kaspersky Embedded Systems Security 將記錄所有指定監控範圍內的事件。

預設情況下，未選中該核取方塊且排除清單為空。

- c. 點擊“**瀏覽**”按鈕。

將開啟標準的 Microsoft Windows“**瀏覽資料夾**”視窗。

- d. 在開啟的視窗中，指定要從監控範圍中排除的資料夾。
- e. 點擊“**確定**”。
- f. 點擊“**新增**”按鈕。

指定的資料夾被新增到排除範圍清單。

您也可以使用與用於指定監控範圍相同的遮罩來新增排除的監控範圍。

14. 點擊“**儲存**”按鈕以套用新的規則配置。

記錄審查

本節包含有關“記錄審查”工作和工作設定的資訊。

本章內容

關於“記錄審查”工作.....	491
“記錄審查”工作預設設定	493
透過管理外掛程式管理記錄審查規則.....	493
透過應用程式主控台管理記錄審查規則	498

關於“記錄審查”工作

當“記錄審查”工作執行時，Kaspersky Embedded Systems Security 將根據 Windows 事件記錄的審查結果監控受防護環境的完整性。一旦偵測到系統中存在異常行為，應用程式將通知管理員，這些異常行為可能表示存在網路攻擊嘗試。

Kaspersky Embedded Systems Security 將考慮 Window 事件記錄，並根據使用者指定的規則或啟發式分析的設定（工作用它來審查記錄）來識別入侵。

預定義規則和啟發式分析

透過套用基於現有啟發的預定義規則，可以使用“記錄審查”工作來監控受防護系統的狀態。啟發式分析可識別受防護電腦上的異常活動，這些異常活動可作為嘗試攻擊的憑證。用於辨識異常行為的範本包括在預定義規則設定中的可用規則內。

“記錄審查”工作的規則清單中包含七條規則。您可以啟用或停用任何一條規則。您不能刪除現有規則或建立新規則。

可以為監控以下操作事件的規則配置觸發條件：

- 密碼暴力破解偵測

- 網路登入偵測

還可在工作設定中配置排除。當登入由受信任使用者執行或從受信任的 IP 位址執行時，不會啟動啟發式分析。

如果工作不使用啟發式分析，則 Kaspersky Embedded Systems Security 不會使用啟發來審查 Windows 記錄。預設情況下，啟用啟發式分析。

當套用規則時，應用程式將在“記錄審查”工作記錄中記錄一個緊急事件。

自訂記錄審查工作的規則

可以使用工作規則設定來指定和變更在 Windows 記錄中偵測到選定事件時的觸發規則條件。預設情況下，記錄審查工作規則的清單包含四種規則。可以啟用和停用這些規則、刪除規則和編輯規則設定。

可以為每種規則配置以下規則觸發條件：

- Windows 事件記錄中的記錄識別碼清單。

如果事件內容包含為該規則指定的事件識別碼，則當在 Windows 事件記錄中建立新的記錄時將觸發該規則。也可以為每個指定的規則新增和刪除識別碼。

- 事件來源。

對於每個規則，可以定義 Windows 事件記錄的子記錄。應用程式將僅在此子記錄中搜尋帶有指定事件識別碼的記錄。您可以選擇其中一個標準子記錄（應用程式、安全性或系統）或在來源選擇欄位中輸入名稱來指定自訂子記錄。

應用程式不會驗證指定的子記錄是否確實存在於 Windows 事件記錄中。

觸發規則後，Kaspersky Embedded Systems Security 將在“記錄審查”工作記錄中記錄一個緊急事件。

預設情況下，記錄審查工作套用自訂規則。

在啟動“記錄審查”工作前，請確保系統系統稽核記錄政策已正確設定。有關詳細資訊，請參見 Microsoft 文章 (<https://technet.microsoft.com/en-us/library/cc952128.aspx>)。

“記錄審查”工作預設設定

預設情況下，“記錄審查”工作具有下表所述的設定。您可以變更這些設定值。

表 57. “檔案完整性監控”工作設定

設定	預設值	敘述
對“記錄審查”套用自訂規則	已套用。	您可以啟用、停用、新增或修改自訂規則。
對“記錄審查”套用預定義規則	已套用。	您可以啟用或停用啟發式分析，它可以偵測受保護伺服器上的異常活動。
暴力破解攻擊偵測	每 300 秒 10 次登入失敗。	您可以設定嘗試次數和這些嘗試出現的期限，這些將被視為啟發式分析的觸發器。
網路登入	12:00:00 AM.	您可以指定時間間隔的開始和結束時間，在此時間間隔中 Kaspersky Embedded Systems Security 將登入嘗試視為異常活動。
排除	未套用。	您可以指定不會觸發啟發式分析的使用者和 IP 位址。
工作啟動排程	不設定工作的初次啟動排程。	您可以配置排程的工作啟動設定。

透過管理外掛程式管理記錄審查規則

在本節中，學習如何透過管理外掛程式新增和配置記錄審查規則。

本章節說明項目

透過管理外掛程式管理預定義工作規則	494
透過管理外掛程式新增記錄審查規則	496

透過管理外掛程式管理預定義工作規則

► 執行以下操作為“記錄審查”工作配置預定義規則：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“政策”標籤，然後開啟“內容：<政策名稱>”視窗（請參見第 144 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“裝置”標籤，然後開啟“應用程式設定”視窗（請參見第 150 頁上的“在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“應用程式設定”視窗中編輯這些設定。

4. 在“系統稽核”部分中，點擊“記錄審查”設定塊中的“設定”按鈕。
將開啟“記錄審查”視窗。
5. 選擇“預定義規則”標籤。
6. 選中或清除“對記錄審查套用自訂規則”核取方塊。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將套用啟發式分析來偵測受防護電腦上的異常活動。

如果清除此核取方塊，則未執行啟發式分析且 Kaspersky Embedded Systems Security 將套用預設或自訂規則來偵測異常活動。

預設將會選定該核取方塊。

為了能夠執行工作，必須選擇至少一種記錄審查規則。

7. 從預定義規則清單中選擇您要套用的規則：

- 系統中存在可能的暴力破解攻擊的模式。
- 系統中存在可能的 Windows 事件記錄濫用的模式。
- 偵測到表示已安裝新服務的異常活動。
- 偵測到使用顯式憑證的異常登入。
- 系統中存在可能的 Kerberos 偽造 PAC (MS14-068) 攻擊的模式。
- 偵測到特權內建群組 Administrators 發出的異常操作。
- 在網路登入工作階段期間偵測到異常活動。

8. 要配置選定規則，請點擊“**進階設定**”按鈕。

將開啟“**記錄審查**”視窗。

9. 在“**暴力破解攻擊偵測**”部分中，設定嘗試次數和這些嘗試出現的期限，這些將被視為啟發式分析的觸發器。

10. 在“**網路登入偵測**”部分中，指定時間間隔的開始和結束時間，在此時間間隔中 Kaspersky Embedded Systems Security 將登入嘗試視為異常活動。

11. 選擇“**排除**”標籤。

12. 執行以下操作新增受信任使用者：

- a. 點擊“**瀏覽**”按鈕。
- b. 選擇使用者。
- c. 點擊“**確定**”。

選定的使用者將被新增到受信任使用者清單中。

13. 執行以下操作新增受信任的 IP 位址：

- a. 輸入 IP 位址。
- b. 點擊“新增”按鈕。

14. 輸入的 IP 位址將被新增到受信任的 IP 位址清單中。

15. 在“工作管理”標籤上，設定工作啟動排程（請參見第 [164](#) 頁上的“配置工作啟動排程設定”部分）。

16. 點擊“確定”。

儲存記錄審查工作配置。

透過管理外掛程式新增記錄審查規則

► 執行以下操作可新增和配置新的記錄審查自訂規則：

1. 展開卡斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳細視窗中執行以下之一操作：
 - 要為一組電腦配置應用程式設定，請選擇“政策”標籤，然後開啟“內容：<政策名稱>”視窗（請參見第 [144](#) 頁上的“配置政策”部分）。
 - 如果要為單台電腦配置應用程式，請選擇“裝置”標籤，然後開啟“應用程式設定”視窗（請參見第 [150](#) 頁上的“在卡斯基安全管理中心的應用程式設定視窗中配置本機工作”部分）。

如果某個活動卡斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“應用程式設定”視窗中編輯這些設定。

4. 在“系統稽核”部分中，點擊“記錄審查”設定塊中的“設定”按鈕。

將開啟“記錄審查”視窗。

5. 在“自訂規則”標籤上，選中或清除“套用記錄審查的自訂規則”標籤。

如果選中該核取方塊，則 Kaspersky Embedded Systems Security 將根據每個規則設定對“記錄審查”套用自訂規則。您可以新增、刪除或配置記錄審查規則。

如果清除該核取方塊，則不能新增或修改自訂規則。Kaspersky Embedded Systems Security 將套用預設規則設定。

預設將會選定該核取方塊。只有應用程式彈出偵測規則處於活動狀態。

可以控制是否對記錄審查套用預設的規則。選擇您要對記錄審查套用的規則所對應的核取方塊。

6. 要新增新的自訂規則，請點擊“新增”按鈕。

將開啟“記錄審查規則”視窗。

7. 在“一般”部分中，輸入有關新規則的以下資訊：

- 規則名稱
- 來源

選擇要將已記錄的事件用於分析的來源記錄。提供以下 Windows 事件記錄類型：

- 應用程式
- 安全性
- 系統

您可以在“來源”欄位中輸入記錄名稱來新增新的自訂記錄。

8. 在“已觸發的事件 ID”部分中，指定偵測時將觸發規則的項目 ID：

- a. 輸入 ID 的數值。
- b. 點擊“新增”按鈕。

選定的規則 ID 將被新增到清單中。可以為每個規則新增無限數量的識別碼。

- c. 點擊“確定”。

記錄審查規則將被新增到規則清單中。

透過應用程式主控台管理記錄審查規則

在本節中，學習如何透過應用程式主控台新增和配置記錄審查規則。

本章節說明項目

透過應用程式主控台管理預定義工作規則.....	498
配置記錄審查規則.....	500

透過應用程式主控台管理預定義工作規則

► 執行以下操作可以為記錄審查工作配置啟發式分析：

1. 在應用程式主控台樹狀目錄中，展開“系統稽核”節點。
2. 選擇“記錄審查”子節點。
3. 在“記錄審查”節點的詳細資訊視窗中，點擊“內容”連結。

將開啟“工作設定”視窗。

4. 選擇“預定義規則”標籤。
5. 選中或清除“對記錄審查套用自訂規則”核取方塊。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將套用啟發式分析來偵測受防護電腦上的異常活動。

如果清除此核取方塊，則未執行啟發式分析且 Kaspersky Embedded Systems Security 將套用預設或自訂規則來偵測異常活動。

預設將會選定該核取方塊。

為了能夠執行工作，必須選擇至少一種記錄審查規則。

6. 從預定義規則清單中選擇您要套用的規則：
 - 系統中存在可能的暴力破解攻擊的模式。
 - 系統中存在可能的 Windows 事件記錄濫用的模式。
 - 偵測到表示已安裝新服務的異常活動。
 - 偵測到使用顯式憑證的異常登入。
 - 系統中存在可能的 Kerberos 偽造 PAC (MS14-068) 攻擊的模式。
 - 偵測到特權內建群組 Administrators 發出的異常操作。
 - 在網路登入工作階段期間偵測到異常活動。
7. 要設定選定的規則，請轉至“**延伸**”標籤。
8. 在“**暴力破解攻擊偵測**”中，設定嘗試次數和這些嘗試出現的期限，這些將被視為啟發式分析的觸發器。
9. 在“**網路登入**”部分中，指定時間間隔的開始和結束時間，在此時間間隔中 Kaspersky Embedded Systems Security 將登入嘗試視為異常活動。
10. 選擇“**排除**”標籤。
11. 執行以下操作新增受信任使用者：
 - a. 點擊“**瀏覽**”按鈕。
 - b. 選擇使用者。
 - c. 點擊“**確定**”。

選定的使用者將被新增到受信任使用者清單中。
12. 執行以下操作新增受信任的 IP 位址：
 - a. 輸入 IP 位址。
 - b. 點擊“**新增**”按鈕。

輸入的 IP 位址將被新增到受信任的 IP 位址清單中。

13. 選擇“**排程**”和“**進階**”標籤以配置工作啟動排程。
14. 點擊“**確定**”。

儲存記錄審查工作配置。

配置記錄審查規則

執行以下操作可新增和配置新的記錄審查自訂規則：

1. 在應用程式主控台樹狀目錄中，展開“**系統稽核**”節點。
2. 選擇“**記錄審查**”子節點。
3. 在“**記錄審查**”節點的詳細資訊視窗中，點擊“**記錄審查規則**”連結。

將開啟“**記錄審查規則**”視窗。

4. 選中或清除“**對記錄審查套用自訂規則**”核取方塊。

如果選中該核取方塊，則 Kaspersky Embedded Systems Security 將根據每個規則設定對“**記錄審查**”套用自訂規則。您可以新增、刪除或配置記錄審查規則。

如果清除該核取方塊，則不能新增或修改自訂規則。Kaspersky Embedded Systems Security 將套用預設規則設定。

預設將會選定該核取方塊。只有應用程式彈出偵測規則處於活動狀態。

可以控制是否對“**記錄審查**”工作套用預設的規則。選擇您要對記錄審查套用的規則所對應的核取方塊。

5. 要建立新的自訂規則，請執行以下操作：
 - a. 輸入新規則的名稱。
 - b. 點擊“**新增**”按鈕。

建立的規則將新增到一般規則清單中。

6. 若要配置任何規則，請執行以下步驟：

a. 使用滑鼠左鍵點擊可在清單中選擇規則。

在視窗的右側區域中，“敘述”標籤將顯示有關該規則的一般資訊。

新規則的敘述為空白。

b. 選擇“規則敘述”標籤。

c. 如果需要，在“一般”部分中，編輯規則名稱。

d. 選擇“來源”。

7. 在“事件識別碼”部分中，指定偵測時將觸發規則的項目 ID：

a. 輸入 ID 的數值。

b. 點擊“新增”按鈕。

選定的規則 ID 將被新增到清單中。可以為每個規則新增無限數量的識別碼。

c. 點擊“儲存”按鈕。

將套用已配置的記錄審查規則。

自訂掃描

本節提供有關自訂掃描工作的資訊，並說明如何配置自訂掃描工作設定和受防護電腦上的安全性設定。

本章內容

關於自訂掃描工作	502
關於掃描範圍	503
預設的掃描範圍	504
雲端儲存檔案掃描	506
自訂掃描工作中所選節點的安全性設定	508
為自訂掃描工作的預設安全等級	508
關於卸除式磁碟機掃描	510
預設自訂掃描工作設定	512
透過管理外掛程式管理自訂掃描工作	514
透過應用程式主控台管理自訂掃描工作	536

關於自訂掃描工作

Kaspersky Embedded Systems Security 會掃描指定區域，以偵測病毒和其他電腦安全威脅。Kaspersky Embedded Systems Security 將掃描電腦檔案、記憶體以及自動執行物件。

Kaspersky Embedded Systems Security 提供了以下自訂掃描系統工作：

- Kaspersky Embedded Systems Security 每次啟動時都會執行“在作業系統啟動時掃描”工作。Kaspersky Embedded Systems Security 將掃描硬碟磁碟機和卸除式磁碟機的開機磁區和主開機記錄、系統記憶體以及處理程序記憶體。Kaspersky Embedded Systems Security 每次執行該工作時，都會建立未感染的開機磁區的副本。下次啟動工作時，如果在這些磁區中偵測到威脅，程式會使用備份副本中的磁區進行替換。
- 預設情況下，會根據排程每週執行一次“關鍵區域掃描”工作。Kaspersky Embedded Systems Security 將掃描作業系統關鍵區域中的物件：自動執行物件、硬碟磁碟機和卸除式磁碟機的開機磁區和主開機記錄、系統記憶體以及處理程序記憶體。應用程式會掃描系統資料夾中的檔案，例如 %windir%\system32 中的檔案。Kaspersky Embedded Systems Security 將套用與建議等級（請參見第 508 頁上的“關於自訂掃描工作的預設安全等級”部分）的值相應的安全性設定。您可以修改“關鍵區域掃描”工作的設定。
- 預設在每次資料庫更新後按排程執行“隔離區掃描”工作。無法修改“隔離區掃描”工作範圍。
- “應用程式完整性控制”工作每天執行。它提供了檢查 Kaspersky Embedded Systems Security 模組是否損壞或修改的選項。檢查程式安裝資料夾。工作執行統計資料套件含有關已檢查和已損壞的模組數目的資訊。預設情況下，工作設定已定義，無法編輯。可以編輯工作啟動排程設定。

此外，您還可以建立自訂的自訂掃描工作，例如，掃描電腦上的共用資料夾的工作。

Kaspersky Embedded Systems Security 可以一次執行多個自訂掃描工作。

關於掃描範圍

您可以配置“在作業系統啟動時掃描”和“關鍵區域掃描”工作，以及自訂“自訂掃描”工作的掃描範圍。

預設情況下，自訂掃描工作將掃描電腦檔案系統中的所有物件。如果不需要對檔案系統中的所有物件進行安全掃描，您可以限制掃描範圍。

在應用程式主控台中，掃描範圍以 Kaspersky Embedded Systems Security 可以控制的電腦檔案資源樹狀目錄或清單的形式顯示。預設情況下，受防護電腦的網路檔案資源以清單圖示模式顯示。

► 若要以樹狀檢視模式顯示網路檔案資源，

請開啟“設定掃描範圍”設定視窗中的下拉清單，然後選擇“樹狀檢視”。

節點將顯示在電腦檔案資源的清單檢視或樹狀檢視模式中，如下所示：

節點包括在掃描範圍內。

該節點已從掃描範圍中排除。

該節點至少有一個子節點排除在掃描範圍之外，或子節點的安全性設定與父節點的安全性設定不同（僅限樹狀檢視模式）。

如果選擇所有子節點，但未選擇父節點，則顯示  圖示。在這種情況下，在為所選子節點修改掃描範圍時，如果父節點所包含的檔案和資料夾發生變更，將自動略過這些變更。

掃描範圍中虛擬節點的名稱以藍色字體顯示。

預設的掃描範圍

所選自訂掃描工作的電腦檔案資源樹狀目錄或清單顯示在“設定掃描範圍”標籤上。

檔案資源樹狀目錄或清單顯示基於 Microsoft Windows 的配置安全設定所擁有的讀取存取權限的節點。

Kaspersky Embedded Systems Security 包含以下預設掃描範圍：

- **我的電腦。** Kaspersky Embedded Systems Security 掃描整台電腦。
- **本機磁碟。** Kaspersky Embedded Systems Security 掃描電腦硬碟磁碟機上的物件。您可以在掃描範圍中包含或排除所有硬碟磁碟機、單個磁碟、資料夾或檔案。
- **卸除式磁碟機。** Kaspersky Embedded Systems Security 掃描外部裝置(如 CD 或 USB 磁碟機)上的檔案。您可以在掃描範圍中包含或排除所有卸除式裝置、單個磁碟、資料夾或檔案。

- **網路。**您可以按照 UNC (通用命名慣例) 格式指定網路資料夾或檔案路徑以將它們新增至掃描範圍。用於啟動工作的帳戶必須擁有對新增網路資料夾和檔案的存取權限。預設情況下，自訂掃描在系統帳戶下執行。

已連線的網路磁碟也不會顯示在電腦檔案資源樹狀目錄中。若要在掃描範圍中包含網路磁碟上的物件，請以 UNC 格式指定對應於該網路磁碟的資料夾。

- **系統記憶體。**在啟動掃描之後，Kaspersky Embedded Systems Security 將掃描作業系統中正在執行的處理程序的可執行檔和模組。
- **啟動物件。**Kaspersky Embedded Systems Security 掃描登錄機碼和設定檔所引用的物件，例如 WIN.INI 或 SYSTEM.INI，以及在電腦啟動時自動啟動的應用程式模組。
- **共用資料夾。**您可以將受防護電腦上的共用資料夾包含在掃描範圍中。
- **虛擬磁碟機。**您可以將動態資料夾和檔案以及連線到電腦的硬碟包含在掃描範圍內，例如共用叢集硬碟 (建立虛擬防護範圍)。

使用 SUBST 指令建立的虛擬硬碟將不會顯示在應用程式主控台的電腦檔案資源樹狀目錄中。若要掃描虛擬硬碟上的物件，請將與此虛擬硬碟關聯的電腦資料夾包含在掃描範圍中。

預設情況下，您可以在網路檔案資源樹狀目錄中檢視和配置預設掃描範圍；還可以在網路檔案資源清單形成期間在掃描範圍設定中向該清單新增預設範圍。

預設情況下，“自訂掃描”工作在以下範圍下執行：

- “在作業系統啟動時掃描”工作：
 - 本機磁碟
 - 卸除式磁碟機
 - 系統記憶體
- 關鍵區域掃描：
 - 本機磁碟 (排除 Windows 資料夾)

- 卸除式磁碟機
- 系統記憶體
- 啟動物件
- 其他工作：
 - 本機磁碟 (排除 Windows 資料夾)
 - 卸除式磁碟機
 - 系統記憶體
 - 啟動物件
 - 共用資料夾

雲端儲存檔案掃描


關於雲端檔案

Kaspersky Embedded Systems Security 可以與 Microsoft OneDrive 雲端檔案進行互動。該應用程式支援新的“OneDrive 檔案自訂”功能。

Kaspersky Embedded Systems Security 不支援其他雲端儲存。

“OneDrive 自訂檔案”幫助您存取您在 OneDrive 中的所有檔案，而無需下載所有檔案和使用裝置上的儲存空間。您可以在需要時將檔案下載到硬碟磁碟機。

當“OneDrive 自訂檔案”功能開啟時，可以在檔案資源管理器的“狀態”列中看到每個檔案旁邊的狀態圖示。每個檔案都具有以下狀態之一：

 此狀態圖示指示檔案 *僅線上可用*。僅線上檔案不會物理儲存在您的硬碟磁碟機中。當裝置未連線到 Internet 時，無法開啟僅線上檔案。

- 🟢 此狀態圖示指示檔案 **本機可用**。當開啟僅線上檔案時會顯示此圖示，該檔案會下載到您的裝置中。您可以隨時開啟本機可用的檔案，即使沒有 Internet 存取權限。要清理空間，可以將檔案變更回 ☁️ 僅線上。
- 🟢 此狀態圖示指示檔案 **儲存在硬碟磁碟機中並且始終可用**。

雲端檔案掃描

Kaspersky Embedded Systems Security 只能掃描受防護電腦上本機儲存的雲端檔案。此類 OneDrive 檔案的狀態為 🟢 和 🟢。在掃描期間會略過 ☁️ 檔案，因為這些檔案沒有物理儲存在受防護電腦上。

Kaspersky Embedded Systems Security 在掃描時不會自動從雲端下載 ☁️ 檔案，即使這些檔案已包括在掃描範圍中。

在各種方案中，雲端檔案由多種 Kaspersky Embedded Systems Security 工作處理，具體取決於工作類型：

- 即時雲端檔案掃描：您可以將包含雲端檔案的資料夾新增到“即時檔案防護”工作的防護範圍中。當使用者存取該檔案時會對該檔案進行掃描。如果使用者存取 ☁️ 檔案，系統會下載該檔案，該檔案將變為本機可用，並且其狀態將變更為 🟢。這樣該檔案可以被“即時檔案防護”工作處理。
- 自訂雲端檔案掃描：您可以將包含雲端檔案的資料夾新增到“自訂掃描”工作的掃描範圍中。該工作會掃描狀態為 🟢 和 🟢 的檔案。如果在範圍中找到任何 ☁️ 檔案，在掃描期間將略過這些檔案，並在工作記錄中記錄資訊事件，指示所掃描的檔案只是雲端檔案的預留位置，並不存在於本機磁碟機中。
- 應用程式控制規則建立和使用：您可以使用“應用程式啟動控制規則產生器”工作為 🟢 和 🟢 檔案建立允許和拒絕規則。“應用程式啟動控制”工作應用“預設拒絕”原則和所建立的規則來處理和封鎖雲端檔案。

“應用程式啟動控制”工作會封鎖所有雲端檔案啟動，不管它們的狀態如何。應用程式不會將 ☁️ 檔案包括在規則建立範圍中，因為它們沒有物理儲存在硬碟磁碟機上。由於不能為此類檔案建立任何允許規則，因此對它們實施“預設拒絕”原則。

在 OneDrive 雲端檔案中偵測到威脅時，應用程式會應用執行掃描的工作的設定中指定的操作。這樣，可以將檔案刪除、解毒、移至隔離區或備份。

按照相關 [Microsoft OneDrive](#) 文件中概述的政策，對本機檔案的變更將與 [OneDrive](#) 中儲存的副本進行同步。

自訂掃描工作中所選節點的安全性設定

在所選的自訂掃描工作中，若要修改安全性設定的預設值，可透過將它們配置為用於整個防護或掃描範圍的一般設定，或為電腦檔案資源樹狀目錄或清單中的不同節點或項配置不同設定。

為所選父節點配置的安全設定將自動套用到所有子節點。父節點的安全設定不會套用到單獨配置的子節點。

您可以使用以下方式之一配置選定掃描範圍或防護範圍的設定：

- 從三個預設的安全等級中選擇一個等級（**最佳效能**、**建議**或**最佳防護**）。
- 在電腦檔案資源樹狀目錄或清單中手動變更選定節點或項的安全性設定（安全等級變更為“**自訂**”）。

您可以將一組節點設定儲存為範本，以便隨後套用至其他節點。

為自訂掃描工作的預設安全等級

安全性設定“[使用 iChecker 技術](#)”、“[使用 iSwift 技術](#)”、“[使用啟發式分析](#)”和“[在檔案中檢查 Microsoft 簽章](#)”並未包含在預設安全等級設定中。如果“[使用 iChecker 技術](#)”、“[使用 iSwift 技術](#)”、“[使用啟發式分析](#)”和“[在檔案中檢查 Microsoft 簽章](#)”等設定的狀態發生改變，則您選擇的預設安全等級不會變更。

電腦檔案資源樹狀目錄中所選的節點可套用三個預設安全性設定：“**最佳效能**”、“**建議**”和“**最佳防護**”。這些等級均有各自的安全設定集（請參閱下表）。

最佳效能

如果除了在電腦上使用 [Kaspersky Embedded Systems Security](#) 外，還在網路內採用了其他電腦安全措施（例如，防火牆和現有安全政策），則建議使用“**最佳效能**”安全等級。

建議

“**建議**”安全等級確保防護與對電腦的效能影響的最佳組合。Kaspersky Lab 專家建議使用該等級，因為它足以防護大多數公司網路上的電腦。預設情況下，將設定“**建議**”安全等級。

最佳防護

如果組織的網路有更高的電腦安全要求，則建議使用“**最佳防護**”安全等級。

表 58. 預設安全等級和相應的安全性設定值

選項	安全等級		
	最佳效能	建議	最佳防護
掃描物件	依格式	所有物件	所有物件
僅掃描新增與變更過的檔案	已啟用	已停用	已停用
對受感染物件和其他物件執行的操作	解毒。解毒失敗則刪除	執行建議的操作（解毒。解毒失敗則刪除）	解毒。解毒失敗則刪除
對可疑物件執行的操作	隔離	執行建議的操作（隔離）	隔離
排除檔案	否	否	否
不偵測	否	否	否
超過以下時間則停止掃描 (秒)	60 秒	否	否
不掃描超過此值複合檔案 (MB)	8 MB	否	否

選項	安全等級		
掃描 NTFS 交換資料串流	是	是	是
掃描開機磁區和 MBR	是	是	是
掃描複合檔案	<ul style="list-style-type: none"> • SFX 壓縮檔案* • 封裝的物件* • 內嵌的 OLE 物件* <p>*僅新物件和已修改的物件</p>	<ul style="list-style-type: none"> • 壓縮檔案* • SFX 壓縮檔案* • 封裝的物件* • 內嵌的 OLE 物件* <p>* 所有物件</p>	<ul style="list-style-type: none"> • 壓縮檔案* • SFX 壓縮檔案* • 電子郵件資料庫* • 純文字郵件* • 封裝的物件* • 內嵌的 OLE 物件* <p>* 所有物件</p>

關於卸除式磁碟機掃描

可以配置透過 USB 連接埠連線到受防護電腦上的卸除式磁碟機的掃描。

Kaspersky Embedded Systems Security 使用自訂掃描工作掃描卸除式磁碟機。當卸除式磁碟機已連線並在完成掃描後刪除工作時，應用程式會自動建立新的自訂掃描工作。系統會根據為卸除式磁碟機掃描定義的預設安全等級來執行建立的工作。您不能配置臨時自訂掃描工作的設定。

如果您已安裝不帶病毒資料庫的 Kaspersky Embedded Systems Security，則將無法執行卸除式磁碟機掃描。

Kaspersky Embedded Systems Security 使用自訂掃描工作掃描卸除式磁碟機。當卸除式磁碟機已連線並在完成掃描後刪除工作時，應用程式會自動建立新的自訂掃描工作。系統會根據為卸除式磁碟機掃描定義的預設安全等級來執行建立的工作。您不能配置臨時自訂掃描工作的設定。

當它們在作業系統中註冊為 USB 大容量儲存裝置時，Kaspersky Embedded Systems Security 將掃描連線的卸除式 USB 磁碟機。如果連線被裝置控制工作封鎖，則應用程式不會掃描卸除式磁碟機。應用程式不會掃描 MTP 連線的行動裝置。

Kaspersky Embedded Systems Security 允許在掃描期間存取卸除式磁碟機。

每個卸除式磁碟機的掃描結果提供在連線卸除式磁碟機時建立的自訂掃描工作的記錄中。

可以變更卸除式磁碟機掃描元件的設定（請參見以下表格）。

表 59. 卸除式磁碟機掃描設定

設定	預設值	敘述
掃描透過 USB 連接的卸除式磁碟機	已清除核取方塊	您可以開啟或關閉透過 USB 連線到受防護電腦上的卸除式磁碟機的掃描。
掃描卸除式磁碟機，如果其儲存的資料量未超過 (MB)	1024 MB	您可透過在卸除式磁碟機上設定最大資料量，來縮小元件的範圍。 如果儲存的資料量超出指定值，Kaspersky Embedded Systems Security 不會執行卸除式磁碟機掃描。
掃描時使用的安全等級	最佳防護	您可透過選擇以下三個安全等級之一來配置建立的自訂掃描工作： <ul style="list-style-type: none"> • 最佳防護 • 建議 • 最佳效能 當偵測到已感染、可疑感染和其他物件時使用的算法，以及每個安全等級的其他掃描設定，對應於自訂掃描工作中的預設安全等級。

預設自訂掃描工作設定

預設情況下，自訂掃描工作將使用下表所述的設定。您可以配置系統和使用者自訂掃描工作。

表 60. 預設自訂掃描工作設定

設定	值	敘述
掃描範圍	套用於系統和自訂工作： <ul style="list-style-type: none"> 在作業系統啟動時掃描：整個伺服器，排除共用資料夾和自動運行的物件。 關鍵區域掃描：整個伺服器，排除共用資料夾和某些作業系統檔案。 自訂自訂掃描工作：整個伺服器。 	您可以變更掃描範圍。不能為“隔離區掃描”和“應用程式完整性控制”系統工作配置掃描範圍。
安全性設定	對應“建議”安全等級的整個掃描範圍的一般設定。	您可以對電腦檔案資源清單或樹狀目錄中選定的節點執行以下操作： <ul style="list-style-type: none"> 選擇不同的預定義安全等級 手動變更安全性設定 您可以將選定節點的安全性設定儲存為範本，以便在以後將其套用至其他節點。
使用啟發式分析	與“關鍵區域掃描”、“在作業系統啟動時掃描”和自訂工作的“中度”分析等級結合使用。 與“隔離區掃描”工作的“深度”分析等級結合使用。	您可以啟用或停用“啟發式分析”並設定分析等級。不能配置“隔離區掃描”工作分析級別。 “應用程式完整性控制”工作中未使用啟發式分析。
套用信任區域	已套用（不適用於“隔離區掃描”工作）	可用於所選工作中的一般排除清單。

設定	值	敘述
在掃描中使用 KSN	已套用	您可以使用卡斯基安全網路雲端服務的基礎架構提高您的伺服器防護能力。
工作啟動設定及權限	在系統帳戶下啟動工作。	您可以編輯所有系統和使用者“自訂掃描”工作的啟動設定及帳戶權限，但“隔離區掃描”和“應用程式完整性控制”工作除外。
在背景模式下執行工作（低優先順序）	未套用	您可以配置自訂掃描工作的優先順序。
工作啟動排程	套用於系統工作： <ul style="list-style-type: none"> 在作業系統啟動時掃描 - 在應用程式啟動時 關鍵區域掃描 - 每週 隔離區掃描 - 應用程式資料庫更新後 應用程式完整性控制 - 每天 新建自訂工作中未使用。	您可以配置排程的工作啟動設定。
記錄掃描執行記錄並更新伺服器防護狀態	執行關鍵區域掃描後，每週更新一次伺服器防護狀態。	可透過以下方式配置記錄關鍵區域掃描執行記錄的相關設定： <ul style="list-style-type: none"> 編輯關鍵區域掃描工作啟動排程的設定。 編輯關鍵區域掃描工作的掃描範圍。 建立使用者自訂掃描工作。

透過管理外掛程式管理自訂掃描工作

在本節中，學習如何導航管理外掛程式介面，以及如何為網路中的一台或所有電腦配置工作設定。

本章節說明項目

導航.....	514
建立自訂掃描工作.....	516
配置工作掃描範圍.....	523
為自訂掃描工作選擇預設的安全等級.....	524
手動配置安全性設定.....	525
配置卸除式磁碟機掃描.....	535

導航

學習如何透過介面導航到所需工作設定。

本章節說明項目

開啟自訂掃描工作精靈.....	514
開啟自訂掃描工作內容.....	516

開啟自訂掃描工作精靈

► *要開始建立新的自訂自訂掃描工作：*

1. 若要建立本機工作，請執行以下步驟：
 - a. 展開卡巴斯基安全管理中心管理主控台中的“受管理裝置”節點。
 - b. 選擇電腦所屬的管理群組。

- c. 在詳細資訊視窗的“裝置”標籤上，開啟受防護伺服器的內容功能表。
- d. 選擇“內容”功能表選項。
- e. 在開啟的視窗中，點擊“工作”部分中的“新增”按鈕。

將開啟“新建工作精靈”視窗。

2. 建立群組工作：

- a. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
- b. 選取要為其建立工作的管理群組。
- c. 開啟“工作”標籤。
- d. 點擊“建立工作”按鈕。

將開啟“新建工作精靈”視窗。

3. 要為自訂的一組電腦建立工作：

- a. 在卡巴斯基安全管理中心管理主控台樹狀目錄的“裝置選擇”節點中，點擊“執行選擇”按鈕以執行裝置選擇。
- b. 開啟“選擇結果(選擇名稱)”標籤。
- c. 在“執行選擇”下拉清單中，選擇“為選擇結果建立工作”選項。

將開啟“新建工作精靈”視窗。

4. 在 Kaspersky Embedded Systems Security 的可用工作清單中選擇“自訂掃描”工作。

5. 點擊“下一步”。

將開啟“設定”視窗。

根據需要配置工作設定。

► 要配置現有自訂掃描工作，

請點擊卡巴斯基安全管理中心工作清單中的工作名稱。

將開啟“內容：自訂掃描”視窗。

開啟自訂掃描工作內容

► 要開啟單台電腦的自訂掃描工作的應用程式內容：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇受防護電腦所屬的管理群組。
3. 選擇“裝置”標籤。
4. 點擊要為其配置掃描範圍的電腦的名稱。

將開啟“內容：<電腦名稱>”視窗。

5. 選擇“工作”部分。
6. 在為裝置建立的工作清單中，選擇您建立的自訂掃描工作。
7. 點擊“內容”按鈕。

將開啟“內容：自訂掃描”視窗。

根據需要配置工作設定。

建立自訂掃描工作

► 要建立自訂自訂掃描工作：

1. 開啟“新建工作精靈”中的“設定”視窗（請參見第 [514](#) 頁上的“開啟自訂掃描工作精靈”部分）。
2. 選擇所需的工作建立方法。
3. 點擊“下一步”。

4. 在“掃描範圍”視窗中建立掃描範圍：

根據預設，掃描範圍包括電腦的關鍵區域。掃描範圍在表格中使用圖示 標記。排除的掃描範圍在表中用圖示 標記。

掃描範圍可以修改：新增特定的預先定義的掃描範圍、磁碟、資料夾及檔案，並為每個新增的範圍指定特定的安全性設定。

- 要從掃描中排除所有關鍵區域，請在每行上開啟內容功能表並選擇“**刪除範圍**”選項。
- 要在掃描範圍中包括預定義的掃描範圍、磁碟、資料夾、網路物件或檔案：
 - a. 右鍵點擊“**掃描範圍**”表，然後選擇“**新增範圍**”或點擊“**新增**”按鈕。
 - b. 在“**新增物件至掃描範圍**”視窗中，選擇“**預設的範圍**”清單中的預設範圍，指定電腦或另外一台網路電腦上的電腦磁碟、資料夾、網路物件或檔案，然後點擊“**確定**”按鈕。
- 要從掃描中排除子資料夾或檔案，請在精靈的“**掃描範圍**”視窗中選擇已新增的資料夾（磁碟）：
 - a. 開啟內容功能表，然後選擇“**配置**”選項。
 - b. 在“**安全等級**”視窗中點擊“**設定**”按鈕。
 - c. 在“**自訂掃描設定**”設定視窗的“**一般**”標籤上，清除“**子檔案和子資料夾**”核取方塊。
- 要變更掃描範圍安全性設定：
 - a. 開啟您希望配置其設定的範圍的內容功能表，然後選擇“**配置**”。
 - b. 在“**自訂掃描設定**”設定視窗中，選擇預設的安全等級之一，或者點擊“**設定**”按鈕以手動配置安全性設定。

安全性設定的設定方式與即時檔案防護工作的設定方式相同(請參見第 313 頁上的“**手動設定安全性設定**”部分)。

- 要略過新增的掃描範圍中的嵌入式物件：
 - a. 開啟“**掃描範圍**”表的內容功能表，選擇“**新增排除項目**”。

b. 指定要排除的物件：在“**預設的範圍**”清單中選擇預設範圍，指定電腦或另一台網路電腦上的電腦磁碟、資料夾、網路物件或檔案。

c. 點擊“**確定**”按鈕。

5. 在“**選項配置卸除式磁碟機掃描**”視窗中，配置啟發式分析以及與其他元件的整合：

- 配置啟發式分析的使用（請參見第 [308](#) 頁上的“配置啟發式分析以及與其他應用程式元件的整合”部分）。
- 如果您希望從工作的掃描範圍中排除已新增到信任區域清單的物件，則選中“**套用信任區域**”核取方塊。

使用此核取方塊可啟用/停用工作的信任區域。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會將受信任處理程序的檔案操作新增到工作設定中配置的掃描排除中。

如果清除該核取方塊，Kaspersky Embedded Systems Security 會在建立工作的防護範圍時略過受信任處理程序的檔案操作。

預設將會選定該核取方塊。

- 如果您想要在工作中使用卡斯基安全網路雲端服務，請選中“**在掃描中使用 KSN**”核取方塊。

此核取方塊可啟用/停用在工作中使用卡斯基安全網路 (KSN) 雲端服務。

如果選中該核取方塊，程式將使用從 KSN 服務接收到的資料確保更快速地對新威脅作出回應，並降低誤報的可能性。

如果清除該核取方塊，則自訂掃描工作將不使用 KSN 服務。

預設將會選定該核取方塊。

- 若要向將執行該工作的程序分配基本優先順序“**低**”，請在“**選項**”視窗中選定“**在背景模式下執行工作**”核取方塊。

該核取方塊將修改工作的優先順序。

如果選中該核取方塊，工作在作業系統中的優先順序會下降。作業系統根據其他 Kaspersky Embedded Systems Security 工作和其他應用程式對 CPU 及電腦檔案系統的負荷，分配用於執行該工作的資源。因此，負荷增加時工作效能將降低，負荷降低時效能將提高。

如果取消選中該核取方塊，工作啟動和執行時的優先順序將與其他 Kaspersky Embedded Systems Security 工作和其他程式的優先順序相同。在這種情況下，工作執行的速度將加快。

預設取消選定該核取方塊。

預設情況下，執行 Kaspersky Embedded Systems Security 工作程序的優先順序為“#”（正常）。

- 要使用所建立的工作作為關鍵區域掃描工作，請選中“選項”視窗中的“將工作視為關鍵區域掃描”核取方塊。

使用該核取方塊可變更工作優先順序：啟用或停用記錄“*關鍵區域掃描*”事件和重新整理電腦防護狀態。卡斯基安全管理中心根據狀態為“*掃描關鍵區域*”的工作的執行結果來評估電腦的安全等級。該核取方塊在本機系統和 Kaspersky Embedded Systems Security 的自訂工作的內容中不可用。您只能在卡斯基安全管理中心編輯此設定。

如果選中此核取方塊，管理電腦會記錄“*關鍵區域掃描已完成*”並根據工作執行結果重新整理電腦防護狀態。掃描工作具有較高優先順序。

如果清除此核取方塊，則工作以較低優先順序執行。

對於自訂自訂工作，該核取方塊預設處於清除狀態。

6. 點擊“下一步”。
7. 在“**排程**”視窗中，設定排程的工作啟動設定。
8. 點擊“下一步”。
9. 在“**選擇帳戶以執行工作**”視窗中，指定要使用的帳戶。

10. 點擊“下一步”。
11. 自訂工作名稱。
12. 點擊“下一步”。

工作名稱不應超過 100 個字元，並且不能包含以下符號：
 " * < > & \ : |

將開啟“完成工作建立”視窗。

13. 您可以透過選中“**精靈完成後執行工作**”核取方塊來在精靈完成後執行工作。
14. 點擊“**完成**”完成建立工作。

將為所選電腦或電腦群組建立新的自訂掃描工作。

本章節說明項目

為自訂掃描工作指定關鍵區域掃描的工作狀態.....	520
執行背景自訂掃描工作.....	521
記錄關鍵區域掃描執行記錄.....	522

為自訂掃描工作指定關鍵區域掃描的工作狀態

根據預設，如果“掃描關鍵區域”工作的執行頻率比 Kaspersky Embedded Systems Security 的“**長時間未執行關鍵區域掃描**”設定的指定頻率低，則卡斯基安全管理中心會為電腦指定“**警告**”狀態。

► 若要設定掃描單一管理群組中的所有電腦，請執行下列步驟：

1. 建立群組自訂掃描（請參見第 [516](#) 頁上的“建立自訂掃描工作”部分）。
2. 在工作建立精靈“**選項**”視窗中，選中“**將工作視為關鍵區域掃描**”核取方塊。指定的工作設定（掃描範圍與安全設定）將套用至群組中的所有電腦。配置工作排程。

您可以在為一組電腦建立自訂掃描工作時選中“將工作視為**關鍵區域掃描**”核取方塊，或稍後在“內容：<工作名稱>”視窗中選中該核取方塊（請參見第 516 頁上的“開啟自訂掃描工作內容”部分）。

3. 使用新的或現有政策停用群組電腦上的系統自訂掃描工作的排程啟動（請參見第 123 頁上的“配置本機系統工作的排程啟動”部分）。

隨後，卡斯基安全管理中心管理電腦將評估受防護電腦的安全狀態，並且將根據上次執行具有“**關鍵區域掃描**”狀態工作的結果而非根據“關鍵區域掃描”系統工作的結果通知您有關該安全狀態的資訊。

您可以為群組自訂掃描工作和電腦群組的工作分配“**關鍵區域掃描**”工作狀態。

可以使用應用程式主控台檢視“自訂掃描”工作是否為“**關鍵區域掃描**”工作。

在應用程式主控台中，“將工作視為**關鍵區域掃描**”核取方塊會顯示在工作設定中，但不可對其進行編輯。

執行背景自訂掃描工作

預設情況下，將為執行 Kaspersky Embedded Systems Security 工作的處理程序分配基本優先順序“**中度**”（正常）。

可以將執行自訂掃描工作的程序分配為“**低**”優先順序。將程序的優先順序降低會增加執行工作所需的時間，但是可能對提高其他活動程式的執行速度有所幫助。

多重背景工作可以以低優先順序別在單個作業程序中執行。您可以將最大數量的程序指定給背景自訂掃描工作。

► 要變更現有自訂掃描工作的優先順序：

1. 開啟“內容：自訂掃描”視窗（請參見第 514 頁上的“開啟自訂掃描工作精靈”部分）。
2. 選中或清除“在背景模式下執行工作”核取方塊。

該核取方塊將修改工作的優先順序。

如果選中該核取方塊，工作在作業系統中的優先順序會下降。作業系統根據其他 Kaspersky Embedded Systems Security 工作和其他應用程式對 CPU 及電腦檔案系統的負荷，分配用於執行該工作的資源。因此，負荷增加時工作效能將降低，負荷降低時效能將提高。

如果取消選中該核取方塊，工作啟動和執行時的優先順序將與其他 Kaspersky Embedded Systems Security 工作和其他程式的優先順序相同。在這種情況下，工作執行的速度將加快。

預設取消選定該核取方塊。

3. 點擊“確定”。

將儲存已配置的工作設定，並將這些設定立即應用到正在執行的工作。如果工作未執行，則將在下次啟動時套用修改後的設定。

記錄關鍵區域掃描執行記錄

預設情況下，電腦防護狀態顯示在 **Kaspersky Embedded Systems Security** 節點的詳細資訊視窗中，並在執行關鍵區域掃描工作後每週更新一次。

電腦防護狀態的更新時間與設定中已選中“**將工作視為關鍵區域掃描**”核取方塊的自訂掃描工作的排程相關聯。預設情況下，僅針對“**關鍵區域掃描**”工作選中該核取方塊且無法針對該工作進行修改。

只能在卡斯基安全管理中心中選擇與電腦防護狀態相關聯的自訂掃描工作。

配置工作掃描範圍

如果在“在作業系統啟動時掃描”和“關鍵區域掃描”工作中修改掃描範圍，可以透過還原 Kaspersky Embedded Systems Security 本身的設定來還原這些工作中的預設掃描範圍（“開始”>“程式”>“Kaspersky Embedded Systems Security”>“修改或移除 Kaspersky Embedded Systems Security”）。在安裝精靈中，選擇“修復已安裝元件”並點擊“下一步>”，然後選中“還原建議的應用程式設定”核取方塊。

► 要配置現有自訂掃描工作的掃描範圍：

1. 開啟“內容：自訂掃描”視窗（請參見第 [516](#) 頁上的“開啟自訂掃描工作內容”部分）。
 2. 選擇“掃描範圍”標籤。
 3. 要在掃描範圍中包括項目：
 - a. 在掃描範圍清單的空白空間中開啟上下文功能表。
 - b. 選擇“新增範圍”上下文功能表選項。
 - c. 在開啟的“新增物件至掃描範圍”視窗中，選擇想要新增的物件類型：
 - **預設的範圍**，以新增受防護伺服器上的某個預設範圍。然後在下拉清單中，選擇必需的掃描範圍。
 - **磁碟、資料夾或網路資料夾**，以便在掃描範圍中包括單個磁碟機、資料夾或網路物件。然後透過點擊“瀏覽”按鈕選擇所需的範圍。
 - **檔案**，以便在掃描範圍中包括單個檔案。然後透過點擊“瀏覽”按鈕選擇所需的範圍。
- 如果某個物件已經作為掃描範圍的排除項新增，則不能再將其新增到掃描範圍中。
4. 要從掃描範圍中排除單個節點，請清除這些節點名稱旁邊的核取方塊，或者執行以下步驟：
 - a. 按右鍵掃描範圍開啟其內容功能表。
 - b. 在內容功能表中，選擇“新增排除項目”選項。
 - c. 在“新增排除項目”視窗中，選擇要作為掃描範圍的排除新增的物件類型，並遵循將物件新增到掃描範圍中的過程的邏輯。

5. 要修改新增的掃描範圍或排除項，請選擇所需掃描範圍內容功能表中的“**編輯範圍**”選項。
6. 若要在網路檔案資源清單中隱藏之前新增的掃描範圍或排除項，請在所需掃描範圍的內容功能表中選擇“**刪除範圍**”選項。

該掃描範圍將從網路檔案資源清單中刪除，同時從自訂掃描工作範圍中排除。

7. 點擊“**確定**”按鈕。

“設定掃描範圍”視窗將關閉。已儲存新配置的設定。

為自訂掃描工作選擇預設的安全等級

可以為電腦網路檔案資源清單中的選定項套用三個預設安全等級之一：“**最佳效能**”、“**建議**”和“**最佳防護**”。

► 要選擇其中一個預設安全等級：

1. 開啟“**內容：自訂掃描**”（請參見第 [516](#) 頁上的“**開啟自訂掃描工作內容**”部分）視窗。
2. 選擇“**掃描範圍**”標籤。
3. 電腦清單中，選擇一個包含在掃描範圍中的項目以設定預設安全等級。
4. 點擊“**配置**”按鈕。

將開啟“**自訂掃描設定**”視窗。

5. 在“**安全等級**”標籤上，選擇要應用的安全等級。

該視窗將顯示與選定安全等級相對應的安全性設定清單。

6. 點擊“**確定**”按鈕。
7. 在“**內容：自訂掃描**”視窗中點擊“**確定**”按鈕。

將儲存已配置的工作設定，並將這些設定立即應用到正在執行的工作。如果工作未執行，則將在下次啟動時套用修改後的設定。

手動配置安全性設定

預設情況下，自訂掃描工作對整個掃描範圍使用通用安全性設定。這些設定對應于“**建議**”預設安全等級（請參見第 [296](#) 頁上的“預設安全等級”部分）。

若要修改安全性設定的預設值，可透過將它們配置為用於整個防護範圍的一般設定，或為電腦檔案資源清單中的不同項目或樹狀目錄中的節點配置不同設定。

► 要手動配置安全設定：

1. 開啟“內容：自訂掃描”視窗（請參見第 [516](#) 頁上的“開啟自訂掃描工作內容”部分）。
2. 選擇“掃描範圍”標籤。
3. 在您要為其配置安全性設定的掃描範圍清單中選擇項目。

可以為掃描範圍內的選定節點或項目套用包含安全設定的預設範本（請參見第 [197](#) 頁上的“關於安全設定範本”部分）。

4. 點擊“配置”按鈕。

將開啟“自訂掃描設定”視窗。

5. 根據需求配置選定節點或項目的所需安全設定：
 - 一般設定（請參見第 [526](#) 頁上的“配置一般工作設定”部分）
 - 操作（請參見第 [530](#) 頁上的“設定操作”部分）
 - 效能（請參見第 [533](#) 頁上的“設定效能”部分）

6. 在“自訂掃描設定”視窗中點擊“確定”按鈕。

7. 在“掃描範圍”視窗中點擊“確定”。

將儲存新的掃描範圍設定。

本章節說明項目

配置一般工作設定	526
配置操作	530
配置效能	533

配置一般工作設定

► 要配置一般自訂掃描工作設定：

1. 開啟“內容：自訂掃描”（請參見第 [516](#) 頁上的“開啟自訂掃描工作內容”部分）視窗。
2. 選擇“掃描範圍”標籤。
3. 點擊“配置”按鈕。

將開啟“自訂掃描設定”視窗。

4. 點擊“設定”按鈕。
5. 在“一般”標籤的“掃描物件”部分中，指定要包含在掃描範圍內的物件類型：

- **掃描物件**

- **所有物件**

Kaspersky Embedded Systems Security 掃描所有物件。

- **按格式掃描物件**

Kaspersky Embedded Systems Security 僅根據檔案格式掃描感染物件。

Kaspersky Lab 編制了該格式清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。

- **按病毒資料庫中指定的副檔名清單掃描物件**

Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。

Kaspersky Lab 編制了該副檔名清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。

- **按指定的副檔名清單掃描物件**

Kaspersky Embedded Systems Security 根據檔案副檔名掃描檔案。可在“副檔名清單”視窗（透過點擊“編輯”按鈕開啟）中手動自訂檔案副檔名清單。

- **子資料夾**

- **子檔案**

- **掃描開機磁區和 MBR**

啟用對開機磁區和主引導記錄的防護。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描電腦的硬碟磁碟機和卸除式磁碟機上的開機磁區和主引導記錄。

預設將會選定該核取方塊。

- **掃描 NTFS 交換資料串流**

掃描 NTFS 檔案系統磁碟機上的替代檔案和資料夾執行緒。

如果選中該核取方塊，應用程式將掃描疑似感染物件以及與該物件關聯的所有 NTFS 執行緒。

如果清除該核取方塊，應用程式將只掃描偵測到並被視為疑似感染的物件。

預設將會選定該核取方塊。

6. 在“效能”部分中，選中或清除“**僅掃描新增與變更過的檔案**”核取方塊。

使用此核取方塊可啟用/停用對自上次掃描以來 Kaspersky Embedded Systems Security 識別為新檔案或已修改的檔案的掃描和防護。

如果選中該核取方塊，Kaspersky Embedded Systems Security 僅掃描和防護自上次掃描以來被識別為新檔案或已修改的檔案。

如果清除該核取方塊，您可以選擇希望僅掃描和防護新檔案，還是掃描和防護所有檔案而略過檔案的修改狀態。

對於“最佳效能”安全等級，預設選定該核取方塊。如果設定“最佳防護”或“建議”安全等級，則取消選中該核取方塊。

如果清除該核取方塊，要在可用選項之間轉換，請點擊每個複合物件類型對應的“全部/僅新建”連結。

7. 在“掃描複合檔案”部分中，指定要包含在掃描範圍內的複合物件：

- **全部/僅新的壓縮檔案**

掃描 ZIP、CAB、RAR、ARJ 壓縮檔案及其他壓縮檔案格式。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描壓縮檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過壓縮檔案。

預設值取決於所選的防護等級。

- **全部/僅新的 SFX 壓縮檔案**

掃描自解壓壓縮檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描 SFX 壓縮檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過 SFX 壓縮檔案。

預設值取決於所選的防護等級。

如果取消選中“**壓縮檔案**”核取方塊，則該選項處於活動狀態。

- **全部/僅新的電子郵件資料庫**

掃描 Microsoft Outlook 和 Microsoft Outlook Express 郵件資料庫檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描郵件資料庫檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過郵件資料庫檔案。

預設值取決於所選的安全等級。

- **全部/僅新的封裝的物件**

掃描由二進位代碼封裝程式 (例如 UPX 或 ASPack) 封裝的可執行檔。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描由封裝程式封裝的可執行檔。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過由封裝程式封裝的可執行檔。

預設值取決於所選的防護等級。

- **全部/僅新的純文字電子郵件**

掃描郵件格式檔案，例如 Microsoft Office Outlook 和 Microsoft Outlook Express 郵件。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描郵件格式檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過郵件格式檔案。

預設值取決於所選的安全等級。

- **全部/僅新嵌入的 OLE 物件**

掃描嵌入到檔案中的物件 (如 Microsoft Word 巨集或電子郵件附件) 。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描嵌入到檔案中的物件。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過嵌入到檔案中的物件。

預設值取決於所選的防護等級。

8. 點擊“確定”。

將儲存新的工作配置。

配置操作

► 要配置“自訂掃描”工作執行過程中對受感染的物件和其他偵測到的物件執行的操作：

1. 開啟“內容：自訂掃描”（請參見第 [516](#) 頁上的“開啟自訂掃描工作內容”部分）視窗。
2. 選擇“掃描範圍”標籤。
3. 點擊“配置”按鈕。

將開啟“自訂掃描設定”視窗。

4. 點擊“設定”按鈕。
5. 選擇“操作”標籤。
6. 選擇要對受感染的物件和其他偵測到的物件執行的操作：
 - 僅通知。

選擇此模式時，Kaspersky Embedded Systems Security 不封鎖存取受感染的物件和其他偵測到的物件，也不對它們執行任何操作。以下事件在工作記錄中註冊：*物件未解毒。原因：由於使用者定義的設定，未執行任何操作使偵測到的物件無效。*該事件指定有關偵測到的物件的所有可用資訊。

應該為每個防護或掃描區域單獨配置“**僅通知**”模式。預設情況下，任何安全等級都不使用此模式。如果選擇此模式，Kaspersky Embedded Systems Security 會自動將安全等級變更為“**自訂**”。

- **解毒。**
- **解毒，無法解毒時刪除。**
- **刪除。**
- **執行建議的操作。**

7. 選擇要對可疑的物件執行的操作：

- **僅通知。**

選擇此模式時，Kaspersky Embedded Systems Security 不封鎖存取受感染的物件和其他偵測到的物件，也不對它們執行任何操作。以下事件在工作記錄中註冊：*物件未解毒。原因：由於使用者定義的設定，未執行任何操作使偵測到的物件無效。*該事件指定有關偵測到的物件的所有可用資訊。

應該為每個防護或掃描區域單獨配置“**僅通知**”模式。預設情況下，任何安全等級都不使用此模式。如果選擇此模式，Kaspersky Embedded Systems Security 會自動將安全等級變更為“**自訂**”。

- **隔離。**
- **刪除。**
- **執行建議的操作。**

8. 選擇依威脅類型對物件執行的操作：

a. 清除或選中“**根據偵測到的物件的類型執行操作**”核取方塊。

如果選中該核取方塊，可以透過點擊該核取方塊旁邊的“**設定**”按鈕來獨立設定針對每種偵測到的物件類型的主要和次要操作。此時，Kaspersky Embedded Systems Security 將不允許開啟或執行受感染的物件，無論您的選擇如何。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將對指定的物件類型分別執行在“**對受感染物件和其他物件執行的操作**”和“**對可疑物件執行的操作**”部分中選擇的操作。

預設取消選定該核取方塊。

b. 點擊“**設定**”按鈕。

c. 在開啟的視窗中，選擇針對每種偵測到的物件類型的主要和次要操作（如果主要操作失敗）。

d. 點擊“**確定**”。

9. 選擇要對不可還原的複合物件執行的操作：選擇或清除“**在偵測到嵌入物件時完全刪除應用程式無法修改的複合檔案**”核取方塊。

此核取方塊用於啟用或停用當偵測到惡意、疑似感染或其他偵測到的子內嵌物件時強制刪除父複合檔案。

如果選中該核取方塊並且工作設定為刪除受感染和疑似感染的物件，Kaspersky Embedded Systems Security 會在偵測到惡意或其他內嵌物件時強制刪除整個父複合物件。如果應用程式無法只刪除偵測到的子物件（例如，如果父物件不可修改），將強制刪除父物件及其所有內容。

如果清除該核取方塊並且工作設定為刪除受感染和疑似感染的物件，當父物件不可修改時，Kaspersky Embedded Systems Security 不會執行所選操作。

10. 點擊“**確定**”。

將儲存新的工作配置。

配置效能

► 要設定自訂掃描工作的效能：

1. 開啟“內容：自訂掃描”（請參見第 [516](#) 頁上的“開啟自訂掃描工作內容”部分）視窗。
2. 選擇“掃描範圍”標籤。
3. 點擊“配置”按鈕。

將開啟“自訂掃描設定”視窗。

4. 點擊“設定”按鈕。
5. 選擇“效能”標籤。
6. 在“排除”部分中：

- 清除或選中“排除檔案”核取方塊。

按檔案名或檔案名遮罩從掃描中排除檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過指定的物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將掃描所有物件。

預設取消選定該核取方塊。

- 清除或選中“不偵測”核取方塊。

按可偵測物件的名稱或名稱遮罩從掃描中排除物件。病毒百科全書

<https://encyclopedia.kaspersky.com/knowledge/classification/> 網站上提供了可偵測物件的名稱清單。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過指定的可偵測物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 預設將偵測程式中指定的所有物件。

預設取消選定該核取方塊。

- 針對每個設定點擊“編輯”按鈕以新增排除項目。

7. 在“進階設定”部分中：

- **超過以下時間則停止掃描(秒)**

限制物件掃描的持續時間。預設值為 60 秒。

如果選中該核取方塊，則掃描持續時間將限制為指定的值。

如果取消選中該核取方塊，則對掃描持續時間沒有限制。

對於“最佳效能”安全等級，預設選定該核取方塊。

- **不掃描超過此值複合檔案(MB)**

將超過指定大小的物件排除在掃描之外。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在病毒掃描期間略過大小超過指定限制值的複合物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將掃描任意大小的複合物件。

對於“最佳效能”安全等級，預設選定該核取方塊。

- **使用 iSwift 技術**

iSwift 將資料庫中儲存的檔案 NTFS 識別碼與目前識別碼進行比較。只對識別碼發生變化的檔案（新檔案和自上次掃描 NTFS 系統物件以來修改過的檔案）執行掃描。

如果選中該核取方塊，Kaspersky Embedded Systems Security 僅掃描自上次掃描 NTFS 系統物件以來新建或修改的檔案。

如果清除該核取方塊，Kaspersky Embedded Systems Security 在掃描 NTFS 系統檔案時將不考慮檔案建立或修改的日期（網路資料夾中的檔案除外）。

預設將會選定該核取方塊。

- 使用 iChecker 技術

iChecker 會計算並記住掃描的檔案的核對總和。如果物件被修改，核對總和會發生變化。應用程式在掃描工作中比較所有核對總和，並且僅掃描新檔案和自上次掃描檔案以來修改過的檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 僅掃描新檔案和修改的檔案。

如果清除該核取方塊，Kaspersky Embedded Systems Security 在掃描檔案時將不考慮檔案建立或修改的日期。

預設將會選定該核取方塊。

8. 點擊“確定”。

將儲存新的工作配置。

配置卸除式磁碟機掃描

► 要配置在卸除式磁碟機連線到受防護電腦時對其進行的掃描：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“受管理裝置”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“政策”標籤。
4. 點擊要設定的政策名稱。

在開啟的“內容：<政策名稱>”視窗中，選擇“選項”部分。

5. 點擊“卸除式磁碟機掃描”子部分中的“設定”按鈕。

將開啟“卸除式磁碟機掃描”視窗。

6. 在“連接時掃描”部分中，執行以下操作：

- 如果想讓 Kaspersky Embedded Systems Security 在卸除式磁碟機連線時自動掃描，請選擇“掃描透過 USB 連接的卸除式磁碟機”核取方塊。

- 如果需要，選中“掃描卸除式磁碟機，如果其儲存的資料量未超過(MB)”，然後在右側的欄位中指定最大值。
- 在“掃描時使用的安全等級”下拉清單中，指定卸除式磁碟機掃描所需設定的安全等級。

7. 點擊“確定”。

即會儲存並套用指定設定。

透過應用程式主控台管理自訂掃描工作

在本節中，學習如何導航應用程式主控台介面以及如何在本地電腦上配置工作設定。

本章節說明項目

導航	536
建立和配置自訂掃描工作	537
自訂掃描工作中的掃描範圍	540
為自訂掃描工作選擇預設的安全等級	545
手動配置安全性設定	546
掃描卸除式磁碟機	556
自訂掃描工作統計	557

導航

學習如何透過介面導航到所需工作設定。

本章節說明項目

開啟自訂掃描工作設定.....	537
-----------------	-----

開啟自訂掃描工作設定

► 要透過應用程式主控台開啟自訂掃描工作的一般設定：

1. 在應用程式主控台樹狀目錄中展開“**自訂掃描**”節點。
2. 選擇與要設定的工作相應的子節點。
3. 在子節點詳細資訊視窗中，點擊“**內容**”連結。

將開啟“**工作設定**”視窗。

► 要透過應用程式主控台開啟掃描範圍設定視窗：

1. 在應用程式主控台樹狀目錄中展開“**自訂掃描**”節點。
2. 選擇與要設定的自訂掃描工作相應的子節點。
3. 在已選擇的節點詳細資訊窗格，點擊**配置掃描範圍**連結。

將開啟“**設定掃描範圍**”視窗。

建立和配置自訂掃描工作

單台電腦的自訂工作可以在“**自訂掃描**”節點中建立。在 Kaspersky Embedded Systems Security 其他功能元件中，無法建立自訂工作。

► 要建立和配置新的自訂掃描工作：

1. 在應用程式主控台樹狀目錄中，開啟“**自訂掃描**”節點的內容功能表。
2. 選擇“**新增工作**”。

將開啟“**新增工作**”視窗。

3. 配置以下工作設定：

- **名稱** - 不超過 100 個字元的工作名稱，可以包含除 " * < > & \ : | " 之外的任何符號。

如果未指定工作名稱，則無法在“排程”、“進階”和“執行帳戶”上儲存工作或配置新工作。

- **敘述** - 工作相關的任何其他資訊，不超過 2000 個字元。此資訊將顯示在工作內容視窗中。
- **使用啟發式分析。**

此核取方塊可在物件掃描過程中啟用/停用啟發式分析。

如果選中該核取方塊，則啟用啟發式分析。

如果取消選中該核取方塊，則停用啟發式分析。

預設將會選定該核取方塊。

- **在背景模式下執行工作。**

該核取方塊將修改工作的優先順序。

如果選中該核取方塊，工作在作業系統中的優先順序會下降。作業系統根據其他 Kaspersky Embedded Systems Security 工作和其他應用程式對 CPU 及電腦檔案系統的負荷，分配用於執行該工作的資源。因此，負荷增加時工作效能將降低，負荷降低時效能將提高。

如果取消選中該核取方塊，工作啟動和執行時的優先順序將與其他 Kaspersky Embedded Systems Security 工作和其他程式的優先順序相同。在這種情況下，工作執行的速度將加快。

預設取消選定該核取方塊。

- **套用信任區域。**

使用此核取方塊可啟用/停用工作的信任區域。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會將受信任處理程序的檔案操作新增到工作設定中配置的掃描排除中。

如果清除該核取方塊，Kaspersky Embedded Systems Security 會在建立工作的防護範圍時略過受信任處理程序的檔案操作。

預設將會選定該核取方塊。

- **將工作視為關鍵區域掃描。**

使用該核取方塊可變更工作優先順序：啟用或停用記錄“*關鍵區域掃描*”事件和重新整理電腦防護狀態。卡斯基安全管理中心根據狀態為“*掃描關鍵區域*”的工作的執行結果來評估電腦的安全等級。該核取方塊在本機系統和 Kaspersky Embedded Systems Security 的自訂工作的內容中不可用。您只能在卡斯基安全管理中心編輯此設定。

如果選中此核取方塊，管理電腦會記錄“*關鍵區域掃描已完成*”並根據工作執行結果重新整理電腦防護狀態。掃描工作具有較高優先順序。

如果清除此核取方塊，則工作以較低優先順序執行。

對於自訂自訂工作，該核取方塊預設處於清除狀態。

- **在掃描中使用 KSN。**

此核取方塊可啟用/停用在工作中使用卡斯基安全網路 (KSN) 雲端服務。

如果選中該核取方塊，程式將使用從 KSN 服務接收到的資料確保更快速地對新威脅作出回應，並降低誤報的可能性。

如果清除該核取方塊，則自訂掃描工作將不使用 KSN 服務。

預設將會選定該核取方塊。

4. 配置“**排程**”和“**進階**”標籤上的工作啟動排程設定 (請參見第 [189](#) 頁上的“配置工作啟動排程設定”部分)。
5. 在“**執行帳戶**”標籤上，配置工作啟動設定及帳戶權限 (請參見第 [192](#) 頁上的“指定使用者帳戶以啟動工作”部分)。
6. 在“**新增工作**”視窗中點擊“**確定**”。

將建立新的自訂掃描工作。將在應用程式主控台樹狀目錄中顯示包含新工作名稱的節點。此操作將會記錄到系統稽核記錄中 (請參閱第 [251](#) 頁) 。

7. 如果需要，在所選節點的詳細資訊窗格中，選擇“**配置掃描範圍**”。

將開啟“**設定掃描範圍**”視窗。

8. 在電腦檔案資源樹狀目錄或清單中，選擇要包含在掃描範圍內的節點。
9. 選擇一項預設安全等級 (請參見第 [508](#) 頁上的“關於自訂掃描工作的預設安全等級”部分) 或手動配置掃描設定 (請參見第 [546](#) 頁上的“手動配置安全性設定”部分) 。
10. 在“**設定掃描範圍**”視窗中，點擊“**儲存**”。

將在下次啟動工作時應用設定的設定。

自訂掃描工作中的掃描範圍

本節包含有關在“自訂掃描”工作中建立和使用掃描範圍的資訊。

本章節說明項目

配置網路檔案資源的視圖模式	540
建立掃描範圍	541
在掃描範圍內包含網路物件	543
建立虛擬掃描範圍	544

配置網路檔案資源的視圖模式

► 要在配置掃描範圍設定期間選擇網路檔案資源的視圖模式：

1. 將開啟“**設定掃描範圍**” (請參見第 [537](#) 頁) 視窗。
2. 開啟視窗左上角部分的下拉清單。執行以下步驟之一：
 - 選擇“**樹狀檢視**”選項以樹狀檢視模式顯示網路檔案資源。

- 選擇“清單檢視”選項以清單檢視模式顯示網路檔案資源。

預設情況下，受防護電腦的網路檔案資源以清單圖示模式顯示。

3. 點擊“儲存”按鈕。

“設定掃描範圍”視窗將關閉。將套用新設定的設定。

建立掃描範圍

如果您正在使用管理員工作站上安裝的應用程式主控台遠端管理受防護電腦上的 Kaspersky Embedded Systems Security，您必須是受防護電腦上管理員群組成員才能檢視資料夾。

在不同 Windows 作業系統中，設定的名稱可能會有所不同。

如果在“在作業系統啟動時掃描”和“關鍵區域掃描”工作中修改掃描範圍，可以透過還原 Kaspersky Embedded Systems Security 本身的設定來還原這些工作中的預設掃描範圍（“開始”>“程式”>“Kaspersky Embedded Systems Security”>“修改或移除 Kaspersky Embedded Systems Security”）。在安裝精靈中，選擇“修復已安裝元件”並點擊“下一步>”，然後選中“還原建議的應用程式設定”核取方塊。

建立自訂掃描工作範圍的過程取決於網路檔案資源視圖模式（請參見第 540 頁上的“配置網路檔案資源的視圖模式”部分）。可以將網路檔案資源檢視模式配置為樹狀目錄或清單（設定為預設值）。

► 要使用網路檔案資源樹狀目錄建立掃描範圍：

1. 將開啟“設定掃描範圍”視窗（請參見第 537 頁）。
2. 在視窗的左側部分中，開啟網路檔案資源樹狀目錄以顯示所有節點和子節點。
3. 執行以下操作：
 - 要從掃描範圍中排除單個節點，請清除這些節點名稱旁邊的核取方塊。

- 要從掃描範圍中排除單個節點，請清除“**我的電腦**”核取方塊，然後執行以下步驟：
 - 如果要將某一類型的所有磁碟機均包含在防護範圍內，請核取所需磁碟機類型名稱旁的方塊（例如，若要新增電腦上的所有卸除式磁碟機，則啟用“**卸除式磁碟機**”核取方塊）。
 - 如果要將特定類型的單個磁碟機包含在掃描範圍內，請展開包含此類型磁碟清單的節點，並核取所需磁碟名稱旁的方塊。例如，要選擇卸除式磁碟機 **F:**，請展開節點“**卸除式磁碟機**”節點，並核取磁碟機 **F:** 對應的核取方塊。
 - 如果您想要僅包含磁碟機上的單個資料夾或檔案，請選中該資料夾或檔案名稱旁邊的核取方塊。

4. 點擊“**儲存**”按鈕。

“設定掃描範圍”視窗將關閉。將儲存新配置的設定。

► 要使用網路檔案資源清單建立掃描範圍：

1. 將開啟“**設定掃描範圍**”視窗（請參見第 [537](#) 頁）。
2. 要從掃描範圍中排除單個節點，請清除“**我的電腦**”核取方塊，然後執行以下步驟：
 - a. 按右鍵掃描範圍開啟其內容功能表。
 - b. 在按鈕的內容功能表中，選擇“**新增掃描範圍**”。
 - c. 在開啟的“**新增掃描範圍**”視窗中，選擇想要新增的物件類型：
 - **預設的範圍**，以新增受防護電腦上的某個預設範圍。然後在下拉清單中，選擇必需的掃描範圍。
 - **磁碟、資料夾或網路資料夾**，以便在掃描範圍中包括單個磁碟機、資料夾或網路物件。然後透過點擊“**瀏覽**”按鈕選擇所需的範圍。
 - **檔案**，以便在掃描範圍中包括單個檔案。然後透過點擊“**瀏覽**”按鈕選擇所需的範圍。

如果某個物件已經作為掃描範圍的排除項新增，則不能再將其新增到掃描範圍中。

3. 要從掃描範圍中排除單個節點，請清除這些節點名稱旁邊的核取方塊，或者執行以下步驟：
 - a. 按右鍵掃描範圍開啟其內容功能表。
 - b. 在內容功能表中，選擇“**新增排除項目**”選項。
 - c. 在“**新增排除項目**”視窗中，選擇要作為掃描範圍的排除新增的物件類型，並遵循將物件新增到掃描範圍中的過程的邏輯。
4. 要修改新增的掃描範圍或排除項，請選擇所需掃描範圍內容功能表中的“**編輯範圍**”選項。
5. 若要在網路檔案資源清單中隱藏之前新增的掃描範圍或排除項，請在所需掃描範圍的內容功能表中選擇“**從清單刪除**”選項。

該掃描範圍將從網路檔案資源清單中刪除，同時從自訂掃描工作範圍中排除。

6. 點擊“**儲存**”按鈕。

“設定掃描範圍”視窗將關閉。將儲存新配置的設定。

在掃描範圍內包含網路物件

您可以按照 UNC (通用命名慣例) 格式指定網路磁碟機、資料夾或檔案的路徑以將它們新增至掃描範圍。

您可以在系統帳戶下掃描網路資料夾。

► 要將網路位置新增到掃描範圍：

1. 將開啟“**設定掃描範圍**” (請參見第 [537](#) 頁) 視窗。
2. 開啟視窗左上角的下拉清單部分，然後選擇**樹狀檢視**。
3. 在“**網路**”節點的內容功能表中：
 - 選擇“**新增網路資料夾**”，如果您想要向掃描範圍中新增網路資料夾。
 - 選擇“**新增網路檔案**”，如果您想要向掃描範圍中新增網路檔案。
4. 以 UNC 格式輸入網路資料夾或檔案路徑，然後點擊 **ENTER** 鍵。

5. 選中新新增的網路物件旁邊的核取方塊以將其包含在掃描範圍內。
6. 如有必要，請變更已新增的網路物件的安全性設定。
7. 點擊“儲存”按鈕。

將儲存修改的工作設定。

建立虛擬掃描範圍

可以將動態磁碟機、資料夾和檔案包含在掃描範圍內以建立虛擬掃描範圍。

僅當防護/掃描範圍以檔案資源樹狀目錄的形式顯示時，您才可透過新增單個虛擬磁碟機、資料夾或檔案來延伸防護/掃描範圍（請參見第 540 頁上的“配置網路檔案資源的視圖模式”部分）。

► 要新增虛擬磁碟機至掃描範圍：

1. 將開啟“設定掃描範圍”（請參見第 537 頁）視窗。
2. 開啟視窗左上角的下拉清單部分，然後選擇**樹狀檢視**。
3. 在電腦檔案資源樹狀目錄中開啟“**虛擬磁碟機**”節點的內容功能表，點擊“**新增虛擬磁碟機**”，然後從可用名稱清單中選擇虛擬磁碟名稱。
4. 選中已新增的磁碟機旁邊的核取方塊，以將該磁碟機包括在掃描範圍中。
5. 點擊“儲存”按鈕。

將儲存修改的工作設定。

► 要新增虛擬資料夾或虛擬檔案至掃描範圍：

1. 將開啟“設定掃描範圍”視窗（請參見第 537 頁）。
2. 開啟視窗左上角的下拉清單部分，然後選擇**樹狀檢視**。
3. 在電腦檔案資源樹狀目錄中，開啟節點的內容功能表以新增資料夾或檔案，然後選擇以下選項之一：
 - **新增虛擬資料夾**，如果您想要向掃描範圍中新增虛擬資料夾。

- **新增虛擬檔案**，如果您想要向掃描範圍中新增虛擬檔案。

4. 在輸入欄位中指定資料夾或檔案的名稱。
5. 在包含所建立資料夾（或檔案）名稱的欄位中，選定相應的核取方塊以將該資料夾（或檔案）包含在掃描範圍中。
6. 點擊“**儲存**”按鈕。

將儲存修改的工作設定。

為自訂掃描工作選擇預設的安全等級

可以為電腦網路檔案資源樹狀目錄或清單中的選定節點或項套用三個預設安全等級之一：“**最佳效能**”、“**建議**”和“**最佳防護**”。

► *要選擇其中一個預設安全等級：*

1. 開啟“**設定掃描範圍**”（請參見第 [537](#) 頁）視窗。
2. 在電腦網路檔案資源樹狀目錄或清單中，選擇一個節點或項以設定預定義安全等級。
3. 確保選定的節點或項包含在掃描範圍中。
4. 在視窗右側的“**安全等級**”標籤中，選擇要應用的安全等級。

該視窗將顯示與選定安全等級相對應的安全性設定清單。

5. 點擊“**儲存**”按鈕。

將儲存已配置的工作設定，並將這些設定立即應用到正在執行的工作。如果工作未執行，則將在下次啟動時套用修改後的設定。

手動配置安全性設定

預設情況下，自訂掃描工作對整個掃描範圍使用通用安全性設定。這些設定對應于“**建議**”預設安全等級（請參見第 [296](#) 頁上的“預設安全等級”部分）。

若要修改安全性設定的預設值，可透過將它們配置為用於整個防護範圍的一般設定，或為電腦檔案資源清單中的不同項目或樹狀目錄中的節點配置不同設定。

在使用網路檔案資源樹狀目錄時，為所選父節點配置的安全性設定將自動套用於所有子節點。父節點的安全設定不會套用到單獨配置的子節點。

► 要手動配置安全設定：

1. 將開啟“**設定掃描範圍**”（請參見第 [537](#) 頁）視窗。
2. 在左側視窗部分中，選擇用於配置安全設定的節點或項目。

可以為掃描範圍內的選定節點或項目套用包含安全設定的預設範本（請參見第 [197](#) 頁上的“關於安全設定範本”部分）。

3. 在以下標籤中，根據需求配置選定節點或項目的所需安全設定：
 - 一般設定（請參見第 [547](#) 頁上的“配置一般工作設定”部分）
 - 操作（請參見第 [551](#) 頁上的“設定操作”部分）
 - 效能（請參見第 [553](#) 頁上的“設定效能”部分）
 - 分級儲存
4. 在“**設定掃描範圍**”視窗中，點擊“**儲存**”。

將儲存新的掃描範圍設定。

本章節說明項目

配置一般工作設定	547
配置操作	551
配置效能	553
配置分級儲存	555

配置一般工作設定

► 要配置自訂掃描工作的一般安全性設定：

1. 將開啟“設定掃描範圍”（請參見第 [537](#) 頁）視窗。
2. 選擇“一般”標籤。
3. 在“掃描物件”部分中，指定要包含在掃描範圍內的物件類型：
 - **掃描物件**
 - **所有物件**

Kaspersky Embedded Systems Security 掃描所有物件。
 - **按格式掃描物件**

Kaspersky Embedded Systems Security 僅根據檔案格式掃描感染物件。

Kaspersky Lab 編制了該格式清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。
 - **按病毒資料庫中指定的副檔名清單掃描物件**

Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。

Kaspersky Lab 編制了該副檔名清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。
 - **按指定的副檔名清單掃描物件**

Kaspersky Embedded Systems Security 根據檔案副檔名掃描檔案。可在“副檔名清單”視窗（透過點擊“編輯”按鈕開啟）中手動自訂檔案副檔名清單。

- **掃描開機磁區和 MBR**

啟用對開機磁區和主引導記錄的防護。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描電腦的硬碟磁碟機和卸除式磁碟機上的開機磁區和主引導記錄。

預設將會選定該核取方塊。

- **掃描 NTFS 交換資料串流**

掃描 NTFS 檔案系統磁碟機上的替代檔案和資料夾執行緒。

如果選中該核取方塊，應用程式將掃描疑似感染物件以及與該物件關聯的所有 NTFS 執行緒。

如果清除該核取方塊，應用程式將只掃描偵測到並被視為疑似感染的物件。

預設將會選定該核取方塊。

4. 在“效能”部分中，選中或清除“**僅掃描新增與變更過的檔案**”核取方塊。

使用此核取方塊可啟用/停用對自上次掃描以來 Kaspersky Embedded Systems Security 識別為新檔案或已修改的檔案的掃描和防護。

如果選中該核取方塊，Kaspersky Embedded Systems Security 僅掃描和防護自上次掃描以來被識別為新檔案或已修改的檔案。

如果清除該核取方塊，您可以選擇希望僅掃描和防護新檔案，還是掃描和防護所有檔案而略過檔案的修改狀態。

對於“最佳效能”安全等級，預設選定該核取方塊。如果設定“最佳防護”或“建議”安全等級，則取消選中該核取方塊。

如果清除該核取方塊，要在可用選項之間轉換，請點擊每個複合物件類型對應的“全部/僅新建”連結。

5. 在“掃描複合檔案”部分中，指定要包含在掃描範圍內的複合物件：

- **全部/僅新的壓縮檔案**

掃描 ZIP、CAB、RAR、ARJ 壓縮檔案及其他壓縮檔案格式。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描壓縮檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過壓縮檔案。

預設值取決於所選的防護等級。

- **全部/僅新的 SFX 壓縮檔案**

掃描自解壓壓縮檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描 SFX 壓縮檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過 SFX 壓縮檔案。

預設值取決於所選的防護等級。

如果取消選中“**壓縮檔案**”核取方塊，則該選項處於活動狀態。

- **全部/僅新的電子郵件資料庫**

掃描 Microsoft Outlook 和 Microsoft Outlook Express 郵件資料庫檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描郵件資料庫檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過郵件資料庫檔案。

預設值取決於所選的安全等級。

- **全部/僅新的封裝的物件**

掃描由二進位代碼封裝程式（例如 UPX 或 ASPack）封裝的可執行檔。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描由封裝程式封裝的可執行檔。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過由封裝程式封裝的可執行檔。

預設值取決於所選的防護等級。

- **全部/僅新的純文字電子郵件**

掃描郵件格式檔案，例如 Microsoft Office Outlook 和 Microsoft Outlook Express 郵件。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描郵件格式檔案。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過郵件格式檔案。

預設值取決於所選的安全等級。

- **全部/僅新嵌入的 OLE 物件**

掃描嵌入到檔案中的物件（如 Microsoft Word 巨集或電子郵件附件）。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將掃描嵌入到檔案中的物件。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過嵌入到檔案中的物件。

預設值取決於所選的防護等級。

6. 點擊“儲存”。

將儲存新的工作配置。

配置操作

► 要為“自訂掃描”工作配置對受感染的物件和其他偵測到的物件執行的操作：

1. 將開啟“設定掃描範圍”(請參見第 [537](#) 頁) 視窗。
2. 選擇“操作”標籤。
3. 選擇要對受感染的物件和其他偵測到的物件執行的操作：

- **僅通知。**

選擇此模式時，Kaspersky Embedded Systems Security 不封鎖存取受感染的物件和其他偵測到的物件，也不對它們執行任何操作。以下事件在工作記錄中註冊：*物件未解毒。原因：由於使用者定義的設定，未執行任何操作使偵測到的物件無效。*該事件指定有關偵測到的物件的所有可用資訊。

應該為每個防護或掃描區域單獨配置“僅通知”模式。預設情況下，任何安全等級都不使用此模式。如果選擇此模式，Kaspersky Embedded Systems Security 會自動將安全等級變更為“自訂”。

- **解毒。**
- **解毒，無法解毒時刪除。**
- **刪除。**
- **執行建議的操作。**

4. 選擇要對可疑的物件執行的操作：

- **僅通知。**

選擇此模式時，Kaspersky Embedded Systems Security 不封鎖存取受感染的物件和其他偵測到的物件，也不對它們執行任何操作。以下事件在工作記錄中註冊：*物件未解毒。原因：由於使用者定義的設定，未執行任何操作使偵測到的物件無效。*該事件指定有關偵測到的物件的所有可用資訊。

應該為每個防護或掃描區域單獨配置“**僅通知**”模式。預設情況下，任何安全等級都不使用此模式。如果選擇此模式，Kaspersky Embedded Systems Security 會自動將安全等級變更為“**自訂**”。

- 隔離。
- 刪除。
- 執行建議的操作。

5. 選擇依威脅類型對物件執行的操作：

- a. 清除或選中“**根據偵測到的物件的類型執行操作**”核取方塊。

如果選中該核取方塊，可以透過點擊該核取方塊旁邊的“**設定**”按鈕來獨立設定針對每種偵測到的物件類型的主要和次要操作。此時，Kaspersky Embedded Systems Security 將不允許開啟或執行受感染的物件，無論您的選擇如何。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將對指定的物件類型分別執行在“**對受感染物件和其他物件執行的操作**”和“**對可疑物件執行的操作**”部分中選擇的操作。

預設取消選定該核取方塊。

- b. 點擊“**設定**”按鈕。
- c. 在開啟的視窗中，選擇針對每種偵測到的物件類型的主要和次要操作（如果主要操作失敗）。
- d. 點擊“**確定**”。

6. 選擇要對不可還原的複合物件執行的操作：選擇或清除“**在偵測到嵌入物件時完全刪除應用程式無法修改的複合檔案**”核取方塊。

此核取方塊用於啟用或停用當偵測到惡意、疑似感染或其他偵測到的子內嵌物件時強制刪除父複合檔案。

如果選中該核取方塊並且工作設定為刪除受感染和疑似感染的物件，Kaspersky Embedded Systems Security 會在偵測到惡意或其他內嵌物件時強制刪除整個父複合物件。如果應用程式無法只刪除偵測到的子物件(例如，如果父物件不可修改)，將強制刪除父物件及其所有內容。

如果清除該核取方塊並且工作設定為刪除受感染和疑似感染的物件，當父物件不可修改時，Kaspersky Embedded Systems Security 不會執行所選操作。

7. 點擊“**儲存**”。

將儲存新的工作配置。

配置效能

► 要設定自訂掃描工作的效能：

1. 將開啟“**設定掃描範圍**”(請參見第 [537](#) 頁)視窗。
2. 選擇“**效能**”標籤。
3. 在“**排除**”部分中：

- 清除或選中“**排除檔案**”核取方塊。

按檔案名或檔案名遮罩從掃描中排除檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過指定的物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將掃描所有物件。

預設取消選定該核取方塊。

- 清除或選中“**不偵測**”核取方塊。

按可偵測物件的名稱或名稱遮罩從掃描中排除物件。病毒百科全書

<https://encyclopedia.kaspersky.com/knowledge/classification/> 網站上提供了可偵測物件的名稱清單。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過指定的可偵測物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 預設將偵測程式中指定的所有物件。

預設取消選定該核取方塊。

- 針對每個設定點擊“編輯”按鈕以新增排除項目。

4. 在“進階設定”部分中：

- **超過以下時間則停止掃描(秒)**

限制物件掃描的持續時間。預設值為 60 秒。

如果選中該核取方塊，則掃描持續時間將限制為指定的值。

如果取消選中該核取方塊，則對掃描持續時間沒有限制。

對於“最佳效能”安全等級，預設選定該核取方塊。

- **不掃描超過此值複合檔案(MB)**

將超過指定大小的物件排除在掃描之外。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在病毒掃描期間略過大小超過指定限制值的複合物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 將掃描任意大小的複合物件。

對於“最佳效能”安全等級，預設選定該核取方塊。

- 使用 iSwift 技術

iSwift 將資料庫中儲存的檔案 NTFS 識別碼與目前識別碼進行比較。只對識別碼發生變化的檔案（新檔案和自上次掃描 NTFS 系統物件以來修改過的檔案）執行掃描。

如果選中該核取方塊，Kaspersky Embedded Systems Security 僅掃描自上次掃描 NTFS 系統物件以來新建或修改的檔案。

如果清除該核取方塊，Kaspersky Embedded Systems Security 在掃描 NTFS 系統檔案時將不考慮檔案建立或修改的日期（網路資料夾中的檔案除外）。

預設將會選定該核取方塊。

- 使用 iChecker 技術

iChecker 會計算並記住掃描的檔案的核對總和。如果物件被修改，核對總和會發生變化。應用程式在掃描工作中比較所有核對總和，並且僅掃描新檔案和自上次掃描檔案以來修改過的檔案。

如果選中該核取方塊，Kaspersky Embedded Systems Security 僅掃描新檔案和修改的檔案。

如果清除該核取方塊，Kaspersky Embedded Systems Security 在掃描檔案時將不考慮檔案建立或修改的日期。

預設將會選定該核取方塊。

5. 點擊“儲存”。

將儲存新的工作配置。

配置分級儲存

► 要為“自訂掃描”工作配置對受感染的物件和其他偵測到的物件執行的操作：

1. 將開啟“設定掃描範圍”（請參見第 [537](#) 頁）視窗。

2. 選擇“分級儲存”標籤。
3. 選擇要對脫機檔案執行的操作：
 - 不掃描。
 - 僅掃描檔案的常駐部分。
 - 掃描完整檔案。

如果選擇此操作，則可以指定以下操作：

- 選中或清除“僅當檔案在指定天數內被存取過”核取方塊並指定天數。
- 選中或清除“如果可能，不將檔案複製到本機硬碟磁碟機”核取方塊。

4. 點擊“儲存”。

將儲存新的工作配置。

掃描卸除式磁碟。

► 要在應用程式主控台中配置在卸除式磁碟機連線到受防護電腦時對其進行的掃描：

1. 在應用程式主控台樹狀目錄中，開啟“Kaspersky Embedded Systems Security”節點的內容功能表並選擇“配置卸除式磁碟機掃描設定”選項。

將開啟“卸除式磁碟機掃描”視窗。

2. 在“連接時掃描”部分中，執行以下操作：
 - 如果想讓 Kaspersky Embedded Systems Security 在卸除式磁碟機連線時自動掃描，請選擇“掃描透過 USB 連接的卸除式磁碟機”核取方塊。
 - 如果需要，選中“掃描卸除式磁碟機，如果其儲存的資料量未超過(MB)”，然後在右側的欄位中指定最大值。
 - 在“掃描時使用的安全等級”下拉清單中，指定卸除式磁碟機掃描所需設定的安全等級。
3. 點擊“確定”。

即會儲存並套用指定設定。

自訂掃描工作統計

執行自訂掃描工作時，您可以檢視有關 Kaspersky Embedded Systems Security 自啟動以來已處理的物件數量的資訊。

即使工作暫停，也仍可檢視該資訊。您可以在工作記錄中檢視工作統計（請參見第 257 頁上的“在工作記錄中檢視 Kaspersky Embedded Systems Security 工作的統計和資訊”部分）。

► 若要檢視自訂掃描工作的統計，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中展開“自訂掃描”節點。
2. 選擇您要檢視統計的自訂掃描工作。

工作統計顯示在選定節點的詳細資訊視窗的“統計”部分中。

下表給出了 Kaspersky Embedded Systems Security 自啟動以來已處理的物件的資訊。

表 61. 自訂掃描工作統計

欄位	敘述
偵測到	Kaspersky Embedded Systems Security 偵測到的物件數量。例如，如果 Kaspersky Embedded Systems Security 在五個檔案中偵測到一個惡意軟體，該欄位中的值將增加 1。
偵測到受感染物件和其他物件	Kaspersky Embedded Systems Security 發現並歸類為“已感染”的物件數量，或者發現的未從即時防護和自訂掃描工作範圍中排除且歸類為可被入侵者用來破壞電腦或個人資料的合法軟體檔案數量。
偵測到可能存在的威脅	Kaspersky Embedded Systems Security 發現的疑似被感染的物件數。
物件未解毒	Kaspersky Embedded Systems Security 因以下原因未解毒的物件數： <ul style="list-style-type: none"> • 無法對偵測到的物件類型進行解毒。 • 解毒時發生錯誤。

欄位	敘述
物件未移至隔離區	Kaspersky Embedded Systems Security 嘗試隔離但無法執行此操作 (例如, 由於磁碟空間不足) 的物件數。
物件未刪除	Kaspersky Embedded Systems Security 嘗試刪除但無法刪除 (例如, 其他應用程式封鎖存取物件) 的物件數。
物件未掃描	Kaspersky Embedded Systems Security 在防護範圍中無法掃描 (例如, 其他應用程式封鎖存取物件) 的物件數。
物件未備份	Kaspersky Embedded Systems Security 嘗試在備份中儲存副本但無法執行此操作 (例如, 由於磁碟空間不足) 的物件數。
處理錯誤	處理中導致錯誤的物件數目。
物件已解毒	Kaspersky Embedded Systems Security 已解毒的物件的數量。
已移至隔離區	Kaspersky Embedded Systems Security 已隔離的物件的數量。
已移至備份區	Kaspersky Embedded Systems Security 儲存至備份的檔案數目。
物件已刪除	Kaspersky Embedded Systems Security 已刪除的物件的數量。
受密碼防護的物件	由於受密碼防護而導致 Kaspersky Embedded Systems Security 錯過的物件 (如壓縮檔案) 數目。
已損壞的物件	由於格式遭損壞而導致 Kaspersky Embedded Systems Security 錯過的物件數目。
物件已處理	Kaspersky Embedded Systems Security 已刪除的物件的總數。

透過點擊詳細資訊窗格中“**管理**”部分的“**開啟工作記錄**”連結，還可以在選定工作記錄中檢視自訂掃描工作統計。

建議您在工作完成後手動處理在“**事件**”標籤上的工作記錄中記錄的事件。

信任區域

本章節提供了有關 Kaspersky Embedded Systems Security 信任區域的資訊，以及如何在執行工作時將物件新增至信任區域的說明。

本章內容

關於信任區域.....	559
透過管理外掛程式管理信任區域.....	561
透過應用程式主控台管理信任區域.....	569

關於信任區域

信任區域是要從防護範圍或掃描範圍中排除的排除清單，您可以建立信任區域並將其套用到自訂掃描和即時檔案防護工作。

如果在安裝 Kaspersky Embedded Systems Security 時選中了“將 **Microsoft 建議的檔案新增到排除清單**”和“將 **Kaspersky Lab 建議的檔案新增到排除清單**”核取方塊，則 Kaspersky Embedded Systems Security 會將 Microsoft 和 Kaspersky Lab 針對即時電腦防護工作建議的檔案新增到信任區域。

您可以在 Kaspersky Embedded Systems Security 中根據以下規則建立信任區域：

- 受信任處理程序將對檔案攔截敏感的應用程式處理程序存取的物件新增信任區域中。
- 備份操作。將被備份硬碟磁碟機到外部裝置的系統存取的物件新增到信任區域中。
- 排除。將按位置指定的物件和/或在指定位置中偵測到的物件新增到信任區域中。

您可以在即時檔案防護工作、新增的自訂掃描工作，以及除隔離區掃描工作之外的所有系統自訂掃描工作中套用信任區域。

預設情況下，在即時檔案防護和自訂掃描工作中套用信任區域。

可以將用於建立信任區域的規則清單匯出為 XML 格式的設定檔，然後再將其匯入到其他電腦上執行的 Kaspersky Embedded Systems Security 中。

信任處理程序

套用於“即時檔案防護”和“流量安全”工作。

如果電腦上某些應用程式存取的檔案被 Kaspersky Embedded Systems Security 攔截，則這些應用程式運作上可能會不穩定。這些應用程式包括系統網域控制站的應用程式。

為了避免此類應用程式執行中斷，您可以對這些應用程式的正在執行的處理程序所存取的檔案停用防護（從而在信任區域中建立受信任處理程序清單）。

Microsoft Corporation 建議從即時檔案防護排除某些 Microsoft Windows 作業系統檔案和 Microsoft 應用程式檔案，因為程式不會被感染。Microsoft 網站（<https://www.microsoft.com/en-us/>（文章代碼：KB822158））上列出了一些此類別檔案的名稱。

您可以在信任區域中啟用或停用受信任處理程序。

如果可執行處理程序檔案發生修改（如已更新），Kaspersky Embedded Systems Security 會將其從信任的應用程式清單中排除。

應用程式不會套用受防護電腦上的檔案路徑值以信任該處理程序。受防護電腦上的檔案路徑僅用於搜尋檔案、計算核對總和和為使用者提供有關可執行檔來源的資訊。

備份操作

套用於即時電腦防護工作。

當將儲存在硬碟磁碟機上的資料備份到外部裝置時，可以停用備份操作過程中存取的物件的防護。

Kaspersky Embedded Systems Security 將掃描備份複製應用程式開啟並以 FILE_FLAG_BACKUP_SEMANTICS 內容讀取的物件。

排除

套用“於即時檔案防護”和“自訂掃描”工作。

您可以為已新增到信任區域的每個排除選擇要應用到的工作。此外，還可以在每一個 Kaspersky Embedded Systems Security 工作的安全等級設定中排除掃描物件。

您可以按物件在電腦上的位置、按這些物件中偵測到的物件名稱或名稱遮罩或者透過同時使用這兩個條件，將物件新增到信任區域。

基於排除規則，Kaspersky Embedded Systems Security 在根據以下設定執行指定工作時可略過某些物件：

- 可在電腦的指定區域中按名稱或名稱遮罩偵測到的指定物件。
- 可在電腦的指定區域中偵測到的所有物件。
- 在整個防護或掃描範圍內按名稱或名稱遮罩指定的偵測物件。

透過管理外掛程式管理信任區域

在本節中，學習如何透過管理外掛程式介面導航，以及如何為網路中的一台或所有電腦配置信任區域。

本章節說明項目

導航	561
透過管理外掛程式配置信任網域設定	563

導航

學習如何透過介面導航到所需工作設定。

本章節說明項目

透過卡巴斯基安全管理中心管理應用程式.....	562
開啟信任區域內容視窗.....	562

透過卡巴斯基安全管理中心管理應用程式

► 要透過卡巴斯基安全管理中心政策開啟信任區域：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“**政策**”標籤。
4. 點擊要設定的政策名稱。
5. 在開啟的“內容：<政策名稱>”視窗中，選擇“**選項**”部分。
6. 在“**信任區域**”子部分中點擊“**設定**”按鈕。

將開啟“**信任區域**”視窗。

根據需要設定政策。

如果某台電腦受卡巴斯基安全管理中心活動政策管理，且該政策禁止變更應用程式設定，則無法透過應用程式主控台編輯這些設定。

開啟信任區域內容視窗

► 要在“應用程式內容”視窗中配置信任區域：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“**裝置**”標籤。

4. 採用以下方法之一開啟“內容：<電腦名稱>”視窗：

- 點擊受防護電腦的名稱。
- 在受防護電腦的上下文功能表中選擇“內容”項。

將開啟“內容：<電腦名稱>”視窗。

5. 在“應用程式”部分中，選擇“Kaspersky Embedded Systems Security”。

6. 點擊“內容”按鈕。

將開啟“Kaspersky Embedded Systems Security 設定”視窗。

7. 選擇“選項”部分。

8. 在“信任區域”子部分中點擊“設定”按鈕。

將開啟“信任區域”視窗。

根據需要配置信任區域。

透過管理外掛程式配置信任網域設定

預設情況下，信任區域套用於所有新建立的政策和工作。

要配置信任區域設定，請執行以下設定：

1. 在“排除”標籤上指定 Kaspersky Embedded Systems Security 在工作執行過程中略過的物件（請參見第 [564](#) 頁上的“新增排除”部分）。
2. 在“受信任處理程序”標籤上指定 Kaspersky Embedded Systems Security 在工作執行過程中略過的處理程序（請參見第 [566](#) 頁上的“新增受信任處理程序”部分）。
3. 應用 not-a-virus 遮罩（請參見第 [569](#) 頁上的“應用 not-a-virus 遮罩”部分）。

本章節說明項目

新增排除	564
新增受信任處理程序	566
套用 not-a-virus 遮罩	569

新增排除

► 要透過卡巴斯基安全管理中心政策向信任區域新增排除：

1. 開啟“信任區域”視窗（請參見第 [562](#) 頁上的“透過卡巴斯基安全管理中心管理應用程式”部分）。
2. 在“排除”標籤上，指定掃描期間 Kaspersky Embedded Systems Security 要略過的物件：

- 要建立建議的排除項目，請點擊“新增建議的排除項目”按鈕。

點擊此按鈕允許您透過新增 Microsoft 建議的排除和 Kaspersky Lab 建議的排除來延伸排除清單。

- 要匯入排除項目，請點擊“匯入”按鈕，並在開啟的視窗中選擇 Kaspersky Embedded Systems Security 將視為受信任的檔案。
- 要手動指定將檔案視為受信任的條件，請點擊“新增”按鈕。

將開啟“排除”視窗。

3. 在“如果符合下列條件則不掃描物件”部分中，指定要從防護/掃描範圍中排除的物件以及要從可偵測物件中排除的物件：

- 如果要從防護或掃描範圍中排除物件：
 - a. 選中“要掃描的物件”核取方塊。

將檔案、資料夾、磁碟機或指令碼檔案新增到排除項目。

如果選中該核取方塊，在使用“**規則使用範圍**”部分中選擇的 Kaspersky Embedded Systems Security 元件執行掃描時，Kaspersky Embedded Systems Security 會略過指定的預定義範圍、檔案、資料夾、磁碟機或指令碼檔案。

預設取消選定該核取方塊。

- b. 點擊“**編輯**”按鈕。

將開啟“**選擇物件**”視窗。

- c. 指定要從掃描範圍中排除的物件。

指定物件時，可以使用特殊符號 **?** 和 *****。

- d. 點擊“**確定**”。

- e. 如果要從防護或掃描範圍中排除指定物件的所有子檔案和資料夾，則選中“**同時套用於子資料夾**”核取方塊。

- 如果要指定可偵測物件的名稱：

- a. 選中“**要偵測的物件**”核取方塊。

按可偵測物件的名稱或名稱遮罩從掃描中排除物件。病毒百科全書網站上提供了可偵測物件的名稱清單。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過指定的可偵測物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 預設將偵測程式中指定的所有物件。

預設取消選定該核取方塊。

- b. 點擊“**編輯**”按鈕。

將開啟“**偵測物件清單**”視窗。

- c. 按照病毒百科全書分類指定可偵測物件的名稱或名稱遮罩。

- d. 點擊“新增”按鈕。
 - e. 點擊“確定”。
4. 在“規則使用範圍”部分中，選中應將排除套用於的工作的名稱旁邊的核取方塊。

套用規則的 Kaspersky Embedded Systems Security 工作的名稱。
 5. 點擊“確定”。
- 排除顯示在“信任區域”視窗的“排除”標籤上的清單中。

新增受信任處理程序

► 向受信任處理程序清單中新增一個或多個處理程序：

1. 開啟“信任區域”視窗（請參見第 [562](#) 頁上的“透過卡巴斯基安全管理中心管理應用程式”部分）。
2. 選擇“受信任處理程序”標籤。
3. 選中“不檢查檔案備份操作”核取方塊可跳過對檔案讀取操作的掃描。

該核取方塊用於啟用或停用當電腦上安裝的備份工具執行檔案讀取操作掃描此類操作。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會略過由電腦上安裝的備份工具執行的檔案讀取操作。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 會掃描由電腦上安裝的備份工具執行的檔案讀取操作。

預設將會選定該核取方塊。

4. 選中“不檢查指定處理程序的檔案活動”核取方塊可跳過對受信任處理程序的檔案操作掃描。

該核取方塊用於啟用或停用掃描受信任處理程序的檔案活動。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會在掃描期間略過受信任處理程序的操作。

如果清除該核取方塊，Kaspersky Embedded Systems Security 會掃描受信任處理程序的檔案操作。

預設取消選定該核取方塊。

5. 點擊“**新增**”按鈕。
6. 從按鈕內容功能表中選擇以下選項之一：

- **多個處理程序。**

在開啟的“**新增受信任處理程序**”視窗中，配置以下設定：

- a. **使用磁碟上的完整處理程序路徑來將它視為受信任。**

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用檔案的完整路徑來確定處理程序是否受信任。

如果清除該核取方塊，則不使用檔案的路徑來確定處理程序是否受信任。

預設取消選定該核取方塊。

- b. **使用處理程序檔案雜湊來將它視為受信任。**

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用選定的檔案雜湊來確定處理程序信任狀態。

如果清除該核取方塊，則不使用檔案哈希來確定處理程序信任狀態。

預設將會選定該核取方塊。

- c. 點擊“**瀏覽**”按鈕以根據可執行處理程序新增資料。

- d. 在開啟的視窗中選擇可執行檔。

一次只能新增一個可執行檔。重複步驟 c-d 以新增其他可執行檔。

- e. 點擊“**處理程序**”按鈕以根據正在執行的處理程序新增資料。

- f. 在開啟的視窗中選擇處理程序。要選擇多個處理程序，請在選擇時按住 **CTRL** 鍵。

- g. 點擊“**確定**”。

執行“即時檔案防護”工作的帳戶在裝有 Kaspersky Embedded Systems Security 的電腦上必須具有管理員權限，才能檢視活動處理程序清單。您可以按檔案名稱、處理程序識別碼 (PID) 或處理程序的可執行檔在本機電腦上的路徑來對活動處理程序清單中的處理程序進行排序。請注意，只有在本機電腦上或透過卡巴斯基安全管理中心以指定的主機設定使用應用程式主控台時，才能透過點擊“處理程序”按鈕來選擇正在執行的處理程序。

- 一個基於檔案名稱和路徑的處理程序。

在開啟的“新增處理程序”視窗中，執行以下操作：

- a. 輸入可執行檔的路徑（包括檔案名稱）。
- b. 點擊“確定”。

- 一個基於物件內容的處理程序。

在開啟的“新增受信任處理程序”視窗中，配置以下設定：

- a. 點擊“瀏覽”按鈕，然後選擇處理程序。
- b. 使用磁碟上的完整處理程序路徑來將它視為受信任。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用檔案的完整路徑來確定處理程序是否受信任。

如果清除該核取方塊，則不使用檔案的路徑來確定處理程序是否受信任。

預設取消選定該核取方塊。

- c. 使用處理程序檔案雜湊來將它視為受信任。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用選定的檔案雜湊來確定處理程序信任狀態。

如果清除該核取方塊，則不使用檔案哈希來確定處理程序信任狀態。

預設將會選定該核取方塊。

- d. 點擊“確定”。

要將所選處理程序新增到受信任處理程序清單，必須選擇至少一種信任條件。

7. 在“新增受信任處理程序”視窗中，點擊“確定”按鈕。

選定的檔案或處理程序將新增到“信任區域”視窗中的受信任處理程序清單。

套用 not-a-virus 遮罩

not-a-virus 遮罩允許略過可能在掃描過程中被視為有害的合法軟體檔案和 Web 資源。該遮罩影響以下工作：

- 即時檔案防護。
- 自訂掃描。

如果未向排除清單新增該遮罩，Kaspersky Embedded Systems Security 將對此類別下的軟體套用在工作設定中指定的操作。

► 要套用 not-a-virus 遮罩：

1. 開啟“信任區域”視窗（請參見第 [562](#) 頁上的“透過卡巴斯基安全管理中心管理應用程式”部分）。
2. 如果清除該核取方塊，則在“排除”標籤上的“偵測物件”列中，捲動清單並選擇具有“not-a-virus:*”值的行。
3. 點擊“確定”。

套用了新設定。

透過應用程式主控台管理信任區域

在本節中，學習如何透過應用程式主控台介面導航以及如何在本地電腦上設定信任區域。

本章節說明項目

在應用程式主控台中對工作套用信任區域.....	570
在應用程式主控台中配置信任區域設定.....	571

在應用程式主控台中對工作套用信任區域

預設情況下，信任區域套用於“即時檔案防護”工作、新增的自訂“自訂掃描”工作以及除“隔離區掃描”工作之外的所有系統“自訂掃描”工作。

啟用或停用信任域後，會在執行的工作內立即應用或停止套用指定的排除。

► 要在 *Kaspersky Embedded Systems Security* 工作中啟用和停用信任區域：

1. 在應用程式主控台樹狀目錄中，開啟要為其配置信任區域的工作的內容功能表。
2. 選擇“內容”。

將開啟“工作設定”視窗。

3. 在開啟的視窗中，選擇“一般”標籤，然後執行以下操作之一：
 - 若要在工作中套用信任區域，請選定“套用信任區域”核取方塊。
 - 要在工作中停用信任區域，請清除“套用信任區域”核取方塊。

4. 如果要設定信任區域設定，請點擊“套用信任區域”核取方塊的名稱中的連結。

將開啟“信任區域”視窗。

5. 點擊“工作設定”視窗中的“確定”儲存變更。

在應用程式主控台中配置信任區域設定

要配置信任區域設定，請執行以下設定：

1. 在“**排除**”標籤上指定 Kaspersky Embedded Systems Security 在工作執行過程中略過的物件 (請參見第 [571](#) 頁上的“將排除新增至信任區域”部分)。
2. 在“**受信任處理程序**”標籤上指定 Kaspersky Embedded Systems Security 在工作執行過程中略過的處理程序 (請參見第 [573](#) 頁上的“受信任處理程序”部分)。
3. 對應用程式工作套用信任區域 (請參見第 [570](#) 頁上的“在應用程式主控台中對工作套用信任區域”部分)。
4. 應用 not-a-virus 遮罩 (請參見第 [576](#) 頁上的“應用 not-a-virus 遮罩”部分)。

本章節說明項目

將排除新增至信任區域.....	571
信任處理程序.....	573
套用 not-a-virus 遮罩.....	576

將排除新增至信任區域

► 要透過應用程式主控台手動向信任區域新增排除項目：

1. 在應用程式主控台樹狀目錄中，開啟 **Kaspersky Embedded Systems Security** 節點的內容功能表。
2. 選擇“**配置信任區域設定**”功能表選項。
將開啟“**信任區域**”視窗。
3. 選擇“**排除**”標籤。
4. 點擊“**新增**”按鈕。
將開啟“**排除**”視窗。

5. 在“如果符合下列條件則不掃描物件”部分中，指定要從防護/掃描範圍中排除的物件以及要從可偵測物件中排除的物件：

- 如果要從防護或掃描範圍中排除物件：

a. 選中“**要掃描的物件**”核取方塊。

將檔案、資料夾、磁碟機或指令碼檔案新增到排除項目。

如果選中該核取方塊，在使用“**規則使用範圍**”部分中選擇的 Kaspersky Embedded Systems Security 元件執行掃描時，Kaspersky Embedded Systems Security 會略過指定的預定義範圍、檔案、資料夾、磁碟機或指令碼檔案。

預設取消選定該核取方塊。

b. 點擊“**編輯**”按鈕。

將開啟“**選擇物件**”視窗。

c. 指定要從掃描範圍中排除的物件。

指定物件時，可以使用特殊符號 **?** 和 *****。

d. 點擊“**確定**”。

e. 如果要從防護或掃描範圍中排除指定物件的所有子檔案和資料夾，則選中“**同時套用於子資料夾**”核取方塊。

- 如果要指定可偵測物件的名稱：

a. 選中“**要偵測的物件**”核取方塊。

按可偵測物件的名稱或名稱遮罩從掃描中排除物件。病毒百科全書網站上提供了可偵測物件的名稱清單。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將在掃描期間略過指定的可偵測物件。

如果清除該核取方塊，Kaspersky Embedded Systems Security 預設將偵測程式中指定的所有物件。

預設取消選定該核取方塊。

- b. 點擊“**編輯**”按鈕。

將開啟“**偵測物件清單**”視窗。

- c. 按照病毒百科全書分類指定可偵測物件的名稱或名稱遮罩。
- d. 點擊“**新增**”按鈕。
- e. 點擊“**確定**”。

6. 在“**規則使用範圍**”部分中，選中應將排除套用於的工作的名稱旁邊的核取方塊。

套用規則的 Kaspersky Embedded Systems Security 工作的名稱。

7. 點擊“**確定**”。

排除顯示在“**信任區域**”視窗的“**排除**”標籤上的清單中。

信任處理程序

您可以使用以下某種方法將程序新增至受信任處理程序清單：

- 從受防護電腦上正在執行的處理程序清單中選擇。
- 選擇處理程序的可執行檔（不管程序目前是否正在執行）。

如果應用程式的可執行檔已修改，Kaspersky Embedded Systems Security 會將此處理程序從受信任清單排除。

► 向受信任處理程序清單中新增一個或多個處理程序：

1. 在應用程式主控台樹狀目錄中，開啟 **Kaspersky Embedded Systems Security** 節點的內容功能表。
2. 選擇“**配置信任區域設定**”功能表選項。

將開啟“**信任區域**”視窗。

3. 選擇“**受信任處理程序**”標籤。

4. 選中“**不檢查檔案備份操作**”核取方塊可跳過對檔案讀取操作的掃描。

該核取方塊用於啟用或停用當電腦上安裝的備份工具執行檔案讀取操作掃描此類操作。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會略過由電腦上安裝的備份工具執行的檔案讀取操作。

如果取消選中該核取方塊，Kaspersky Embedded Systems Security 會掃描由電腦上安裝的備份工具執行的檔案讀取操作。

預設將會選定該核取方塊。

5. 選中“**不檢查指定處理程序的檔案活動**”核取方塊可跳過對受信任處理程序的檔案操作掃描。

該核取方塊用於啟用或停用掃描受信任處理程序的檔案活動。

如果選中該核取方塊，Kaspersky Embedded Systems Security 會在掃描期間略過受信任處理程序的操作。

如果清除該核取方塊，Kaspersky Embedded Systems Security 會掃描受信任處理程序的檔案操作。

預設取消選定該核取方塊。

6. 點擊“**新增**”按鈕。

7. 從按鈕內容功能表中選擇以下選項之一：

- **多個處理程序。**

在開啟的“**新增受信任處理程序**”視窗中，配置以下設定：

- a. **使用磁碟上的完整處理程序路徑來將它視為受信任。**

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用檔案的完整路徑來確定處理程序是否受信任。

如果清除該核取方塊，則不使用檔案的路徑來確定處理程序是否受信任。

預設取消選定該核取方塊。

- b. 使用處理程序檔案雜湊來將它視為受信任。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用選定的檔案雜湊來確定處理程序信任狀態。

如果清除該核取方塊，則不使用檔案哈希來確定處理程序信任狀態。

預設將會選定該核取方塊。

- c. 點擊“**瀏覽**”按鈕以根據可執行處理程序新增資料。
- d. 在開啟的視窗中選擇可執行檔。

一次只能新增一個可執行檔。重複步驟 c-d 以新增其他可執行檔。

- e. 點擊“**處理程序**”按鈕以根據正在執行的處理程序新增資料。
- f. 在開啟的視窗中選擇處理程序。要選擇多個處理程序，請在選擇時按住 **CTRL** 鍵。
- g. 點擊“**確定**”。

執行“即時檔案防護”工作的帳戶在裝有 Kaspersky Embedded Systems Security 的電腦上必須具有管理員權限，才能檢視活動處理程序清單。您可以按檔案名稱、處理程序識別碼 (PID) 或處理程序的可執行檔在本機電腦上的路徑來對活動處理程序清單中的處理程序進行排序。請注意，只有在本機電腦上或透過卡斯基安全管理中心以指定的主機設定使用應用程式主控台時，才能透過點擊“**處理程序**”按鈕來選擇正在執行的處理程序。

- 一個基於檔案名稱和路徑的處理程序。

在開啟的“**新增處理程序**”視窗中，執行以下操作：

- a. 輸入可執行檔的路徑（包括檔案名稱）。
- b. 點擊“**確定**”。

- 一個基於物件內容的處理程序。

在開啟的“**新增受信任處理程序**”視窗中，配置以下設定：

- a. 點擊“**瀏覽**”按鈕，然後選擇處理程序。
- b. **使用磁碟上的完整處理程序路徑來將它視為受信任。**

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用檔案的完整路徑來確定處理程序是否受信任。

如果清除該核取方塊，則不使用檔案的路徑來確定處理程序是否受信任。

預設取消選定該核取方塊。

- c. **使用處理程序檔案雜湊來將它視為受信任。**

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用選定的檔案雜湊來確定處理程序信任狀態。

如果清除該核取方塊，則不使用檔案哈希來確定處理程序信任狀態。

預設將會選定該核取方塊。

- d. 點擊“**確定**”。

要將所選處理程序新增到受信任處理程序清單，必須選擇至少一種信任條件。

8. 在“**新增受信任處理程序**”視窗中，點擊“**確定**”按鈕。

選定的檔案或處理程序將新增到“**信任區域**”視窗中的受信任處理程序清單。

套用 not-a-virus 遮罩

not-a-virus 遮罩允許略過可能在掃描過程中被視為有害的合法軟體檔案和 Web 資源。該遮罩影響以下工作：

- 即時檔案防護。
- 自訂掃描。

如果未向排除清單新增該遮罩，Kaspersky Embedded Systems Security 將對此類別下的軟體或 Web 資源套用在工作設定中指定的操作。

► 要套用 *not-a-virus* 遮罩：

1. 在應用程式主控台樹狀目錄中，開啟 **Kaspersky Embedded Systems Security** 節點的內容功能表。
2. 選擇“**配置信任區域設定**”功能表選項。
將開啟“**信任區域**”視窗。
3. 選擇“**排除**”標籤。
4. 如果清除該核取方塊，則捲動清單並選擇具有“**not-a-virus:***”值的行。
5. 點擊“**確定**”。

套用了新設定。

弱點利用防禦

本節包含有關如何配置處理程序記憶體防護設定的說明。

本章內容

關於弱點利用防禦.....	578
透過管理外掛程式管理弱點利用防禦.....	580
透過應用程式主控台管理弱點利用防禦.....	585
弱點利用防禦技術.....	590

關於弱點利用防禦

Kaspersky Embedded Systems Security 提供防護處理程序記憶體免受弱點利用的能力。此功能在“弱點利用防禦”元件中實現。可以變更該元件的活動狀態和配置處理程序記憶體防護設定。

該元件透過在受防護的處理程序中插入外部“處理程序防護代理”（“代理”）防護處理程序記憶體免受弱點利用。

“處理程序防護代理”是一個動態載入的 Kaspersky Embedded Systems Security 模組，該模組可以插入到受防護的處理程序中，以便監控處理程序的完整性並降低被弱點利用的風險。

該代理在受防護的處理程序內的執行需要啟動和停止處理程序：只有處理程序已重新啟動，才能實現首次載入代理到已新增到受防護的處理程序清單中。此外，從受防護的處理程序清單中刪除處理程序後，只有該處理程序已重新啟動才能移除代理。

必須停止代理才能從受防護的處理程序中移除它：如果已移除“弱點利用防禦”元件，則應用程式將凍結環境並強制從受防護的處理程序中移除代理。如果在元件移除過程中在任一受防護處理程序中插入代理，則必須終止受影響的處理程序。可能需要重新啟動電腦(例如，如果系統處理程序正在受到防護)。

如果偵測到受防護的處理程序中存在弱點利用攻擊的跡象，則 Kaspersky Embedded Systems Security 執行以下操作之一：

- 如果進行弱點利用嘗試，則終止該處理程序。
- 報告處理程序已遭到入侵的事實。

您可採用以下方法之一停止處理程序防護：

- 移除該元件。
- 從受防護的處理程序清單中移除該處理程序並重新啟動該處理程序。

Kaspersky Security 弱點利用防禦服務

受防護電腦上必須提供 Kaspersky Security 弱點利用防禦服務，這樣“弱點利用防禦”元件才能發揮最大效果。此服務和“弱點利用防禦”元件是建議安裝的一部分。在受防護電腦上安裝該服務的過程中，將建立和啟動 kavfsw 處理程序。此處理程序從元件將有關受防護的處理程序的資訊傳輸到安全性代理。

Kaspersky Security 弱點利用防禦服務停止後，Kaspersky Embedded Systems Security 繼續防護已新增到受防護的處理程序清單中的處理程序，同時也載入到新新增的處理程序中，並使用所有可用的弱點利用防禦技術來防護處理程序記憶體。

如果您的電腦執行 Windows 10 或更高版本的作業系統，當 Kaspersky Security 弱點利用防禦服務停止後，應用程式將不繼續防護處理程序和處理程序記憶體。

如果 Kaspersky Security 弱點利用防禦服務已停止，則應用程式將不會接收隨受防護的處理程序出現的有關事件的資訊（包括有關弱點利用攻擊和處理程序終止的資訊）。此外，代理將無法接收新防護設定和新增新處理程序到受防護的處理程序清單中的有關資訊。

弱點利用防禦模式

可以選擇以下一種模式來配置操作，以降低弱點在受防護處理程序中被利用的風險：

- **發現弱點利用時終止**：當嘗試進行弱點利用時，應用此模式可終止處理程序。

當偵測到嘗試在受防護的關鍵作業系統處理程序中利用弱點時，無論“弱點利用防禦”元件設定中所指定的模式如何，Kaspersky Embedded Systems Security 都不會終止處理程序。

- **僅通知**：應用此模式可以使用安全記錄中的事件來接收受防護處理程序中的弱點實例的有關資訊。

如果選擇此模式，則 Kaspersky Embedded Systems Security 將透過建立事件來記錄所有利用弱點的嘗試。

透過管理外掛程式管理弱點利用防禦

在本節中，學習如何導航管理外掛程式介面，以及如何為網路中的一台或所有電腦配置元件設定。

本章節說明項目

導航	580
配置處理程序記憶體防護設定	582
新增進行防護的處理程序	584

導航

學習如何透過介面導航到所需工作設定。

本章節說明項目

開啟弱點利用防禦的政策設定	581
開啟弱點利用防禦內容視窗	581

開啟弱點利用防禦的政策設定

► 要透過卡巴斯基安全管理中心政策開啟弱點利用防禦設定：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“**政策**”標籤。
4. 點擊要設定的政策名稱。
5. 在開啟的“內容：<政策名稱>”視窗中，選擇“**即時電腦防護**”部分。
6. 在“**弱點利用防禦**”子部分中點擊“**設定**”按鈕。

將開啟“**弱點利用防禦**”視窗。

根據需要配置弱點利用防禦。

開啟弱點利用防禦內容視窗

► 要開啟弱點利用防禦的“內容：<伺服器名稱>”視窗：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的“**受管理裝置**”節點。
2. 選擇要為其設定工作的管理群組。
3. 選擇“**裝置**”標籤。

4. 採用以下方法之一開啟“內容：<電腦名稱>”視窗：

- 點擊受防護電腦的名稱。
- 在受防護電腦的上下文功能表中選擇“內容”項。

將開啟“內容：<電腦名稱>”視窗。

5. 在“應用程式”部分中，選擇“Kaspersky Embedded Systems Security”。

6. 點擊“內容”按鈕。

將開啟“Kaspersky Embedded Systems Security 設定”視窗。

7. 選擇“即時電腦防護”部分。

8. 在“弱點利用防禦”子部分中點擊“設定”按鈕。

將開啟“弱點利用防禦”視窗。

根據需要配置弱點利用防禦。

配置處理程序記憶體防護設定

► 要配置設定以防護新增到受防護的處理程序清單中的處理程序記憶體，請執行以下操作：

1. 開啟“弱點利用防禦”（請參見第 [581](#) 頁上的“開啟弱點利用防禦的政策設定”部分）視窗。

2. 在“弱點利用防禦模式”設定塊中，配置以下設定：

- 防止易受感染的處理程序被弱點利用。

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 可降低受防護的處理程序清單中的處理程序被利用弱點的風險。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不會防護電腦處理程序免遭弱點利用。

預設取消選定該核取方塊。

- **發現弱點利用時終止。**

如果選擇此模式，則 Kaspersky Embedded Systems Security 在偵測到弱點利用嘗試時（如果已對該處理程序應用積極的攻擊緩解技術），將終止受防護的處理程序。

- **僅通知。**

如果選擇此模式，則 Kaspersky Embedded Systems Security 透過顯示一個終端視窗報告弱點利用。被入侵的處理程序將繼續執行。

如果 Kaspersky Embedded Systems Security 在“**發現弱點利用時終止**”模式下執行時偵測到關鍵處理程序中存在弱點利用，則該元件會強制轉換到“**僅通知**”模式。

3. 在“防禦操作”設定塊中，配置以下設定：

- **透過“終端服務”來通知被利用的處理程序。**

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 會顯示一個終端視窗，其中有一個說明，解釋防護被啟動的原因以及指示在其中偵測到弱點利用嘗試的處理程序。

如果清除該核取方塊，則當偵測到弱點利用嘗試或被入侵的處理程序終止時 Kaspersky Embedded Systems Security 顯示一個終端視窗。無論 Kaspersky Security 弱點利用防禦服務的狀態如何，都會顯示終端視窗。預設將會選定該核取方塊。

- **即使 Kaspersky Security 服務已停用，也會防止易受感染的處理程序被弱點利用。**

如果選中此核取方塊，則無論 Kaspersky Security 服務是否執行，Kaspersky Embedded Systems Security 都將降低弱點在已啟動的處理程序中被利用的風險。Kaspersky Embedded Systems Security 不會防護 Kaspersky Security 服務停止後新增的處理程序。服務啟動後，所有處理程序將停止弱點利用風險減輕。

如果清除此核取方塊，則當 Kaspersky Security 服務停止時，Kaspersky Embedded Systems Security 不會防護處理程序免遭弱點利用。

預設將會選定該核取方塊。

4. 點擊“確定”。

Kaspersky Embedded Systems Security 將儲存並套用配置的處理程序防護設定。

新增進行防護的處理程序

“弱點利用防禦”元件預設防護多個處理程序。可以透過清除清單中的相應核取方塊來將處理程序從防護範圍中排除。

► 要向受防護的處理程序清單中新增處理程序：

1. 開啟“弱點利用防禦”（請參見第 [581](#) 頁上的“開啟弱點利用防禦的政策設定”部分）視窗。
2. 在“受防護處理程序”標籤上，點擊“瀏覽”按鈕。

將開啟標準 Microsoft Windows 資源管理器視窗。

3. 選擇您要新增到該清單的處理程序。
4. 點擊“開啟”按鈕。

處理程序名稱顯示在行中。

5. 點擊“新增”按鈕。

處理程序將被新增到受防護的處理程序清單中。

6. 選擇新增的處理程序。
7. 點擊“設定弱點利用防禦技術”。

將開啟“弱點利用防禦技術”視窗。

8. 選擇其中一個選項以應用攻擊緩解技術：

- 套用所有可用的弱點利用防禦技術。

如果選擇此選項，則不能編輯清單。預設情況下應用所有可用於處理程序的技術。

- 套用選定的弱點利用防禦技術。

如果選擇此選項，則您可以編輯已應用攻擊緩解技術：

- a. 選擇您要應用的技術旁邊的核取方塊，以防護選定的處理程序。

b. 選中或清除“套用受攻擊面減少技術來減輕弱點利用風險”核取方塊。

9. 配置“受攻擊面減少”技術的設定：

- 輸入其啟動將受到“拒絕模組”欄位中受防護的處理程序封鎖的模組的名稱。
- 在“不拒絕在網際網路區域中啟動的模組”欄位中，選擇您要在其下方允許模組啟動的選項旁邊的核取方塊：
 - 網際網路
 - 本機網際網路
 - 受信任的網站
 - 受限制的網站
 - 電腦

這些設定僅適用於 Internet Explorer®。

10. 點擊“確定”。

該處理程序將新增到工作防護範圍中。

透過應用程式主控台管理弱點利用防禦

在本節中，學習如何導航應用程式主控台介面以及如何在本地電腦上配置元件設定。

本章節說明項目

導航	586
配置處理程序記憶體防護設定	587
新增進行防護的處理程序	588

導航

學習如何透過介面導航到所需工作設定。

本章節說明項目

開啟弱點利用防禦一般設定.....	586
開啟弱點利用防禦處理程序防護設定.....	586

開啟弱點利用防禦一般設定

► 要開啟“**弱點利用防禦設定**”視窗：

1. 在應用程式主控台樹狀目錄中，選擇“**Kaspersky Embedded Systems Security**”節點。
2. 開啟內容功能表，然後選擇“**弱點利用防禦：一般設定**”功能表選項。

將開啟“**弱點利用防禦設定**”視窗。

根據需要配置弱點利用防禦的一般設定。

開啟弱點利用防禦處理程序防護設定

► 要開啟“**處理程序防護設定**”視窗：

1. 在應用程式主控台樹狀目錄中，選擇“**Kaspersky Embedded Systems Security**”節點。
2. 開啟內容功能表，然後選擇“**弱點利用防禦：處理程序防護設定**”功能表選項。

將開啟“**處理程序防護設定**”視窗。

根據需要配置弱點利用防禦的處理程序防護設定。

配置處理程序記憶體防護設定

► 要向受防護的處理程序清單中新增處理程序：

1. 開啟“弱點利用防禦設定”視窗。
2. 在“弱點利用防禦模式”設定塊中，配置以下設定：

- **防止易受感染的處理程序被弱點利用。**

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 可降低受防護的處理程序清單中的處理程序被利用弱點的風險。

如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不會防護電腦處理程序免遭弱點利用。

預設取消選定該核取方塊。

- **發現弱點利用時終止。**

如果選擇此模式，則 Kaspersky Embedded Systems Security 在偵測到弱點利用嘗試時（如果已對該處理程序應用積極的攻擊緩解技術），將終止受防護的處理程序。

- **僅通知。**

如果選擇此模式，則 Kaspersky Embedded Systems Security 透過顯示一個終端視窗報告弱點利用。被入侵的處理程序將繼續執行。

如果 Kaspersky Embedded Systems Security 在“發現弱點利用時終止”模式下執行時偵測到關鍵處理程序中存在弱點利用，則該元件會強制轉換到“僅通知”模式。

3. 在“防禦操作”設定塊中，配置以下設定：

- **透過“終端服務”來通知被利用的處理程序。**

如果選中此核取方塊，則 Kaspersky Embedded Systems Security 會顯示一個終端視窗，其中有一個說明，解釋防護被啟動的原因以及指示在其中偵測到弱點利用嘗試的處理程序。

如果清除該核取方塊，則當偵測到弱點利用嘗試或被入侵的處理程序終止時 Kaspersky Embedded Systems Security 顯示一個終端視窗。無論 Kaspersky Security 弱點利用防禦服務的狀態如何，都會顯示終端視窗。預設將會選定該核取方塊。

- **即使 Kaspersky Security 服務已停用，也會防止易受感染的處理程序被弱點利用。**

如果選中此核取方塊，則無論 Kaspersky Security 服務是否執行，Kaspersky Embedded Systems Security 都將降低弱點在已啟動的處理程序中被利用的風險。Kaspersky Embedded Systems Security 不會防護 Kaspersky Security 服務停止後新增的處理程序。服務啟動後，所有處理程序將停止弱點利用風險減輕。

如果清除此核取方塊，則當 Kaspersky Security 服務停止時，Kaspersky Embedded Systems Security 不會防護處理程序免遭弱點利用。

預設將會選定該核取方塊。

4. 在“弱點利用防禦設定”視窗中，點擊“確定”。

Kaspersky Embedded Systems Security 將儲存並套用配置的處理程序防護設定。

新增進行防護的處理程序

“弱點利用防禦”元件預設防護多個處理程序。您可以在受防護處理程序清單中取消選中您不想防護的處理程序。

► *要向受防護的處理程序清單中新增處理程序：*

1. 開啟“處理程序防護設定”視窗。
2. 要新增處理程序以防護其不被濫用並減少可能的弱點利用影響，請執行以下操作：
 - a. 點擊“瀏覽”按鈕。
將開啟標準 Microsoft Windows“開啟”視窗。
 - b. 在開啟的視窗中，選擇您要新增到該清單的處理程序。
 - c. 點擊“開啟”按鈕。

d. 點擊“新增”按鈕。

處理程序將被新增到受防護的處理程序清單中。

3. 在清單中選擇處理程序。

4. 在“處理程序防護設定”上將顯示目前設定：

- 處理程序名稱。
- 正在執行。
- 已套用弱點利用防禦技術。
- 受攻擊面減少設定。

5. 要修改套用於該處理程序的弱點利用防禦技術，請選擇“弱點利用防禦技術”標籤。

6. 選擇其中一個選項以應用攻擊緩解技術：

- 套用所有可用的弱點利用防禦技術。

如果選擇此選項，則不能編輯清單。預設情況下應用所有可用於處理程序的技術。

- 針對處理程序套用列出的弱點利用防禦技術。

如果選擇此選項，則您可以編輯已應用攻擊緩解技術：

a. 選擇您要應用的技術旁邊的核取方塊，以防護選定的處理程序。

7. 配置“受攻擊面減少”技術的設定：

- 輸入其啟動將受到“拒絕模組”欄位中受防護的處理程序封鎖的模組的名稱。
- 在“不拒絕在網際網路區域中啟動的模組”欄位中，選擇您要在其下方允許模組啟動的選項旁邊的核取方塊：
 - 網際網路
 - 本機網際網路
 - 受信任的網站
 - 受限制的網站
 - 電腦

這些設定僅適用於 Internet Explorer®。

8. 點擊“確定”。

該處理程序將新增到工作防護範圍中。

弱點利用防禦技術

表 62. 弱點利用防禦技術

弱點利用防禦技術	敘述
資料執行防護 (DEP)	資料執行防護封鎖在受防護的記憶體區域中執行任意代碼。
位址空間佈局隨機化 (ASLR)	改變處理程序位址空間內資料結構佈局。
結構化例外處理常式覆蓋防護 (SEHOP)	異常記錄的取代或異常處理程式的取代。
空頁分配	防護重定向空指針。
LoadLibrary 網路調用檢查 (ROP 防護)	防止從網路路徑載入 DLL。

弱點利用防禦技術	敘述
可執行檔堆疊 (ROP 防護)	封鎖堆疊區域的非授權執行。
RET 防護檢查 (ROP 防護)	檢查確保安全調用 CALL 指令。
堆疊透視防護 (ROP 防護)	防止將 ESP 堆疊指標重新定位到可執行檔位址。
簡單匯出位址表存取監視(EAT 存取監視和透過調試寄存器的 EAT 存取監視)	防止對 kernel32.dll、kernelbase.dll 和 ntdll.dll 匯出位址表的讀取存取
堆噴射分配 (Heapspray)	防止將記憶體分配用於執行惡意程式碼。
執行流模擬 (返回導向編程防護)	偵測 Windows API 元件中的可疑指令鏈 (潛在 ROP 小工具)。
IntervalProfile 調用監視 (協助工具驅動程式防護 (AFDP))	防止透過 AFD 驅動程式中的弱點進行提權 (透過 QueryIntervalProfile 調用在 Ring 0 中執行任意代碼)。
受攻擊面減少 (ASR)	透過受防護的處理程序封鎖啟動易受攻擊的載入項。
處理程序挖空防護 (Hollowing)	防止建立和執行受信任處理程序的惡意副本。
AtomBombing 防護(APC)	透過非同步程序呼叫 (APC) 利用全域原子表弱點。
CreateRemoteThread 防護 (RThreadLocal)	其他處理程序已在受防護處理程序中建立執行緒。
CreateRemoteThread 防護 (RThreadRemote)	受防護處理程序已在其他處理程序中建立執行緒。

與協力廠商系統整合

本節介紹 Kaspersky Embedded Systems Security 與協力廠商功能和技術的整合。

本章內容

監控效能。Kaspersky Embedded Systems Security 計數器	592
與 WMI 整合	613

監控效能。Kaspersky Embedded Systems Security 計數器

本章節包含有關 Kaspersky Embedded Systems Security 計數器的資訊：系統監控效能計數器以及 SNMP 計數器和 TRAP。

本章節說明項目

系統監視器的效能計數器	592
Kaspersky Embedded Systems Security SNMP 計數器和 TRAP	600

系統監視器的效能計數器

本節包含有關安裝期間由 Kaspersky Embedded Systems Security 註冊的 Microsoft Windows 系統監視器的效能計數器的資訊。

本章節說明項目

關於 Kaspersky Embedded Systems Security 效能計數器	593
拒絕需求總數	594
略過需求總數	595
因為系統資源不足而未處理的需求數	595
傳送以供處理的要求數	596
檔案截取調度程式執行緒的平均數	597
檔案截取調度程式執行緒的最大數	597
已感染物件佇列中的元素數	598
每秒處理的物件數	599

關於 Kaspersky Embedded Systems Security 效能計數器

預設情況下，“效能計數器”元件包含在 Kaspersky Embedded Systems Security 的已安裝元件中。

Kaspersky Embedded Systems Security 在安裝期間在 Microsoft Windows 系統監視器中註冊其自己的效能計數器。

使用 Kaspersky Embedded Systems Security 計數器，您可用於監視執行即時防護工作時應用程式的效能。搭配其他應用程式共同執行時，可能會發生空間不足或資源短缺。您可能會診斷出不需要的 Kaspersky Embedded Systems Security 設定與操作當機情況。

透過在 Windows 控制台的“管理”項中開啟“效能”主控台，來檢視 Kaspersky Embedded Systems Security 效能計數器。

下列章節列出了計數器定義、獲取讀數的建議時間間隔、上限值以及在計數器值超過 Kaspersky Embedded Systems Security 設定時的建議。

拒絕需求總數

表 63. 拒絕需求總數

名稱	拒絕需求總數
定義	來自檔案攔截驅動程式但未被應用程式處理程序接受的物件處理請求總數，從 Kaspersky Embedded Systems Security 上次啟動時開始計數。 程式將略過被 Kaspersky Embedded Systems Security 處理程序拒絕的物件處理要求。
用途	此計數器可讓您偵測： <ul style="list-style-type: none"> • 因為 Kaspersky Embedded Systems Security 的工作程序滿載，造成即時防護品質降低。 • 因檔案截取調度程式失敗，造成即時防護中斷。
標準值/上限值	0/1。
建議的讀取間隔時間	1 小時。
如果值超過上限值時的設定建議	遭拒的處理要求數等於略過的物件數。 視計數器的行為而定，可能會發生以下情況： <ul style="list-style-type: none"> • 計數器在較長的時間段內顯示了許多被拒絕的請求：由於完全載入了所有 Kaspersky Embedded Systems Security 處理程序，Kaspersky Embedded Systems Security 無法掃描物件。 若要避免略過物件，請增加用於完成即時防護工作的應用程式處理程序的數量。您可以使用“最大活動程序數”和“用於即時防護的程序數”等 Kaspersky Embedded Systems Security 設定。 • 要求遭拒數明顯超過上限值，且還在快速成長中：檔案截取調度程式已失效。Kaspersky Embedded Systems Security 未在存取物件時對其進行掃描。 重新啟動 Kaspersky Embedded Systems Security。

略過需求總數

表 64. 略過需求總數

名稱	略過請求總數
定義	<p>來自檔案攔截驅動程式且由 Kaspersky Embedded Systems Security 收到但未產生處理完成事件的物件處理請求總數；從應用程式上次啟動時開始計數。</p> <p>如果有其中一種工作程序接受物件程序要求，但並未傳送處理完程式事件，則驅動程式會將要求傳遞至其他程序，而計數器“要求略過總數”的值會加 1。如果驅動程序已進行過所有工作程序，且無任何程序接受過處理的要求（因為忙碌），或並未傳送處理完程式鍵，Kaspersky Embedded Systems Security 會略過該物件，而計數器“要求略過總數”的值會加 1。</p>
用途	此計數器使您能夠偵測，因為檔案截取調度程式故障而產生的效能降低情況。
標準值/上限值	0/1
建議的讀取間隔時間	1 小時
如果值超過上限值時的設定建議	<p>如果計數器值並非零，表示有一或多個檔案截取調度程式執行緒已凍結，且停止作業。計數器等於目前閒置的執行緒數。</p> <p>如果掃描速度緩慢，請重新啟動 Kaspersky Embedded Systems Security 來還原離線的資料流。</p>

因為系統資源不足而未處理的需求數

表 65. 因為系統資源不足而未處理的需求數

名稱	因為資源不足而未處理的要求數。
----	-----------------

定義	因為系統資源（例如 RAM）不足，而未處理的檔案截取驅動程式要求總數； 從上次啟動 Kaspersky Embedded Systems Security 的時間算起。 Kaspersky Embedded Systems Security 會略過檔案截取驅動程式未處理其掃描要求的物件。
用途	此計數器可用來消除即時防護品質可能因系統資源不足而降低的情況。
標準值/上限值	0/1。
建議的讀取間隔時間	1 小時。
如果值超過上限值時的設定建議	如果計數器值不為零，則表明 Kaspersky Embedded Systems Security 工作處理程序需要更多 RAM 來處理請求。 其他應用程式的作用中程序可能會使用所有可用的 RAM。

傳送以供處理的需求數

表 66. 傳送以供處理的需求數

名稱	傳送以供處理的需求數。
定義	等待工作處理程序處理的物件數量。
用途	此計數器可用於追蹤 Kaspersky Embedded Systems Security 工作程序的負載，以及電腦上檔案活動的整體程度。
標準值/上限值	該計數器值可能因電腦上的檔案活動水平而異。
建議的讀取間隔時間	1 分鐘
如果值超過上限值時的設定建議	否

檔案截取調度程式執行緒的平均數

表 67. 檔案截取調度程式執行緒的平均數

名稱	檔案截取調度程式執行緒的平均數。
定義	一個處理程序中的檔案攔截調度程式流數量，對於目前參與即時防護工作的所有處理程序而言，則為檔案攔截調度程式流的平均數量。
用途	此計數器可用來消除即時防護品質可能因 Kaspersky Embedded Systems Security 處理程序滿載而降低的情況。
標準值/上限值	視情況有所不同 / 40。
建議的讀取間隔時間	1 分鐘
如果值超過上限值時的設定建議	<p>每個工作程序中最多可建立 60 個檔案截取調度程式執行緒。如果計數器值接近 60，則可能會有工作程序無法處理佇列中下一個檔案截取驅動程式要求的風險，且 Kaspersky Embedded Systems Security 會略過物件。</p> <p>請增加用於完成即時防護工作的 Kaspersky Embedded Systems Security 處理程序的數量。您可以使用“最大活動程序數”和“用於即時防護的程序數”等 Kaspersky Embedded Systems Security 設定。</p>

檔案截取調度程式執行緒的最大數

表 68. 檔案截取調度程式執行緒的最大數

名稱	檔案截取調度程式執行緒的最大數。
定義	一個處理程序中的檔案攔截調度程式流數量，對於目前參與即時防護工作的所有處理程序而言，則為檔案攔截調度程式流的最大數量。
用途	此計數器可讓您偵測與修除因執行中程序負載分配不平均所造成的效能低落。
標準值/上限值	視情況有所不同 / 40。
建議的讀取間隔時間	1 分鐘

<p>如果值超過上限值時的設定建議</p>	<p>如果計數器的值超過“檔案截取調度程式執行緒的平均數”計數器的值並繼續增加，則表示 Kaspersky Embedded Systems Security 正在執行的處理程序分配負載時不夠平均。</p> <p>重新啟動 Kaspersky Embedded Systems Security。</p>
-----------------------	--

已感染物件佇列中的元素數

表 69. 已感染物件佇列中的元素數

<p>名稱</p>	<p>已感染物件佇列中的項目數。</p>
<p>定義</p>	<p>目前等候處理（未受感染或已刪除）的已感染物件數。</p>
<p>用途</p>	<p>此計數器可讓您偵測：</p> <ul style="list-style-type: none"> • 檔案截取調度程式可能失敗，造成即時防護中斷。 • 因不同工作處理程序與 Kaspersky Embedded Systems Security 間的處理器時間分配不平均，而造成處理程序過載。 • 病毒爆發。
<p>標準值/上限值</p>	<p>當 Kaspersky Embedded Systems Security 正在處理已感染或可疑物件時，此計數器值可能大於零；但當處理完成時會傳回零，或計數器值會長久保持非零的狀態。</p>
<p>建議的讀取間隔時間</p>	<p>1 分鐘</p>

<p>如果值超過上限值時的設定建議</p>	<p>如果此計數器值常久未傳回零：</p> <ul style="list-style-type: none"> • Kaspersky Embedded Systems Security 並未處理物件（檔案截取調度程式可能已當機）。 <p>重新啟動 Kaspersky Embedded Systems Security。</p> <ul style="list-style-type: none"> • 處理物件的處理器時間不足。 <p>請確定 Kaspersky Embedded Systems Security 可取得更多處理時間（例如，降低電腦上其他應用程式的負載）。</p> <ul style="list-style-type: none"> • 病毒已爆發。 <p>在“即時檔案防護”工作中有大量已感染或可疑物件，也表示病毒爆發。可以在工作統計或工作記錄中檢視有關偵測到的物件的數量的資訊。</p>
-----------------------	---

每秒處理的物件數

表 70. 每秒處理的物件數

名稱	每秒處理的物件數。
定義	已處理的物件數除以處理那些物件所花的時間量（以相等間隔時間來計算）。
用途	此計數器會反映物件處理的速度；可用於偵測與消除因分配至 Kaspersky Embedded Systems Security 處理程序的處理器時間不足，或 Kaspersky Embedded Systems Security 作業錯誤，所造成的電腦效能低落。
標準值/上限值	視情況有所不同 / 無。
建議的讀取間隔時間	1 分鐘。

<p>如果值超過上限值時的設定建議</p>	<p>此計數器中的值，要視 Kaspersky Embedded Systems Security 設定，以及電腦上來自其他應用程式的負載而定。</p> <p>注意一段長時間時計數器數字的平均程度。如果一般程度計數器值的降低，表示可能發生以下其中一種情況：</p> <ul style="list-style-type: none"> • Kaspersky Embedded Systems Security 處理程序處理物件的處理器時間不足。 <p>請確定 Kaspersky Embedded Systems Security 可取得更多處理時間（例如，降低電腦上其他應用程式的負載）。</p> <ul style="list-style-type: none"> • Kaspersky Embedded Systems Security 出錯（多個流空間）。 <p>重新啟動 Kaspersky Embedded Systems Security。</p>
------------------------------	---

Kaspersky Embedded Systems Security SNMP 計數器和 TRAP

本節包含有關 Kaspersky Embedded Systems Security 計數器和 TRAP 的資訊。

本章節說明項目

關於 Kaspersky Embedded Systems Security SNMP 計數器和 TRAP	600
Kaspersky Embedded Systems Security SNMP 計數器.....	601
Kaspersky Embedded Systems Security SNMP TRAP.....	604

關於 Kaspersky Embedded Systems Security SNMP 計數器和 TRAP

如果要安裝一組防毒元件中包括 SNMP 計數器和 TRAP，則可以使用簡單網路管理協定 (SNMP) 檢視 Kaspersky Embedded Systems Security 計數器和 TRAP。

若要從管理員的工作站檢視 Kaspersky Embedded Systems Security 計數器與 TRAP，請啟動受防護電腦上的 SNMP 服務，並啟動管理員工作站上的 SNMP 與 SNMP TRAP 服務。

Kaspersky Embedded Systems Security SNMP 計數器

本節包含介紹 Kaspersky Embedded Systems Security SNMP 計數器的設定的表。

本章節說明項目

效能計數器	601
隔離計數器	601
備份計數器	602
一般計數器	602
更新計數器	603
即時防護計數器	603

效能計數器

表 71. 效能計數器

計數器	定義
currentRequestsAmount	傳送以供處理的要求數 (請參見第 596 頁)
currentInfectedQueueLength	已感染物件佇列中的項目數 (請參見第 598 頁上的“已感染物件佇列中的項目數”部分)
currentObjectProcessingRate	每秒處理的物件數 (請參見第 599 頁)
currentWorkProcessesNumber	Kaspersky Embedded Systems Security 所使用的工作處理程序的目前數量

隔離計數器

表 72. 隔離計數器

計數器	定義
-----	----

計數器	定義
totalObjects	目前在隔離中的物件數
totalSuspiciousObjects	目前在隔離中的可疑物件數
currentStorageSize	隔離中的資料大小總計(MB)

備份計數器

表 73. 備份計數器

計數器	定義
currentBackupStorageSize	備份中的資料大小總計(MB)

一般計數器

表 74. 一般計數器

計數器	定義
lastCriticalAreasScanAge	電腦關鍵區域自上次完成掃描以來的期限 (自從上次完成“ <i>掃描關鍵區域</i> ”的工作後所經過的時間，單位為秒)。
licenseExpirationDate	產品授權到期日期。如果新增了啟動金鑰和備用金鑰，則將顯示與備用金鑰關聯的產品授權到期日期。
currentApplicationUptime	Kaspersky Embedded Systems Security 自從上次啟動起的執行時間 (單位為百分之一秒)。
currentFileMonitorTaskStatus	“即時檔案防護”工作狀態： 開啟 – 正在執行； 關閉 – 已停止或已暫停。

更新計數器

表 75. 更新計數器

計數器	定義
avBasesAge	資料庫“時效”（最近一次更新已安裝資料庫的建立日期後所經過的時間，單位為百分之一秒）。

即時防護計數器

表 76. 即時防護計數器

計數器	定義
totalObjectsProcessed	上次執行“即時檔案防護”工作時掃描的物件總數
totalInfectedObjectsFound	上次“執行即時檔案防護”工作時受感染和其他的物件總數
totalSuspiciousObjectsFound	上次執行“即時檔案防護”工作時可疑的物件總數
totalVirusesFound	上次執行“即時檔案防護”工作時偵測到的威脅總數
totalObjectsQuarantined	Kaspersky Embedded Systems Security 放入隔離的已感染、可疑感染和其他物件的總數；從上次啟動“即時檔案防護”工作的時間算起
totalObjectsNotQuarantined	Kaspersky Embedded Systems Security 嘗試隔離但無法隔離成功的已感染或可疑物件總數；從上次啟動“即時檔案防護”工作的時間算起
totalObjectsDisinfected	Kaspersky Embedded Systems Security 解毒的已感染物件總數；從上次啟動“即時檔案防護”工作的時間算起
totalObjectsNotDisinfected	Kaspersky Embedded Systems Security 嘗試解毒但無法成功解毒的已感染物件總數；從上次啟動“即時檔案防護”工作的時間算起
totalObjectsDeleted	Kaspersky Embedded Systems Security 解毒的已感染、可疑感染和其他物件的總數；自上一次啟動“即時檔案防護”工作的時間算起

計數器	定義
totalObjectsNotDeleted	Kaspersky Embedded Systems Security 嘗試清除但未成功解毒的已感染、可疑感染和其他物件的總數；從上次啟動“即時檔案防護”工作的時間算起
totalObjectsBackedUp	Kaspersky Embedded Systems Security 放入備份中的已感染和其他物件的總數；從上次啟動“即時檔案防護”工作的時間算起
totalObjectsNotBackedUp	Kaspersky Embedded Systems Security 嘗試放入備份中但未成功的已感染和其他物件的總數；從上次啟動“即時檔案防護”工作的時間算起

Kaspersky Embedded Systems Security SNMP TRAP

下面匯總了 Kaspersky Embedded Systems Security 中的 SNMP TRAP 選項：

- eventThreatDetected：偵測到一個物件。

TRAP 的選項如下所示：

- eventDateAndTime
- eventSeverity
- computerName
- userName
- objectName
- threatName
- detectType
- detectCertainty
- eventBackupStorageSizeExceeds：已超過最大備份大小。備份中的資料總大小已超過“**最大備份空間 (MB)**”所指定的值。Kaspersky Embedded Systems Security 繼續備份受感染的物件。

TRAP 的選項如下所示：

- eventDateAndTime
- eventSeverity

- eventSource
- eventThresholdBackupStorageSizeExceeds : 已達到備份可用空間上限值。“可用空間上限值(MB)”指派的備份可用空間量等於或低於指定值。Kaspersky Embedded Systems Security 繼續備份受感染的物件。

TRAP 的選項如下所示：

- eventDateAndTime
- eventSeverity
- eventSource
- eventQuarantineStorageSizeExceeds : 已超過最大隔離容量。隔離中資料的總大小已超過“**隔離區最大容量 (MB)**”所指定的值。Kaspersky Embedded Systems Security 會繼續隔離可疑物件。

TRAP 的選項如下所示：

- eventDateAndTime
- eventSeverity
- eventSource
- eventObjectNotQuarantined : 隔離區錯誤。

TRAP 的選項如下所示：

- eventSeverity
- eventDateAndTime
- eventSource
- userName
- computerName
- objectName
- storageObjectNotAddedEventReason
- eventObjectNotBackuped : 在副本中儲存物件副本時發生錯誤。

TRAP 的選項如下所示：

- eventSeverity
- eventDateAndTime
- eventSource

- objectName
 - userName
 - computerName
 - storageObjectNotAddedEventReason
- eventQuarantineInternalError : 隔離區內部錯誤。

TRAP 的選項如下所示 :

- eventSeverity
 - eventDateAndTime
 - eventSource
 - eventReason
- eventBackupInternalError : 備份錯誤。

TRAP 的選項如下所示 :

- eventSeverity
 - eventDateAndTime
 - eventSource
 - eventReason
- eventAVBasesOutdated : 防毒軟體資料庫已過期。正在計算從上次執行資料庫更新工作 (本機工作、群組工作或多組電腦的工作) 起的天數。

TRAP 的選項如下所示 :

- eventSeverity
 - eventDateAndTime
 - eventSource
 - days
- eventAVBasesTotallyOutdated : 防毒軟體資料庫嚴重過期。正在計算從上次執行資料庫更新工作 (本機工作、群組工作或多組電腦的工作) 起的天數。

TRAP 的選項如下所示 :

- eventSeverity
- eventDateAndTime

- eventSource
- days
- eventApplicationStarted : Kaspersky Embedded Systems Security 正在執行。

TRAP 的選項如下所示：

- eventSeverity
- eventDateAndTime
- eventSource
- eventApplicationShutdown : Kaspersky Embedded Systems Security 已停止。

TRAP 的選項如下所示：

- eventSeverity
- eventDateAndTime
- eventSource
- eventCriticalAreasScanWasntPerformForALongTime : 很長時間未掃描關鍵區域。以自上次完成“關鍵區域掃描”工作以來的天數進行計算。

TRAP 的選項如下所示：

- eventSeverity
- eventDateAndTime
- eventSource
- days
- eventLicenseHasExpired : 產品授權已到期。

TRAP 的選項如下所示：

- eventSeverity
- eventDateAndTime
- eventSource

- eventLicenseExpiresSoon：產品授權即將到期。計算距離產品授權到期日之前的天數。

TRAP 的選項如下所示：

- eventSeverity
 - eventDateAndTime
 - eventSource
 - days
- eventTaskInternalError：工作完成錯誤。

TRAP 的選項如下所示：

- eventSeverity
 - eventDateAndTime
 - eventSource
 - errorCode
 - knowledgeBaseId
 - taskName
- eventUpdateError：更新工作效能時發生錯誤。

TRAP 的選項如下所示：

- eventSeverity
- eventDateAndTime
- taskName
- updaterErrorEventReason

TRAP 選項及其可能的參數值的說明如下：

- eventDateAndTime：事件日期和時間。
- eventSeverity：重要性等級。

該選項可以採用以下值：

- critical (1) - 重要

- warning (2) - 警告
- info (3) - 資訊
- userName：使用者名稱（例如，嘗試存取已感染檔案之使用者的名稱）。
- computerName：電腦名稱（例如，嘗試存取已感染檔案之使用者所用電腦的名稱）。
- eventSource：產生事件的功能性元件。

該選項可以採用以下值：

- unknown (0) - 不明的功能性元件
- quarantine (1) - 隔離
- backup (2) - 備份
- reporting (3) - 工作記錄
- updates (4) - 更新
- realTimeProtection (5) - 即時檔案防護
- onDemandScanning (6) - 自訂掃描
- product (7) - 整體而言與操作 Kaspersky Embedded Systems Security 而非個別元件相關的事件
- systemAudit (8) - 系統稽核記錄
- eventReason：事件觸發：是什麼原因引發了該事件。

該選項可以採用以下值：

- reasonUnknown (0) - 不明原因
- reasonInvalidSettings (1) - 僅有在無法使用“隔離”或“備份”時，才適用於“隔離”或“備份”的事件（存取權限不足，或在“隔離”設定中指定錯誤的資料夾，例如指定了網路路徑）。在這種情況中，Kaspersky Embedded Systems Security 會使用預設的“備份”或“隔離”資料夾。

- `objectName` : 物件名稱 (例如 , 偵測到含病毒之檔案的名稱) 。
- `threatName` : 根據病毒百科全書 <https://encyclopedia.kaspersky.com/knowledge/classification/> 分類確定的物件名稱。該名稱包含在 Kaspersky Embedded Systems Security 偵測物件時回傳的物件全名中。您可以在工作記錄中檢視偵測到的物件的全名 (請參見第 [127](#) 頁上的“配置記錄設定”部分) 。

- `detectType` : 偵測到的威脅類型。

該選項可以採用以下值 :

- `undefined (0)` - 未定義
 - `virware` - 典型病毒與網路蠕蟲
 - `trojware` - 木馬程式
 - `malware` - 其他惡意程式
 - `adware` - 廣告軟體
 - `pornware` - 色情軟體
 - `riskware` - 可能被入侵者用以破壞使用者電腦或個人資料的合法程式
- `detectCertainty` : 偵測威脅的確認等級。

該選項可以採用以下值 :

- 可疑 (`suspicious`) - Kaspersky Embedded Systems Security 在物件的一段程式碼中偵測到部分符合不明威脅程式碼的結果。
- 確定 (`Sure`) - Kaspersky Embedded Systems Security 在物件的一段程式碼中偵測到完全符合不明威脅程式碼的結果。

- days：天數（例如，授權到期日前的天數）。
- errorCode：錯誤代碼。
- knowledgeBaseId：知識庫文章的位址（例如說明特定錯誤之文章的位址）。
- taskName：工作名稱。
- updaterErrorEventReason：出現更新錯誤的原因。

該選項可以採用以下值：

- reasonUnknown (0) - 不明原因
- reasonAccessDenied - 存取遭拒
- reasonUrlsExhausted - 已用盡更新來源的清單
- reasonInvalidConfig - 無效的設定檔
- reasonInvalidSignature - 無效的特徵碼
- reasonCantCreateFolder - 無法建立資料夾
- reasonFileOperError - 檔案操作錯誤
- reasonDataCorrupted - 物件已損毀
- reasonConnectionReset - 連線重設
- reasonTimeOut - 已超過連線逾時
- reasonProxyAuthError - 代理驗證錯誤
- reasonServerAuthError - 電腦驗證錯誤
- reasonHostNotFound - 找不到電腦
- reasonServerBusy - 無法使用伺服器
- reasonConnectionError - 連線錯誤
- reasonModuleNotFound - 找不到物件

- reasonBlstCheckFailed(16) - 檢查列入黑名單的金鑰時發生錯誤。可能是在更新期間同時發佈資料庫更新；請於幾分鐘內再執行一次。
- storageObjectNotAddedEventReason：未備份或未隔離物件的原因。

該選項可以採用以下值：

- reasonUnknown (0) - 不明原因
- reasonStorageInternalError - 資料庫錯誤；必須還原 Kaspersky Embedded Systems Security。
- reasonStorageReadOnly - 資料庫唯讀；必須還原 Kaspersky Embedded Systems Security。
- reasonStorageIOError - 輸入輸出錯誤：a) Kaspersky Embedded Systems Security 已毀損，必須還原 Kaspersky Embedded Systems Security；b) Kaspersky Embedded Systems Security 檔案所在的磁碟已毀損。
- reasonStorageCorrupted - 儲存空間已毀損；必須還原 Kaspersky Embedded Systems Security。
- reasonStorageFull - 資料庫已滿；需要可用磁碟空間。
- reasonStorageOpenError - 無法開啟資料庫檔案；必須還原 Kaspersky Embedded Systems Security。
- reasonStorageOSFeatureError - 某些作業系統功能不符合 Kaspersky Embedded Systems Security 的需求。
- reasonObjectNotFound - 磁碟中沒有放置於隔離中的物件。
- reasonObjectAccessError - 使用備份 API 的權限不足；執行操作的帳戶沒有備份操作程式的權限。
- reasonDiskOutOfSpace - 磁碟空間不足。

與 WMI 整合

Kaspersky Embedded Systems Security 支援與 Windows Management Instrumentation (WMI) 整合：您可以使用支援 WMI 的用戶端系統透過基於 Web 的企業管理 (WBEM) 標準接收資料，以收集有關 Kaspersky Embedded Systems Security 及其元件的狀態的資訊。

安裝 Kaspersky Embedded Systems Security 後，它會在系統中註冊專有模組，促使在本機電腦上的 WMI 根命名空間中建立 Kaspersky Embedded Systems Security 命名空間。透過 Kaspersky Embedded Systems Security 命名空間可以使用 Kaspersky Embedded Systems Security 類和實例及其內容。

某些實例內容的值取決於工作類型。

*非週期性工作*是沒有時間限制的應用程式工作，可以持續執行或停止。此類工作不存在執行進度。當工作作為單個事件執行（例如，任一“即時電腦防護”工作偵測受感染物件）時，將不停記錄工作執行的結果。此類型的工作透過卡巴斯基安全管理中心政策進行管理。

*週期性工作*是有時間限制且以百分比形式顯示執行進度的應用程式工作。工作結果在工作完成後建立，並表示為單個項目或變更的應用程式狀態（例如，完成的應用程式資料庫更新、為規則建立工作建立的設定檔）。同一類型的多個週期性工作可以在單台電腦上同時執行（三個具有不同掃描範圍的自訂掃描工作）。可以透過卡巴斯基安全管理中心將週期性工作作為組工作進行管理。

如果在公司網路中使用工具建立 WMI 命名空間查詢並從 WMI 命名空間接收動態資料，您將能夠接收有關目前應用程式狀態的資訊（請參見下表）。

表 77. 有關應用程式的啟動狀態的資訊

實例內容	敘述	值
ProductName	安裝的應用程式的名稱。	不帶版本號的應用程式全名。
ProductVersion	安裝的應用程式的完整版本。	應用程式完整版本號，包括內部版本號。

實例內容	敘述	值
InstalledPatches	為應用程式佈署的一系列修補程式的顯示名稱。	為應用程式安裝的關鍵修復程式清單。
IsLicenseInstalled	應用程式啟動狀態。	用於啟動應用程式的金鑰的狀態。 可能的值： <ul style="list-style-type: none"> • False - 尚未在應用程式中設定金鑰或啟動碼。 • True - 已將金鑰或啟動碼新增到應用程式。
LicenseDaysLeft	顯示目前產品授權到期前剩餘的天數。	目前產品授權到期前剩餘的天數。 可能的非正值： <ul style="list-style-type: none"> • 0 - 產品授權已到期 • -1 - 無法獲取目前金鑰的資訊，或者指定金鑰無法用於啟動應用程式（例如，根據金鑰黑名單將其封鎖）。
AVBasesDatetime	目前病毒資料庫版本的時間戳記。	目前使用中的病毒資料庫的建立日期和時間。 如果已安裝的應用程式不使用病毒資料庫，則該欄位的值為“未安裝”。

實例內容	敘述	值
IsExploitPreventionEnabled	“弱點利用防禦”元件的狀態。	“弱點利用防禦”元件的狀態。 可能的值： <ul style="list-style-type: none"> • True - “弱點利用防禦”元件已啟用並正在提供防護。 • False - “弱點利用防禦”元件未提供防護。 例如：已停用、未安裝、已違反產品授權協議。
ProtectionTasksRunning	目前正在執行的一系列防護工作。	目前正在執行的防護、控制和監控工作的清單。此欄位應表示所有正在執行的非週期性工作。如果沒有非週期性工作正在執行，該欄位的值為“否”。
IsAppControlRunning	“應用程式啟動控制”工作的狀態。	“應用程式啟動控制”工作的狀態。 <ul style="list-style-type: none"> • True - “應用程式啟動控制”工作目前正在執行。 • False - “應用程式啟動控制”工作目前未執行或“應用程式啟動控制”元件未安裝。
AppControlMode	“應用程式啟動控制”工作模式。	敘述“應用程式啟動控制”元件的目前狀態，以及相應工作的選定模式。 可能的值： <ul style="list-style-type: none"> • 活動 - “活動”模式在工作設定中選擇。 • 僅統計 - “僅統計”模式在工作設定中選擇。 • 未安裝 - “應用程式啟動控制”元件未安裝

實例內容	敘述	值
AppControlRulesNumber	應用程式啟動控制規則總數。	“應用程式啟動控制”工作設定中目前指定的規則數量。
AppControlLastBlocking	“應用程式啟動控制”工作上次在任一模式下封鎖應用程式啟動的時間戳記。	“應用程式啟動控制”元件上次封鎖應用程式啟動時的日期和時間。該欄位包括所有已封鎖的應用程式，不管工作模式為何。 如果在處理 WMI 查詢時未註冊已封鎖的應用程式啟動的實例，該欄位將被分配值“否”。
PeriodicTasksRunning	目前正在執行的一系列週期性工作。	目前正在執行的自訂掃描、更新和清單編制工作的清單。此欄位應包括所有正在執行的週期性工作。 如果目前沒有週期性工作正在執行，則該欄位的值為“否”。
ConnectionState	WMI 提供程式元件與 Kaspersky Security 服務 (KAVFS) 之間的連線的狀態。	有關 WMI 提供程式模組與 Kaspersky Security 服務之間的連線狀態的資訊。 可能的值： <ul style="list-style-type: none"> 成功 - 連線已成功建立：WMI 用戶端可以接收有關應用程式狀態的資訊。 失敗。錯誤代碼：<代碼> - 由於出現指定代碼的錯誤，無法建立連線。

此資料表示實例內容 KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security , 其中：

- KasperskySecurity_ProductInfo 是 Kaspersky Embedded Systems Security 類的名稱
- ProductName=Kaspersky Embedded Systems Security 是 Kaspersky Embedded Systems Security 關鍵參數

該實例在 ROOT\Kaspersky\Security 命名空間中建立。

從命令列使用 Kaspersky Embedded Systems Security

本節敘述從命令列使用 Kaspersky Embedded Systems Security。

本章內容

命令列指令	618
命令列回傳代碼	652

命令列指令

如果您在 Kaspersky Embedded Systems Security 安裝期間將“命令列實用工具”包含在安裝的功能清單中，則可透過受防護電腦的命令列執行基本的 Kaspersky Embedded Systems Security 管理指令。

使用命令列指令，您僅可管理那些可以根據 Kaspersky Embedded Systems Security 分配給您的權限來存取的功能。

某些 Kaspersky Embedded Systems Security 指令在以下模式下執行：

- 同步模式：管理僅在執行指令後回傳到主控台。
- 非同步模式：管理在執行指令後立即回傳到主控台。

► 在同步模式下中斷指令執行

按 **Ctrl+C** 鍵盤快速鍵。

輸入 Kaspersky Embedded Systems Security 指令時，應遵循以下規則：

- 使用大寫和小寫輸入參數和指令。
- 使用空白字元分隔參數。

- 如果將其路徑指定為參數值的檔案/資料夾名稱包含空格，請提供括在引號中的檔案/資料夾路徑，例如 "C:\TEST\test cpp.exe"
- 若有需要，可在檔案名稱或路徑遮罩中使用佔位字元，例如：“C:\Temp\Temp*”，“C:\Temp\Temp???.doc”，“C:\Temp\Temp*.doc”

在管理 Kaspersky Embedded Systems Security 所需的所有各項操作中均可使用命令列（請參見下表）。

表 78. Kaspersky Embedded Systems Security 指令

指令	敘述
KAVSHELL APPCONTROL (請參見第 637 頁上的“填寫應用程式啟動控制規則清單 KAVSHELL APPCONTROL”部分)	根據選定的新增原則更新指定的規則清單。
KAVSHELL APPCONTROL /CONFIG (請參見第 633 頁上的“管理應用程式啟動控制工作 KAVSHELL APPCONTROL /CONFIG”部分)	控制“應用程式啟動控制”工作的執行模式
KAVSHELL APPCONTROL /GENERATE (請參見第 634 頁上的“應用程式啟動控制規則產生器 KAVSHELL APPCONTROL /GENERATE”部分)	啟動“應用程式啟動控制規則產生器”工作。
KAVSHELL VACUUM (請參見“Kaspersky Embedded Systems Security 記錄檔案磁碟整理。KAVSHELL VACUUM”部分 (位於第 646 頁上))	對 Kaspersky Embedded Systems Security 記錄檔案進行磁碟整理。

指令	敘述
KAVSHELL PASSWORD	管理密碼防護設定。
KAVSHELL HELP(請參見“顯示 Kaspersky Embedded Systems Security 指令說明。KAVSHELL HELP”部分 (位於第 621 頁上))	顯示 Kaspersky Embedded Systems Security 指令說明。
KAVSHELL START(請參見第 622 頁上的“啟動和停止 Kaspersky Security 服務 KAVSHELL START , KAVSHELL STOP”部分)	啟動 Kaspersky Embedded Systems Security 服務。
KAVSHELL STOP (請參見第 622 頁上的“啟動和停止 Kaspersky Security 服務 KAVSHELL START , KAVSHELL STOP”部分)	停止 Kaspersky Embedded Systems Security 服務。
KAVSHELL SCAN(請參見“掃描選定區域。KAVSHELL SCAN”部分 (位於第 623 頁上))	建立並啟動暫時自訂掃描工作 (其掃描範圍和安全性設定由指令修飾符設定) 。
KAVSHELL SCANCritical (請參見“啟動‘關鍵區域掃描’工作。KAVSHELL SCANCritical”部分 (位於第 629 頁上))	啟動關鍵區域掃描系統工作。
KAVSHELL TASK (請參見“非同步管理指定工作。KAVSHELL TASK”部分 (位於第 630 頁上))	非同步開始、暫停/繼續、停止選擇的工作、返回目前工作狀態/統計。
KAVSHELL RTP (請參見“啟動及停止即時防護工作。KAVSHELL RTP”部分 (位於第 632 頁上))	開始或停止即時防護工作。
KAVSHELL UPDATE (請參見“啟動 Kaspersky Embedded Systems Security 資料庫更新工作。KAVSHELL UPDATE”部分 (位於第 639 頁上))	啟動 Kaspersky Embedded Systems Security 資料庫更新工作 (其設定使用指令修飾符指定) 。
KAVSHELL ROLLBACK (請參見“回溯 Kaspersky Embedded Systems Security 資料庫更新。KAVSHELL ROLLBACK”部分 (位於第 644 頁上))	將資料庫回溯至之前版本。

指令	敘述
KAVSHELL LICENSE	新增或刪除金鑰。顯示有關新增的金鑰的資訊。
KAVSHELL TRACE (請參見“啟用、設定和停用偵錯記錄。KAVSHELL TRACE”部分(位於第 645 頁上))	啟用或停用偵錯記錄,管理偵錯記錄的設定。
KAVSHELL DUMP (請參見“啟用和停用傾印檔案建立。KAVSHELL DUMP”部分(位於第 648 頁上))	在處理程序異常終止時,啟用或停用 Kaspersky Embedded Systems Security 處理程序傾印檔案。
KAVSHELL IMPORT (請參見“匯入設定。KAVSHELL IMPORT”部分(位於第 650 頁上))	從預先建立的設定檔匯入 Kaspersky Embedded Systems Security 設定、功能及工作。
KAVSHELL EXPORT (請參見“匯出設定。KAVSHELL EXPORT”部分(位於第 650 頁上))	將所有 Kaspersky Embedded Systems Security 設定和現有工作匯出至設定檔。
KAVSHELL DEVCONTROL (請參見“填寫裝置控制規則清單。KAVSHELL DEVCONTROL”部分(位於第 638 頁上))	根據選定的方法新增到已建立的裝置控制規則清單中。

顯示 Kaspersky Embedded Systems Security 指令說明。KAVSHELL HELP

若要獲得所有 Kaspersky Embedded Systems Security 指令的清單,請執行以下指令之一:

KAVSHELL

KAVSHELL HELP

KAVSHELL /?

若要獲得指令概覽及其語法，請執行下列一個指令：

```
KAVSHELL HELP <指令>
```

```
KAVSHELL <指令> /?
```

KAVSHELL HELP 指令範例

若要檢視有關 KAVSHELL SCAN 指令的詳細資訊，請執行下列指令：

```
KAVSHELL HELP SCAN
```

啟動和停止 Kaspersky Security 服務 KAVSHELL START , KAVSHELL STOP

若要執行 Kaspersky Security 服務，請執行指令

```
KAVSHELL START
```

預設情況下，Kaspersky Security Service 啟動時，“即時檔案防護”和“系統啟動時掃描”工作以及其他排在“在應用程式啟動時”啟動的工作也會一起啟動。

若要停止 Kaspersky Security 服務，請執行指令

```
KAVSHELL STOP
```

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

掃描指定區域。KAVSHELL SCAN

若要開始掃描受防護電腦特定區域的工作，請使用 KAVSHELL SCAN 指令。指令參數指定選定節點的掃描範圍和安全性設定。

使用 KAVSHELL SCAN 指令啟動的自訂掃描工作為暫時工作。它僅在執行時才顯示在應用程式主控台中（您無法在應用程式主控台中檢視工作設定）。同一時間，會產生工作效能記錄。它會顯示在應用程式主控台的“工作記錄”中。

在自訂掃描工作中指定路徑時，可設定環境變數。如果使用由使用者的環境變數，請使用該使用者的權限執行 KAVSHELL SCAN 指令。

KAVSHELL SCAN 指令在同步模式下執行。

要從命令列啟動現有自訂掃描工作，請使用 KAVSHELL TASK(請參見“非同步管理指定工作。KAVSHELL TASK”部分(位於第 [630](#) 頁上)) 指令。

KAVSHELL SCAN 指令語法

```
KAVSHELL SCAN <掃描範圍> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP]
[/L:<具有掃描範圍清單的檔案路徑>] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>] [/EM:<“遮罩”>]
[/ES:<大小>] [/ET:<秒數>] [/TZOFF] [/OF:<SKIP|RESIDENT|SCAN[=<天數>] [NORECALL]>]
[/NOICHECKER][[/NOISWIFT][[/ANALYZERLEVEL][[/NOCHECKMSSIGN][[/W:<工作記錄檔案的路徑>]
[/ANSI] [/ALIAS:<工作別名>]
```

KAVSHELL SCAN 指令有必要和選用指令參數兩種(請參閱下表)。

KAVSHELL SCAN 指令範例

```
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
```

表 79. KAVSHELL SCAN 指令修飾符

鍵	敘述
掃描範圍。強制參數。	
<檔案>	指定掃描範圍 - 檔案清單、資料夾、網路路徑及預先定義的區域。
<資料夾>	以 UNC 格式 (通用命名慣例) 指定網路路徑。
<網路路徑>	<p>在下列範例中，資料夾 Folder4 未指定路徑 - 它位於執行 KAVSHELL 指令的資料夾中：</p> <pre>KAVSHELL SCAN Folder4</pre> <p>如果要檢查的物件名稱包含空格，則必須將其括在引號中。</p> <p>選定某個資料夾後，Kaspersky Embedded Systems Security 也會檢查該資料夾的所有子資料夾。</p> <p>可以使用符號 * 或 ? 來掃描一組檔案。</p>
/MEMORY	掃描 RAM 中的物件。
/SHARED	掃描電腦上的共用資料夾
/STARTUP	掃描自動執行物件
/REMDRIVES	掃描卸除式磁碟。
/FIXDRIVES	掃描硬碟。
/MYCOMP	掃描受防護電腦所有的區域

鍵	敘述
/L: <帶有掃描範圍清單的檔案路徑>	<p>帶有掃描範圍清單的檔案名稱，包括檔案的完整路徑。</p> <p>使用換行鍵界定檔案的掃描範圍。如下圖所示，您可指定預先定義的掃描範圍：</p> <p>C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED</p>
<p>掃描的物件 (檔案類型)。如果您未指定此指令參數值，Kaspersky Embedded Systems Security 將依據物件格式掃描物件。</p>	
/FA	掃描所有物件
/FC	依據格式掃描物件 (預設)。Kaspersky Embedded Systems Security 只掃描受感染的物件格式清單中所包含的格式物件。
/FE	依據副檔名掃描物件。Kaspersky Embedded Systems Security 只掃描受感染物件副檔名清單中包含的副檔名物件。
/NEWONLY	<p>僅掃描新增與變更過的檔案。</p> <p>如果您未提供此指令參數，Kaspersky Embedded Systems Security 將掃描所有物件。</p>
<p>對受感染物件和其他物件執行的操作。如果未指定此指令參數，Kaspersky Embedded Systems Security 將執行“略過”操作。</p>	
DISINFECT	<p>解毒，如果無法解毒則略過</p> <p>在最新版本的 Kaspersky Embedded Systems Security 中保留了 DISINFECT 和 DELETE 設定，以便確保與以前版本的相容性。可以使用這些設定取代按鍵指令 /AI: 和 /AS: 這種情況下，Kaspersky Embedded Systems Security 不會處理可疑物件。</p>
DISINFDEL	解毒，如果無法解毒則刪除

鍵	敘述
DELETE	刪除 在最新版本的 Kaspersky Embedded Systems Security 中保留了 DISINFECT 和 DELETE 設定，以便確保與以前版本的相容性。可以使用這些設定取代按鍵指令 /AI: 和 /AS: 這種情況下，Kaspersky Embedded Systems Security 不會處理可疑物件。
REPORT	傳送報告 (預設)
AUTO	執行建議的操作
/AS: 針對可疑的物件執行的操作/ 如果未指定此指令參數，Kaspersky Embedded Systems Security 將執行“略過”操作。	
QUARANTINE	隔離
DELETE	刪除
REPORT	傳送報告 (預設)
AUTO	執行建議的操作
排除	
/E:ABMSPO	排除以下複合檔案類型的指令參數： A – 壓縮檔案 (僅掃描 SFX 壓縮檔案) B – 電子郵件資料庫 M – 一般郵件 S – 壓縮檔案和 SFX 壓縮檔案 P – 封裝的物件 O – 內嵌 OLE 物件
/EM:<“遮罩”>	透過遮罩排除檔案 您可以指定數個遮罩，例如：EM:“*.txt; *.png; C:\Videos*.avi”。

鍵	敘述
/ET:<秒數>	如果處理物件的速度比 <秒數> 值中所指定的秒數長，則停止處理物件。 預設沒有時間限制。
/ES:<大小>	不要掃描比 <大小> 值中所指定之大小 (MB) 還要大的複合物件。 預設情況下，Kaspersky Embedded Systems Security 掃描所有大小的物件。
/TZOFF	停用“信任區域”排除
進階設定 (選項)	
/NOICHECKER	停用 iChecker (預設為啟用狀態)。
/NOISWIFT	停用 iSwift (預設為啟用狀態)。
/ANALYZERLEVEL:<分析等級>	啟用啟發式分析並配置分析等級。 以下啟發式分析等級可用： 1 – 輕度 2 – 中度 3 – 深度 如果刪除此指令參數，Kaspersky Embedded Systems Security 將不會使用啟發式分析。
/ALIAS:<工作別名>	此指令參數可讓您指定一個暫時的名稱給自訂掃描工作，工作執行期間需要用此名稱存取工作，例如，使用 TASK 指令檢視工作統計。在 Kaspersky Embedded Systems Security 的所有功能元件的工作別名中，每一個工作別名都必須是唯一的。 如果未指定此指令參數，將使用 scan_<kavshell_pid> 的暫時名稱，例如 scan_1234。在應用程式主控台中，為工作分配掃描物件的名稱 (<日期和時間>)，例如，掃描物件 8/16/2007 5:13:14 PM。
工作記錄的設定 (報告設定)	

鍵	敘述
/W:<工作記錄檔案的路徑>	<p>如果指定了此指令參數，Kaspersky Embedded Systems Security 將用該鍵的值定義的名稱儲存工作記錄檔案。</p> <p>該記錄檔包含工作執行統計、工作開啟及結束（停止）的時間，以及工作中相關事件資訊。</p> <p>該記錄用於在事件檢視器中註冊由工作記錄和 Kaspersky Embedded Systems Security 事件記錄的設定定義的事件。</p> <p>您可指定記錄檔的絕對路徑或相對路徑。如果僅指定了檔案名稱但未指定其路徑，則記錄檔將於目前所在的資料夾中建立。</p> <p>以相同的記錄設定重新執行此指令將覆寫現有的記錄檔。</p> <p>執行工作時，可檢視此記錄檔案。</p> <p>此記錄會出現在應用程式主控台的“工作記錄”節點中。</p> <p>如果 Kaspersky Embedded Systems Security 無法建立記錄檔案，這將不會停止執行此指令，但會顯示一個錯誤訊息。</p>
/ANSI	<p>可以將事件以 ANSI 編碼記錄到工作執行記錄中的指令參數。</p> <p>若未定義 W 指令參數，將無法套用 ANSI 指令參數。</p> <p>如果未指定 ANSI 指令參數，將以 UNICODE 編碼產生工作記錄。</p>

啟動“掃描關鍵區域”工作 KAVSHELL SCANCRITICAL

使用 KAVSHELL SCANCRITICAL 指令可使用在應用程式主控台中定義的設定啟動系統自訂掃描工作“關鍵區域掃描”。

KAVSHELL SCANCRITICAL 指令語法

KAVSHELL SCANCRITICAL [/W:<工作記錄檔案的路徑>]

KAVSHELL SCANCRITICAL 指令範例

要執行“掃描關鍵區域”手動掃描工作，並在目前所在的資料夾中儲存 scancritical.log 工作執行記錄，請執行以下指令：

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

根據上面的 /W 指令語法，您可設定工作記錄的位置（請參閱下表）。

表 80. KAVSHELL SCANCritical 指令的 /W 指令語法

鍵	敘述
/W:<工作記錄檔案的路徑>	<p>如果指定了此指令參數，Kaspersky Embedded Systems Security 將用該鍵的值定義的名稱儲存工作記錄檔案。</p> <p>該記錄檔包含工作執行統計、工作開啟及結束 (停止) 的時間，以及工作中相關事件資訊。</p> <p>該記錄用來註冊工作執行記錄設定與應用程式事件記錄所定義的事件。</p> <p>您可指定記錄檔的絕對路徑或相對路徑。如果僅指定了檔案名稱但未指定其路徑，則記錄檔將於目前所在的資料夾中建立。</p> <p>以相同的記錄設定重新執行此指令將覆寫現有的記錄檔。</p> <p>執行工作時，可檢視此記錄檔案。</p> <p>此記錄會出現在應用程式主控台的“工作記錄”節點中。</p> <p>如果 Kaspersky Embedded Systems Security 無法建立記錄檔案，這將不會停止執行此指令，但會顯示一個錯誤訊息。</p>

以非同步模式管理指定的工作 KAVSHELL TASK

KAVSHELL TASK 指令可用來管理指定的工作，如執行、暫停、繼續和停止指定工作與檢視目前的工作狀態和統計。此指令應在非同步模式下執行。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

KAVSHELL TASK 指令語法

KAVSHELL TASK [<工作名稱別名> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]

KAVSHELL TASK 指令範例

KAVSHELL TASK

KAVSHELL TASK on- access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan- computer /STATE

KAVSHELL TASK 可以不搭配指令參數或搭配一或多個指令參數執行 (請參閱下表) 。

表 81. KAVSHELL TASK 指令修飾符

鍵	敘述
不搭配指令參數	回傳所有現有 Kaspersky Embedded Systems Security 工作的清單。該清單包含欄位：代替工作名稱、工作類別 (系統或自訂) 及目前工作狀態。
<工作別名>	除工作名稱外，SCAN TASK 指令中可另外使用 Kaspersky Embedded Systems Security 指定給工作的簡短工作別名。要檢視 Kaspersky Embedded Systems Security 工作別名，輸入 KAVSHELL TASK 但不必輸入任何指令參數
/START	以非同步模式開始指定的工作。
/STOP	停止指定的工作。
/PAUSE	暫停指定的工作。
/RESUME	以非同步模式繼續指定的工作。
/STATE	回傳目前的工作狀態 (例如，正在執行、已完成、已暫停、已停止、已失敗、正在啟動、還原中) 。
/STATISTICS	擷取工作統計 – 截至目前為止，從工作開始執行時的物件數資訊。

請注意，並非所有 Kaspersky Embedded Systems Security 工作都完全支援這些鍵。

KAVSHELL TASK 指令的回傳代碼 (請參見第 [654](#) 頁上的“KAVSHELL TASK 指令的回傳代碼”部分) 。

將 KAVFS 註冊為系統防護處理程序。KAVSHELL CONFIG

KAVSHELL CONFIG 指令允許您使用 ELAM 驅動程式 (在應用程式安裝期間安裝在作業系統中) 控制是否將 Kaspersky Security 服務註冊為系統防護處理程序 (輕度受防護處理程序) 。

KAVSHELL CONFIG 指令語法

KAVSHELL CONFIG /PPL:<ON|OFF>

表 82. KAVSHELL CONFIG 指令鍵

鍵	敘述
/PPL:ON	將 Kaspersky Security 服務註冊為 PPL。
/PPL:OFF	刪除 Kaspersky Security 服務的 PPL 內容。

當執行以下任一操作時，應用程式自動執行服務的取消註冊：

- 應用程式移除
- 應用程式升級
- 修補程式安裝
- 應用程式元件修復

KAVSHELL CONFIG 指令的回傳代碼。

啟動及停止即時防護工作。KAVSHELL RTP

KAVSHELL RTP 指令可用來啟動或停止所有的即時防護工作。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

KAVSHELL RTP 指令語法

KAVSHELL RTP {/START | /STOP}

KAVSHELL RTP 指令範例

若要啟動所有即時防護工作，請執行以下指令：

```
KAVSHELL RTP /START
```

KAVSHELL RTP 指令可搭配兩個必要指令參數任意一個使用（請參閱下表）。

表 83. KAVSHELL RTP 指令參數

鍵	敘述
/START	啟動所有即時防護工作：“即時檔案防護”和“KSN 使用”。
/STOP	停止所有即時防護工作。

管理應用程式啟動控制工作 KAVSHELL APPCONTROL /CONFIG

可以使用 KAVSHELL APPCONTROL /CONFIG 指令來配置模式，在該模式中“應用程式啟動控制”工作將執行和監控 DLL 模組的載入。

KAVSHELL APPCONTROL /CONFIG 指令語法

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config /savetofile:<XML 檔案路徑>
```

KAVSHELL APPCONTROL /CONFIG 指令示例

- ▶ 要在“活動”模式中執行“應用程式啟動控制”工作而不載入 DLL 並在完成時儲存工作設定，請執行以下指令：

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no> /savetofile:c:\appcontrol\config.xml
```

可以使用命令列參數來配置“應用程式啟動控制”工作設定（請參閱以下表格）。

表 84. KAVSHELL APPCONTROL /GENERATE 指令開關

鍵	敘述
---	----

鍵	敘述
/mode:<applyrules statistics>	“應用程式啟動控制”工作的執行模式。 您可以選擇以下模式之一： <ul style="list-style-type: none"> • 活動 – 套用“應用程式啟動控制”規則； • 統計 – 僅統計。
/dll:<no yes>	啟用或停用 DLL 載入監控。
/savetofile: <XML 檔案路徑>	匯出指定檔案中的指定規則為 XML 格式。
/savetofile: <XML 檔案全名>	將規則清單儲存到檔案。
/savetofile: <XML 檔案全名> /sdc	將軟體分發控制規則清單儲存到檔案。
/clearsdc	從清單中移除軟體分發控制規則。

應用程式啟動控制規則產生器 KAVSHELL APPCONTROL /GENERATE

使用 KAVSHELL APPCONTROL /GENERATE 指令，可以建立應用程式啟動控制規則清單。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

KAVSHELL APPCONTROL /GENERATE 指令語法

KAVSHELL APPCONTROL /GENERATE <資料夾路徑> | /source:<包含資料夾清單的檔案路徑> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<使用者或使用者組>] [/export:<XML 檔案路徑>] [/import:<a|r|m>] [/ prefix:<規則名稱首碼>] [/unique]

KAVSHELL APPCONTROL /GENERATE 指令示例

- ▶ 若要為指定資料夾中的檔產生規則，請執行以指令：

```
KAVSHELL APPCONTROL/GENERATE /source:c:\folderslist.txt /export:c:\rules\appctrlrules.xml
```

- ▶ 若要為指定資料夾中所有副檔名的可執行檔產生規則，並在工作完成時，將建立的規則儲存在指定的 XML 檔案中，請執行以下指令：

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c:\rules\appctrlrules.xml
```

根據鍵語法的不同，您可以為“應用程式啟動控制”工作配置自動規則建立設定（請參見下表）。

表 85. KAVSHELL APPCONTROL /GENERATE 指令鍵

鍵	敘述
允許規則的使用範圍	
<資料夾路徑>	指定包含可執行檔的資料夾路徑，這些可執行檔需要自動建立的允許規則。
/source: <包含資料夾清單的檔案路徑>	指定包含資料夾清單的 TXT 檔案的路徑，這些資料夾包含需要自動建立的允許規則的可執行檔。

鍵	敘述
/masks: <edms>	<p>指定包含可執行檔的副檔名，這些可執行檔需要自動建立的允許規則。</p> <p>您可以將以下副檔名的規則使用範圍檔案包括在內：</p> <ul style="list-style-type: none"> • e - EXE 檔案 • d - DLL 檔案 • m - MSI 檔案 • s - 指令碼
/runapp	產生允許規則時，應考慮在執行工作的那一刻在受防護電腦上執行的應用程式。
自動建立允許規則時的操作	
/rules: <ch cp h>	<p>指定在“應用程式啟動控制”允許規則建立期間要執行的操作：</p> <ul style="list-style-type: none"> • ch - 使用數位憑證。如果憑證遺失，請使用 SHA256 雜湊。 • cp - 使用數位憑證。如果憑證遺失，請使用可執行檔路徑。 • h - 使用 SHA256 雜湊。
/strong	在自動建立“應用程式啟動控制”允許規則時使用數位憑證主旨和指紋。如果指定 /rules: <ch cp> 鍵，則將執行該指令。
/user: <使用者或使用者群組>	指定將套用規則的使用者名或一群組使用者。應用程式將監控透過指定的使用者和/或使用者群組執行的任何應用程式。
應用程式啟動控制規則產生器完成後的操作	
/export <XML 檔案路徑>	將建立的規則儲存到 XML 檔案中。
/unique	新增安裝有應用程式的電腦的相關資訊，這些資訊是建立應用程式啟動控制允許規則時的依據。
/prefix : <規則名稱的前置詞>	指定用於建立應用程式啟動控制允許規則的名稱首碼。

鍵	敘述
/import: <a r m>	<p>根據選定的新增規則，將建立的規則匯入指定的應用程式啟動控制規則清單中：</p> <ul style="list-style-type: none"> • a - 新增到現有規則 (將複製具有相同設定的規則) • r - 取代現有規則 (不新增具有相同參數的規則；如果至少一個規則參數是唯一的，則會新增規則) • m - 與現有規則合併 (不新增具有相同參數的規則；如果至少一個規則參數是唯一的，則會新增規則)

填寫應用程式啟動控制規則清單 KAVSHELL APPCONTROL

使用 KAVSHELL APPCONTROL，您可根據所選原則將規則從 XML 檔新增到應用程式啟動控制工作規則清單，也可以從清單中刪除所有設定的規則。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

KAVSHELL APPCONTROL 指令語法

KAVSHELL APPCONTROL /append <XML 檔案路徑> | /replace <XML 檔案路徑> | /merge <XML 檔案路徑> | /clear

KAVSHELL APPCONTROL 指令示例

- ▶ 若要根據“新增到現有規則”政策，從 XML 檔案向已經指定的應用程式啟動控制工作規則新增規則，請執行以下指令：

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

根據鍵值語法，您可以選擇從指定的 XML 檔案向應用程式啟動控制定義的規則清單新增新規則的原則(請參見下表)。

表 86. KAVSHELL APPCONTROL 指令鍵

鍵	敘述
/append <XML 檔案路徑>	基於指定的 XML 檔案更新應用程式啟動控制規則清單。新增原則 - 新增到現有規則 (將複製具有相同設定的規則) 。
/replace <XML 檔案路徑>	基於指定的 XML 檔案更新應用程式啟動控制規則清單。新增原則 - 取代現有規則 (不新增具有相同參數的規則；如果至少一個規則參數是唯一的，則會新增規則) 。
/merge <XML 檔案路徑>	基於指定的 XML 檔案更新應用程式啟動控制規則清單。新增原則 - 與現有規則合併 (新規則不會複製已設定的規則) 。
/clear	填寫應用程式啟動控制規則清單。

填寫裝置控制規則清單。KAVSHELL DEVCONTROL

使用 KAVSHELL DEVCONTROL，您可根據所選原則將規則從 XML 檔新增到裝置控制工作規則清單，也可以從清單中刪除所有設定的規則。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

KAVSHELL DEVCONTROL 指令語法

```
KAVSHELL DEVCONTROL /append <XML 檔案路徑> | /replace <XML 檔案路徑> | /merge <XML 檔案路徑> | /clear
```

KAVSHELL DEVCONTROL 指令示例

- ▶ 若要根據“**新增到現有規則**”原則，從 XML 檔向已經指定的裝置控制工作規則新增規則，請執行以下指令：

```
KAVSHELL DEVCONTROL /append c:\rules\devctrlrules.xml
```

根據鍵值語法，您可以選擇從指定的 XML 檔向裝置控制定義的規則清單新增新規則的原則(請參見下表)。

表 87. KAVSHELL DEVCONTROL 指令鍵

鍵	敘述
/append <XML 檔案路徑>	基於指定的 XML 檔更新裝置控制規則清單。新增原則 - 新增到現有規則 (將複製具有相同設定的規則)。
/replace <XML 檔案路徑>	基於指定的 XML 檔更新裝置控制規則清單。新增原則 - 取代現有規則 (不新增具有相同參數的規則；如果至少一個規則參數是唯一的，則會新增規則)。
/merge <XML 檔案路徑>	基於指定的 XML 檔更新裝置控制規則清單。新增原則 - 與現有規則合併 (新規則不會複製已設定的規則)。
/clear	清除裝置控制規則清單。

啟動 Kaspersky Embedded Systems Security 資料庫更新工作。 KAVSHELL UPDATE

KAVSHELL UPDATE 指令可以用於按非同步模式啟動 Kaspersky Embedded Systems Security 資料庫更新工作。

使用 KAVSHELL UPDATE 指令執行的 Kaspersky Embedded Systems Security 資料庫更新工作是臨時工作。它僅在執行時顯示在應用程式主控台中。同一時間，會產生工作記錄。它會顯示在應用程式主控台的“工作記錄”中。卡斯基安全管理中心政策可套用到使用 KAVSHELL UPDATE 指令所建立與啟動的更新工作，以及病毒防護應用程式主控台中所建立的更新工作。有關使用卡斯基安全管理中心管理電腦上的 Kaspersky Embedded Systems Security 的資訊，請參見“使用卡斯基安全管理中心管理 Kaspersky Embedded Systems Security”部分。

在此工作中指定更新來源路徑時，可設定環境變數。如果使用了使用者的環境變數，請使用該使用者的權限執行 KAVSHELL UPDATE 指令。

KAVSHELL UPDATE 指令語法

```
KAVSHELL UPDATE <更新來源路徑 | /AK | /KL> [/NOUSEKL] [/PROXY:<位址>:<連接埠>]
[/AUTHTYPE:<0-2>] [/PROXYUSER:<使用者名稱>] [/PROXYPWD:<密碼>] [/NOPROXYFORKL]
[/USEPROXYFORCUSTOM] [/NOFTPPASSIVE] [/TIMEOUT:<秒>] [/REG:<iso3166 程式碼>] [/W:<工作
記錄檔案路徑>] [/ALIAS:<工作別名>]
```

KAVSHELL UPDATE 指令有必要和選用指令參數兩種（請參閱下表）。

KAVSHELL UPDATE 指令範例

- ▶ 要啟動自訂的資料庫更新工作，請執行以下指令：

```
KAVSHELL UPDATE
```

- ▶ 要使用 \\server\databases 網路資料夾中的更新檔案啟動資料庫更新工作，請執行以下指令：

```
KAVSHELL UPDATE \\server\databases
```

- ▶ 若要從 FTP 伺服器 <ftp://dnl-ru1.kaspersky-labs.com/> 啟動更新工作並將所有工作事件寫入到 c:\update_report.log 檔案，請執行以下指令：

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

- ▶ 要從 Kaspersky Lab 的更新電腦下載 Kaspersky Embedded Systems Security 資料庫更新，請透過代理伺服器連線到更新來源（代理電腦位址 proxy.company.com，連接埠 8080）。要透過內建 Microsoft Windows NTLM 身分驗證使用使用者名稱 inetuser 及密碼 123456 存取電腦，請執行以下指令：

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

表 88. KAVSHELL UPDATE 指令參數

鍵	敘述
---	----

鍵	敘述
	<p>更新來源 (強制參數)。指定一或多個來源。Kaspersky Embedded Systems Security 將按照更新來源的清單順序存取更新來源。使用空白鍵界定來源。</p>
<UNC 格式中的路徑>	使用者定義的更新來源。UNC 格式中的網路更新資料夾路徑。
<URL>	使用者定義的更新來源。更新資料夾所在的 HTTP 或 FTP 伺服器位址。
<本機資料夾>	使用者定義的更新來源。受防護電腦上的資料夾。
/AK	使用卡斯基安全管理中心管理伺服器作為更新來源。
/KL	使用 Kaspersky Lab 的更新伺服器作為更新來源。
/NOUSEKL	如果不能使用其他更新來源 (預設使用) ，就不使用 Kaspersky Lab 的更新伺服器。
代理伺服器設定	
/PROXY:<位址>:<連接埠>	代理伺服器的網路名稱或 IP 位址及埠號。如果未指定此指令參數，Kaspersky Embedded Systems Security 將自動偵測區域網路中使用的代理伺服器設定。
/AUTHTYPE:<0-2>	<p>此指令參數可指定存取代理伺服器的身分驗證方法。它可能呈現是以下設定值：</p> <p>0 - 內建的 Microsoft Windows NTLM 身分驗證；Kaspersky Embedded Systems Security 將與本機系統 (SYSTEM) 帳戶下的代理伺服器聯絡</p> <p>1 - 內建的 Microsoft Windows NTLM 身分驗證；Kaspersky Embedded Systems Security 將與其登入名稱和密碼分別由鍵 /PROXYUSER 和 /PROXYPWD 指定的帳戶下的代理伺服器聯絡</p> <p>2 - 透過 /PROXYUSER 和 /PROXYPWD 指令參數指定的登入名稱和密碼進行身分驗證 (基本身分驗證)</p> <p>如果存取代理伺服器不需要驗證，就不需要指定指令參數。</p>
/PROXYUSER:<使用者名稱>	存取代理伺服器所需的使用者名稱。如果指定了 /AUTHTYPE:0 指令參數值，將略過 /PROXYUSER:<使用者名稱> 和 /PROXYPWD:<密碼> 指令參數。

鍵	敘述
/PROXYPWD:<密碼>	存取代理伺服器所需的使用者密碼。如果指定了 /AUTHTYPE:0 指令參數值，將略過 /PROXYUSER:<使用者名稱> 和 /PROXYPWD:<密碼> 指令參數。如果指定了 /PROXYUSER 指令參數但刪除了 /PROXYPWD，將視密碼為空白值。
/NOPROXYFORKL	不使用代理伺服器設定連線 Kaspersky Lab 的更新伺服器（預設為使用）。
/USEPROXYFORCUSTOM	使用代理伺服器設定連線使用者定義的更新來源（預設為不使用）。
/USEPROXYFORLOCAL	使用代理伺服器連線本機更新來源。如果不指定，將套用對於本機位址不使用代理伺服器。
FTP 和 HTTP 伺服器一般設定	
/NOFTPPASSIVE	如果指定了指令參數，Kaspersky Embedded Systems Security 將使用主動 FTP 電腦模式連線至受防護電腦。如果未指定指令參數，Kaspersky Embedded Systems Security 將使用被動 FTP 伺服器模式（如果可能的話）。
/TIMEOUT:<秒數>	FTP 或 HTTP 伺服器連線逾時。如果未指定此指令參數，Kaspersky Embedded Systems Security 將使用預設值為 10 秒。此指令參數值必須為整數。
/REG:<iso3166 代碼>	<p>區域設定。從 Kaspersky Lab 的更新伺服器接收更新時需使用此指令參數。Kaspersky Embedded Systems Security 會選擇與其電腦最近的更新電腦，以減輕受防護電腦上的更新負載。</p> <p>對於此指令參數值，請根據 ISO 3166-1 標準替受防護電腦指定所在國家/地區的字母程式碼，例如 /REG: gr 或 /REG:RU。如果省略該鍵或指定不存在的國家/地區代碼，Kaspersky Embedded Systems Security 將會基於安裝應用程式主控台的電腦上的地區設定偵測受防護電腦的位置。</p>

鍵	敘述
/ALIAS:<工作別名>	<p>此指令可讓您為工作指派一個暫時名稱，以在工作執行期間用來存取該工作。</p> <p>例如，您可使用 TASK 指令檢視工作統計。在 Kaspersky Embedded Systems Security 的所有功能元件的工作別名中，每一個工作別名都必須是唯一的。</p> <p>如果不指定該鍵，則會使用暫時名稱 update_<kavshell_pid>，例如 update_1234。在應用程式主控台中，將為工作分配名稱 Update-databases (<日期時間>)；例如，Update-databases 8/16/2007 5:41:02 PM。</p>
/W:<工作記錄檔案的路徑>	<p>如果指定了此指令參數，Kaspersky Embedded Systems Security 將用該鍵的值定義的名稱儲存工作記錄檔案。</p> <p>該記錄檔包含工作執行統計、工作開啟及結束（停止）的時間，以及工作中相關事件資訊。</p> <p>該記錄用來註冊工作執行記錄設定與“事件檢視器”中 Kaspersky Embedded Systems Security 事件記錄所定義的事件。</p> <p>您可指定記錄檔的絕對路徑或相對路徑。如果僅指定檔案名稱但未指定其路徑，則記錄檔將於目前所在的資料夾中建立。</p> <p>以相同的記錄設定重新執行此指令將覆寫現有的記錄檔。</p> <p>執行工作時，可檢視此記錄檔案。</p> <p>此記錄會出現在應用程式主控台的“工作記錄”節點中。</p> <p>如果 Kaspersky Embedded Systems Security 無法建立記錄檔案，這將不能停止執行此指令或顯示一個錯誤訊息。</p>

KAVSHELL UPDATE 指令回傳代碼（請參閱第 [656](#) 頁）。

回溯 Kaspersky Embedded Systems Security 資料庫更新。KAVSHELL ROLLBACK

KAVSHELL ROLLBACK 指令可用來執行 Kaspersky Embedded Systems Security 資料庫回溯系統工作 (將 Kaspersky Embedded Systems Security 資料庫回溯至上一個安裝版)。此指令會同步執行：

指令語法：

KAVSHELL ROLLBACK

KAVSHELL ROLLBACK 指令回傳代碼 (請參閱第 [656](#) 頁)。

管理記錄審查。KAVSHELL TASK LOG-INSPECTOR

KAVSHELL TASK LOG-INSPECTOR 指令可用於根據 Windows 事件記錄分析來監控環境完整性。

指令語法

KAVSHELL TASK LOG-INSPECTOR

指令範例

KAVSHELL TASK LOG-INSPECTOR /stop

表 89. KAVSHELL TASK LOG-INSPECTOR 指令修飾符

鍵	敘述
/START	以非同步模式開始指定的工作。
/STOP	停止指定的工作。
/STATE	回傳目前的工作狀態 (例如 , 正在執行、已完成、已暫停、已停止、已失敗、正在啟動、還原中)。
/STATISTICS	擷取工作統計 – 截至目前為止 , 從工作開始執行時的物件數資訊。

KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼 (請參見第 [654](#) 頁上的“KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼”部分)。

啟用、設定和停用偵錯記錄。KAVSHELL TRACE

KAVSHELL TRACE 指令可用來啟用或停用 Kaspersky Embedded Systems Security 所有子系統的即時偵錯記錄，以及設定記錄詳細等級。

Kaspersky Embedded Systems Security 會以未加密的形式將資訊寫入到偵錯檔案和傾印檔案。

KAVSHELL TRACE 指令語法

```
KAVSHELL TRACE </ON /F:<偵錯記錄檔資料夾路徑> [/S:<記錄大小上限 (MB)>]
[/LVL:debug|info|warning|error|critical] | /OFF>
```

如果您保留了偵錯記錄並想變更它的設定，請輸入 KAVSHELL TRACE 與 /ON 指令參數，並以 /S 和 /LVL 指令參數值指定偵錯記錄設定（請參閱下表）。

表 90. KAVSHELL TRACE 指令參數

鍵	敘述
/ON	啟用偵錯記錄。
/F:<偵錯記錄的檔案資料夾>	<p>此指令用來指定儲存偵錯記錄檔的資料夾完整路徑。</p> <p>如果指定的資料夾路徑不存在，將不會建立偵錯記錄。不能指定其他電腦的網路磁碟機上的資料夾位置。</p> <p>如果指令參數值指定的資料夾路徑名稱帶有空白字元，此資料夾路徑前後請加上引號，例如：/F:"C:\Trace Folder"。</p> <p>指定偵錯檔案路徑時可以使用系統環境變數；不允許使用者環境變數。</p>
/S: <記錄檔案大小上限 (MB)>	<p>此指令可設定一個偵錯記錄檔的大小上限。一旦記錄檔案大小達到上限時，Kaspersky Embedded Systems Security 會將資訊記錄到新檔案中；之前的記錄檔案會被儲存。</p> <p>如果未指定此指令參數值，一個記錄檔的大小上限為 50 MB。</p>

鍵	敘述
/LVL:debug info warning error critical	此指令鍵設定記錄的詳細程度，詳細程度最大 (所有診斷資訊) 會將所有事件記錄到記錄檔中，程度最小 (緊急事件) 則只會記錄緊急事件。 如果未指定此指令鍵，偵錯記錄中將記錄詳細程度為 所有診斷資訊 的事件。
/OFF	此指令可停用偵錯記錄。

KAVSHELL TRACE 指令範例

- ▶ 要使用“**所有診斷資訊**”詳細程度及上限為 200 MB 的記錄檔案大小來啟用偵錯記錄，並將記錄檔案儲存到 C:\Trace Folder 資料夾，請執行以下指令：

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

- ▶ 要使用“**重要事件**”詳細程度啟用偵錯記錄，並將記錄檔案儲存到 C:\Trace Folder 資料夾，請執行以下指令：

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

- ▶ 要停用偵錯記錄，請執行以下指令：

```
KAVSHELL TRACE /OFF
```

KAVSHELL TRACE 指令的回傳代碼(請參見第 [658](#) 頁上的“KAVSHELL TRACE 指令的回傳代碼”部分)。

Kaspersky Embedded Systems Security 記錄檔案磁碟整理。KAVSHELL VACUUM

使用 KAVSHELL VACUUM 指令，您可以對應用程式記錄檔案進行磁碟整理。它可以避免由於儲存基於應用程式事件建立的大量記錄檔案而導致系統和應用程式出錯。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

建議您應用 `KAVSHELL VACUUM` 指令，以便在自訂掃描頻繁掃描和更新工作頻繁啟動時最佳化記錄檔案儲存。在執行該指令時，Kaspersky Embedded Systems Security 將透過指定的路徑更新受防護電腦上儲存的應用程式記錄檔案的邏輯結構。

預設情況下，應用程式記錄檔案儲存在 `C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports`。如果您手動為記錄儲存指定了另一個路徑，`KAVSHELL VACUUM` 指令將對 Kaspersky Embedded Systems Security 記錄設定中指定的資料夾中的檔案執行磁碟整理。

對較大的檔案進行磁碟整理會增加 `KAVSHELL VACUUM` 指令的執行時間。

在執行 `KAVSHELL VACUUM` 指令期間，將無法執行即時防護和電腦控制工作。持續磁碟整理過程會限制對 Kaspersky Embedded Systems Security 記錄的存取並拒絕事件記錄。為了避免降低安全等級，建議您提前將 `KAVSHELL VACUUM` 指令安排在停機時執行。

► 若要對 Kaspersky Embedded Systems Security 記錄檔案進行磁碟整理，請執行以下指令：

```
KAVSHELL VACUUM
```

如果以本機管理員帳戶權限啟動，則可執行指令。

清除 iSwift 庫。KAVSHELL FBRESET

Kaspersky Embedded Systems Security 使用的 iSwift 技術可避免應用程式重新掃描上次掃描後未修改的檔案（使用 iSwift 技術）。

Kaspersky Embedded Systems Security 會在 %SYSTEMDRIVE%\System Volume Information 資料夾建立 klamfb.dat 和 klamfb2.dat 檔案，這些檔案包含有關已掃描過的乾淨物件資訊。檔案 klamfb.dat (klamfb2.dat) 隨著 Kaspersky Embedded Systems Security 掃描的檔案數目的增加而增大。該檔案僅包含有關系統中存在的檔案的目前資訊：如果刪除一個檔案，Kaspersky Embedded Systems Security 將從 klamfb.dat 清除相關資訊。

要清除某個檔案，請使用指令 KAVSHELL FBRESET。

操作 KAVSHELL FBRESET 指令時請注意以下細節：

- 透過 KAVSHELL FBRESET 指令清除 klamfb.dat 檔案時，Kaspersky Embedded Systems Security 不會暫停防護（與手動刪除 klamfb.dat 的情況不同）。
- 在 Klamfb.dat 中清除資料後，可能會增加 Kaspersky Embedded Systems Security 的電腦負載。在這種情況下，Kaspersky Embedded Systems Security 將掃描在清除 klamfb.dat 後第一次存取的所有檔案。在掃描後，Kaspersky Embedded Systems Security 將有關每個掃描物件的資訊會再次新增到 klamfb.dat 中。在嘗試存取新物件的情況下，iSwift 技術將避免重新掃描未經變更的檔案。

只有在 SYSTEM 帳戶下啟動命令列時，才能執行 KAVSHELL FBRESET 指令。

啟用和停用建立傾印檔案。KAVSHELL DUMP

您可使用 KAVSHELL DUMP，在 Kaspersky Embedded Systems Security 處理程序不正常終止的情況下啟用或停用建立記憶體快照（傾印檔案）（請參見下表）。您可隨時替正在執行的 Kaspersky Embedded Systems Security 處理程序拍攝快照。

為了能夠成功建立傾印檔案，必須在本機系統帳戶 (SYSTEM) 下執行 KAVSHELL DUMP 指令。

KAVSHELL DUMP 指令語法

KAVSHELL DUMP </ON /F:<傾印檔案的資料夾>|/SNAPSHOT /F:< 傾印檔案的資料夾> / P:<pid> | /OFF>

表 91. KAVSHELL DUMP 指令參數

鍵	敘述
/ON	在不正常終止的情況下，啟用建立處理程序的記憶體傾印檔案功能。
/F:<傾印檔案的資料夾路徑 >	此指令參數為必要的設定值。它可指定要儲存傾印檔案的資料夾路徑。不能指定其他不受防護電腦的網路磁碟機上的資料夾位置。 在指定包含記憶體傾印檔案的資料夾的路徑時，可以使用系統環境變數；不允許使用使用者環境變數。
/SNAPSHOT	獲取正在執行的具有指定 PID 的處理程序拍攝記憶體快照，並將傾印檔案儲存到 /F 指令參數所指定的資料夾路徑中。
/P	Microsoft Windows 工作管理員中會顯示 PID 處理程序識別碼。
/OFF	在不正常終止的情況下，停用建立處理程序的記憶體傾印檔案功能。

KAVSHELL DUMP 指令的回傳代碼(請參閱第 [658](#) 頁上的“KAVSHELL DUMP 指令的回傳代碼 ”部分)。

KAVSHELL DUMP 指令範例

- ▶ 要啟用建立傾印檔案的功能，並將傾印檔案儲存到 C:\Dump Folder 資料夾，請執行以下指令：

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

- ▶ 要使用 ID 1234 將處理程序的傾印檔案儲存到 C:/Dumps 資料夾，請執行以下指令：

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /F:1234
```

- ▶ 要停用產生傾印檔案的功能，請執行以下指令：

```
KAVSHELL DUMP /OFF
```

匯入設定。KAVSHELL IMPORT

您可使用 KAVSHELL IMPORT 指令來匯入受防護電腦上的 Kaspersky Embedded Systems Security 設定、功能及 Kaspersky Embedded Systems Security 設定檔及副本等工作。您可使用 KAVSHELL EXPORT 指令建立設定檔。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>] 鍵。

KAVSHELL IMPORT 指令語法

KAVSHELL IMPORT <設定檔名稱及檔案路徑>

KAVSHELL IMPORT 指令範例

KAVSHELL IMPORT Host1.xml

表 92. KAVSHELL IMPORT 指令參數

鍵	敘述
<設定檔名稱及檔案路徑>	設定檔名稱可當作匯入設定來源使用。 指定檔案路徑時可以使用系統環境變數；不允許使用者環境變數。

KAVSHELL IMPORT 指令的回傳代碼 (請參閱第 [659](#) 頁上的“KAVSHELL IMPORT 指令的回傳代碼”部分) 。

匯出設定。KAVSHELL EXPORT

KAVSHELL EXPORT 指令可用來匯出 Kaspersky Embedded Systems Security 及其現有工作所有的設定，以便之後將設定匯入其他電腦所安裝的 Kaspersky Embedded Systems Security 副本。

KAVSHELL EXPORT 指令語法

KAVSHELL EXPORT <設定檔名稱及檔案路徑>

KAVSHELL EXPORT 指令範例

KAVSHELL EXPORT Host1.xml

表 93. KAVSHELL EXPORT 指令參數

鍵	敘述
<設定檔名稱及檔案路徑>	<p>包含設定的設定檔名稱。</p> <p>設定檔可指派任何副檔名。</p> <p>指定檔案路徑時可以使用系統環境變數；不允許使用者環境變數。</p>

KAVSHELL EXPORT 指令的回傳代碼 (請參閱第 [660](#) 頁上的“KAVSHELL EXPORT 指令的回傳代碼”部分) 。

與 Microsoft Operations Management Suite 整合。KAVSHELL OMSINFO

使用 KAVSHELL OMSINFO 指令可檢視應用程式的狀態以及反病毒資料庫和 KSN 服務偵測到的威脅的相關資訊。關於威脅的資料取自可用的事件記錄。

KAVSHELL OMSINFO 指令語法

KAVSHELL OMSINFO <建立的檔案的完整路徑與檔名>

KAVSHELL OMSINFO 指令範例

KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json

表 94. KAVSHELL OMSINFO 指令參數

鍵	敘述
<建立的檔案的路徑與檔案名稱>	建立的檔案的名稱，該檔案將包含應用程式狀態和偵測到的威脅的相關資訊。

命令列回傳代碼

本章節說明項目

KAVSHELL START 和 KAVSHELL STOP 指令的回傳代碼	652
KAVSHELL SCAN 和 KAVSHELL SCANCritical 指令的回傳代碼	653
KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼	654
KAVSHELL TASK 指令的回傳代碼	654
KAVSHELL RTP 指令的回傳代碼	655
KAVSHELL UPDATE 指令的回傳代碼	656
KAVSHELL ROLLBACK 指令的回傳代碼	656
KAVSHELL LICENSE 指令的回傳代碼	657
KAVSHELL TRACE 指令的回傳代碼	658
KAVSHELL FBRESET 指令的回傳代碼	658
KAVSHELL DUMP 指令的回傳代碼	658
KAVSHELL IMPORT 指令的回傳代碼	659
KAVSHELL EXPORT 指令的回傳代碼	660

KAVSHELL START 和 KAVSHELL STOP 指令的回傳代碼

表 95. KAVSHELL START 和 KAVSHELL STOP 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-3	權限錯誤
-5	指令語法無效

回傳代碼	敘述
-6	操作無效 (例如 Kaspersky Embedded Systems Security 服務已經執行或已經停止)
-7	服務未註冊
-8	已停用自動服務啟動。
-9	試圖從另一個失效的使用者帳戶啟動電腦失敗 (依預設 Kaspersky Embedded Systems Security 會從本機系統使用者帳戶執行服務)
-99	未知錯誤

KAVSHELL SCAN 和 KAVSHELL SCANCritical 指令的回傳代碼

表 96. KAVSHELL SCAN 和 KAVSHELL SCANCritical 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成 (未偵測到威脅)
1	已取消操作
-2	未執行服務
-3	權限錯誤
-4	找不到物件 (找不到含有掃描區域清單的檔案)
-5	指令語法無效或未定義掃描區域
-80	偵測到受感染物件和其他物件
-81	偵測到可能存在的威脅
-82	偵測到處理程序錯誤
-83	找到未掃描的物件
-84	偵測到已損毀物件

回傳代碼	敘述
-85	建立工作執行記錄失敗
-99	未知錯誤
-301	金鑰無效

KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼

表 97. KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-6	操作無效 (例如 Kaspersky Embedded Systems Security 服務已經執行或已經停止)
402	工作執行中 (適用指令 /STATE)

KAVSHELL TASK 指令的回傳代碼

表 98. KAVSHELL TASK 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-4	找不到物件 (找不到工作項目)
-5	指令語法無效
-6	操作無效 (例如 , 工作未執行、工作執行中或無法暫停)

回傳代碼	敘述
-99	未知錯誤
-301	金鑰無效
401	工作未執行 (適用指令 /STATE)
402	工作執行中 (適用指令 /STATE)
403	工作已暫停 (適用指令 /STATE)
-404	操作執行錯誤 (工作狀態改變導至失敗)

KAVSHELL RTP 指令的回傳代碼

表 99. KAVSHELL RTP 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-4	找不到物件 (找不到其中一個即時防護工作或全部的即時防護工作)
-5	指令語法無效
-6	操作無效 (例如, 工作已執行中或已停止工作)
-99	未知錯誤
-301	金鑰無效

KAVSHELL UPDATE 指令的回傳代碼

表 100. KAVSHELL UPDATE 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
200	所有物件都是最新的 (資料庫或程式元件為最新的)
-2	未執行服務
-3	權限錯誤
-5	指令語法無效
-99	未知錯誤
-206	指定來源中的更新檔遺失或檔案格式不明
-209	連線更新來源錯誤
-232	連線到代理伺服器時發生身分驗證錯誤
-234	連線安全管理中心時發生錯誤
-235	Kaspersky Embedded Systems Security 在連線到更新來源時未透過身分驗證
-236	應用程式資料庫已損壞
-301	金鑰無效

KAVSHELL ROLLBACK 指令的回傳代碼

表 101. KAVSHELL ROLLBACK 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務

回傳代碼	敘述
-3	權限錯誤
-99	未知錯誤
-221	找不到資料庫備份副本或資料庫已損毀
-222	資料庫備份副本已損毀

KAVSHELL LICENSE 指令的回傳代碼

表 102. KAVSHELL LICENSE 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限不足無法管理金鑰
-4	找不到指定的金鑰序號
-5	指令語法無效
-6	操作無效 (已安裝金鑰)
-99	未知錯誤
-301	金鑰無效
-303	授權適用於其他程式

KAVSHELL TRACE 指令的回傳代碼

表 103. KAVSHELL TRACE 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-4	找不到物件 (找不到偵錯記錄資料夾的指定路徑)
-5	指令語法無效
-6	操作無效 (如果已停用偵錯記錄建立功能，試圖執行 KAVSHELL TRACE /OFF 指令)
-99	未知錯誤

KAVSHELL FBRESET 指令的回傳代碼

表 104. KAVSHELL FBRESET 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-99	未知錯誤

KAVSHELL DUMP 指令的回傳代碼

表 105. KAVSHELL DUMP 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務

回傳代碼	敘述
-3	權限錯誤
-4	找不到物件 (找不到傾印檔案資料夾的指定路徑；找不到含有指定 PID 的處理程序)
-5	指令語法無效
-6	操作無效 (如果已停用傾印檔案建立功能，試圖執行 KAVSHELL DUMP/OFF 指令)
-99	未知錯誤

KAVSHELL IMPORT 指令的回傳代碼

表 106. KAVSHELL IMPORT 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-4	找不到物件 (找不到匯入設定檔)
-5	無效的語法
-99	未知錯誤
501	操作順利完成，但是執行指令期間出現錯誤 / 備註，例如 Kaspersky Embedded Systems Security 未匯入某些功能元件的設定
-502	遺失匯入檔案或無法辨識匯入檔案格式
-503	不相容的設定(設定檔從不同的程式或新版或不相容的 Kaspersky Embedded Systems Security 匯出)

KAVSHELL EXPORT 指令的回傳代碼

表 107. KAVSHELL EXPORT 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-5	無效的語法
-10	無法建立設定檔 (例如 , 無法存取檔案路徑中所指定的資料夾)
-99	未知錯誤
501	操作順利完成 , 但是執行指令期間出現錯誤/備註 , 例如 Kaspersky Embedded Systems Security 未匯出某些功能元件的設定

聯絡技術支援

本章節提供有關如何與 Kaspersky Lab 技術支援服務聯絡的資訊。

本章內容

如何獲取技術支援	661
透過電話獲取技術支援	662
透過 Kaspersky CompanyAccount 取得技術支援	662
使用偵錯檔案和 AVZ 指令碼	663

如何獲取技術支援

如果您無法透過手冊及相關資源自行排除問題，建議您與技術支援聯絡。技術支援服務專家會為您解答關於安裝和使用該應用程式的任何問題。

技術支援服務僅適用擁有正式版授權的使用者。試用版授權的使用者將不包含在技術支援服務範圍內。

在聯絡技術支援服務前，請閱讀技術支援規則。

可以透過以下方法之一與技術支援部門聯絡：

- 致電技術支援。
- 透過 Kaspersky CompanyAccount 網站 (<https://companyaccount.kaspersky.com>) 向 Kaspersky Lab 技術支援服務部門傳送問題。

透過電話獲取技術支援

您可以從全球大多數地區撥打技術支援專家的電話。您可以在 Kaspersky Lab 技術支援網站 (<https://support.kaspersky.com/b2b>) 找到有關如何在您的地區獲取技術支援的資訊以及技術支援的聯絡人資訊。

在聯絡技術支援服務前，請閱讀技術支援規則 (https://support.kaspersky.com/support/rules#en_us)。

透過 Kaspersky CompanyAccount 取得技術支援

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) 是一種可用於向 Kaspersky Lab 傳送請求，並追蹤 Kaspersky Lab 專家處理請求進度的網頁服務。Kaspersky CompanyAccount 設計用於方便使用者與 Kaspersky Lab 專家之間透過線上請求進行互動。透過使用 Kaspersky CompanyAccount 網站，您可以監視 Kaspersky Lab 專家處理電子請求的進度並儲存電子請求的歷史記錄。

可以在 Kaspersky CompanyAccount 上的單個使用者帳戶中註冊您組織的所有員工。透過使用單一帳戶，您可以集中管理註冊的員工傳送到 Kaspersky Lab 的電子請求，以及在 Kaspersky CompanyAccount 中管理員工的權限。

Kaspersky CompanyAccount 適用於以下語言：

- 英語
- 西班牙語
- 義大利語
- 德語
- 波蘭語
- 葡萄牙語
- 俄語
- 法語

- 日語

有關 Kaspersky CompanyAccount 操作的更多資訊，請參閱技術支援網站 http://support.kaspersky.com/faq/companyaccount_help。

使用偵錯檔案和 AVZ 指令碼

向 Kaspersky Lab 技術支援專家報告問題後，他們可能需求您建立一份包含有關 Kaspersky Embedded Systems Security 執行情況的資訊的報告，然後將報告傳送給 Kaspersky Lab 技術支援部門。Kaspersky Lab 技術支援專家還可能需要您建立偵錯檔案。偵錯檔案可以追蹤程式指令的每一步執行，以偵測錯誤發生時的程式執行階段。

在 Kaspersky Lab 技術支援專家分析您所傳送的資料後，他們可以建立 AVZ 指令碼並將其傳送給您。透過使用 AVZ 指令碼，可以分析活動處理程序以尋找威脅，掃描電腦以尋找威脅，清除或刪除感染的檔案以及建立系統掃描報告。

爲了提供針對程式問題的更加有效的支援和故障排除，技術支援專家可能需求您暫時變更設定，以便在診斷過程中進行診斷。這可能需要進行以下操作：

- 啟動用於處理和儲存延伸診斷資訊的功能。
- 對於無法透過標準使用者介面元素使用的各個軟體元件，微調這些元件的設定。
- 變更已處理的診斷資訊的儲存和傳輸設定。
- 設定網路流量的攔截和記錄。

詞彙表

啟動金鑰

應用程式目前使用的金鑰。

管理伺服器

卡斯基安全管理中心的一個元件，可集中儲存公司網路內所有安裝 Kaspersky Lab 應用程式的資訊。它也可用於管理這些應用程式。

病毒特徵碼資料庫

該資料庫中包含截至病毒資料庫發佈日期為止 Kaspersky Lab 已知的電腦安全威脅相關資訊。資料庫中的項目用於在掃描物件時偵測到惡意程式。Kaspersky Lab 的專家維護資料庫每小時更新一次。

壓縮檔案

一個或多個檔案透過壓縮封裝到單個檔案中。壓縮和解壓縮資料需要一個名為壓縮應用程式的專用應用程式。

備份

用來儲存檔案備份副本的特殊儲存，在嘗試解毒或刪除前建立。

解毒

一種處理受感染檔案的方法，該方法會導致完全或部份還原資料，或裁定無法解毒檔案。不是所有的受感染物件都可以解毒。

事件嚴重性

在 Kaspersky Lab 應用程式執行過程中遇到的事件的內容。有四個嚴重等級：

- 緊急事件。
- 錯誤。

- 警告。
- 資訊。

同一類型的事件可能有不同的嚴重等級，具體取決於發生事件時的情況。

誤報

Kaspersky Lab 應用程式因物件的程式碼與病毒的程式碼類似而將未感染的物件視為受感染物件的情況。

檔案遮罩

使用萬用字元表示檔案名稱。檔案遮罩中使用的標準萬用字元為 * 和 ? ,其中 * 表示任意數量的任意字元 ,? 表示單個任意字元。

啟發式分析

用於偵測其資訊尚未新增到 Kaspersky Lab 資料庫中的威脅技術。啟發式分析用於透過偵測運作行為，判斷對作業系統構成安全威脅的物件。啟發式分析偵測到的物件將被視為可疑感染。例如，如果一個物件包含惡意物件通常具有的運作行為（檔案開啟、寫入），則可能會將該物件視為可疑感染。

可感染的檔案

一種由於其結構或格式，可被罪犯用作儲存和傳播惡意程式碼的“容器”的檔案。通常為可執行檔，此類檔案副檔名為 .com、.exe 和 .dll。此類檔案被惡意程式碼侵入的風險非常高。

受感染的物件

其部分程式碼完全比對已知惡意軟體部分程式碼的物件。Kaspersky Lab 不推薦存取此類物件。

卡斯基安全網路 (KSN)

一個雲端服務基礎架構，提供對 Kaspersky Lab 資料庫的存取，該資料庫不斷更新關於檔案、Web 資源和軟體的信譽的資訊。卡斯基安全網路允許 Kaspersky Lab 十分迅速地對新威脅作出回應，提高許多防護元件的效能，以降低誤報可能性。

產品授權期限

一個時間段，在此時間段內您可以存取應用程式功能，並有權使用附加服務。您可以使用的服務取決於產品授權類型。

本機工作

定義為在單台用戶端電腦上執行的工作。

OLE 物件

附加到其他檔案或透過使用物件連結與嵌入 (OLE) 技術嵌入其他檔案的物件。一個 OLE 物件範例是嵌入到 Microsoft Office Word 文件中的 Microsoft Office Excel® 電子表格。

政策

政策確定應用程式的設定並管理在管理群組內的電腦上配置該應用程式的能力。必須為每個應用程式建立單獨政策。您可以為每個管理群組內的電腦上安裝的應用程式建立無限數量的不同政策，但在一個管理群組內一次只能對每個應用程式套用一個政策。

防護狀態

目前防護狀態，反映電腦安全性的等級。

隔離

Kaspersky Lab 應用程式將偵測到的可疑感染物件移動到的資料夾。在此以加密形式儲存在隔離，以避免對電腦造成任何影響。

即時防護

應用程式的執行模式，在該模式下即時掃描物件是否存在惡意程式碼。

應用程式將攔截所有開啟任何物件（讀取、寫入或執行）的嘗試，並掃描物件是否存在威脅。未受感染的物件將傳遞給使用者；包含威脅的物件或可疑感染物件將按照工作設定進行處理（解毒、刪除或隔離）。

安全等級

安全等級定義為一組預先配置的應用程式元件設定。

SIEM

一種用於分析來源於各種網路裝置和應用程式的安全事件的技術。

啟動物件

電腦上安裝的作業系統和軟體正常啟動和執行所需的一組應用程式集。每次啟動作業系統時，都會執行這些物件。有些病毒專門感染此類物件，例如，可能會導致作業系統無法啟動。

工作

Kaspersky Lab 程式執行的功能是以工作形式呈現，如：即時檔案防護、電腦完整掃描和資料庫更新。

工作設定

特定於每個類型工作的程式設定。

更新

替換/新增從 Kaspersky Lab 更新伺服器上擷取的新檔案（資料庫或應用程式模組）的過程。

弱點

作業系統或應用程式存在的弱點，惡意軟體研發者會利用這種弱點入侵系統或應用程式並破壞其完整性。作業系統中的許多弱點都會導致作業系統執行不可靠，因為侵入作業系統的病毒可能會導致作業系統本身和安裝的應用程式損壞。

AO Kaspersky Lab

Kaspersky Lab 是防護電腦免受諸如病毒和其他惡意軟體、未經請求所傳送的電子郵件（垃圾郵件）以及網路和駭客攻擊等數位威脅的系統的世界知名供應商。

2008 年，Kaspersky Lab 被評為全球四大資訊安全解決方案供應商之一（根據 IDC Worldwide Endpoint Security Revenue by Vendor）。Kaspersky Lab 是俄羅斯家庭使用者首選的電腦防護系統供應商（IDC Endpoint Tracker 2014）。

Kaspersky Lab 於 1997 年成立於俄羅斯。如今，Kaspersky Lab 已成長為一家在 33 個國家/地區擁有 38 個辦事處的國際性企業集團。並且團隊組織共擁有 3,000 多名的技術專家。

產品。 Kaspersky Lab 的產品為家用電腦到大型企業網路的所有系統提供安全防護。

個人產品範圍包括桌上型電腦、筆記型電腦和可攜式電腦，以及智慧型手機和其他行動裝置的安全應用程式。

公司提供用於工作站和行動裝置、虛擬機、檔案伺服器 and Web 伺服器、郵件閘道以及防火牆的防護和控制解決方案和技術。公司的產品群組還包括用於防止 DDoS 攻擊、防護工業控制系統以及防止金融欺詐的專用產品。並透過與集中管理工具整合起來之後，這些解決方案能夠為任何規模的公司和組織提供高效能且自動化的安全防護，以防範各式的電腦威脅。同時，Kaspersky Lab 產品獲得主要測試實驗室的認證，相容於許多供應商的軟體，經過最佳化設定以便應用在多種硬體平台上執行。

Kaspersky Lab 病毒分析人員不捨晝夜地工作。他們每天都會發現成千上萬的新型電腦威脅，並且建立工具以偵測和解毒它們，同時會將這些威脅的簽章加入在 Kaspersky Lab 應用程式所使用的資料庫中。

技術。許多現在已經成為現代防毒工具組成部分的技術最初都是由 Kaspersky Lab 開發的。很多其他開發商在其產品中使用卡斯基病毒防護引擎絕非巧合，這包括：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 和 ZyXEL。公司的許多創新性技術都獲得了專利認證。

成就。多年以來，Kaspersky Lab 因為在對抗電腦威脅方面提供的服務贏得數以百計的獎項。在 2014 年由著名奧地利測試實驗室 AV-Comparatives 進行測試和研究後，Kaspersky Lab 贏得多項 Advanced+ 憑證，躋身前兩大供應商之一，且最終被授予最受好評憑證。不過，Kaspersky Lab 最主要的成就來自於全球使用者對它的信賴。Kaspersky Lab 目前在全球間為超過 4 億名使用者及超過 27 萬家的企業使用者提供令人安心的資訊安全防護。

Kaspersky Lab 網站：<https://www.kaspersky.com>

病毒百科全書：<https://securelist.com>

Kaspersky VirusDesk：<https://virusdesk.kaspersky.com> (用於分析可疑檔案和網站)

Kaspersky Lab 網路社區：<https://community.kaspersky.com>

有關協力廠商程式碼資訊

有關協力廠商程式碼資訊被包含在文件 `legal_notices.txt` 中，並位於應用程式的安裝資料夾中。

商標聲明

註冊商標和服務標誌均為其各自所有者擁有的財產。

Intel 和 Pentium 是 Intel Corporation 在美國和/或其他國家/地區的商標。

Linux 是 Linus Torvalds 在美國和/或其他國家/地區註冊的商標。

Microsoft、Active Directory、Excel、Internet Explorer 和 Windows 是 Microsoft Corporation 在美國和其他國家/地區註冊的商標。

UNIX 是在美國和其他國家/地區的註冊商標，透過 X/Open Company Limited 獨家授權。

索引

F

FTP 伺服器..... 152, 155, 156

H

HTTP 伺服器.....149, 152, 155, 156

I

iSwift 檔案..... 160, 230, 349

三劃

工作..... 129

工作托盤通知區域內的圖示..... 127

工作排程..... 130, 132

五劃

主控台..... 118, 124, 128

 啟動..... 188

 連線..... 128

主視窗..... 124

代理伺服器..... 152

可執行檔..... 230, 251, 275, 280, 282, 286

七劃

即時防護	237
更新	
安排程	130, 152
軟體模組	147
更新內容	155
更新來源	152, 155, 156
防護模式	224

八劃

事件記錄	173, 179
受信任裝置	295
物件的解毒	230

九劃

威脅類型	
操作	230

十劃

記錄資料夾	180
配置	
工作	129, 152, 224, 245, 275, 280, 311, 315
安全性設定	230, 349

十一劃

啟動略過的工作	130
掃描	
安全等級	349
最大物件掃描時間	230
僅新物件和已修改的物件	230
掃描 NTFS 交換資料串流	230
掃描範圍排除項目	230
清除系統稽核記錄	175
統計	139
規則	251, 296, 297, 298
裝置控制	296, 297, 298, 312, 313, 314, 315
應用程式啟動控制	251, 274, 275, 286, 289, 290

十二劃

備份	167
刪除物件	171
配置設定	171
還原物件	169
備份儲存資料夾	171
最大大小	
已掃描的物件	230
隔離	165

十三劃

資料庫	147, 148
手冊更新	152
自動更新	130, 148, 152
建立日期	139
隔離	
可用空間上限值	165
刪除物件	164
物件還原	162
檢視物件	159, 160
隔離和備份	158
預設拒絕	295, 311

十四劃

對物件的操作	230, 245, 349
--------------	---------------

十六劃

操作	
可疑物件	230
受感染的物件	230

十七劃

儲存更新的資料夾	155
儲存病毒掃描	160

壓縮檔案.....	230
應用程式介面.....	124
工具列通知區域內的圖示.....	127
還原物件.....	162, 169
還原資料夾	
隔離.....	165
還原預設設定.....	349