KASPERSKY lab

Kaspersky Embedded Systems Security

Manual do Administrador

Versão do aplicativo: 2.3.0.754

Prezado usuário,

Obrigado por escolher a Kaspersky Lab como seu provedor de software de segurança. Esperamos que este documento o ajude a usar o nosso produto.

Data de revisão do documento: 19.04.2019

https://www.kaspersky.com.br
https://support.kaspersky.com.br

Conteúdo

Sobre este Manual 17
Nesta documentação 17
Convenções da documentação 19
Fontes de informação sobre o Kaspersky Embedded Systems Security 21
Fontes para a recuperação independente de informações 21
Discutindo os aplicativos da Kaspersky Lab na comunidade 22
Kaspersky Embedded Systems Security 23
Sobre o Kaspersky Embedded Systems Security 23
O que há de novo 25
Kit de distribuição 25
Requisitos de hardware e software 28
Requisitos e limitações funcionais 30
Instalação e desinstalação 30
Monitor de Integridade de Arquivos 31
Gerenciamento de Firewall 31
Outras limitações 32
Instalação e remoção do aplicativo 34
Códigos de componentes de software do Kaspersky Embedded Systems Security para o serviço do Windows Installer 34
Componentes de software do Kaspersky Embedded Systems Security 35
Conjunto de “Ferramentas de administração” de componentes de software 37
Modificações de sistema após a instalação do Kaspersky Embedded Systems Security 38
Processos do Kaspersky Embedded Systems Security 41
Configurações de instalação e desinstalação e opções de linha de comando para o serviço do Windows Installer 41
Logs de instalação e desinstalação do Kaspersky Embedded Systems Security 44
Planejamento da instalação 45
Seleção das ferramentas de administração 45
Seleção do tipo de instalação 46
Instalação e desinstalação do aplicativo usando um assistente 47
Instalação usando o Assistente de instalação 48
Instalação do Kaspersky Embedded Systems Security 48
Instalação do Console do Kaspersky Embedded Systems Security 50
Configurações avançadas após a instalação do Console do Aplicativo em outro computador 52
Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security 55
Alteração do conjunto de componentes e reparação do Kaspersky Embedded Systems Security 57
Desinstalação usando o Assistente de instalação 59
Desinstalação do Kaspersky Embedded Systems Security 59
Desinstalação do Console do Kaspersky Embedded Systems Security 60

Instalação e desinstalação do aplicativo a partir da linha de comando 61
Sobre a instalação e desinstalação do Kaspersky Embedded Systems Security a partir da linha de comando 61
Exemplos de comandos para instalar o Kaspersky Embedded Systems Security 62
Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security 63
Adicionar/remover componentes. Exemplos de comandos 64
Desinstalação do Kaspersky Embedded Systems Security. Exemplos de comandos 65
Códigos de retorno 65
Instalação e desinstalação do aplicativo usando o Kaspersky Security Center 66
Informações gerais sobre a instalação por meio do Kaspersky Security Center 66
Direitos para instalar ou desinstalar o Kaspersky Embedded Systems Security 67
Instalação do Kaspersky Embedded Systems Security através do Kaspersky Security Center 67
Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security 69
Instalação do Console do Aplicativo por meio do Kaspersky Security Center 70
Desinstalação do Kaspersky Embedded Systems Security através do Kaspersky Security Center 71
Instalação e desinstalação via políticas de grupo do Active Directory 71
Instalação do Kaspersky Embedded Systems Security através das políticas de grupo do Active Directory 71
Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security 72
Desinstalação do Kaspersky Embedded Systems Security através das políticas de grupo do Active Directory 73
Verificação das funções do Kaspersky Embedded Systems Security. Uso do vírus de teste EICAR 73
Sobre o vírus de teste EICAR 74
Verificação dos recursos de Proteção em Tempo Real e Verificação por Demanda 75
Interface do aplicativo 77
Licenciamento do aplicativo 78
Sobre o Contrato de Licença do Usuário Final 78
Sobre a licença 79
Sobre o certificado da licença 79
Sobre a chave 80
Sobre o arquivo de chave 80
Sobre o código de ativação 80
Sobre a coleta de dados 81
Ativar o aplicativo com uma chave de licença 83
Ativação do aplicativo com um código 84
Visualizando informações sobre a licença atual 84
Limitações funcionais quando a licença expira 86
Renovação da licença 87
Exclusão da chave 87
Trabalhar como Plug-in de administração 89
Gerenciamento do Kaspersky Embedded Systems Security a partir do Kaspersky Security Center 89
Gerenciamento das configurações do aplicativo 91

Gerenciamento do Kaspersky Embedded Systems Security a partir do Kaspersky Security Center 91
Navegação.....92
Abrir as configurações gerais a partir da política 92
Abrir as configurações gerais na janela de propriedades do aplicativo 92
Definindo as configurações gerais do aplicativo no Kaspersky Security Center 93
Configuração de escalabilidade e interface no Kaspersky Security Center 93
Definição das configurações de segurança no Kaspersky Security Center 94
Definição das configurações de conexão usando o Kaspersky Security Center.....96
Configuração da inicialização programada de tarefas locais do sistema 97
Definindo as configurações de Quarentena e de Backup no Kaspersky Security Center 99
Configurações de logs e notificações.....100
Definição de configurações de log 101
Log de segurança.....102
Definições das configurações de integração SIEM.....102
Definição de configurações de notificação.....105
Configuração de interações com o Servidor de Administração 106
Criação e configuração de políticas 108
Criando políticas.....109
Seções de configurações de política do Kaspersky Embedded Systems Security 111
Configuração de políticas.....115
Criando e configurando uma tarefa usando o Kaspersky Security Center 116
Sobre a criação de tarefa no Kaspersky Security Center 116
Criação de uma tarefa usando o Kaspersky Security Center 117
Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center 119
Configurando tarefas de grupo no Kaspersky Security Center.....120
Ativação da tarefa de Aplicativo 125
Tarefas de atualização 125
Controle de Integridade de Aplicativos 127
Definir configurações de diagnóstico de travamento no Kaspersky Security Center 128
Gerenciando programações de tarefas.....130
Definição das configurações da programação de inicialização da tarefa 130
Ativando e desativando tarefas programadas.....132
Relatórios do Kaspersky Security Center.....133
Trabalhar com o Console do Kaspersky Embedded Systems Security 136
Configurações do Kaspersky Embedded Systems Security no Console do Aplicativo 136
Sobre o Console do Kaspersky Embedded Systems Security.....143
Interface do Console do Kaspersky Embedded Systems Security 143
Ícone da bandeja do sistema na área de notificação 147
Gerenciando o Kaspersky Embedded Systems Security por meio do Console do Aplicativo em outro computador 148
Gerenciando as tarefas do Kaspersky Embedded Systems Security.....148

Categorias de tarefa do Kaspersky Embedded Systems Security....149
Como salvar uma tarefa depois de alterar suas configurações....149
Executando / pausando / reiniciando / interrompendo tarefas manualmente....150
Gerenciando programações de tarefas....150
Definição das configurações da programação de inicialização da tarefa....151
Ativando e desativando tarefas programadas....152
Uso de contas de usuário para iniciar tarefas....152
Sobre como usar contas para iniciar tarefas....153
Especificação de uma conta de usuário para iniciar uma tarefa....153
Configurações de importação e exportação....154
Sobre a importação e exportação de configurações....154
Exportando configurações....155
Importando configurações....156
Usando os modelos de configurações de segurança....157
Sobre os modelos de configurações de segurança....157
Criação de um modelo de configurações de segurança....157
Exibindo configurações de segurança em um modelo....158
Aplicação de um modelo de configurações de segurança....158
Exclusão de um modelo de configurações de segurança....159
Visualizando o status de proteção e as informações do Kaspersky Embedded Systems Security....161
Interface de diagnóstico compacta....166
Sobre a interface de diagnóstico compacta....166
Revisão do status do Kaspersky Embedded Systems Security por meio da Interface de diagnóstico compacta....167
Revisando estatística de evento de segurança....168
Revisando a atividade atual do aplicativo....168
Configuração da escrita de arquivos de despejo e de rastreamento....169
Atualização de bancos de dados e módulos de software do Kaspersky Embedded Systems Security....171
Sobre as tarefas de atualização....171
Sobre a Atualização de módulos de software do Kaspersky Embedded Systems Security....172
Sobre a Atualização do Banco de Dados do Kaspersky Embedded Systems Security....173
Esquemas para atualizar bancos de dados e módulos de aplicativos antivírus usados em uma organização....173
Configurando tarefas de Atualização....177
Definindo as configurações para trabalhar com fontes de atualização do Kaspersky Embedded Systems Security....177
Otimizando o uso da E/S de disco ao executar a tarefa de Atualização do banco de dados....180
Configurações da tarefa Copiar atualizações....181
Definindo as configurações da tarefa de Atualização de módulos de software....182
Revertendo atualizações do banco de dados do Kaspersky Embedded Systems Security....183
Revertendo atualizações dos módulos do aplicativo....183
Estatísticas da tarefa de atualização....184

Isolamento de objetos e cópia de backup 185
Isolando objetos possivelmente infectados. Quarentena 185
Sobre a colocação na Quarentena de objetos possivelmente infectados 185
Exibindo objetos da Quarentena 185
Verificação da quarentena 187
Restauração de objetos da quarentena 189
Movimentação de objetos para a Quarentena 191
Excluindo objetos da Quarentena 191
Enviando objetos possivelmente infectados à Kaspersky Lab para análise 191
Configurando a Quarentena 192
Estatísticas da Quarentena 193
Como fazer cópias de backup de objetos. Backup 194
Sobre o backup de objetos antes da desinfecção ou exclusão 194
Visualizando objetos armazenados no Backup 195
Restaurando arquivos do Backup 196
Excluindo arquivos do Backup 198
Configurando o Backup 199
Estatísticas do backup 200
Registro de eventos. Logs do Kaspersky Embedded Systems Security 201
Modos para registrar eventos do Kaspersky Embedded Systems Security 201
Log de auditoria do sistema 202
Classificando eventos no Log de auditoria do sistema 202
Filtrando eventos no Log de auditoria do sistema 203
Excluir eventos do Log de auditoria do sistema 203
Logs de tarefas 204
Sobre os Logs de tarefas 204
Visualizando a lista de eventos em Logs de tarefas 205
Classificando eventos em Logs de tarefas 205
Filtrar eventos em Logs de tarefas 205
Visualizando estatísticas e informações sobre uma tarefa do Kaspersky Embedded Systems Security em logs de tarefas 206
Exportando informações de um Log de tarefas 206
Excluindo eventos de Logs de tarefas 207
Log de segurança 208
Visualizando o log de eventos do Kaspersky Embedded Systems Security no Visualizador de eventos 208
Definindo configurações de log no Console do Kaspersky Embedded Systems Security 209
Sobre a integração SIEM 211
Definições das configurações de integração SIEM 212
Configurações de notificação 215
Métodos de notificação do administrador e dos usuários 215
Configurando notificações do administrador e dos usuários 216

Inicialização e interrupção do Kaspersky Embedded Systems Security 219
Iniciando o Plug-in de Administração do Kaspersky Embedded Systems Security 219
Iniciando o Console do Kaspersky Embedded Systems Security a partir do menu Iniciar 219
Inicialização e interrupção do Kaspersky Security Service 220
Inicialização dos componentes do Kaspersky Embedded Systems Security no modo seguro do sistema operacional 222
Sobre o funcionamento do Kaspersky Embedded Systems Security no modo seguro do sistema operacional 222
Inicialização do Kaspersky Embedded Systems Security no modo seguro 223
Autodefesa do Kaspersky Embedded Systems Security 224
Sobre a autodefesa do Kaspersky Embedded Systems Security 224
Proteção contra alterações em pastas com componentes do Kaspersky Embedded Systems Security instalados 224
Proteção contra alterações em chaves de registro do Kaspersky Embedded Systems Security 224
Registrar o Kaspersky Security Service como um serviço protegido 225
Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security 226
Sobre permissões para gerenciar o Kaspersky Embedded Systems Security 226
Sobre permissões de gerenciamento de serviços registrados 228
Sobre permissões para gerenciar o Kaspersky Security Service 228
Sobre permissões de acesso para o Kaspersky Security Management Service 230
Configurando permissões de acesso para gerenciar o Kaspersky Embedded Systems Security e o Kaspersky Security Service 231
Acesso protegido por senha às funções do Kaspersky Embedded Systems Security 233
Configurando permissões de acesso no Kaspersky Security Center 234
Proteção de Arquivos em Tempo Real 235
Sobre a tarefa de Proteção de Arquivos em Tempo Real 235
Sobre o escopo de proteção da tarefa e configurações de segurança 236
Sobre o escopo da proteção virtual 237
Escopos da proteção predefinidos 237
Níveis de segurança predefinidos 238
Extensões de arquivos verificadas por padrão na tarefa de Proteção de Arquivos em Tempo Real 240
Configurações padrão da tarefa de Proteção de arquivos em tempo real 241
Gerenciamento da tarefa de Proteção de Arquivos em Tempo Real por meio do Plug-in de Administração 241
Navegação 242
Abertura das definições de política para a tarefa de proteção de Arquivos em Tempo Real 242
Abertura das propriedades da tarefa de Proteção de Arquivos em Tempo Real 243
Configuração da tarefa de Proteção de Arquivos em Tempo Real 243
Selecionando o modo de proteção 244
Configuração do Analisador Heurístico e integração com outros componentes do aplicativo 245
Definição das configurações da programação de inicialização da tarefa 246
Criação e configuração do escopo de proteção da tarefa 248
Definição manual de configurações de segurança 249

Definir configurações gerais de tarefas 250
Configurar ações 252
Configurar o desempenho 254
Gerenciamento da tarefa de Proteção de Arquivos em Tempo Real por meio do Console do Aplicativo 256
Navegação 256
Abertura das configurações de escopo da Proteção de Arquivos em Tempo Real 257
Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real 257
Configuração da tarefa de Proteção de Arquivos em Tempo Real 257
Selecionando o modo de proteção 258
Configuração do Analisador Heurístico e integração com outros componentes do aplicativo 259
Definição das configurações da programação de inicialização da tarefa 260
Criando um escopo da proteção 261
Criando um escopo da proteção 262
Criando o escopo da proteção virtual 264
Definição manual de configurações de segurança 264
Definir configurações gerais de tarefas 265
Configurar ações 268
Configurar o desempenho 270
Estatísticas da tarefa de Proteção de Arquivos em Tempo Real 271
Uso da KSN 274
Sobre a tarefa de Uso da KSN 274
Configurações padrão da tarefa de Uso da KSN 276
Gerenciando o Uso da KSN por meio do Plug-in de Administração 277
Configurando a tarefa de Uso da KSN por meio do Plug-in de Administração 277
Configurando o Manuseio de Dados por meio do Plug-in de Administração 279
Gerenciando o Uso da KSN por meio do Console do Aplicativo 280
Configurando a tarefa de Uso da KSN por meio do Console do Aplicativo 281
Configurando o Manuseio de dados por meio do Console do Aplicativo 282
Configurando a transferência de dados adicionais 283
Estatísticas da tarefa de Uso da KSN 285
Controle de Inicialização de Aplicativos 286
Sobre a tarefa de Controle de Inicialização de Aplicativos 286
Sobre as regras de Controle de inicialização de aplicativos 287
Sobre o Controle de Distribuição de Software 289
Sobre o uso da KSN para a tarefa de Controle de inicialização de aplicativos 292
Geração de regras de Controle de inicialização de aplicativos 293
Configurações padrão da tarefa de Controle de Inicialização de Aplicativos 295
Gerenciamento do Controle de Inicialização de Aplicativos por meio do Plug-in de Administração 298
Navegação 298
Abertura das definições de política para a tarefa de Controle de Inicialização de Aplicativos 298
Abertura da lista de regras de Controle de Inicialização de Aplicativos 299

Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos 299
Definição de configurações da tarefa de Controle de Inicialização de Aplicativos 300
Configuração do controle de distribuição de software 303
Configuração da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos 305
Configuração de regras de Controle de inicialização de aplicativos por meio do Kaspersky Security Center 307
Adição de uma regra de Controle de Inicialização de Aplicativos 308
Ativar o modo de Permissão padrão 311
Criação de regras de permissão dos eventos do Kaspersky Security Center 311
Importação de regras a partir de um relatório do Kaspersky Security Center sobre aplicativos bloqueados 312
Importação de regras de Controle de inicialização de aplicativos de um arquivo XML 314
Verificação da inicialização de aplicativos 315
Criação de uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos 316
Restrição do escopo de uso da tarefa 317
Ações a serem executadas durante a geração automática de regras 318
Ações a serem executadas após a conclusão da geração automática de regras 319
Gerenciamento do Controle de Inicialização de Aplicativos por meio do Console do Aplicativo 320
Navegação 321
Abertura das configurações da tarefa de Controle de Inicialização de Aplicativos 321
Abertura da janela de regras de Controle de Inicialização de Aplicativos 321
Abertura das definições da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos 322
Definição de configurações da tarefa de Controle de Inicialização de Aplicativos 322
Seleção do modo da tarefa de Controle de Inicialização de Aplicativos 323
Configuração do escopo da tarefa de Controle de Inicialização de Aplicativos 324
Configuração do uso da KSN 325
Controle de Distribuição de Software 326
Configuração de regras de Controle de Inicialização de Aplicativos 329
Adição de uma regra de Controle de Inicialização de Aplicativos 329
Ativar o modo de Permissão padrão 332
Criação de regras de permissão a partir de eventos da tarefa de Controle de Inicialização de Aplicativos 332
Exportando regras de Controle de inicialização de aplicativos 333
Importação de regras de Controle de inicialização de aplicativos de um arquivo XML 333
Removendo regras de Controle de inicialização de aplicativos 334
Configuração de uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos 334
Restrição do escopo de uso da tarefa 335
Ações a serem executadas durante a geração automática de regras 335
Ações a serem executadas após a conclusão da geração automática de regras 337
Controle de Dispositivos 339
Sobre a tarefa Controle de Dispositivos 339

Sobre as regras de Controle de dispositivos ... 340
Sobre o preenchimento da lista de regras de Controle de dispositivos ... 342
Sobre a tarefa do Gerador de Regras de Controle de Dispositivos ... 344
Cenários de geração de regras de Controle de Dispositivos ... 344
Configurações padrão de tarefa Controle de dispositivos ... 345
Gerenciamento do Controle de Dispositivos por meio do Plug-in de Administração ... 346
Navegação ... 346
Abertura das configurações de política para a tarefa Controle de Dispositivos ... 346
Abertura da lista de regras de Controle de Dispositivos ... 347
Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Dispositivos ... 347
Configuração da tarefa Controle de Dispositivos ... 348
Geração de regras de Controle de dispositivos para todos os computadores por meio do Kaspersky Security Center ... 349
Configurando a tarefa do Gerador de Regras de Controle de Dispositivos ... 351
Configuração de regras de Controle de Dispositivos por meio do Kaspersky Security Center ... 351
Criação de regras de permissão com base nos dados de sistema em uma política do Kaspersky Security Center ... 352
Geração de regras para dispositivos conectados ... 352
Importação de regras a partir do relatório do Kaspersky Security Center sobre dispositivos bloqueados ... 353
Criação de regras usando a tarefa do Gerador de Regras de Controle de Dispositivos ... 354
Adicionar as regras geradas à lista de regras de Controle de dispositivos ... 356
Gerenciamento do Controle de Dispositivos por meio do Console do Aplicativo ... 357
Navegação ... 357
Abertura das configurações da tarefa Controle de Dispositivos ... 357
Abertura da janela de regras de Controle de dispositivos ... 358
Abertura das configurações da tarefa do Gerador de Regras de Controle de Dispositivos ... 358
Definição das configurações de tarefa Controle de Dispositivos ... 358
Configuração de regras de Controle de dispositivos ... 359
Importação das regras de Controle de dispositivos do arquivo XML ... 360
Preenchendo a lista de regras com base em eventos de tarefa Controle de dispositivos ... 360
Adicionar uma regra de permissão para um ou vários dispositivos externos ... 361
Removendo regras de Controle de dispositivos ... 362
Exportando regras de Controle de dispositivos ... 362
Ativando e desativando regras de Controle de dispositivos ... 362
Expandindo o escopo de uso das regras de Controle de dispositivos ... 363
Configurando a tarefa do Gerador de Regras de Controle de Dispositivos ... 364
Gerenciamento de Firewall ... 366
Sobre a tarefa de Gerenciamento de Firewall ... 366
Sobre as Regras de Firewall ... 367
Configurações padrão da tarefa de Gerenciamento de Firewall ... 369

Gerenciamento das regras de Firewall por meio do Plug-in de Administração 369
Como ativar e desativar as regras de Firewall 369
Adição de regras de Firewall manualmente 370
Exclusão de regras de Firewall 372
Gerenciamento das regras de Firewall por meio do Console do Aplicativo 373
Como ativar e desativar as regras de Firewall 373
Adição de regras de Firewall manualmente 373
Exclusão de regras de Firewall 374
Monitor de Integridade de Arquivos 376
Sobre a tarefa Monitor de Integridade de Arquivos 376
Sobre regras de monitoramento de operações de arquivos 377
Configurações padrão da tarefa de Monitor de Integridade de Arquivos 379
Gerenciamento do Monitor de Integridade de Arquivos por meio do Plug-in de Administração 380
Definição de configurações da tarefa Monitor de Integridade de Arquivos 381
Configuração de regras de monitoramento 382
Gerenciamento do Monitor de Integridade de Arquivos por meio do Console do Aplicativo 385
Definição de configurações da tarefa Monitor de Integridade de Arquivos 385
Configuração de regras de monitoramento 386
Inspeção de Log 390
Sobre a tarefa de Inspeção de Log 390
Configurações padrão da tarefa de Inspeção de Log 391
Gerenciamento das regras de inspeção de log por meio do Plug-in de Administração 392
Gerenciamento de regras de tarefa predefinidas por meio do Plug-in de Administração 392
Adicionando regras de inspeção de log por meio do Plug-in de Administração 394
Gerenciamento das regras de inspeção de log por meio do Console do Aplicativo 395
Gerenciamento de regras de tarefa predefinidas por meio do Console do Aplicativo 396
Configuração de regras de Inspeção de Log 397
Verificação por Demanda 399
Sobre tarefas de Verificação por Demanda 399
Sobre o escopo da verificação 400
Escopos de verificação predefinidos 401
Verificação de arquivos no armazenamento na nuvem 402
Configurações de segurança do nó selecionado nas tarefas de Verificação por Demanda 404
Sobre os níveis de segurança predefinidos para tarefas de Verificação por Demanda 404
Sobre a Verificação de Unidades Removíveis 406
Configurações padrão das tarefas de Verificação por Demanda 407
Gerenciamento da Verificação por demanda por meio do Plug-in de Administração 409
Navegação 410
Abertura do assistente da tarefa de Verificação por Demanda 410
Abertura das propriedades da tarefa de Verificação por Demanda 411
Criando uma tarefa de Verificação por Demanda 411

Atribuindo o status de tarefa de Verificação de Áreas Críticas a uma tarefa de Verificação por Demanda 414
Executando uma tarefa de Verificação por Demanda em segundo plano 415
Registrando a execução de Verificação de áreas críticas 416
Configuração do escopo da verificação da tarefa 416
Seleção de níveis de segurança predefinidos para tarefas de Verificação por Demanda 417
Definição manual de configurações de segurança 418
Definir configurações gerais de tarefas 419
Configurar ações 422
Configurar o desempenho 423
Configuração da Verificação de Unidades Removíveis 425
Gerenciamento da Verificação por demanda por meio do Console do Aplicativo 426
Navegação 426
Abertura das configurações da tarefa de Verificação por Demanda 426
Criação e configuração de uma tarefa de Verificação por Demanda 427
Escopo da verificação em tarefas de Verificação por Demanda 429
Configurando o modo de visualização de recursos de arquivos de rede 429
Criando um escopo de verificação 429
Incluindo objetos de rede no escopo da verificação 431
Criando um escopo de verificação virtual 432
Seleção de níveis de segurança predefinidos para tarefas de Verificação por Demanda 433
Definição manual de configurações de segurança 433
Definir configurações gerais de tarefas 434
Configurar ações 437
Configurar o desempenho 438
Configuração de armazenamento hierárquico 440
Verificação de unidades removíveis 440
Estatísticas da tarefa de Verificação por Demanda 441
Zona Confiável 443
Sobre a Zona Confiável 443
Gerenciamento da Zona Confiável por meio do Plug-in de Administração 444
Navegação 445
Gerenciamento do aplicativo por meio do Kaspersky Security Center 445
Abertura da janela de propriedades da Zona Confiável 445
Configuração da Zona Confiável por meio do Plug-in de Administração 446
Adição de uma exclusão 446
Adicionar processos confiáveis 448
Aplicar a máscara de não vírus 450
Gerenciamento da Zona Confiável por meio do Console do Aplicativo 450
Aplicar Zona Confiável para tarefas no Console do Aplicativo 451
Configuração da Zona Confiável no Console do Aplicativo 451

Adição de uma exclusão à Zona Confiável ... 452
Processos confiáveis ... 453
Aplicar a máscara de não vírus ... 455
Prevenção de Exploits ... 457
Sobre a Prevenção de Exploits ... 457
Gerenciamento da Prevenção de Exploits por meio do Plug-in de Administração ... 458
Navegação ... 459
Abertura das configurações de política para a Prevenção de Exploits ... 459
Abertura da janela de propriedades de Prevenção de Exploits ... 459
Definição das configurações de proteção da memória do processo ... 460
Adição de um processo para proteção ... 461
Gerenciamento da Prevenção de Exploits por meio do Console do Aplicativo ... 462
Navegação ... 463
Abertura das configurações gerais de Prevenção de Exploits ... 463
Abertura das configurações de proteção de processo de Prevenção de Exploits ... 463
Definição das configurações de proteção da memória do processo ... 463
Adição de um processo para proteção ... 464
Técnicas de prevenção de exploits ... 466
Integração com sistemas de terceiros ... 468
Monitoramento do desempenho. Contadores do Kaspersky Embedded Systems Security ... 468
Contadores de desempenho do Monitor do Sistema ... 468
Sobre os contadores de desempenho do Kaspersky Embedded Systems Security ... 469
Número total de solicitações negadas ... 469
Número total de solicitações ignoradas ... 470
Número de solicitações não processadas devido à falta de recursos do sistema ... 471
Número de solicitações enviadas para serem processadas ... 471
Número médio de fluxos de triagem de interceptação de arquivos ... 472
Número máximo de fluxos de triagem de interceptação de arquivos ... 472
Número de elementos na fila de objetos infectados ... 473
Número de objetos processados por segundo ... 473
Contadores SNMP e interceptações do Kaspersky Embedded Systems Security ... 474
Sobre contadores e interceptações SNMP do Kaspersky Embedded Systems Security ... 474
Contadores SNMP do Kaspersky Embedded Systems Security ... 475
Interceptações SNMP do Kaspersky Embedded Systems Security ... 477
Integração com WMI ... 484
Trabalhar com o Kaspersky Embedded Systems Security na linha de comando ... 488
Comandos da linha de comando ... 488
Exibindo a ajuda de comando do Kaspersky Embedded Systems Security. KAVSHELL HELP ... 491
Iniciando e interrompendo o Kaspersky Security Service KAVSHELL START, KAVSHELL STOP ... 491
Verifica a área selecionada. KAVSHELL SCAN ... 492
Iniciando a tarefa de Verificação de áreas críticas. KAVSHELL SCANCRITICAL ... 496

Gerenciando a tarefa especificada de maneira assíncrona. KAVSHELL TASK 497
Registro do KAVFS como um processo protegido do sistema. KAVSHELL CONFIG 498
Inicialização e interrupção de tarefas de Proteção em Tempo Real. KAVSHELL RTP 499
Gerenciamento da tarefa de Controle de Inicialização de Aplicativos KAVSHELL APPCONTROL /CONFIG 500
Gerador de Regras de Controle de Inicialização de Aplicativos KAVSHELL APPCONTROL /GENERATE 501
Preenchendo a lista de regras de Controle de inicialização de aplicativos KAVSHELL APPCONTROL 503
Preenchimento da lista de regras de Controle de Dispositivos. KAVSHELL DEVCONTROL 504
Iniciando a tarefa de atualização dos bancos de dados do Kaspersky Embedded Systems Security. KAVSHELL UPDATE 505
Revertendo atualizações do banco de dados do Kaspersky Embedded Systems Security. KAVSHELL ROLLBACK 508
Gerenciando inspeção de log KAVSHELL TASK LOG-INSPECTOR 509
Ativando, configurando e desativando o log de rastreamento. KAVSHELL TRACE 509
Desfragmentação de arquivos de log do Kaspersky Embedded Systems Security. KAVSHELL VACUUM 511
Limpando a base iSwift. KAVSHELL FBRESET 512
Ativando e desativando a criação do arquivo de despejo. KAVSHELL DUMP 512
Importando configurações. KAVSHELL IMPORT 513
Exportando configurações. KAVSHELL EXPORT 514
Integração com Microsoft Operations Management Suite. KAVSHELL OMSINFO 514
Códigos de retorno da linha de comando 515
Código de retorno dos comandos KAVSHELL START e KAVSHELL STOP 516
Código de retorno dos comandos KAVSHELL SCAN e KAVSHELL SCANCRITICAL 516
Códigos de retorno do comando KAVSHELL TASK LOG-INSPECTOR 517
Códigos de retorno do comando KAVSHELL TASK 517
Códigos de retorno do comando KAVSHELL RTP 518
Códigos de retorno do comando KAVSHELL UPDATE 518
Códigos de retorno do comando KAVSHELL ROLLBACK 519
Códigos de retorno do comando KAVSHELL LICENSE 519
Códigos de retorno do comando KAVSHELL TRACE 520
Códigos de retorno do comando KAVSHELL FBRESET 520
Códigos de retorno do comando KAVSHELL DUMP 520
Códigos de retorno do comando KAVSHELL IMPORT 521
Códigos de retorno do comando KAVSHELL EXPORT 521
Entrando em contato com o Suporte Técnico 523
Como obter suporte técnico 523
Obtenha suporte técnico por telefone 523
Suporte Técnico por meio do Kaspersky CompanyAccount 524
Usando arquivos de rastreamento e scripts do AVZ 524

Glossário 526
AO Kaspersky Lab 531
Informações sobre código de terceiros 532
Notificações de marcas registradas 533
Índice 534

Sobre este Manual

O Manual do Administrador do Kaspersky Embedded Systems Security 2.3 (doravante referido como “Kaspersky Embedded Systems Security”, “o aplicativo”) é destinado a especialistas que instalam e administram o Kaspersky Embedded Systems Security em todos os dispositivos protegidos e aos que fornecem suporte técnico a organizações que usam o Kaspersky Embedded Systems Security.

Este Manual contém informações sobre como configurar e usar o Kaspersky Embedded Systems Security.

Ele também fornecerá fontes de informação sobre o aplicativo e formas de receber suporte técnico.

Neste capítulo

Nesta documentação 17

Convenções da documentação 19

Nesta documentação

O Manual do Administrador do Kaspersky Embedded Systems Security contém as seções seguintes:

Fontes de informação sobre o Kaspersky Embedded Systems Security

Esta seção lista as fontes de informação sobre o aplicativo.

Kaspersky Embedded Systems Security

Esta seção descreve as funções, os componentes e o kit de distribuição do Kaspersky Embedded Systems Security, e fornece uma lista dos requisitos de hardware e software do Kaspersky Embedded Systems Security.

Instalação e remoção do aplicativo

Esta seção fornece instruções passo a passo para instalar e remover o Kaspersky Embedded Systems Security.

Interface do aplicativo

Esta seção contém informações sobre os elementos da interface do Kaspersky Embedded Systems Security.

Licenciamento do aplicativo

Esta seção fornece informações sobre os principais conceitos relacionados ao licenciamento do aplicativo.

Inicialização e interrupção do Kaspersky Embedded Systems Security

Esta seção contém informações sobre como inicializar e interromper o Plug-in de Administração do Kaspersky Embedded Systems Security (doravante referido como Plug-in de Administração) e o Kaspersky Security Service.

Sobre permissões de acesso para funções do Kaspersky Embedded Systems Security

Esta seção contém informações sobre permissões para gerenciar o Kaspersky Embedded Systems Security e os serviços Windows® registrados pelo aplicativo, bem como as instruções sobre como configurar essas permissões.

Criação e configuração de políticas

Esta seção contém informações sobre como utilizar as políticas do Kaspersky Security Center para gerenciar o Kaspersky Embedded Systems Security em vários computadores.

Criando e configurando uma tarefa usando o Kaspersky Security Center

Esta seção contém informação sobre tarefas do Kaspersky Embedded Systems Security e como criá-las, definir suas configurações, iniciá-las e interrompê-las.

Gerenciamento das configurações do aplicativo

Esta seção contém informações sobre como definir as configurações gerais do Kaspersky Embedded Systems Security no Kaspersky Security Center.

Proteção do Computador em Tempo Real

Esta seção fornece informações sobre componentes de Proteção do Computador em Tempo Real:: Proteção de Arquivos em Tempo Real, Uso da KSN e Prevenção de Exploits. Esta seção também fornece instruções sobre como configurar tarefas de Proteção do Computador em Tempo Real e gerenciar as configurações de segurança de um computador protegido.

Controle de atividade local

Esta seção fornece informações sobre a funcionalidade do Kaspersky Embedded Systems Security que controla inicializações de aplicativos, conexões de dispositivos externos via USB.

Controle de atividade de rede

Esta seção contém informações sobre a tarefa Gerenciamento de Firewall.

Inspeção do sistema

Esta seção contém informações sobre a tarefa Monitor de Integridade de Arquivos e recursos para inspecionar o log do sistema operacional.

Integração com sistemas de terceiros

Esta seção descreve a integração do Kaspersky Embedded Systems Security com recursos e tecnologias de terceiros.

Trabalhar com o Kaspersky Embedded Systems Security na linha de comando

Esta seção descreve como trabalhar com o Kaspersky Embedded Systems Security na linha de comando.

Entrando em contato com o Suporte Técnico

Esta seção descreve as formas de receber suporte técnico e as condições em que ele está disponível.

Glossário

Esta seção contém uma lista dos termos mencionados no documento, bem como suas respetivas definições.

AO Kaspersky Lab

Esta seção fornece informações sobre a AO Kaspersky Lab.

Informações sobre código de terceiros

Esta seção contém informações sobre códigos de terceiros utilizados no aplicativo.

Notificações de marcas registradas

Esta seção lista marcas registradas reservadas a proprietários terceiros e mencionados no documento.

Índice

Esta seção permite encontrar rapidamente informações no documento.

Convenções da documentação

Este documento utiliza as seguintes convenções (consulte a tabela abaixo).

Tabela 1. Convenções da documentação

Texto de exemplo	Descrição das convenções da documentação
Observe que...	Os avisos são realçados em vermelho e exibidos em uma caixa. Os avisos contêm informações sobre as ações que podem ter consequências indesejáveis.
Recomenda-se usar...	As observações são exibidas em uma caixa. As observações contêm informações adicionais e de referência.
Exemplo: …	Os exemplos são dados em blocos sobre fundo azul, sob o título "Exemplo".
Atualização significa... Ocorreu o evento *Bancos de dados desatualizados*.	Os seguintes elementos são exibidos no texto em *itálico*: • Termos novos • Nomes de status e eventos do aplicativo
Pressione **ENTER**. Pressione **ALT**+**F4**.	Os nomes de teclas do teclado são exibidos em **negrito** e em letras maiúsculas. Os nomes das teclas seguidos de um sinal de + (adição) indicam o uso de uma combinação de teclas. Estas teclas devem ser pressionadas simultaneamente.
Clique no botão **Ativar**.	Os nomes de elementos da interface do aplicativo, como caixas de texto, itens de menu e botões são exibidos em **negrito**.
► *Para configurar a programação da tarefa:*	As frases introdutórias de instruções são exibidas em itálico e acompanhadas de um símbolo de seta.

Texto de exemplo	Descrição das convenções da documentação
Na linha de comandos, insira `help` Em seguida, a seguinte mensagem será exibida: Especifique a data no formato `dd:mm:aa`.	Os seguintes tipos de conteúdo de texto são exibidos com uma fonte especial: • Texto da linha de comando • O texto de mensagens exibido na tela pelo aplicativo • Dados que devem ser inseridos a partir do teclado
<Nome de usuário>	As variáveis são colocadas entre colchetes angulares. Em vez do nome da variável, o valor correspondente deve ser inserido, sem os colchetes angulares.

Fontes de informação sobre o Kaspersky Embedded Systems Security

Esta seção lista as fontes de informação sobre o aplicativo.

Você pode selecionar a fonte de informações mais adequada de acordo com o nível de importância e a urgência do problema.

Neste capítulo

Fontes para a recuperação independente de informações 21

Discutindo os aplicativos da Kaspersky Lab na comunidade 22

Fontes para a recuperação independente de informações

Você pode usar as fontes a seguir para encontrar informação sobre o Kaspersky Embedded Systems Security:

- Página do Kaspersky Embedded Systems Security no site da Kaspersky Lab.
- Página do Kaspersky Embedded Systems Security no site do Suporte Técnico (Base de dados de conhecimento).
- Manuais.

Se você não encontrou uma solução para o seu problema, entre em contato com o Suporte Técnico da Kaspersky Lab https://support.kaspersky.com.br.

É requerida uma conexão da Internet para usar fontes de informação on-line.

Página do Kaspersky Embedded Systems Security no site da Kaspersky Lab

Na página do Kaspersky Embedded Systems Security (https://www.kaspersky.com.br/enterprise-security/embedded-systems), você pode visualizar informações gerais sobre o aplicativo, suas funções e recursos.

A página do Kaspersky Embedded Systems Security contém um link para a Loja Virtual. Lá, você pode comprar o aplicativo ou renovar sua licença.

Página do Kaspersky Embedded Systems Security na Base de dados de conhecimento

A Base de Dados de Conhecimento é uma seção do site de Suporte Técnico.

A página do Kaspersky Embedded Systems Security na Base de Dados de Conhecimento https://support.kaspersky.com/kess2/ inclui artigos que fornecem informações úteis, recomendações e respostas a perguntas frequentes sobre como comprar, instalar e usar o aplicativo.

Os artigos da Base de Dados de Conhecimento podem responder a perguntas relacionadas não só com o Kaspersky Embedded Systems Security mas também com outros aplicativos da Kaspersky Lab. Os artigos da Base de Dados de Conhecimento podem também incluir notícias sobre o Suporte Técnico.

Documentação do Kaspersky Embedded Systems Security

O Manual do Administrador do Kaspersky Embedded Systems Security contém informações sobre a instalação, desinstalação, definição das configurações e uso do aplicativo.

Discutindo os aplicativos da Kaspersky Lab na comunidade

Se a sua pergunta não precisar de uma resposta urgente, você poderá discuti-la com os especialistas da Kaspersky Lab e com outros usuários na nossa comunidade https://community.kaspersky.com/.

Nessa comunidade, é possível visualizar os tópicos existentes, deixar seus comentários e criar novos tópicos de discussão.

Kaspersky Embedded Systems Security

Esta seção descreve as funções, os componentes e o kit de distribuição do Kaspersky Embedded Systems Security, e fornece uma lista dos requisitos de hardware e software do Kaspersky Embedded Systems Security.

Neste capítulo

Sobre o Kaspersky Embedded Systems Security 23

O que há de novo 25

Kit de distribuição 25

Requisitos de hardware e software 28

Requisitos e limitações funcionais 30

Sobre o Kaspersky Embedded Systems Security

O Kaspersky Embedded Systems Security protege computadores e outros sistemas incorporados do Microsoft® Windows contra vírus e outras ameaças de computador. Os usuários do Kaspersky Embedded Systems Security são administradores da rede corporativa e especialistas responsáveis pela proteção antivírus da rede corporativa.

Você pode instalar o Kaspersky Embedded Systems Security em uma variedade de sistemas incorporados do Windows, incluindo os seguintes tipos de dispositivos:

- Caixas eletrônicos;
- PDV (pontos de venda).

O Kaspersky Embedded Systems Security pode ser gerenciado das seguintes formas:

- Por meio do Console do Aplicativo instalado no mesmo computador em que o Kaspersky Embedded Systems Security está instalado, ou em um computador diferente.
- Usando comandos na linha de comandos.
- Por meio do Console de Administração do Kaspersky Security Center.

O aplicativo Kaspersky Security Center também pode ser usado para a administração centralizada de vários computadores executando o Kaspersky Embedded Systems Security.

É possível examinar os Contadores de desempenho do Kaspersky Embedded Systems Security para o aplicativo "Monitor do Sistema", além de Medidores e interceptações SNMP.

Componentes e funções do Kaspersky Embedded Systems Security

O aplicativo inclui os seguintes componentes:

- **Proteção em Tempo Real**. O Kaspersky Embedded Systems Security verifica objetos quando eles são acessados. O Kaspersky Embedded Systems Security verifica os seguintes objetos:
  - Arquivos;

  - Fluxos alternativos do sistema de arquivos (Fluxos NTFS);
  - Registros mestres de inicialização e setores de inicialização nos discos rígidos locais e unidades removíveis.
- **Verificação por Demanda**. O Kaspersky Embedded Systems Security executa uma única verificação da área especificada quanto à existência de vírus e outras ameaças à segurança do computador. O aplicativo verifica arquivos, RAM e objetos de execução automática em um computador protegido.
- **Controle de Inicialização de Aplicativos**. O componente rastreia todas as tentativas dos usuários de iniciar os aplicativos e controla as inicializações de aplicativos em um computador protegido.
- **Controle de Dispositivos**. O componente controla o registro e o uso de dispositivos de armazenamento em massa e unidades de CD/DVD para proteger o computador contra ameaças à segurança que possam surgir enquanto os arquivos são trocados com pendrives conectados por USB ou outros tipos de dispositivo externo.
- **Gerenciamento de Firewall**. Este componente fornece a capacidade de gerenciar o Firewall do Windows: definir configurações e regras de Firewall do sistema operacional e bloquear qualquer possibilidade de configuração externa do Firewall.
- **Monitor de Integridade de Arquivos**. O Kaspersky Embedded Systems Security detecta mudanças nos arquivos dentro dos escopos de monitoramento especificados nas configurações da tarefa. Essas mudanças podem indicar uma violação de segurança no computador protegido.
- **Inspeção de Log**. Este componente monitora a integridade do ambiente protegido com base nos resultados de uma inspeção dos logs de evento do Windows.

As funções a seguir são implementadas no aplicativo:

- **Atualização do Banco de Dados e Atualização de módulos de software**. O Kaspersky Embedded Systems Security baixa atualizações para os bancos de dados e módulos do aplicativo a partir de servidores de atualização FTP ou HTTP da Kaspersky Lab, do Servidor de Administração do Kaspersky Security Center ou de outras fontes de atualização.
- **Quarentena**. O Kaspersky Embedded Systems Security coloca em Quarentena objetos possivelmente infectados movendo esses objetos da sua localização original para a pasta da *Quarentena*. Por questões de segurança, os objetos são armazenados na pasta da Quarentena em formato criptografado.
- **Backup**. O Kaspersky Embedded Systems Security armazena cópias criptografadas de objetos classificados como *Infectados* no *Backup* antes de desinfectá-los ou excluí-los.
- **Notificações do administrador e dos usuários**. Você pode configurar o aplicativo para notificar o administrador e os usuários que acessam o computador protegido sobre eventos na operação do Kaspersky Embedded Systems Security e no status da proteção de antivírus no computador.
- **Configurações de importação e exportação**. Você pode exportar as configurações do Kaspersky Embedded Systems Security para um arquivo de configuração XML e importar configurações para o Kaspersky Embedded Systems Security a partir do arquivo de configuração. É possível salvar todas as configurações do aplicativo ou apenas aquelas de componentes individuais como um arquivo de configuração.
- **Aplicando modelos**. É possível definir manualmente as configurações de segurança de um nó na árvore ou em uma lista dos recursos de arquivos de computador e salvar os valores das configurações definidas como um modelo. Esse modelo pode então ser usado para definir as configurações de segurança de outros nós nas tarefas de proteção e de verificação do Kaspersky Embedded Systems Security.
- **Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security**. É possível configurar os direitos para gerenciar o Kaspersky Embedded Systems Security e os serviços do Windows registrados pelo aplicativo, para usuários e grupos deles.

- **Gravação de eventos no log de eventos de aplicativo**. O Kaspersky Embedded Systems Security registra informações sobre as configurações dos componentes de software, o status atual de tarefas, eventos que ocorreram durante a sua execução, eventos associados ao gerenciamento do Kaspersky Embedded Systems Security e informações necessárias para o diagnóstico de erros no Kaspersky Embedded Systems Security.
- **Zona Confiável**. Você pode gerar a lista de exclusões da proteção ou do escopo da verificação que o Kaspersky Embedded Systems Security aplicará nas tarefas de proteção por demanda e em tempo real.
- **Prevenção de Exploits**. É possível proteger a memória do processo contra exploits usando um agente injetado no processo.

O que há de novo

O Kaspersky Embedded Systems Security oferece os seguintes novos recursos e aprimoramentos:

- Suporte para novas versões de sistemas operacionais Microsoft Windows.

  Windows 10 Redstone 6 (x32 e x64).
- O código de ativação completo não pode ser visualizado na GUI do aplicativo.

  O código de ativação já acrescentado fica parcialmente escondido enquanto exibido na GUI do aplicativo e não pode ser visualizado completamente por nenhum usuário.

Kit de distribuição

O kit de distribuição inclui o aplicativo de boas-vindas que permite executar as seguintes ações:

- Iniciar o Assistente de instalação do Kaspersky Embedded Systems Security.
- Iniciar o Assistente de instalação do Console do Kaspersky Embedded Systems Security.
- Iniciar o Assistente de instalação que instalará o Plug-in de Administração do Kaspersky Embedded Systems Security para gerenciar o aplicativo por meio do Kaspersky Security Center.
- Ler o Manual do Administrador.
- Acessar a página do Kaspersky Embedded Systems Security no site da Kaspersky Lab.
- Visitar o site do Suporte Técnico https://support.kaspersky.com.br.
- Leia as informações sobre a versão atual do Kaspersky Embedded Systems Security.

A pasta \console contêm arquivos para instalação do Console do Aplicativo (conjunto de componentes “Ferramentas de Administração do Kaspersky Embedded Systems Security”).

A pasta \product contém:

- Arquivos para a instalação dos componentes do Kaspersky Embedded Systems Security em um computador que executa um sistema operacional Microsoft Windows de 32 bits ou de 64 bits.
- Arquivo para a instalação do Plug-in de Administração para gerenciar o Kaspersky Embedded Systems Security por meio do Kaspersky Security Center.

- Arquivo compactado de bancos de dados de antivírus atuais no momento do lançamento do aplicativo.
- Arquivo com o texto do Contrato de Licença do Usuário Final e Política de Privacidade.

A pasta \product_no_avbases contém arquivos de instalação de componentes do Kaspersky Embedded Systems Security e do Plug-in de Administração sem os bancos de dados de antivírus.

A pasta \setup contém os arquivos de inicialização do programa de boas-vindas.

Os arquivos do kit de distribuição são armazenados em pastas diferentes, dependendo do uso pretendido (consulte a tabela abaixo).

Tabela 2. Arquivos do kit de distribuição do Kaspersky Embedded Systems Security

Arquivo	Finalidade
autorun.inf	Arquivo de execução automática para o Assistente de instalação do Kaspersky Embedded Systems Security ao instalar o aplicativo a partir de mídias removíveis.
ess_admin_guide_pt.pdf	Manual do Administrador.
release_notes.txt	O arquivo contém informações da versão.
setup.exe	Arquivo de inicialização do programa de boas-vindas (inicia setup.hta).
\console\esstools_x86(x64).msi	Pacote do Windows Installer; instala o Console do Aplicativo no computador protegido.
\console\setup.exe	O arquivo que inicia o assistente de configuração para o conjunto de componentes "Ferramentas de administração" (incluindo o Console do Aplicativo); inicia o arquivo do pacote de instalação esstools.msi usando as configurações especificadas no assistente de configuração.
\product\bases.cab	Arquivo comprimido dos bancos de dados de antivírus atuais do antivírus no momento da liberação do aplicativo.
\product\setup.exe	O arquivo para instalação do Kaspersky Embedded Systems Security no computador protegido por meio do assistente; ele inicializa o arquivo do pacote de instalação ess.msi com as configurações de instalação especificadas no assistente.
\product\ess_x86(x64).msi	Pacote do Windows Installer; instala o Kaspersky Embedded Systems Security no computador protegido.
\product\ess.kud	Arquivo no formato Kaspersky Unicode Definition com uma descrição do pacote de instalação para a instalação remota do Kaspersky Embedded Systems Security através do Kaspersky Security Center.
\product\klcfginst.exe	Instalador do Plug-in de Administração para gerenciar o Kaspersky Embedded Systems Security por meio do Kaspersky Security Center. Instale o Plug-in de Administração em cada computador em que o Console de Administração do Kaspersky Security Center está instalado se planejar usá-lo para gerenciar o Kaspersky Embedded Systems Security.
\product\license.txt	Texto do Contrato de Licença do Usuário Final e da Política de Privacidade.

Arquivo	Finalidade
\product\migration.txt	O arquivo descreve a migração de versões anteriores do aplicativo.
\setup\setup.hta	Arquivo de inicialização do programa de boas-vindas.

Requisitos de hardware e software

Antes de instalar o Kaspersky Embedded Systems Security, você deve desinstalar outros aplicativos antivírus do computador.

Requisitos de software para o computador protegido

Você pode instalar o Kaspersky Embedded Systems Security em um computador com sistema operacional Microsoft Windows de 32 ou 64 bits.

O Windows Installer 3.1 é necessário para uma instalação e funcionamento adequados do aplicativo em um computador com sistema operacional Microsoft Windows XP.

Para instalar e usar o Kaspersky Embedded Systems Security nos computadores com sistemas operacionais incorporados, é necessário o componente Gerenciador de Filtro.

Você pode instalar o Kaspersky Embedded Systems Security em um computador com um dos seguintes sistemas operacionais Microsoft Windows de 32 ou 64 bits:

- Windows XP Embedded SP3 (32 bits)
- Windows Embedded POSReady 2009 (32 bits)
- Windows XP Professional SP2 / SP3 (32 bits, 64 bits)
- Windows Embedded Standard 7 SP1 (32 bits, 64 bits)
- Windows Embedded Enterprise 7 SP1 (32 bits, 64 bits)
- Windows Embedded POSReady 7 (32 bits, 64 bits)
- Windows 7 Professional / Enterprise SP1 (32 bits, 64 bits)
- Windows Embedded 8.1 Industry Professional / Enterprise (32 bits, 64 bits)
- Windows Embedded 8.0 Standard (32 bits, 64 bits)
- Windows 8 Professional / Enterprise (32 bits, 64 bits)
- Windows 8.1 Professional / Enterprise (32 bits, 64 bits)
- Windows 10 Professional / Enterprise (32 bits, 64 bits)
- Windows 10 IoT Enterprise (32 bits, 64 bits)
- Windows 10 Redstone 1 Professional / Enterprise / IoT Enterprise (32 bits, 64 bits)
- Windows 10 Redstone 2 Professional / Enterprise / IoT Enterprise (32 bits, 64 bits)
- Windows 10 Redstone 3 Professional / Enterprise / IoT Enterprise (32 bits, 64 bits)

- Windows 10 Redstone 4 Professional / Enterprise / IoT Enterprise (32 bits, 64 bits)
- Windows 10 Redstone 5 Professional / Enterprise / IoT Enterprise (32 bits, 64 bits)
- Windows 10 Redstone 6 Professional / Enterprise / IoT Enterprise (32 bits, 64 bits)

Requisitos de hardware para o computador protegido

Os requisitos de hardware para o computador protegido variam dependendo do sistema operacional Windows instalado:

- Requisitos de hardware para um computador com sistema operacional Windows XP (32/64 bits), Windows 7 (32 bits), Windows 8 (32 bits), Windows Embedded XP, Windows Embedded POSReady 2009 ou Windows Embedded POSReady 7:
  - Configuração mínima:
    - Requisitos de espaço em disco:
      - Para instalar o componente de Controle de Inicialização de Aplicativos – 50 MB;
      - Para instalar todos os componentes do Kaspersky Embedded Systems Security – 2 GB.
    - RAM:
      - 256 MB para instalar apenas o componente do Controle de Inicialização de Aplicativos no computador com sistema operacional Microsoft Windows.
      - 512 MB para executar a instalação completa de todos os componentes.
    - Requisitos de processador:
      - para sistemas operacionais Microsoft Windows de 32 bits: processador single-core de 1.4 GHz Intel® Pentium® III.
      - para sistemas operacionais Microsoft Windows de 64 bits: processador single-core de 1.4 GHz Intel Pentium IV.
  - Configuração recomendada:
    - Requisitos de espaço em disco:
      - Para instalar o componente de Controle de Inicialização de Aplicativos – 2 GB;
      - Para instalar todos os componentes do Kaspersky Embedded Systems Security – 4 GB.
    - RAM: 2 GB.
    - Requisitos de processador: processador quad-core de 2.4 GHz.
- Requisitos de hardware para um computador com sistema operacional Windows 7 (64 bits), Windows 8 (64 bits), Windows 10 (64 bits), Windows Embedded 7 ou Windows Embedded 8:
  - Configuração mínima:
    - Requisitos de espaço em disco:
      - Para instalar o componente de Controle de Inicialização de Aplicativos – 50 MB;
      - Para instalar todos os componentes do Kaspersky Embedded Systems Security – 2 GB.
    - RAM: 1 GB.
    - Requisitos de processador:
      - para sistemas operacionais Microsoft Windows de 32 bits: processador single-core de 1.4 GHz

Intel Pentium III.

- para sistemas operacionais Microsoft Windows de 64 bits: processador single-core de 1.4 GHz Intel Pentium IV.

- Configuração recomendada
  - Requisitos de espaço em disco:
    - Para instalar o componente de Controle de Inicialização de Aplicativos – 2 GB;
    - Para instalar todos os componentes do Kaspersky Embedded Systems Security – 4 GB.
  - RAM: 2 GB.
  - Requisitos de processador: processador quad-core de 2.4 GHz.

Requisitos e limitações funcionais

Esta seção descreve os requisitos funcionais adicionais e as limitações existentes dos componentes do Kaspersky Embedded Systems Security.

Nesta seção

Instalação e desinstalação 30
Monitor de Integridade de Arquivos 31
Gerenciamento de Firewall 31
Outras limitações 32

Instalação e desinstalação

- Durante a instalação do aplicativo um aviso será exibido se um novo caminho para a pasta de instalação do Kaspersky Embedded Systems Security contiver mais de 150 símbolos. O aviso não afeta o processo de instalação:o Kaspersky Embedded Systems Security será instalado e executado com êxito.
- Para a instalação do componente de suporte do protocolo SNMP, o serviço SNMP deve ser reiniciado se estiver em execução.
- Para a instalação e o uso do Kaspersky Embedded Systems Security no dispositivo gerenciado pelo sistema operacional incorporado, o componente Gerenciador de Filtro deve ser instalado.
- A instalação das Ferramentas de Administração do Kaspersky Embedded Systems Security não está disponível por meio das políticas de grupo do Microsoft Active Directory®.
- Ao instalar o aplicativo em computadores executando sistemas operacionais mais antigos que não podem ser atualizados regularmente, é necessário verificar os seguintes certificados de raiz: DigiCert Assured ID Root CA, DigiCert_High_Assurance_EV_Root_CA, DigiCertAssuredIDRootCA. A falta dos certificados especificados pode ocasionar o funcionamento incorreto do aplicativo. Recomenda-se instalar os certificados especificados de qualquer modo possível.
- O Console do Kaspersky Embedded Systems Security não pode ser desinstalado pelo menu **Iniciar**. É possível desinstalar o Console do Kaspersky Embedded Systems Security usando o link na janela Adicionar/Remover Programas.

Monitor de Integridade de Arquivos

Por padrão, o Monitor de Integridade de Arquivos não monitora alterações em pastas do sistema ou em arquivos de manutenção do sistema de arquivos, para evitar que informações sobre alterações rotineiras de arquivos, executadas constantemente pelo sistema operacional, sejam inseridas em relatórios de tarefas. O usuário não pode incluir manualmente tais pastas no escopo de monitoramento.

As seguintes pastas e os seguintes arquivos são excluídos do escopo de monitoramento:

- Arquivos de manutenção NTFS com id de arquivo de 0 a 33
- "%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\\"

O aplicativo exclui as pastas de nível superior.

O componente não monitora alterações em arquivos que ignoram o sistema de arquivos ReFS/NTFS (alterações em arquivos feitas pela BIOS, LiveCD etc.).

Gerenciamento de Firewall

- Trabalhar com endereços IP no formato IPv6 não está disponível quando o escopo especificado de regra aplicada consiste em um endereço.
- As regras de política predefinidas de Firewall oferecem a execução de cenários básicos de interação entre computadores locais e o Servidor de Administração. Para o uso completo das funções do Kaspersky

Security Center, é necessário configurar as regras para as portas manualmente. As informações sobre números de portas, protocolos e as suas funções estão contidas na Base de Dados de Conhecimento do Kaspersky Security Center (artigo ID: 9297).

- O aplicativo não controla a modificação das regras do Firewall do Windows e dos grupos de regras durante as consultas detalhadas da tarefa de gerenciamento do Firewall se tais regras não tiverem sido adicionadas à configuração da tarefa após a instalação do aplicativo. Para atualizar o status e incluir tais regras, a tarefa de gerenciamento de Firewall deve ser reiniciada.
- Quando a tarefa de Gerenciamento de Firewall for iniciada, os seguintes tipos de regras são automaticamente removidas das configurações do firewall do sistema operacional:
  - regras de negação;
  - regras que monitoram o tráfego de saída.

Outras limitações

Verificação por Demanda, Proteção de Arquivos em Tempo Real:

- A verificação de dispositivos MTP conectados não está disponível.
- A verificação de objeto de arquivo compactado não está disponível sem a verificação do arquivo compactado SFX: se a verificação do arquivo compactado estiver ativa nas configurações de proteção do Kaspersky Embedded Systems Security, o aplicativo verifica objetos automaticamente nos arquivos compactados e nos arquivos compactados SFX. A verificação de arquivos compactados SFX sem verificação de arquivos compactados está disponível.

Licenciamento:

- A ativação do aplicativo com a chave por meio do Assistente de configuração não está disponível se a chave for armazenada no disco, criado com o comando SUBST, ou se o caminho de rede para o arquivo de chave for especificado.

Atualizações:

- Depois da instalação das atualizações de módulos críticos do Kaspersky Embedded Systems Security, o ícone do aplicativo é ocultado por padrão.
- KLRAMDISK não é compatível em computadores executando o sistema operacional Windows XP ou Windows 2003.

Interface:

- Se você usar a filtragem no Console do Aplicativo na Quarentena, Backup, Log de auditoria do sistema ou Log de tarefas, o caso deve ser mantido.
- É possível usar apenas uma máscara e apenas no final do caminho ao configurar o escopo da proteção ou da verificação no Console do Aplicativo. Exemplos de uso correto de máscara: "C:\Temp\Temp*", ou "C:\Temp\Temp???.doc", ou "C:\Temp\Temp*.doc". A limitação não afeta a configuração da Zona Confiável.

Segurança:

- Se o Controle de Conta de Usuário nas configurações do sistema operacional for ativado, uma conta de usuário deve ser parte do grupo de Administradores KAVWSEE para abrir o Console do Aplicativo clicando duas vezes no ícone do aplicativo na área de notificação da bandeja de aplicativos. Em outro caso, será necessário efetuar o login como um usuário que possa abrir a Interface de diagnóstico compacta ou o

snap-in do Console de Gerenciamento da Microsoft.

- A desinstalação do aplicativo pela janela **Programas e Recursos** do Microsoft Windows não está disponível se o Controle de Conta de Usuário estiver ativo.

Integração com o Kaspersky Security Center:

- O Servidor de Administração verifica a validade das atualizações do banco de dados ao receber os pacotes de atualização, e antes de enviar as atualizações aos computadores da rede. O Servidor de Administração não verifica a validade das atualizações de módulo de software recebidas.
- Assegure-se de que as caixas de seleção necessárias estejam selecionadas nas configurações de Interação com o Servidor de Administração ao usar os componentes que transmitem dados dinamicamente alterados ao Kaspersky Security Center com a ajuda de listas de rede (Quarentena, Backup).

Prevenção de Exploits:

- A Prevenção de Exploits não está disponível se as bibliotecas apphelp.dll não forem carregadas na configuração de ambiente atual.
- O componente de Prevenção de Exploits é incompatível com o utilitário Microsoft EMET em computadores que executam o sistema operacional Microsoft Windows 10: o Kaspersky Embedded Systems Security bloqueia o EMET se o componente de Prevenção de Exploits estiver sendo instalado em um computador em que o EMET estiver instalado.

Instalação e remoção do aplicativo

Esta seção fornece instruções passo a passo para instalar e remover o Kaspersky Embedded Systems Security.

Neste capítulo

Códigos de componentes de software do Kaspersky Embedded Systems Security para o serviço do Windows Installer 34
Modificações de sistema após a instalação do Kaspersky Embedded Systems Security 38
Processos do Kaspersky Embedded Systems Security 41
Configurações de instalação e desinstalação e opções de linha de comando para o serviço do Windows Installer 41
Logs de instalação e desinstalação do Kaspersky Embedded Systems Security 44
Planejamento da instalação 45
Instalação e desinstalação do aplicativo usando um assistente 47
Instalação e desinstalação do aplicativo a partir da linha de comando 61
Instalação e desinstalação do aplicativo usando o Kaspersky Security Center 66
Instalação e desinstalação via políticas de grupo do Active Directory 71
Verificação das funções do Kaspersky Embedded Systems Security. Uso do vírus de teste EICAR 73

Códigos de componentes de software do Kaspersky Embedded Systems Security para o serviço do Windows Installer

Por padrão, os arquivos \product\ess_x86.msi e \product\ess_x64.msi são projetados para instalar todos os componentes do Kaspersky Embedded Systems Security. Você pode instalar esses componentes incluindo-os em uma instalação personalizada.

Os arquivos \console\esstools_x86.msi e \console\esstools_x64.msi instalam todos os componentes de software no conjunto de "Ferramentas de Administração".

As seções a seguir enumeram os códigos dos componentes do Kaspersky Embedded Systems Security para o serviço do Windows Installer. Estes códigos podem ser usados para definir uma lista de componentes a serem instalados ao instalar o Kaspersky Embedded Systems Security na linha de comando.

Nesta seção

Componentes de software do Kaspersky Embedded Systems Security 35
Conjunto de “Ferramentas de administração” de componentes de software 37

Componentes de software do Kaspersky Embedded Systems Security

A tabela a seguir contém os códigos e descrições dos componentes de software do Kaspersky Embedded Systems Security.

Tabela 3. Descrição dos componentes de software do Kaspersky Embedded Systems Security

Componente	Identificador	Funções realizadas
Funcionalidade básica	Core	Este componente contém o conjunto de funções básicas do aplicativo e assegura a sua operação.
Controle de Inicialização de Aplicativos	AppCtrl	Este componente monitora as tentativas do usuário de executar aplicativos e permite ou nega a inicialização deles conforme as regras de Controle de Inicialização de Aplicativos definidas. É implementado na tarefa de Controle de Inicialização de Aplicativos.
Controle de Dispositivos	DevCtrl	Este componente rastreia tentativas de conexão de dispositivos de armazenamento em massa via USB a um computador protegido e permite ou nega o uso desses dispositivos de acordo com as regras de controle de dispositivos especificadas. O componente é implementado na tarefa Controle de Dispositivos.
Proteção antivírus	AVProtection	Este componente fornece proteção antivírus e contém os componentes a seguir: • Verificação por Demanda • Proteção de Arquivos em Tempo Real
Verificação por Demanda	Ods	Este componente instala arquivos de sistema do Kaspersky Embedded Systems Security e oferece tarefas de Verificação por Demanda (verificação de objetos no computador protegido mediante solicitação). Se outros componentes do Kaspersky Embedded Systems Security forem especificados durante a instalação do Kaspersky Embedded Systems Security na linha de comando, mas o componente Core não for especificado, o componente Core será instalado automaticamente.

Componente	Identificador	Funções realizadas
Proteção de Arquivos em Tempo Real	Oas	Este componente executa verificações de antivírus de arquivos no computador protegido quando estes arquivos são acessados. Ele implementa a tarefa de Proteção de Arquivos em Tempo Real.
Uso da Kaspersky Security Network	KSN	Este componente fornece proteção com base em tecnologias na nuvem da Kaspersky Lab. Ele implementa a tarefa de Uso da KSN (enviando solicitações para e recebendo conclusões do serviço Kaspersky Security Network).
Monitor de Integridade de Arquivos	Fim	Este componente registra as operações executadas em arquivos no escopo de monitoramento especificado. O componente implementa a tarefa do Monitor de Integridade de Arquivos.
Prevenção de Exploits	AntiExploit	Este componente possibilita gerenciar as configurações para proteger a memória utilizada pelos processos na memória de um computador protegido.
Gerenciamento de Firewall	Firewall	Este componente possibilita gerenciar o Firewall do Windows por meio da interface gráfica do usuário do Kaspersky Embedded Systems Security. O componente implementa a tarefa de Gerenciamento de Firewall.
Módulo para a integração com o Agente de Rede do Kaspersky Security Center	AKIntegration	Este componente fornece uma conexão entre o Kaspersky Embedded Systems Security e o Agente de rede do Kaspersky Security Center. Você pode instalar este componente no computador protegido caso pretenda gerenciar o aplicativo através do Kaspersky Security Center.
Inspeção de Log	LogInspector	Este componente monitora a integridade do ambiente protegido com base nos resultados de uma inspeção dos logs de evento do Windows.

Componente	Identificador	Funções realizadas
Conjunto de contadores de desempenho do "Monitor do Sistema"	PerfMonCounters	Este componente instala um conjunto de contadores de desempenho do Monitor do Sistema. Os contadores de desempenho permitem a medição do desempenho do Kaspersky Embedded Systems Security e a localização de gargalos potenciais no computador quando o Kaspersky Embedded Systems Security for usado com outros programas.
Contadores e interceptações SNMP	SnmpSupport	Este componente publica contadores e interceptações do Kaspersky Embedded Systems Security através do Simple Network Management Protocol (SNMP) no Microsoft Windows. Este componente pode ser instalado no computador protegido apenas se o serviço Microsoft SNMP for instalado no mesmo computador.
Ícone do Kaspersky Embedded Systems Security na área de notificação	TrayApp	Este componente exibe o ícone do Kaspersky Embedded Systems Security na área de notificação da bandeja de tarefas do computador protegido. O ícone do Kaspersky Embedded Systems Security exibe o status da proteção do computador e pode ser usado para abrir o Console do Kaspersky Embedded Systems Security no Console de Gerenciamento Microsoft (se instalado) e na janela **Sobre o aplicativo**.

Conjunto de “Ferramentas de administração” de componentes de software

A tabela a seguir contém códigos e descrições do conjunto de componentes de software de “Ferramentas de administração”.

Tabela 4. Descrição dos componentes de software das "Ferramentas de administração"

Componente	Código	Funções do componente
Snap-ins do Kaspersky Embedded Systems Security	MmcSnapin	Este componente instala o snap-in do Console de Gerenciamento da Microsoft através do Console do Kaspersky Embedded Systems Security. Se outros componentes forem especificados durante a instalação das “Ferramentas de administração” a partir da linha de comando e o componente MmcSnapin não for especificado, o componente será instalado automaticamente.

Componente	Código	Funções do componente
Ajuda	Help	Este é um arquivo de ajuda .chm, salvo na pasta com os arquivos das Ferramentas de administração do Kaspersky Embedded Systems Security. Você pode abrir o arquivo de Ajuda usando o menu **Iniciar** ou clicando na tecla **F1** com a janela do Console do Aplicativo aberta.
Documentação	Help	O Kaspersky Embedded Systems Security adiciona um atalho para o site da Kaspersky Lab onde o Manual do Administrador está disponível em formato PDF. O atalho está disponível no menu **Iniciar**.

Modificações de sistema após a instalação do Kaspersky Embedded Systems Security

Quando o Kaspersky Embedded Systems Security e o conjunto de “Ferramentas de administração” (incluindo o Console do Aplicativo) forem instalados juntos, o serviço do Windows Installer fará as seguintes modificações no computador protegido:

- Pastas do Kaspersky Embedded Systems Security são criadas no computador protegido e no computador em que o Console do Aplicativo for instalado.
- Os serviços do Kaspersky Embedded Systems Security são registrados.
- Um grupo de usuário do Kaspersky Embedded Systems Security é criado.
- Chaves do Kaspersky Embedded Systems Security são registradas no registro de sistema.

Estas modificações são descritas abaixo.

Pastas do Kaspersky Embedded Systems Security em um computador protegido

Quando o Kaspersky Embedded Systems Security é instalado, as seguintes pastas são criadas em um computador protegido:

- A pasta da instalação padrão do Kaspersky Embedded Systems Security, que contém os arquivos executáveis do Kaspersky Embedded Systems Security depende da arquitetura do sistema operacional. Portanto, as pastas de instalação padrão são as seguintes:
  - Na versão de 32 bits do Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
  - Na versão de 64 bits do Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- Arquivos da Management Information Base (MIB), que contêm uma descrição dos contadores e hooks publicados pelo Kaspersky Embedded Systems Security através do protocolo SMNP:
  - %Kaspersky Embedded Systems Security%\mibs
- Versões de 64 bits dos arquivos executáveis do Kaspersky Embedded Systems Security (a pasta será criada somente durante a instalação do Kaspersky Embedded Systems Security na versão de 64 bits do Microsoft Windows):

    - %Kaspersky Embedded Systems Security%\x64
- Arquivos de serviço do Kaspersky Embedded Systems Security:
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Data\
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Settings\
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Dskm\
- Arquivos com configurações para fontes de atualização:
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Update\
- Atualizações de bancos de dados e módulos de software baixados usando a tarefa Copiar atualizações (a pasta será criada na primeira vez que as atualizações forem baixadas usando a tarefa Copiar atualizações):
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Update\Distribution\
- Logs de tarefas e log de auditoria do sistema:
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports\
- Conjunto de bancos de dados em uso:
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Current\
- Cópias de backup dos bancos de dados; elas serão substituídas sempre que os bancos de dados forem atualizados:
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Backup\
- Arquivos temporários criados durante a execução das tarefas de atualização:
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Temp\
- Objetos na Quarentena (pasta padrão):
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Quarantine\
- Objetos no backup (pasta padrão):
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Backup\
- Objetos restaurados do backup e da quarentena (pasta padrão para objetos restaurados):
    - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored\

Pastas criadas durante a instalação do Console do Aplicativo

As pastas de instalação padrão do Console do Aplicativo que contém os arquivos de "Ferramentas de

administração" dependem da arquitetura do sistema operacional. Portanto, as pastas de instalação padrão são as seguintes:

- Na versão de 32 bits do Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\
- Na versão de 64 bits do Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\

Serviços do Kaspersky Embedded Systems Security

Os serviços do Kaspersky Embedded Systems Security a seguir são inicializados utilizando a conta do sistema local (SYSTEM):

- Kaspersky Security Service (KAVFS) – serviço essencial do Kaspersky Embedded Systems Security que gerencia tarefas e fluxos de trabalho do Kaspersky Embedded Systems Security.
- Kaspersky Security Management Service (KAVFSGT) – este serviço é destinado ao gerenciamento de aplicativos do Kaspersky Embedded Systems Security por meio do Console do Aplicativo.
- Serviço de Kaspersky Security Exploit Prevention (KAVFSSLP) – um serviço que funciona como um intermediário para comunicar as configurações de segurança aos agentes de segurança externos e para receber dados sobre eventos de segurança.

Grupo Kaspersky Embedded Systems Security

Administradores de ESS é um grupo no computador protegido, que possui acesso total ao Kaspersky Security Management Service e a todas as funções do Kaspersky Embedded Systems Security.

Chaves do registro do sistema

Quando o Kaspersky Embedded Systems Security é instalado, as seguintes chaves do registro do sistema são criadas:

- Propriedades do Kaspersky Embedded Systems Security:[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Configurações de log de eventos do Kaspersky Embedded Systems Security (Log de Eventos Kaspersky): [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Propriedades do serviço de gerenciamento do Kaspersky Embedded Systems Security: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- Configurações dos contadores de desempenho:
  - Na versão de 32 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - Na versão de 64 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- Configurações do componente de Suporte do Protocolo SNMP:
  - Na versão de 32 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\SnmpAgent]
  - Na versão de 64 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\SnmpAgent]
- Configurações do arquivo de despejo:

  - Na versão de 32 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\CrashDump]
  - Na versão de 64 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\CrashDump]
- Configurações do arquivo de rastreamento:
  - Na versão de 32 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\Trace]
  - Na versão de 64 bits do Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Trace]
- Configuração das tarefas e funções do aplicativo: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Environment]

Processos do Kaspersky Embedded Systems Security

O Kaspersky Embedded Systems Security inicia os processos descritos na tabela abaixo.

Tabela 5. Processos do Kaspersky Embedded Systems Security

Nome do arquivo	Finalidade
kavfswp.exe	Fluxo de trabalho do Kaspersky Embedded Systems Security
kavtray.exe	Processo para ícone de bandeja do sistema
kavfsmui.exe	Processo do componente de Interface de diagnóstico compacta
kavshell.exe	Processo do utilitário de linha de comando
kavfsrcn.exe	Processo de gerenciamento remoto do Kaspersky Embedded Systems Security
kavfs.exe	Processo do Kaspersky Security Service
kavfsgt.exe	Processos do Kaspersky Security Management Service
kavfswh.exe	Processo do Serviço de Kaspersky Security Exploit Prevention

Configurações de instalação e desinstalação e opções de linha de comando para o serviço do Windows Installer

Esta seção contém descrições das configurações para a instalação e desinstalação do Kaspersky Embedded Systems Security, seus valores padrão, chaves para alterar as configurações de instalação e seus possíveis valores. Essas chaves podem ser usadas em conjunto com as chaves padrão para o comando `msiexec` do serviço do Windows Installer ao instalar o Kaspersky Embedded Systems Security a partir da linha de comando.

Configurações de instalação e opções da linha de comando no Windows Installer

- Aceitação dos termos do Contrato de Licença do Usuário Final: você deve aceitar os termos para instalar o Kaspersky Embedded Systems Security.

  Os valores possíveis para a opção `EULA=<valor>` na linha de comando são os seguintes:

  - `0` – você não aceita os termos do Contrato de Licença do Usuário Final (valor padrão).
  - `1` – você aceita os termos do Contrato de licença do usuário final.

- Aceitação dos termos da Política de Privacidade: você deve aceitar os termos para instalar o Kaspersky Embedded Systems Security.

  Os valores possíveis para a opção `PRIVACYPOLICY=<valor>` na linha de comando são os seguintes:

  - `0` – você não aceita os termos da Política de Privacidade (valor padrão).
  - `1` – você aceita os termos da Política de Privacidade.

- Instalação do Kaspersky Embedded Systems Security com uma verificação preliminar dos processos ativos e setores de inicialização dos discos locais.

  Os valores possíveis para a opção `PRESCAN=<valor>` na linha de comando são os seguintes:

  - `0` – não executar uma verificação preliminar de processos ativos e setores de inicialização de discos locais durante a instalação (valor padrão).
  - `1` – executar uma verificação preliminar de processos ativos e setores de inicialização de discos locais durante a instalação.

- Pasta de destino onde os arquivos do Kaspersky Embedded Systems Security serão salvos durante a instalação. Uma pasta diferente pode ser especificada.

  Os valores padrão da opção `INSTALLDIR=<caminho completo para a pasta>` na linha de comando são os seguintes:

  - Kaspersky Embedded Systems Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - Ferramentas de administração: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
  - Na versão de 64 bits do Microsoft Windows: %ProgramFiles(x86)%

- A tarefa de Proteção de Arquivos em Tempo Real é iniciada imediatamente após a inicialização do Kaspersky Embedded Systems Security. Ative esta configuração para iniciar a Proteção de Arquivos em Tempo Real na inicialização do Kaspersky Embedded Systems Security (recomendado).

  Os valores possíveis para a opção `RUNRTP=<valor>` na linha de comando são os seguintes:

  - `1` – iniciar (valor padrão).
  - `0` – não iniciar.

- Exclusões de proteção recomendadas pela Microsoft Corporation. Na tarefa Proteção de Arquivos em Tempo Real, exclua do escopo da proteção objetos no computador que são recomendados pela Microsoft Corporation para exclusão. Alguns aplicativos no computador podem ficar instáveis quando o aplicativo de antivírus intercepta ou modifica arquivos usados por esses aplicativos. Por exemplo, a Microsoft Corporation inclui alguns aplicativos de controladores de domínio na lista de tais objetos.

  Os valores possíveis para a opção `ADDMSEXCLUSION=<valor>` na linha de comando são os seguintes:

- `1` – excluir (valor padrão).
- `0` – não excluir.

- Objetos excluídos do escopo da verificação segundo as recomendações da Kaspersky Lab. Na tarefa Proteção de Arquivos em Tempo Real, exclua do escopo da proteção objetos no computador que são recomendados pela Kaspersky Lab para exclusão.

  Os valores possíveis para a opção `ADDKLEXCLUSION=<valor>` na linha de comando são os seguintes:

  - `1` – excluir (valor padrão).
  - `0` – não excluir.

- Permitir a conexão remota ao Console do Aplicativo. Por padrão, a conexão remota ao Console do Aplicativo instalado no computador protegido não é permitida. Durante a instalação, você pode permitir a conexão. O Kaspersky Embedded Systems Security cria regras de permissão para o processo kavfsgt.exe usando o protocolo TCP para todas as portas.

  Os valores possíveis para a opção `ALLOWREMOTECON=<valor>` na linha de comando são os seguintes:

  - `1` – permitir.
  - `0` – negar (valor padrão).

- Caminho do arquivo de chave. Por padrão, o instalador do Windows tenta encontrar o arquivo com a extensão .key na pasta \product do kit de distribuição. Se a pasta \product contiver vários arquivos de chave, o instalador do Windows selecionará o arquivo de chave com a data de expiração mais avançada. Um arquivo de chave pode ser salvo antecipadamente na pasta \product ou especificando outro caminho para o arquivo de chave usando a configuração **Adicionar chave**. É possível adicionar uma chave depois que o Kaspersky Embedded Systems Security tiver sido instalado usando uma ferramenta de administração de sua escolha: por exemplo, o Console do Aplicativo. Se você não adicionar uma chave durante a instalação do aplicativo, o Kaspersky Embedded Systems Security não funcionará.

- Caminho do arquivo de configuração. O Kaspersky Embedded Systems Security importa configurações do arquivo de configuração especificado criado no aplicativo. O Kaspersky Embedded Systems Security não importa senhas do arquivo de configuração, por exemplo, senhas de contas para tarefas de inicialização ou senhas para conexão com um servidor proxy. Com configurações importadas, você terá que inserir todas as senhas manualmente. Se o arquivo de configuração não for especificado, o aplicativo começará a trabalhar com as configurações padrão após a configuração.

  O valor padrão de `CONFIGPATH=<nome do arquivo de configuração>` não é especificado.

- Permitindo conexões de rede para o Console do Aplicativo. Use esta opção para instalar o Kaspersky Embedded Systems Security em outro computador. É possível gerenciar remotamente a proteção de um computador a partir de outro computador com o Console do Kaspersky Embedded Systems Security instalado. A porta 135 (TCP) é aberta no firewall do Microsoft Windows, são permitidas as conexões de rede para o arquivo executável kavfsrcn.exe para o gerenciamento remoto do Kaspersky Embedded Systems Security e o acesso é concedido aos aplicativos DCOM. Após a conclusão da instalação, adicione usuários ao grupo Administradores de ESS para que eles possam gerenciar remotamente o aplicativo e permitir conexões de rede ao Kaspersky Security Management Service (arquivo kavfsgt.exe) no computador. Você pode ler mais sobre a configuração adicional quando o Console do Kaspersky Embedded Systems Security for instalado em outro computador (consulte a Seção "Configurações avançadas após a instalação do Console do Aplicativo em outro computador" na página 52).

  Os valores possíveis para a opção `ADDWFEXCLUSION=<valor>` na linha de comando são os seguintes:

  - `1` – permitir.

  - `0` – negar (valor padrão).
- Desativação da verificação de software incompatível. Use esta configuração para ativar ou desativar a verificação de software incompatível durante a instalação em segundo plano do aplicativo no computador. Independentemente do valor dessa configuração, durante a instalação do Kaspersky Embedded Systems Security, o aplicativo sempre alerta sobre outras versões do aplicativo instaladas no computador.

  Os valores possíveis para a opção `SKIPINCOMPATIBLESW=<valor>` na linha de comando são os seguintes:

  - `0` – a verificação de software incompatível é realizada (valor padrão).
  - `1` – a verificação de software incompatível não é realizada.

Configurações de desinstalação e opções de linha de comando no Windows Installer

- Restauração de objetos da quarentena.

  Os valores possíveis para a opção `RESTOREQTN=<valor>` na linha de comando são os seguintes:

  - `0` – remover o conteúdo em quarentena (valor padrão).
  - `1` – restaurar o conteúdo em quarentena para a pasta especificada pelo parâmetro RESTOREPATH na subpasta \Quarantine.
- Restauração do conteúdo do backup.

  Os valores possíveis para a opção `RESTOREBCK=<valor>` na linha de comando são os seguintes:

  - `0` – remover o conteúdo do backup (valor padrão).
  - `1` – restaurar o conteúdo do backup para a pasta especificada pelo parâmetro RESTOREPATH na subpasta \Backup.
- Insira a senha atual para confirmar a desinstalação (se a proteção de senha estiver ativa).

  O valor padrão de `UNLOCK_PASSWORD=<senha especificada>` não é especificado.
- Pasta para a objetos restaurados. Objetos restaurados serão salvos na pasta especificada:

  O valor padrão para a opção `RESTOREPATH=<caminho completo para a pasta>` na linha de comando é %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored.

Logs de instalação e desinstalação do Kaspersky Embedded Systems Security

Se o Kaspersky Embedded Systems Security for instalado ou desinstalado usando o Assistente de instalação (Desinstalação), o serviço do Windows Installer cria um log de instalação (desinstalação). Um arquivo de log ess_install_<uid>.log (onde <uid> é um identificador de log único de 8 caracteres) será salvo na pasta %temp% do usuário cuja conta foi usada para executar o arquivo setup.exe.

Se você executar a opção **Modificar ou Remover Kaspersky Embedded Systems Security 2.3 Ferramentas de Administração** para o Console do Aplicativo ou para o Kaspersky Embedded Systems Security a partir do menu **Iniciar** , um arquivo de log com o nome ess_2.3_maintenance.log será criado automaticamente na pasta %temp%.

Se o Kaspersky Embedded Systems Security for instalado ou desinstalado a partir da linha de comando, o arquivo

de log da instalação não será criado por padrão.

► *Para instalar o Kaspersky Embedded Systems Security e criar o arquivo de log no disco C:\:*

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

Planejamento da instalação

Esta seção contém a descrição do conjunto de Ferramentas de administração do Kaspersky Embedded Systems Security e de aspectos especiais de instalação e desinstalação do Kaspersky Embedded Systems Security usando um assistente (consulte a seção "Instalação e desinstalação do aplicativo usando um assistente" na página 47), a linha de comando (consulte a seção "Instalação e desinstalação do aplicativo a partir da linha de comando" na página 61), por meio do Kaspersky Security Center (consulte a seção "Instalação e desinstalação do aplicativo usando o Kaspersky Security Center" na página 66) e por meio da política de grupo do Active Directory (consulte a seção "Instalação e desinstalação via políticas de grupo do Active Directory" na página 71).

Antes de iniciar a instalação do Kaspersky Embedded Systems Security, planeje as etapas principais.

1. Determine que ferramentas de administração serão usadas para gerenciar e configurar o Kaspersky Embedded Systems Security.
2. Selecione os componentes necessários do aplicativo para instalação (consulte a seção "Códigos de componentes de software do Kaspersky Embedded Systems Security para o serviço do Windows Installer" na página 34).
3. Selecione o método de instalação.

Nesta seção

Seleção das ferramentas de administração 45
Seleção do tipo de instalação 46

Seleção das ferramentas de administração

Determine as ferramentas de administração que serão usadas para configurar e gerenciar o Kaspersky Embedded Systems Security. O Kaspersky Embedded Systems Security pode ser gerenciado usando o Console do Aplicativo, o utilitário de linha de comando e o Console de Administração do Kaspersky Security Center.

Console do Kaspersky Embedded Systems Security

O Console do Kaspersky Embedded Systems Security é um snap-in isolado adicionado ao Console de Gerenciamento da Microsoft. O Kaspersky Embedded Systems Security pode ser gerenciado por meio do Console do Aplicativo instalado no computador protegido ou em outro computador da rede corporativa.

Vários snap-ins do Kaspersky Embedded Systems Security podem ser adicionados a um Console de Gerenciamento da Microsoft aberto no modo autor para gerenciar a proteção de vários computadores nos quais o Kaspersky Embedded Systems Security esteja instalado.

O Console do Aplicativo está incluído no conjunto de componentes "Ferramentas de administração" do aplicativo.

Utilitário de linha de comando

Você pode gerenciar o Kaspersky Embedded Systems Security na linha de comando de um computador protegido.

O utilitário da linha de comando está incluído no grupo dos componentes do software Kaspersky Embedded Systems Security.

Kaspersky Security Center

Se o aplicativo do Kaspersky Security Center for usado para o gerenciamento centralizado da proteção antivírus de computadores na sua empresa, você poderá gerenciar o Kaspersky Embedded Systems Security por meio do Console de Administração do Kaspersky Security Center.

Os componentes a seguir devem ser instalados:

- **Módulo para a integração com o Agente de Rede do Kaspersky Security Center**. Este componente está incluído no grupo dos componentes do software do Kaspersky Embedded Systems Security. Ele permite a comunicação do Kaspersky Embedded Systems Security com o Agente de Rede. Instale o módulo para a integração com o Agente de Rede do Kaspersky Security Center no computador protegido.
- **Agente de Rede do Kaspersky Security Center**. Instale este componente em cada computador protegido. Esse componente suporta a interação entre o Kaspersky Embedded Systems Security instalado no computador e o Servidor de Administração do Kaspersky Security Center. O arquivo de instalação do Agente de Rede está incluído na pasta do kit de distribuição do Kaspersky Security Center.
- **Plug-in de administração do Kaspersky Embedded Systems Security 2.3**. Adicionalmente, instale o Plug-in de Administração do Kaspersky Embedded Systems Security por meio do Console de Administração no computador em que o Servidor de Administração do Kaspersky Security Center estiver instalado. Ele fornece a interface de gerenciamento de aplicativos por meio do Kaspersky Security Center. O arquivo de instalação do Plug-in de Administração, \product\klcfginst.exe, está incluído no kit de distribuição do Kaspersky Embedded Systems Security.

Seleção do tipo de instalação

Depois de especificar os componentes de software para a instalação do Kaspersky Embedded Systems Security (consulte a seção “Códigos de componentes de software do Kaspersky Embedded Systems Security para o serviço do Windows Installer” na página 34), será necessário selecionar o método de instalação do aplicativo.

Selecione o método de instalação dependendo da arquitetura de rede e das seguintes condições:

- Se você precisar de configurações especiais de instalação para o Kaspersky Embedded Systems Security ou as configurações de instalação recomendadas (consulte a seção "Configurações de instalação e desinstalação e opções de linha de comando para o serviço do Windows Installer" na página 41).
- Se as configurações de instalação forem as mesmas para todos os computadores ou específicas para cada um deles.

O Kaspersky Embedded Systems Security pode ser instalado interativamente usando o Assistente de instalação ou em modo silencioso sem a participação do usuário, e pode ser chamado executando o arquivo do pacote de instalação com as configurações de instalação a partir da linha de comando. Uma instalação remota centralizada do Kaspersky Embedded Systems Security pode ser executada usando políticas de grupo do Active Directory ou usando a tarefa de instalação remota do Kaspersky Security Center.

O Kaspersky Embedded Systems Security pode ser instalado e configurado em um único computador, com suas configurações salvas em um arquivo de configuração; o arquivo criado pode então ser usado para instalar o Kaspersky Embedded Systems Security em outros computadores. Observe que essa possibilidade não existe quando o produto é instalado usando as políticas de grupo do Active Directory.

Inicialização do assistente de instalação

O assistente de instalação pode instalar o seguinte:

- Componentes do Kaspersky Embedded Systems Security (consulte a seção "Componentes de software do Kaspersky Embedded Systems Security" na página 35) em um computador protegido a partir do arquivo \product\setup.exe incluído no kit de distribuição.
- Console do Kaspersky Embedded Systems Security (consulte a seção "Instalação do Console do Kaspersky Embedded Systems Security " na página 50) a partir do arquivo \console\setup.exe do kit de distribuição no computador protegido ou em outro host de LAN.

Executando o arquivo do pacote de instalação a partir da linha de comando com as configurações de instalação necessárias

Se o arquivo do pacote de instalação for iniciado sem opções de linha de comando, o Kaspersky Embedded Systems Security será instalado com a configuração padrão. As opções especiais do Kaspersky Embedded Systems Security podem ser usadas para modificar as configurações de instalação.

O Console do Aplicativo pode ser instalado no computador protegido e / ou na estação de trabalho do administrador.

Você também pode usar os comandos de exemplo para a instalação do Kaspersky Embedded Systems Security e do Console do Aplicativo (consulte a seção "Instalação e desinstalação do aplicativo a partir da linha de comando" na página 61).

Instalação centralizada por meio do Kaspersky Security Center

Se o Kaspersky Security Center for usado para gerenciamento da proteção antivírus dos computadores na sua rede, o Kaspersky Embedded Systems Security poderá ser instalado em vários computadores usando a tarefa de instalação remota.

Os computadores em que você quiser instalar o Kaspersky Embedded Systems Security por meio do Kaspersky Security Center (consulte a seção “Instalação e desinstalação do aplicativo usando o Kaspersky Security Center” na página 66) podem estar localizados no mesmo domínio do Kaspersky Security Center, em um domínio diferente ou não pertencer a nenhum domínio.

Instalação centralizada utilizando as políticas de grupo do Active Directory

As políticas de grupo do Active Directory podem ser usadas para instalar o Kaspersky Embedded Systems Security no computador protegido. O Console do Aplicativo pode ser instalado no computador protegido ou na estação de trabalho do administrador.

O Kaspersky Embedded Systems Security pode ser instalado usando somente as configurações de instalação recomendadas.

Os computadores nos quais o Kaspersky Embedded Systems Security for instalado usando políticas de grupo do Active Directory (consulte a seção “Instalação e desinstalação via políticas de grupo do Active Directory” na página 71) devem estar localizados no mesmo domínio e na mesma unidade organizacional. A instalação é realizada na inicialização do computador, antes de fazer login no Microsoft Windows.

Instalação e desinstalação do aplicativo usando um assistente

Esta seção descreve a instalação e desinstalação do Kaspersky Embedded Systems Security e do Console do Aplicativo por meio do assistente de instalação e contém informações sobre as configurações adicionais do

Kaspersky Embedded Systems Security e ações a serem executadas após a instalação.

Nesta seção

Instalação usando o Assistente de instalação....48
Alteração do conjunto de componentes e reparação do Kaspersky Embedded Systems Security 57
Desinstalação usando o Assistente de instalação 59

Instalação usando o Assistente de instalação

As seções a seguir contêm informações sobre a instalação do Kaspersky Embedded Systems Security e do Console do Aplicativo.

► *Para instalar e prosseguir com a utilização do Kaspersky Embedded Systems Security, siga as etapas a seguir:*

1. Instale o Kaspersky Embedded Systems Security em um computador protegido.
2. Instale o Console do Aplicativo nos computadores a partir dos quais você pretende gerenciar o Kaspersky Embedded Systems Security.
3. Se o Console do Aplicativo tiver sido instalado em algum computador na rede, além do computador protegido, execute a configuração adicional para permitir que usuários do Console do Aplicativo gerenciem remotamente o Kaspersky Embedded Systems Security.
4. Realize ações após a instalação do Kaspersky Embedded Systems Security.

Nesta seção

Instalação do Kaspersky Embedded Systems Security 48
Instalação do Console do Kaspersky Embedded Systems Security....50
Configurações avançadas após a instalação do Console do Aplicativo em outro computador....52
Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security....55

Instalação do Kaspersky Embedded Systems Security

Antes de instalar o Kaspersky Embedded Systems Security, siga as etapas a seguir:

Certifique-se de que nenhum outro programa de antivírus esteja instalado no computador.

- Certifique-se de que a conta que você está utilizando para iniciar o Assistente de instalação faça parte do grupo de administradores no computador protegido.

Após concluir as ações descritas acima, prossiga com o procedimento de instalação. Especifique as configurações para instalação do Kaspersky Embedded Systems Security de acordo com as instruções do Assistente de instalação. O processo de instalação do Kaspersky Embedded Systems Security pode ser interrompido em qualquer etapa do Assistente de instalação. Para isso, clique no botão **Cancelar** na janela do Assistente de instalação.

Você pode ler mais sobre as configurações de instalação (desinstalação) (consulte a seção "Configurações de instalação e desinstalação e opções de linha de comando para o serviço do Windows Installer" na página 41).

► *Para instalar o Kaspersky Embedded Systems Security usando o assistente de instalação:*

1. Execute o arquivo setup.exe no computador.
2. Na janela exibida, na seção **Instalação**, clique no link **os termos e condições deste EULA**.
3. Na tela de boas-vindas do Assistente de instalação do Kaspersky Embedded Systems Security, clique no botão **Avançar**.

   A janela **EULA e Política de Privacidade** é aberta.
4. Revise os termos do Contrato de Licença e da Política de Privacidade.
5. Se você concordar com os termos e as condições do Contrato de Licença do Usuário Final e da Política de Privacidade, selecione as caixasos **os termos e condições deste EULA** e **Política de Privacidade descrevendo o manuseio de dados** para prosseguir com a instalação.

   Se você não aceitar o Contrato de Licença do Usuário Final e/ou a Política de Privacidade, a instalação será interrompida.
6. Clique no botão **Avançar**.

   A janela de **Verificação rápida do computador antes da instalação** será exibida.
7. Em **Verificação rápida do computador antes da instalação**, marque a caixa de seleção **Verificar o computador quanto à presença de vírus** para verificar a memória do sistema e setores de inicialização das unidades locais do computador quanto à presença de ameaças. Clique no botão **Avançar**. Ao concluir o procedimento de verificação, o assistente abrirá uma janela reportando os resultados da verificação.

   Esta janela exibe informações sobre os objetos do computador verificado: o número total de objetos verificados, o número de ameaças detectadas, o número de objetos infectados ou possivelmente infectados detectados, o número de processos perigosos ou suspeitos removidos da memória pelo Kaspersky Embedded Systems Security e o número de processos perigosos ou suspeitos que o Kaspersky Embedded Systems Security não foi capaz de remover.

   Para ver exatamente quais objetos foram verificados, clique no botão **Lista de objetos processados**.
8. Clique no botão **Avançar** na janela **Verificação rápida do computador antes da instalação**.

   A janela **Instalação personalizada** é exibida.
9. Selecione os componentes a serem instalados.

   Por padrão, todos os componentes do Kaspersky Embedded Systems Security estão incluídos no conjunto de instalação recomendado, exceto o componente de Gerenciamento de Firewall.

   O componente de suporte do protocolo SNMP do Kaspersky Embedded Systems Security aparecerá na lista de componentes sugeridos para a instalação apenas se o serviço do Microsoft Windows SNMP estiver instalado no computador.
10. Para cancelar todas as alterações, clique no botão **Redefinir** na janela **Instalação personalizada**. Clique no botão **Avançar**.
11. Na janela **Selecionar pasta de destino**:
    - Se necessitado, especifique uma pasta à qual os arquivos do Kaspersky Embedded Systems Security

serão copiados.

- Se necessário, leia as informações sobre o espaço disponível nas unidades locais clicando no botão **Disco**.

Clique no botão **Avançar**.

12. Na janela **Configurações avançadas de instalação**, defina as seguintes configurações de instalação:
    - **Ativar a proteção em tempo real após a instalação do aplicativo**.
    - **Adicionar arquivos recomendados pela Microsoft à lista de exclusões**.
    - **Adicionar arquivo recomendado pela Kaspersky Lab à lista de exclusões**.

    Clique no botão **Avançar**.
13. Na janela **Importar configurações do arquivo de configuração**:
    a. Especifique o arquivo de configuração do qual importar as configurações do Kaspersky Embedded Systems Security a partir de um arquivo de configuração existente criado em qualquer versão anterior compatível do aplicativo.
    b. Clique no botão **Avançar**.
14. Na janela **Ativação do aplicativo**, execute uma das seguintes ações:
    - Se desejar ativar o aplicativo, especifique um arquivo de chave do Kaspersky Embedded Systems Security para a ativação do aplicativo.
    - Se quiser ativar o aplicativo mais tarde, pressione o botão **Avançar**.
    - Se um arquivo de chave tiver sido salvo anteriormente na pasta \product do kit de distribuição, o nome desse arquivo será exibido no campo **Chave**.

    > Para adicionar uma chave usando um arquivo de chave armazenado em outra pasta, especifique o arquivo de chave.

    Após o arquivo de chave ser adicionado, as informações da licença serão mostradas na janela. O Kaspersky Embedded Systems Security exibirá a data calculada da expiração da licença. O período da licença inicia no momento em que você adiciona uma chave e expira até a data de expiração do arquivo de chave.

    Clique no botão **Avançar** para aplicar o arquivo de chave ao aplicativo.
15. Na janela **Pronto para instalar**, clique no botão **Instalar**. O assistente iniciará a instalação dos componentes do Kaspersky Embedded Systems Security.
16. A janela **Instalação concluída** será exibida quando a instalação for concluída.
17. Marque a caixa de seleção **Exibir Notas de Versão** para visualizar informações sobre a versão depois que o Assistente de instalação for concluído.
18. Clique em **Finalizar**.

O Assistente de instalação será fechado. Após a conclusão da instalação, o Kaspersky Embedded Systems Security estará pronto para uso se você tiver adicionado a chave de ativação.

Instalação do Console do Kaspersky Embedded Systems Security

Siga as instruções do Assistente de instalação para ajustar as configurações de instalação do Console do Aplicativo. O processo de instalação pode ser interrompido em qualquer etapa do assistente. Para isso, pressione o

botão **Cancelar** na janela do Assistente de instalação.

► *Para instalar o Console do Aplicativo, siga as etapas a seguir:*

1. Certifique-se de que a conta utilizada para executar o Assistente de instalação faça parte do grupo de administradores no computador protegido.
2. Execute o arquivo setup.exe no computador.

   A janela de boas-vindas é exibida.
3. Clique no link **Instalar o console do Kaspersky Embedded Systems Security**.

   A janela de boas-vindas do Assistente de instalação é aberta.
4. Clique no botão **Avançar**.
5. Revise os termos do Contrato de Licença do Usuário Final na janela aberta e marque a caixa de seleção **Confirmo que li, entendi e aceitei completamente os termos e condições deste Contrato de Licença do Usuário Final** para prosseguir com a instalação.
6. Clique no botão **Avançar**.

   A janela **Configurações avançadas de instalação** é exibida.
7. Na janela **Configurações avançadas de instalação**:
   - Se você pretende usar o Console do Aplicativo para gerenciar o Kaspersky Embedded Systems Security instalado em um computador remoto, marque a caixa de seleção **Permitir acesso remoto**.
   - Para abrir a janela **Instalação personalizada** e selecionar componentes:
     a. Clique no botão **Avançado**.

        A janela **Instalação personalizada** é exibida.
     b. Selecione os componentes de "Ferramentas de administração" a partir da lista.

        Por padrão, todos os componentes são instalados.
     c. Clique no botão **Avançar**.

   Você pode encontrar mais informações sobre os componentes do Kaspersky Embedded Systems Security (consulte a seção "Códigos de componentes de software do Kaspersky Embedded Systems Security para o serviço do Windows Installer" na página 34).
8. Na janela **Selecionar pasta de destino**:
   a. Se for solicitado, especifique uma pasta diferente na qual os arquivos instalados devem ser salvos.
   b. Clique no botão **Avançar**.
9. Na janela **Pronto para instalar**, clique no botão **Instalar**.

   O assistente começará a instalação dos componentes selecionados.
10. Clique em **Finalizar**.

O Assistente de instalação será fechado. O Console do Aplicativo será instalado no computador protegido.

Se o conjunto de “Ferramentas de administração” tiver sido instalado em algum computador da rede, além do computador protegido, defina as configurações avançadas (consulte a seção "Configurações avançadas após a instalação do Console do Aplicativo em outro computador" na página 52).

Configurações avançadas após a instalação do Console do Aplicativo em outro computador

Se o Console do Aplicativo tiver sido instalado em algum computador na rede, além do computador protegido, execute as seguintes ações para permitir que os usuários gerenciem o Kaspersky Embedded Systems Security remotamente:

- Adicione usuários do Kaspersky Embedded Systems Security ao grupo Administradores do ESS no computador protegido.
- Permita conexões da rede para o Kaspersky Security Management Service (kavfsgt.exe) (consulte a seção "Sobre permissões de acesso para o Kaspersky Security Management Service" na página 230), se o computador protegido usar o firewall do Windows ou um firewall de terceiros.
- Se a caixa de seleção **Permitir acesso remoto** não for marcada durante a instalação do Console do Aplicativo em um computador com Microsoft Windows, permita conexões de rede para o Console do Aplicativo manualmente por meio do Firewall do computador.

O Console do Aplicativo no computador remoto usa o protocolo DCOM para receber informações sobre eventos do Kaspersky Embedded Systems Security (objetos verificados, tarefas concluídas, etc.) do Kaspersky Security Management Service no computador protegido. Você deve permitir conexões de rede para o Console do Aplicativo nas configurações do firewall do Windows para estabelecer conexões entre o Console do Aplicativo e o Kaspersky Security Management Service.

No computador remoto, onde o Console do Aplicativo estiver instalado, faça o seguinte:

- Verifique se é permitido acesso remoto anônimo a aplicativos COM (mas não a inicialização e ativação remotas de aplicativos COM).
- No Firewall do Windows, abra a porta TCP 135 e permita conexões de rede para o arquivo executável do processo de gerenciamento remoto do Kaspersky Embedded Systems Security, kavfsrcn.exe.

  O computador cliente no qual o Console do Aplicativo está instalado usa a porta TCP 135 para acessar o computador protegido e receber uma resposta.
- Configure uma regra de saída no Firewall do Windows para permitir a conexão.

  Diferentemente dos serviços TCP/IP e UDP/IP tradicionais, em que um protocolo único tem uma porta fixa, o DCOM atribui portas dinamicamente aos objetos COM remotos. Se existir um firewall entre o cliente (onde o Console do Aplicativo está instalado) e o ponto de extremidade do DCOM (o computador protegido), um grande intervalo de portas deverá ser aberto.

As mesmas etapas devem ser aplicadas para configurar qualquer outro software ou hardware de firewall.

► *Se o Console do Aplicativo estiver aberto enquanto você configura a conexão entre o computador protegido e o computador no qual o Console do Aplicativo está instalado:*

1. Feche o Console do Aplicativo.
2. Espere até que o processo de gerenciamento remoto do Kaspersky Embedded Systems Security tenha terminado.
3. Reiniciar o Console do Aplicativo.

   As novas configurações de conexão serão aplicadas.

Nesta seção

Permitir o acesso remoto anônimo a aplicativos COM 53

Permitir conexões de rede para o processo de gerenciamento remoto do Kaspersky Embedded Systems Security 53

Adicionar regra de saída no Firewall do Windows 54

Permitir o acesso remoto anônimo a aplicativos COM

Os nomes de configurações podem variar dependendo do sistema operacional Windows instalado.

► *Para permitir o acesso remoto anônimo a aplicativos COM, siga as etapas a seguir:*

1. No computador remoto com o Console do Kaspersky Embedded Systems Security instalado, abra o console de Serviços do componente.
2. Selecione **Iniciar** → **Executar**.
3. Digite o comando `dcomcnfg`.
4. Clique em **OK**.
5. Expanda o nó **Computadores** no console de **Serviços do componente** em seu computador.
6. Abra o menu de contexto no nó **Meu computador**.
7. Selecione **Propriedades**.
8. Na guia **Segurança COM** da janela **Propriedades**, clique no botão **Editar limites** no grupo de configurações **Permissões de acesso**.
9. Certifique-se de que a caixa de seleção **Permitir Acesso Remoto** esteja marcada para o usuário ANONYMOUS LOGON na janela **Permitir Acesso Remoto**.
10. Clique em **OK**.

Permitir conexões de rede para o processo de gerenciamento remoto do Kaspersky Embedded Systems Security

Os nomes de configurações podem variar dependendo do sistema operacional Windows instalado.

► *Para abrir a porta TCP 135 no Firewall do Windows e permitir conexões de rede para o processo de gerenciamento remoto do Kaspersky Embedded Systems Security, siga as etapas a seguir:*

1. Feche o Console do Kaspersky Embedded Systems Security no computador remoto.
2. Execute uma das seguintes etapas:
   - No Microsoft Windows XP SP2 ou posterior:

a. Selecione **Iniciar** > **Windows Firewall**.

b. Na janela do **Firewall do Windows** (ou Configurações do Firewall do Windows), clique no botão **Adicionar porta** na guia **Exclusões**.

c. No campo **Nome**, especifique o nome da porta RPC (TCP/135) ou insira outro nome, por exemplo, Kaspersky Embedded Systems Security DCOM, e especifique o número da porta (135) no campo **Nome da porta**.

d. Selecione o protocolo **TCP**.

e. Clique em **OK**.

f. Clique no botão **Adicionar** na guia **Exclusões**.

- No Microsoft Windows 7 ou posterior:

  a. Selecione **Iniciar** > **Painel de Controle** > **Firewall do Windows**.

  b. Na janela **Firewall do Windows**, selecione **Permitir um programa ou recurso pelo Firewall do Windows**.

  c. Na janela **Permitir que programas comuniquem através do Firewall do Windows**, clique no botão **Permitir outro programa...**.

3. Especifique o arquivo kavfsrcn.exe na janela **Adicionar Programa**. Ele está localizado na pasta especificada como pasta de destino durante a instalação do Console do Kaspersky Embedded Systems Security usando o Console de Gerenciamento Microsoft.
4. Clique em **OK**.
5. Clique no botão **OK** na janela **Firewall do Windows (Configurações do Firewall do Windows)**.

Adicionar regra de saída no Firewall do Windows

Os nomes de configurações podem variar dependendo do sistema operacional Windows instalado.

► *Para adicionar a regra de saída no Firewall do Windows:, siga as etapas a seguir:*

1. Selecione **Iniciar** > **Painel de Controle** > **Firewall do Windows**.
2. Na janela **Firewall do Windows**, clique no link **Configurações avançadas**.

   A janela **Firewall do Windows com Segurança Avançada** é exibida.
3. Selecione o nó filho **Regras de Saída**.
4. Clique na opção **Nova Regra** no painel **Ações**.
5. Na janela **Assistente para Nova Regra de Saída** exibida, selecione a opção **Porta** e clique em **Avançar**.
6. Selecione o protocolo **TCP**.
7. No campo **Portas remotas específicas**, especifique o seguinte intervalo de portas para permitir conexões de saída: 1024-65535.
8. Na janela **Ação** selecione a opção **Permitir a conexão**.
9. Salve a nova regra e feche a janela **Firewall do Windows com Segurança Avançada**.

O Firewall do Windows agora permitirá conexões de rede entre o Console do Aplicativo e Kaspersky Security

Management Service.

Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security

O Kaspersky Embedded Systems Security iniciará as tarefas de proteção e verificação imediatamente após a instalação se o aplicativo tiver sido ativado. Se a opção **Ativar a proteção em tempo real após a instalação do aplicativo** (opção padrão) tiver sido selecionada durante a instalação do Kaspersky Embedded Systems Security, o aplicativo verificará os objetos do sistema de arquivos do computador quando eles forem acessados. O Kaspersky Embedded Systems Security executará a tarefa de Verificação de áreas críticas todas as sextas-feiras às 20h.

Recomendamos seguir as seguintes etapas após instalar o Kaspersky Embedded Systems Security:

- Inicie a tarefa Atualização do Banco de Dados do aplicativo. Após a instalação, o Kaspersky Embedded Systems Security verificará objetos usando o banco de dados incluído no kit de distribuição do aplicativo.

  Recomendamos atualizar os bancos de dados do Kaspersky Embedded Systems Security imediatamente, pois eles podem estar desatualizados.

  O aplicativo então atualizará os bancos de dados a cada hora segundo a programação padrão configurada na tarefa.
- Execute uma Verificação de áreas críticas no computador se nenhum software antivírus com a proteção de arquivos em tempo real estiver instalado no computador protegido antes da instalação do Kaspersky Embedded Systems Security.
- Configure notificações de administrador sobre eventos do Kaspersky Embedded Systems Security.

Nesta seção

Inicialização e configuração da tarefa de atualização do banco de dados do Kaspersky Embedded Systems Security 55

Verificação de Áreas Críticas 57

Inicialização e configuração da tarefa de atualização do banco de dados do Kaspersky Embedded Systems Security

► *Para atualizar o banco de dados do aplicativo após a instalação, faça o seguinte:*

1. Nas configurações da tarefa de Atualização do Banco de Dados, configure uma conexão com uma fonte de atualização - Kaspersky Lab HTTP ou servidores de atualização FTP.
2. Inicie a tarefa de Atualização do Banco de Dados.

O Web Proxy Auto-Discovery Protocol (WPAD) pode não estar configurado na sua rede para detectar as configurações do servidor proxy automaticamente na LAN. Nesse caso, a sua rede pode requerer autenticação para acessar o servidor proxy.

► *Para especificar configurações opcionais de servidor proxy e autenticação para acesso ao servidor proxy, faça o seguinte:*

1. Abra o menu de contexto do nó **Kaspersky Embedded Systems Security**.
2. Selecione o item **Propriedades**.

   A janela **Configurações do aplicativo** é exibida.
3. Selecione a guia **Configurações de conexão**.
4. Na seção **Configurações do servidor proxy**, marque a caixa de seleção **Usar configurações especificadas de servidor proxy**.
5. Insira o endereço do servidor proxy no campo **Endereço** e insira o número da porta do servidor proxy no campo **Porta**.
6. Na seção **Configurações de autenticação do servidor proxy**, selecione o método de autenticação necessário na lista suspensa:
   - **Usar autenticação NTLM** se o servidor proxy suportar a autenticação NTLM integrada do Microsoft Windows. O Kaspersky Embedded Systems Security usará a conta de usuário especificada nas configurações da tarefa para acessar o servidor proxy (por padrão, a tarefa é executada sob a conta de usuário do **sistema local** (**SYSTEM**)).
   - **Usar autenticação NTLM com nome de usuário e senha** se o servidor proxy for compatível com a autenticação NTLM integrada do Microsoft Windows. O Kaspersky Embedded Systems Security usará a conta especificada para acessar o servidor proxy. Insira um nome de usuário e a senha ou selecione um usuário na lista.
   - **Aplicar nome de usuário e senha** para selecionar a autenticação básica. Insira um nome de usuário e a senha ou selecione um usuário na lista.
7. Clique em **OK** na janela **Configurações do aplicativo**.

► *Para configurar a conexão com os servidores de atualização da Kaspersky Lab, na tarefa de Atualização do Banco de Dados:*

1. Inicie o Console do Aplicativo de uma das seguintes maneiras:
   - Abra o Console do Aplicativo no computador protegido. Para isso, selecione **Iniciar** > **Todos os Programas** > **Kaspersky Embedded Systems Security** > **Ferramentas de Administração** > **Kaspersky Embedded Systems Security 2.3 Console**.
   - Se o Console do Aplicativo tiver sido iniciado em um computador diferente do computador protegido, conecte-se ao computador protegido:
     a. Abra o menu de contexto do nó **Kaspersky Embedded Systems Security** na árvore do Console do Aplicativo.
     b. Selecione o item **Conectar a outro computador**.
     c. Na janela **Selecionar computador**, selecione **Outro computador** e, no campo de texto, indique o nome da rede do computador protegido.

> Se a conta você usou para efetuar login no Microsoft Windows não tiver permissões de acesso para o Kaspersky Security Management Service (consulte a seção "Sobre permissões de acesso para o Kaspersky Security Management Service" na página 230), indique uma conta com as permissões necessárias.

A janela do Console do Aplicativo é exibida.

2. Na árvore do Console do Aplicativo, expanda o nó **Atualização**.
3. Selecionar o nó filho **Atualização do Banco de Dados**.
4. Clique no link **Propriedades** no painel de detalhes.
5. Na janela **Configurações de tarefa** exibida, abra a guia **Configurações de conexão**.
6. Selecione **Usar as configurações do servidor proxy para se conectar aos servidores de atualização da Kaspersky Lab**.
7. Clique em **OK** na janela **Configurações de tarefa**.

As configurações para se conectar à fonte de atualização na tarefa de Atualização do banco de dados serão salvas.

► *Para executar a tarefa de Atualização do banco de dados:*

1. Na árvore do Console do Aplicativo, expanda o nó **Atualização**.
2. No menu de contexto no nó filho **Atualização do Banco de Dados**, selecione o item **Iniciar**.

A tarefa de Atualização do banco de dados é iniciada.

Após a tarefa ter sido concluída com sucesso, você pode visualizar a data de lançamento das últimas atualizações do banco de dados instaladas no painel de detalhes do nó **Kaspersky Embedded Systems Security**.

Verificação de Áreas Críticas

Após ter atualizado os bancos de dados do Kaspersky Embedded Systems Security, verifique o computador para a presença de malware usando a tarefa de Verificação de áreas críticas.

► *Para executar uma tarefa de Verificação de Áreas Críticas, siga as etapas a seguir:*

1. Expanda o nó **Verificação por Demanda** na árvore do Console do Aplicativo.
2. No menu de contexto do nó filho **Verificação de Áreas Críticas**, selecione o comando **Iniciar**.

A tarefa será iniciada; o status da tarefa **Executando** será exibido no painel de detalhes.

► *Para visualizar o log de tarefas,*

no painel de detalhes do nó **Verificação de Áreas Críticas**, clique no link **Abrir log da tarefa**.

Alteração do conjunto de componentes e reparação do Kaspersky Embedded Systems Security

Os componentes do Kaspersky Embedded Systems Security podem ser adicionados ou removidos. Você deve

interromper a tarefa de Proteção de Arquivos em Tempo Real antes que possa remover o componente de Proteção de Arquivos em Tempo Real. Em outras circunstâncias, não há necessidade de interromper a tarefa de Proteção de Arquivos em Tempo Real ou o Kaspersky Security Service.

Se o acesso ao gerenciamento do aplicativo for protegido por senha, o Kaspersky Embedded Systems Security vai solicitá-la quando você tentar remover ou modificar o conjunto de componentes no Assistente de instalação.

► *Para modificar o conjunto de componentes do Kaspersky Embedded Systems Security:*

1. No menu **Iniciar**, selecione **Todos os programas** > **Kaspersky Embedded Systems Security** > **Modificar ou remover o Kaspersky Embedded Systems Security**.

   A janela **Modificar, reparar ou remover a instalação** do assistente de instalação é exibida.

2. Selecione **Modificar conjunto de componentes**. Clique no botão **Avançar**.

   A janela **Instalação personalizada** é exibida.

3. Na janela **Instalação personalizada**, na lista de componentes disponíveis, selecione os componentes que deseja adicionar ao Kaspersky Embedded Systems Security ou remover. Para isso, execute as seguintes ações:

   - Para alterar o conjunto de componentes, clique no botão ao lado do nome do componente selecionado. E, no menu de contexto, selecione:
     - **O componente será instalado no disco rígido local**, se você desejar instalar um componente;
     - **O componente e seus subcomponentes serão instalados no disco rígido local**, se você desejar instalar um grupo de componentes.
   - Para remover componentes instalados anteriormente, clique no botão ao lado do nome do componente selecionado. No menu de contexto selecione **O componente não estará disponível**.

   Clique no botão **Avançar**.

4. Na janela **Pronto para instalar**, confirme a modificação do conjunto de componentes do software clicando no botão **Instalar**.

5. Na janela exibida quando a instalação for concluída, clique no botão **OK**.

   O conjunto de componentes do Kaspersky Embedded Systems Security será modificado com base nas configurações especificadas.

Se ocorrerem problemas na operação do Kaspersky Embedded Systems Security (travamentos do Kaspersky Embedded Systems Security; tarefas que travam ou não iniciam), é possível tentar reparar o Kaspersky Embedded Systems Security. Você pode executar um reparo salvando as configurações atuais do Kaspersky Embedded Systems Security ou pode selecionar uma opção para reinicializar todas as configurações do Kaspersky Embedded Systems Security com os seus valores padrão.

► *Para reparar o Kaspersky Embedded Systems Security após o travamento do aplicativo ou de uma tarefa, siga as etapas a seguir:*

1. No menu **Iniciar**, selecione **Todos os programas**.
2. Selecione **Kaspersky Embedded Systems Security**.
3. Selecione **Modificar ou remover o Kaspersky Embedded Systems Security**.

A janela **Modificar, reparar ou remover a instalação** do assistente de instalação é exibida.

4. Selecione **Reparar componentes instalados**. Clique no botão **Avançar**.

   Isso abre a janela **Reparar componentes instalados**.

5. Na janela **Reparar componentes instalados**, marque a caixa de seleção **Restaurar configurações recomendadas do aplicativo** se desejar redefinir as configurações do aplicativo e restaurar o Kaspersky Embedded Systems Security com suas configurações padrão. Clique no botão **Avançar**.
6. Na janela **Pronto para reparar**, confirme a operação de reparo clicando no botão **Instalar**.
7. Na janela exibida quando a operação de reparação for concluída, clique no botão **OK**.

O Kaspersky Embedded Systems Security será reparado com base nas configurações especificadas.

Desinstalação usando o Assistente de instalação

Esta seção contém instruções sobre a remoção do Kaspersky Embedded Systems Security e do Console do Aplicativo de um computador protegido usando o Assistente de instalação/desinstalação.

Nesta seção

Desinstalação do Kaspersky Embedded Systems Security....59
Desinstalação do Console do Kaspersky Embedded Systems Security....60

Desinstalação do Kaspersky Embedded Systems Security

Os nomes de configurações podem variar em diferentes sistemas operacionais Windows.

O Kaspersky Embedded Systems Security pode ser desinstalado do computador protegido usando o Assistente de instalação/Desinstalação.

Pode ser necessária uma reinicialização do computador após a desinstalação do Kaspersky Embedded Systems Security de um computador protegido. A reinicialização poderá ser adiada.

A desinstalação, reparação e instalação do aplicativo por meio do painel de controle do Windows não estarão disponíveis se o sistema operacional utilizar o recurso UAC (Controle de Conta de Usuário) ou o acesso ao aplicativo for protegido por senha.

Se o acesso ao gerenciamento do aplicativo for protegido por senha, o Kaspersky Embedded Systems Security vai solicitá-la quando você tentar remover ou modificar o conjunto de componentes no Assistente de instalação.

► *Para desinstalar o Kaspersky Embedded Systems Security:*

1. No menu **Iniciar**, selecione **Todos os programas**.
2. Selecione **Kaspersky Embedded Systems Security**.
3. Selecione **Modificar ou remover o Kaspersky Embedded Systems Security**.

   A janela **Modificar, reparar ou remover a instalação** do assistente de instalação é exibida.
4. Selecione **Remover componentes do software**. Clique no botão **Avançar**.

   A janela **Configurações avançadas de desinstalação do aplicativo** é exibida.
5. Se necessário, na janela **Configurações avançadas de desinstalação do aplicativo**:
   a. Marque a caixa de seleção **Exportar objetos da quarentena** para que o Kaspersky Embedded Systems Security exporte objetos que foram colocados em quarentena. Esta caixa é desmarcada por padrão.
   b. Marque a caixa de seleção **Exportar objetos do backup**, para exportar objetos do Backup do Kaspersky Embedded Systems Security. Esta caixa é desmarcada por padrão.
   c. Clique no botão **Salvar em** e selecione a pasta para onde deseja exportar os objetos. Por padrão, os objetos serão exportados para %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall.

      Clique no botão **Avançar**.
6. Na janela **Pronto para desinstalar**, confirme a desinstalação clicando no botão **Desinstalar**.
7. Na janela exibida quando a desinstalação for concluída, clique no botão **OK**.

O Kaspersky Embedded Systems Security será desinstalado do computador protegido.

Desinstalação do Console do Kaspersky Embedded Systems Security

Os nomes de configurações podem variar em diferentes sistemas operacionais Windows.

Você pode desinstalar o Console do Aplicativo do computador usando o Assistente de configuração/desinstalação.

Após desinstalar o Console do Aplicativo, não será necessário reiniciar o computador.

► *Para desinstalar o Console do Aplicativo:*

1. No menu **Iniciar**, selecione **Todos os programas**.
2. Selecione **Kaspersky Embedded Systems Security**.
3. Selecione **Modificar ou Remover Kaspersky Embedded Systems Security 2.3 Ferramentas de Administração**.

   A janela **Modificar, reparar ou remover a instalação** do assistente é exibida.
4. Selecione **Remover componentes do software** e clique no botão **Avançar**.
5. A janela **Pronto para desinstalar** é exibida. Clique no botão **Desinstalar**.

   A janela **Desinstalação concluída** é exibida.

6. Clique em **OK**.

A desinstalação estará concluída e o Assistente de instalação será fechado.

Instalação e desinstalação do aplicativo a partir da linha de comando

Esta seção descreve as particularidades da instalação e desinstalação do Kaspersky Embedded Systems Security na linha de comando e contém exemplos de comandos para instalar e desinstalar o Kaspersky Embedded Systems Security na linha de comando e exemplos de comandos para adicionar e remover os componentes do Kaspersky Embedded Systems Security na linha de comando.

Nesta seção

Sobre a instalação e desinstalação do Kaspersky Embedded Systems Security a partir da linha de comando 61

Exemplos de comandos para instalar o Kaspersky Embedded Systems Security 62

Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security 63

Adicionar/remover componentes. Exemplos de comandos 64

Desinstalação do Kaspersky Embedded Systems Security. Exemplos de comandos 65

Códigos de retorno 65

Sobre a instalação e desinstalação do Kaspersky Embedded Systems Security a partir da linha de comando

O Kaspersky Embedded Systems Security pode ser instalado ou desinstalado e seus componentes adicionados ou removidos, executando os arquivos do pacote de instalação \product\ess_x86(x64).msi da linha de comando após as configurações de instalação terem sido especificadas usando chaves.

O conjunto de “Ferramentas de administração” pode ser instalado no computador protegido ou em outro computador na rede para funcionar com o Console do Aplicativo local ou remotamente. Para isso, use o pacote de instalação \console\esstools.msi.

Execute a instalação usando uma conta incluída no grupo de administradores no computador onde o aplicativo estiver instalado.

Se um dos arquivos \product\ess_x86.msi ou \product\ess_x64.msi for executado no computador protegido sem chaves adicionais, o Kaspersky Embedded Systems Security será instalado com as configurações de instalação recomendadas.

O conjunto de componentes a ser instalado pode ser atribuído usando a opção de linha de comando ADDLOCAL listando os códigos dos componentes selecionados ou conjuntos de componentes.

Exemplos de comandos para instalar o Kaspersky Embedded Systems Security

Essa seção fornece exemplos de comandos usados para instalar o Kaspersky Embedded Systems Security.

Em computadores executando uma versão de 32 bits do Microsoft Windows, execute os arquivos com o sufixo x86 no kit de distribuição. Em computadores executando uma versão de 64 bits do Microsoft Windows, execute os arquivos com o sufixo x64 no kit de distribuição.

Informações detalhadas sobre o uso dos comandos padrão do Windows Installer e as opções de linha de comando são fornecidas na documentação enviada pela Microsoft.

Exemplos de instalação do Kaspersky Embedded Systems Security usando o arquivo setup.exe

► *Para instalar o Kaspersky Embedded Systems Security com as configurações de instalação recomendadas sem interação do usuário, execute o seguinte comando:*

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

Você pode instalar o Kaspersky Embedded Systems Security com as seguintes configurações:

- instale apenas os componentes de Proteção de Arquivos em Tempo Real e de Verificação por Demanda;
- não execute a Proteção de Arquivos em Tempo Real ao iniciar o Kaspersky Embedded Systems Security;
- não exclua do escopo da verificação os arquivos recomendados pela Microsoft Corporation;

Para fazer isso, execute o seguinte comando:

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

Exemplos de comandos usados para a instalação: executando um arquivo .msi

► *Para instalar o Kaspersky Embedded Systems Security com as configurações de instalação recomendadas sem interação do usuário, execute o seguinte comando:*

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

► *Para instalar o Kaspersky Embedded Systems Security com as configurações de instalação recomendadas e visualizar a interface da instalação, execute o seguinte comando:*

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

► *Para instalar e ativar o Kaspersky Embedded Systems Security usando o arquivo de chave C:\0000000A.key:*

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

- *Para instalar o Kaspersky Embedded Systems Security com uma verificação preliminar dos processos ativos e setores de inicialização dos discos locais, execute o seguinte comando:*

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

- *Para instalar o Kaspersky Embedded Systems Security na pasta de instalação C:\ESS, execute o seguinte comando:*

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

- *Para instalar o Kaspersky Embedded Systems Security e salvar um arquivo de log de instalação com o nome ess.log na pasta onde o arquivo msi do Kaspersky Embedded Systems Security está armazenado, execute o seguinte comando:*

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

- *Para instalar o Console do Kaspersky Embedded Systems Security, execute o seguinte comando:*

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

- *Para instalar e ativar o Kaspersky Embedded Systems Security usando o arquivo de chave C:\0000000A.key e configurar o Kaspersky Embedded Systems Security de acordo com as configurações descritas no arquivo de configuração C:\settings.xml, execute o seguinte comando:*

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

- *Para instalar o patch do aplicativo quando o Kaspersky Embedded Systems Security estiver protegido por senha, execute o seguinte comando:*

```
msiexec /p "<msp file name with path>" UNLOCK_PASSWORD=<password>
```

Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security

O Kaspersky Embedded Systems Security iniciará as tarefas de proteção e verificação imediatamente após a instalação se o aplicativo tiver sido ativado. Se você selecionar **Ativar a proteção em tempo real após a instalação do aplicativo** durante a instalação do Kaspersky Embedded Systems Security, o aplicativo verificará os objetos do sistema de arquivos do computador quando eles forem acessados. O Kaspersky Embedded Systems Security executará a tarefa de Verificação de áreas críticas todas as sextas-feiras às 20h.

Recomendamos seguir as seguintes etapas após instalar o Kaspersky Embedded Systems Security:

- Inicie a tarefa de atualização dos bancos de dados do Kaspersky Embedded Systems Security. Após a instalação, o Kaspersky Embedded Systems Security verificará objetos usando o banco de dados incluído no respectivo kit de distribuição. Recomendamos atualizar imediatamente o banco de dados do Kaspersky Embedded Systems Security. Para isso, você deve executar a tarefa de Atualização do Banco de Dados. O banco de dados será atualizado a cada hora de acordo com a programação padrão.

  Por exemplo, você pode executar a tarefa Atualização do banco de dados do aplicativo, executando o comando seguinte:

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

/PROXYPWD:123456

Neste caso, as atualizações dos bancos de dados do Kaspersky Embedded Systems Security são baixadas dos servidores de atualização da Kaspersky Lab. A conexão com a fonte de atualização é estabelecida por meio do servidor proxy (endereço do servidor proxy: proxy.company.com, porta: 8080) usando a autenticação NTLM incluída no Windows para acessar o servidor em uma conta (nome de usuário: inetuser; senha: 123456).

- Execute uma Verificação de áreas críticas no computador se nenhum software antivírus com proteção de arquivos em tempo real estiver instalado no computador protegido antes da instalação do Kaspersky Embedded Systems Security.

► *Para iniciar a tarefa de Verificação de Áreas Críticas usando a linha de comando:*

KAVSHELL SCANCRITICAL /W:scancritical.log

Esse comando salva o log de tarefas em um arquivo chamado scancritical.log incluído na pasta atual.

- Configure notificações de administrador sobre eventos do Kaspersky Embedded Systems Security.

Adicionar/remover componentes. Exemplos de comandos

O componente de Verificação por Demanda é instalado automaticamente. Você não precisa especificá-lo na lista de valores de chave ADDLOCAL, adicionando ou excluindo os componentes do Kaspersky Embedded Systems Security.

► *Para adicionar o componente de Controle de inicialização de aplicativos aos componentes já instalados, execute o seguinte comando:*

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

ou

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

Se você enumerar os componentes que deseja instalar junto com os componentes já instalados, o Kaspersky Embedded Systems Security vai reinstalar os componentes existentes.

► *Para remover os componentes instalados, execute o comando a seguir:*

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

Desinstalação do Kaspersky Embedded Systems Security. Exemplos de comandos

► *Para desinstalar o Kaspersky Embedded Systems Security do computador protegido, execute o seguinte comando:*

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

ou

- Para sistemas operacionais de 32 bits:

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

- Para sistemas operacionais de 64 bits:

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

► *Para desinstalar o Console do Kaspersky Embedded Systems Security, execute o seguinte comando:*

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

ou

- Para sistemas operacionais de 32 bits:

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

- Para sistemas operacionais de 64 bits:

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

► *Para desinstalar o Kaspersky Embedded Systems Security de um computador protegido em que a proteção de senha esteja ativa, execute o comando a seguir:*

- Para sistemas operacionais de 32 bits:

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

- Para sistemas operacionais de 64 bits:

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

Códigos de retorno

A tabela abaixo contém uma lista de códigos de retorno da linha de comando.

Tabela 6. Códigos de retorno

Código	Descrição
1324	O nome da pasta de destino contém caracteres inválidos.
25001	Direitos insuficientes para instalar o Kaspersky Embedded Systems Security. Para instalar o aplicativo, inicie o assistente de instalação com direitos de administrador local.
25003	O Kaspersky Embedded Systems Security não pode ser instalado em computadores que executam essa versão do Microsoft Windows. Inicie o assistente de instalação paras versões de 64 bits do Microsoft Windows.

Código	Descrição
25004	Software incompatível detectado. Para continuar a instalação, desinstale os seguintes softwares: <lista de softwares incompatíveis>.
25010	O caminho indicado não pode ser utilizado para salvar objetos em quarentena.
25011	O nome da pasta para salvar objetos em quarentena contém caracteres inválidos.
26251	Não é possível fazer download de Contadores de desempenho DLL.
26252	Não é possível fazer download de Contadores de desempenho DLL.
27300	O driver não pode ser instalado.
27301	O driver não pode ser desinstalado.
27302	O componente de rede não pode ser instalado. O número máximo possível de dispositivos filtrados foi alcançado.
27303	Bancos de dados de antivírus não encontrados.

Instalação e desinstalação do aplicativo usando o Kaspersky Security Center

Esta seção contém informações gerais sobre a instalação do Kaspersky Embedded Systems Security através do Kaspersky Security Center. Ela descreve também como instalar e desinstalar o Kaspersky Embedded Systems Security através do Kaspersky Security Center e as ações a serem executadas após a instalação do Kaspersky Embedded Systems Security.

Nesta seção

Informações gerais sobre a instalação por meio do Kaspersky Security Center 66
Direitos para instalar ou desinstalar o Kaspersky Embedded Systems Security 67
Instalação do Kaspersky Embedded Systems Security através do Kaspersky Security Center 67
Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security 69
Instalação do Console do Aplicativo por meio do Kaspersky Security Center 70
Desinstalação do Kaspersky Embedded Systems Security através do Kaspersky Security Center 71

Informações gerais sobre a instalação por meio do Kaspersky Security Center

Você pode instalar o Kaspersky Embedded Systems Security através do Kaspersky Security Center usando a tarefa de instalação remota.

Após a conclusão da tarefa de instalação remota, o Kaspersky Embedded Systems Security será instalado com

configurações idênticas em vários computadores.

Todos os computadores podem ser combinados em um único grupo de administração e uma tarefa de grupo pode ser criada para instalar o Kaspersky Embedded Systems Security nos computadores desse grupo.

Você pode criar uma tarefa para instalar remotamente o Kaspersky Embedded Systems Security em um conjunto de computadores que não estão no mesmo grupo de administração. Ao criar essa tarefa você deve gerar uma lista dos computadores individuais nos quais o Kaspersky Embedded Systems Security deve ser instalado.

Informações detalhadas sobre a tarefa de instalação remota são fornecidas na *Ajuda do Kaspersky Security Center*.

Direitos para instalar ou desinstalar o Kaspersky Embedded Systems Security

A conta especificada na tarefa de instalação (remoção) remota deve estar incluída no grupo de administradores em cada um dos computadores protegidos em todos os casos exceto nos casos descritos abaixo:

- Se o Agente de rede do Kaspersky Security Center já estiver instalado em computadores onde o Kaspersky Embedded Systems Security será instalado (qualquer que seja o domínio onde os computadores estão localizados ou se eles pertencem a algum domínio).

  Se o Agente de rede ainda não estiver instalado nos computadores, você pode instalá-lo com o Kaspersky Embedded Systems Security usando uma tarefa de instalação remota. Antes de instalar o Agente de Rede, certifique-se de que a conta que você deseja especificar na tarefa esteja incluída no grupo de administradores de cada um dos computadores.

- Todos os computadores onde você deseja instalar o Kaspersky Embedded Systems Security estão no mesmo domínio do Servidor de Administração e este está registrado como a conta do **Admin do Domínio** (se essa conta possuir direitos de administrador local nos computadores do domínio).

Por padrão, ao usar o método de **Instalação forçada**, a tarefa de instalação remota será executada a partir da conta que está executando o Servidor de Administração.

Ao trabalhar com tarefas de grupo ou com tarefas para conjuntos de computadores no modo de instalação (desinstalação) forçada, uma conta deve ter os seguintes direitos em um computador cliente:

- Direito de executar aplicativos remotamente.
- Direitos ao compartilhamento **Admin$**.
- Direito de **Fazer logon como um serviço**.

Instalação do Kaspersky Embedded Systems Security através do Kaspersky Security Center

As informações detalhadas sobre a geração de um pacote de instalação e criação de uma tarefa de instalação remota são fornecidas no Manual de implementação do Kaspersky Security Center.

Se você pretende gerenciar o Kaspersky Embedded Systems Security através do Kaspersky Security Center no

futuro, certifique-se de que as seguintes condições sejam cumpridas:

- O computador em que o Servidor de Administração do Kaspersky Security Center está instalado também tem o Plug-in de Administração instalado (arquivo \product\klcfginst.exe no kit de distribuição do Kaspersky Embedded Systems Security).
- O Agente de Rede do Kaspersky Security Center está instalado nos computadores protegidos. Se o Agente de rede do Kaspersky Security Center não estiver instalado nos computadores protegidos, você poderá instalá-lo junto com o Kaspersky Embedded Systems Security usando uma tarefa de instalação remota.

Os computadores também podem ser combinados em um grupo de administração para que seja possível gerenciar as configurações de proteção usando políticas e tarefas de grupo do Kaspersky Security Center.

► *Para instalar o Kaspersky Embedded Systems Security usando uma tarefa de instalação remota:*

1. Inicialize do Console de Administração do Kaspersky Security Center.
2. No Kaspersky Security Center, expanda o nó **Avançado**.
3. Expanda o nó filho **Instalação remota**.
4. No painel de detalhes do nó filho **Pacotes de instalação**, clique no botão **Criar pacote de instalação**.
5. Selecione o tipo de pacote de instalação **Criar pacote de instalação para um aplicativo da Kaspersky Lab**.
6. Insira o nome do pacote de instalação.
7. Especifique o arquivo `ess`.kud do kit de distribuição do Kaspersky Embedded Systems Security como o arquivo do pacote de instalação.

   A janela **Contrato de Licença do Usuário Final e Política de Privacidade** é aberta.
8. Se você concordar com os termos e as condições do Contrato de Licença do Usuário Final e da Política de Privacidade, selecione as caixas **os termos e as condições deste Contrato de Licença do Usuário Final** e **Política de Privacidade descrevendo o manuseio de dados** para prosseguir com a instalação.

   Você deve aceitar o Contrato de Licença e a Política de Privacidade para prosseguir.
9. Para alterar o conjunto de componentes do Kaspersky Embedded Systems Security a ser instalado (consulte a seção "Alteração do conjunto de componentes e reparação do Kaspersky Embedded Systems Security " na página 57) e as configurações de instalação padrão (consulte a seção "Configurações de instalação e desinstalação e opções de linha de comando para o serviço do Windows Installer" na página 41) no pacote de instalação:
   a. No Kaspersky Security Center, expanda o nó **Instalação remota**.
   b. Na painel de detalhes do nó filho **Pacotes de instalação**, abra o menu de contexto do pacote de instalação do Kaspersky Embedded Systems Security criado e selecione **Propriedades**.
   c. Na janela **Propriedades: <nome do pacote de instalação>** na seção **Configurações**, faça o seguinte:
      a. No grupo de configurações **Componentes a instalar**, marque as caixas de seleção junto dos nomes dos componentes do Kaspersky Embedded Systems Security que você deseja instalar.
      b. Para poder indicar uma pasta de destino que não a pasta padrão, especifique o nome da pasta e o caminho no campo **Pasta de destino**.

         O caminho para a pasta de destino pode conter variáveis de ambiente do sistema. Se a pasta não

existir no computador, ela será criada.

c. No grupo **Configurações avançadas de instalação**, defina as seguintes configurações:

- **Verificar o computador quanto à existência de vírus antes da instalação.**
- **Ativar a proteção em tempo real após a instalação do aplicativo**.
- **Adicionar arquivos recomendados pela Microsoft à lista de exclusões**.

d. **Adicionar arquivos recomendados pela Kaspersky Lab à lista de exclusões**.

d. Na janela de diálogo **Propriedades: <nome do pacote de instalação>**, clique em **OK**.

10. No nó **Pacotes de instalação**, crie uma tarefa para instalar remotamente o Kaspersky Embedded Systems Security nos computadores selecionados (grupo de administração). Defina as configurações da tarefa.

    Para obter mais informações sobre a criação e configuração de tarefas de instalação remotas, consulte a *Ajuda do Kaspersky Security Center*.

11. Execute a tarefa de instalação remota do Kaspersky Embedded Systems Security.

O Kaspersky Embedded Systems Security será instalado nos computadores especificados na tarefa.

Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security

Após instalar o Kaspersky Embedded Systems Security, recomendamos que você atualize os bancos de dados do Kaspersky Embedded Systems Security nos computadores e execute uma Verificação de áreas críticas dos computadores caso nenhum aplicativo de antivírus com a função de Proteção em tempo real ativada estivesse instalado nos computadores antes da instalação do Kaspersky Embedded Systems Security.

Se os computadores onde o Kaspersky Embedded Systems Security tiver sido instalado fizerem parte de um único grupo de administração no Kaspersky Security Center, você pode executar essas tarefas usando os seguintes métodos:

1. Criar tarefas de atualização do banco de dados para o grupo de computadores nos quais o Kaspersky Embedded Systems Security foi instalado. Defina o Servidor de Administração do Kaspersky Security Center como a fonte de atualização.
2. Crie uma tarefa de grupo de Verificação por Demanda com o status de Verificação de Áreas Críticas. O Kaspersky Security Center avalia o status de segurança de cada computador no grupo com base nos resultados da execução dessa tarefa, não com base nos resultados da tarefa de Verificação de Áreas Críticas.
3. Criar uma nova política para o grupo de computadores. Nas propriedades de política, na seção **Configurações do aplicativo**, desative o início programado das tarefas de verificação por demanda do sistema e das tarefas de Atualização do banco de dados nos computadores do grupo de administração nas configurações da subseção **Executar tarefas do sistema**.

Você também pode configurar notificações de administrador sobre eventos do Kaspersky Embedded Systems Security.

Instalação do Console do Aplicativo por meio do Kaspersky Security Center

As informações detalhadas sobre a criação de um pacote de instalação e de uma tarefa de instalação remota são fornecidas no Manual de Implementação do Kaspersky Security Center.

► *Para instalar o Console do Aplicativo usando a tarefa de instalação remota:*

1. No Console de Administração do Kaspersky Security Center, expanda o nó **Avançado**.
2. Expanda o nó filho **Instalação remota**.
3. No painel de detalhes do nó filho Pacotes de instalação, clique no botão **Criar pacote de instalação**. Ao criar o novo pacote de instalação:
   a. Na janela **Assistente de Novo pacote**, selecione **Criar** um pacote de instalação para o arquivo executável especificado como o tipo do pacote.
   b. Insira o nome do novo pacote de instalação.
   c. Selecione o arquivo console\setup.exe na pasta do kit de distribuição do Kaspersky Embedded Systems Security e marque a caixa de seleção **Copiar toda a pasta no pacote de instalação**.
   d. Se necessário, use a opção de linha de comando ADDLOCAL para modificar o conjunto de componentes a ser instalado no campo **Configurações de inicialização do arquivo executável (opcional)** e altere a pasta de destino.

      Por exemplo, para instalar apenas o Console do Aplicativo na pasta C:\KasperskyConsole sem instalar o arquivo de ajuda e a documentação, use as seguintes opções de linha de comando:

      ```
      /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1"
      ```
4. No nó filho **Pacotes de instalação**, crie uma tarefa para instalar remotamente o Console do Aplicativo nos computadores selecionados (grupo de administração). Defina as configurações da tarefa.

   Para obter mais informações sobre a criação e configuração de tarefas de instalação remotas, consulte a Ajuda do Kaspersky Security Center.
5. Execute a tarefa de instalação remota.

O Console do Aplicativo será instalado nos computadores especificados na tarefa.

Desinstalação do Kaspersky Embedded Systems Security através do Kaspersky Security Center

Se o acesso ao gerenciamento do Kaspersky Embedded Systems Security em computadores da rede for protegido por senha, insira a senha ao criar uma tarefa de desinstalação de vários aplicativos. Se a proteção de senha não for gerenciada centralmente por uma política do Kaspersky Security Center, o Kaspersky Embedded Systems Security será desinstalado com êxito dos computadores protegidos nos quais a senha inserida corresponder ao valor definido. O Kaspersky Embedded Systems Security não será desinstalado de outros computadores.

► *Para desinstalar o Kaspersky Embedded Systems Security, execute os passos a seguir no Console de Administração do Kaspersky Security Center:*

1. No Console de Administração do Kaspersky Security Center, crie e inicie uma tarefa de remoção do aplicativo.
2. Na tarefa, selecione o método de desinstalação (similar à seleção do método de instalação; consulte a seção anterior) e especifique uma conta que o Servidor de Administração usará para acessar os computadores. Você pode desinstalar o Kaspersky Embedded Systems Security apenas com as configurações de desinstalação padrão (consulte a seção "Configurações de instalação e desinstalação e opções de linha de comando para o serviço do Windows Installer" na página 41).

Instalação e desinstalação via políticas de grupo do Active Directory

Esta seção descreve a instalação e desinstalação do Kaspersky Embedded Systems Security através das políticas de grupo do Active Directory (Diretório Ativo). Ela contém também informações sobre ações a serem executadas após a instalação do Kaspersky Embedded Systems Security por meio das políticas de grupo.

Nesta seção

Instalação do Kaspersky Embedded Systems Security através das políticas de grupo do Active Directory 71

Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security.....72

Desinstalação do Kaspersky Embedded Systems Security através das políticas de grupo do Active Directory.....73

Instalação do Kaspersky Embedded Systems Security através das políticas de grupo do Active Directory

Você pode instalar o Kaspersky Embedded Systems Security em vários computadores através da política de grupo do Active Directory. Você pode instalar o Console do Aplicativo do mesmo modo.

Os computadores nos quais você quiser instalar o Kaspersky Embedded Systems Security ou o Console do

Aplicativo devem estar em um único domínio e em uma única unidade organizacional.

Os sistemas operacionais nos computadores onde você deseja instalar o Kaspersky Embedded Systems Security por meio da política devem ter os mesmos bits (32 ou 64 bits).

Você deve ter direitos de administrador do domínio.

Para instalar o Kaspersky Embedded Systems Security, use os pacotes de instalação ess_x86(x64).msi. Para instalar o Console do Aplicativo, use os pacotes de instalação `ess`tools.msi.

As informações detalhadas sobre o uso de políticas de grupo do Active Directory são fornecidas na documentação enviada pela Microsoft.

► *Para instalar o Kaspersky Embedded Systems Security (ou o Console do Aplicativo):*

1. Salve o arquivo msi do pacote de instalação correspondente à arquitetura (32 ou 64 bits) da versão instalada do sistema operacional Microsoft Windows na pasta pública do controlador do domínio.
2. Salve o arquivo de chave (consulte a Seção "Sobre o arquivo de chave" na página 80) na mesma pasta pública no controlador de domínio.
3. Na mesma pasta pública no controlador de domínio, crie um arquivo install_props.json com o conteúdo abaixo, indicando que você aceita os termos do Contrato de Licença e da Política de Privacidade.

   ```
   {
   "EULA": "1",
   "PRIVACYPOLICY": "1"
   }
   ```
4. No controlador do domínio, crie uma nova política para o grupo ao qual os computadores pertencem.
5. Usando o **Editor de Objetos de Política de Grupo**, crie um novo pacote de instalação no nó **Configuração do Computador**. Especifique o caminho para o arquivo msi do Kaspersky Embedded Systems Security (ou do Console do Aplicativo) no formato UNC (Universal Naming Convention).
6. Marque a caixa de seleção do Windows Installer **Instalar sempre com privilégios elevados** tanto no nó **Configuração do Computador** quanto no nó **Configuração do Usuário** do grupo selecionado.
7. Aplique as alterações com o comando `gpupdate /force`.

O Kaspersky Embedded Systems Security será instalado nos computadores do grupo depois que tiverem sido reiniciados.

Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security

Após instalar o Kaspersky Embedded Systems Security nos computadores protegidos, é recomendado que você atualize imediatamente o banco de dados do aplicativo e execute uma Verificação de áreas críticas. Você pode executar essas ações (consulte a seção "Ações a serem executadas após a instalação do Kaspersky Embedded Systems Security" na página 55) a partir do Console do Aplicativo.

Você também pode configurar notificações de administrador sobre eventos do Kaspersky Embedded Systems

Security.

Desinstalação do Kaspersky Embedded Systems Security através das políticas de grupo do Active Directory

Se você instalou o Kaspersky Embedded Systems Security (ou o Console do Aplicativo) no grupo de computadores usando uma política de grupo do Active Directory, você poderá usar esta política para desinstalar o Kaspersky Embedded Systems Security (ou o Console do Aplicativo).

Você só pode desinstalar o aplicativo com os parâmetros de desinstalação padrão.

As informações detalhadas sobre o uso de políticas de grupo do Active Directory são fornecidas na documentação enviada pela Microsoft.

Se o gerenciamento do aplicativo for protegido por senha, você não poderá desinstalar o Kaspersky Embedded Systems Security usando as políticas de grupo do Active Directory.

► *Para desinstalar o Kaspersky Embedded Systems Security (ou o Console do Aplicativo):*

1. No controlador do domínio, selecione a unidade organizacional a qual pertencem os computadores dos quais você quer desinstalar o Kaspersky Embedded Systems Security ou o Console do Aplicativo.
2. Selecione a política criada para a instalação do Kaspersky Embedded Systems Security e no **Editor de Objeto de Políticas de Grupo**, no nó **Instalação de software** (**Configuração do Computador** >**Configuração de software** > **Instalação de software**) abra o menu de contexto do pacote de instalação do Kaspersky Embedded Systems Security (ou do Console do Aplicativo) e selecione o comando **Todas as tarefas > Remover**.
3. Selecione o método de desinstalação **Desinstalar o software de usuários e computadores imediatamente**.
4. Aplique as alterações com o comando `gpupdate / force`.

O Kaspersky Embedded Systems Security é removido dos computadores após eles serem reiniciados e antes de fazer login no Microsoft Windows.

Verificação das funções do Kaspersky Embedded Systems Security. Uso do vírus de teste EICAR

Esta seção descreve o vírus de teste EICAR e como usá-lo para verificar a Proteção em tempo real e os recursos da Verificação por demanda do Kaspersky Embedded Systems Security.

Nesta seção

Sobre o vírus de teste EICAR.....74
Verificação dos recursos de Proteção em Tempo Real e Verificação por Demanda 75

Sobre o vírus de teste EICAR

Esse vírus de teste é projetado para verificar a operação dos aplicativos de antivírus. Ele foi desenvolvido pelo European Institute for Computer Antivirus Research (EICAR).

O vírus de teste não é um objeto malicioso e não contém um código executável para o seu computador, mas os aplicativos antivírus da maioria dos fornecedores o identificam como uma ameaça.

O arquivo que contém esse vírus de teste chama-se eicar.com. Você pode baixá-lo no site do EICAR http://www.eicar.org/anti_virus_test_file.htm.

Antes de salvar o arquivo em uma pasta no disco rígido do computador, certifique-se de que a Proteção de Arquivos em Tempo Real nessa unidade esteja desativada.

O arquivo eicar.com contém uma linha de texto. Ao verificar o arquivo, o Kaspersky Embedded Systems Security detecta a ameaça de teste nesta linha de texto, atribui o status **Infectado** ao arquivo e o exclui. As informações sobre a ameaça detectada no arquivo aparecerão no Console do Aplicativo e no log de tarefas.

Você pode usar o arquivo eicar.com para verificar como o Kaspersky Embedded Systems Security desinfecta objetos infectados e como ele detecta objetos possivelmente infectados. Para fazer isso, abra o arquivo usando um editor de texto, adicione um dos prefixos listados na tabela abaixo ao início da linha de texto no arquivo e salve o arquivo com um novo nome, por exemplo, eicar_cure.com.

Para certificar-se de que o Kaspersky Embedded Systems Security processe o arquivo eicar.com com um prefixo, na seção de configurações de segurança **Proteção de objetos** defina o valor **Todos os objetos** para as tarefas de Proteção de Arquivos em Tempo Real e de Verificação por Demanda padrão do Kaspersky Embedded Systems Security.

Tabela 7. Prefixos em arquivos EICAR

Prefixo	Status do arquivo após a verificação e a ação do Kaspersky Embedded Systems Security
Nenhum prefixo	O Kaspersky Embedded Systems Security atribui o status **Infectado** ao objeto e o exclui.
SUSP–	O Kaspersky Embedded Systems Security atribui o status **Possivelmente infectado** ao objeto detectado pelo analisador heurístico e o exclui já que objetos possivelmente infectados não são desinfetados.

Prefixo	Status do arquivo após a verificação e a ação do Kaspersky Embedded Systems Security
Nenhum prefixo	O Kaspersky Embedded Systems Security atribui o status **Infectado** ao objeto e o exclui.
WARN–	O Kaspersky Embedded Systems Security atribui o status **Possivelmente infectado** ao objeto (o código do objeto corresponde em parte ao código de uma ameaça conhecida) e o exclui, já que objetos possivelmente infectados não são desinfectados.
CURE–	O Kaspersky Embedded Systems Security atribui o status **Infectado** ao objeto e o desinfecta. Se a desinfecção for bem-sucedida, o texto inteiro no arquivo será substituído pela palavra "CURE".

Verificação dos recursos de Proteção em Tempo Real e Verificação por Demanda

Após instalar o Kaspersky Embedded Systems Security, você pode confirmar se o Kaspersky Embedded Systems Security encontra objetos contendo códigos maliciosos. Para verificar, você pode usar um vírus de teste do EICAR (consulte a seção "Sobre o vírus de teste EICAR" na página 74).

► *Para verificar o recurso de Proteção em Tempo Real, siga as etapas a seguir:*

1. Baixe o arquivo eicar.com do site EICAR http://www.eicar.org/anti_virus_test_file.htm. Salve-o em uma pasta pública na unidade local de qualquer um dos computadores da rede.

   Antes de salvar o arquivo na pasta, certifique-se de que a Proteção de Arquivos em Tempo Real esteja desativada na pasta.

2. Se você desejar verificar o funcionamento das notificações de usuário de rede, certifique-se de que o Windows Messenger Service da Microsoft esteja ativado tanto no computador protegido quanto no computador onde você salvou o arquivo eicar.com.
3. Abrir o Console do Aplicativo.
4. Copie o arquivo eicar.com salvo na unidade local do computador protegido usando um dos seguintes métodos:
   - Para testar as notificações por meio da janela de Serviços de Terminal, copie o arquivo eicar.com para o computador após conectar-se ao mesmo usando o utilitário Remote Desktop Connection.
   - Para testar notificações por meio do Windows Messenger Service da Microsoft, use os locais da rede do computador para copiar o arquivo eicar.com do computador onde você o salvou.

A Proteção de Arquivos em Tempo Real estará funcionando corretamente se as seguintes condições forem atendidas:

- O arquivo eicar.com for excluído do computador protegido.
- No Console do Aplicativo, o log de tarefas recebe o status de *Crítico*. O log contiver uma nova linha com informações sobre uma ameaça no arquivo eicar.com. (Para visualizar o log de tarefas, na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**, selecione a tarefa de

Proteção de Arquivos em Tempo Real e, no painel de detalhes do nó, clique no link **Abrir log da tarefa**).

- A seguinte mensagem do Windows Messenger Service da Microsoft aparece no computador de onde você copiou o arquivo: `O Kaspersky Embedded Systems Security bloqueou o acesso ao <caminho do arquivo no computador>\eicar.com no computador <nome do computador na rede> às <hora em que o evento ocorreu>. Razão: Ameaça detectada. Vírus: EICAR-Test-File. Nome de usuário: <nome de usuário>. Nome do computador: <nome da rede do computador a partir da qual você copiou o arquivo>`.

> Certifique-se de que o Windows Messenger Service da Microsoft esteja funcionando no computador a partir do qual você copiou o arquivo eicar.com.

► *Para verificar o recurso de Verificação por Demanda, siga as etapas a seguir:*

1. Baixe o arquivo eicar.com do site EICAR http://www.eicar.org/anti_virus_test_file.htm. Salve-o em uma pasta pública na unidade local de qualquer um dos computadores da rede.

   > Antes de salvar o arquivo na pasta, certifique-se de que a Proteção de Arquivos em Tempo Real esteja desativada na pasta.

2. Abrir o Console do Aplicativo.
3. Faça o seguinte:
   a. Expanda o nó **Verificação por Demanda** na árvore do Console do Aplicativo.
   b. Selecione o nó filho **Verificação de Áreas Críticas**.
   c. Na guia **Configurações do escopo da verificação**, abra o menu de contexto no nó **Rede** e selecione **Adicionar arquivo de rede**.
   d. Insira o caminho de rede para o arquivo eicar.com no computador remoto no formato UNC (Universal Naming Convention).
   e. Marque a caixa de seleção para incluir o caminho de rede adicionado ao escopo da verificação.
   f. Executar a tarefa de Verificação de áreas críticas.

A Verificação por Demanda estará funcionando corretamente se as seguintes condições forem atendidas:

- O arquivo eicar.com for excluído da unidade de disco rígido do computador.
- No Console do Aplicativo, o log de tarefas recebe o status de *Crítico*. O log de tarefas de Verificação de Áreas Críticas contiver uma nova linha com informações sobre uma ameaça no arquivo eicar.com. (Para visualizar o log de tarefas, na árvore do Console do Aplicativo, expanda o nó filho **Verificação por Demanda**, selecione a tarefa Verificação de Áreas Críticas e, no painel de detalhes, clique no link **Abrir log da tarefa**).

Interface do aplicativo

Você pode controlar o Kaspersky Embedded Systems Security usando o Plug-in de Administração e o Console do Aplicativo local.

As ações na interface do Console do Aplicativo local são descritas na seção Trabalhar com o Console do Aplicativo (consulte a seção "Trabalhar com o Console do Kaspersky Embedded Systems Security" na página 136).

A interface do Console de Administração do Kaspersky Security Center é usada para executar ações com o Plug-in de Administração. Consulte informações detalhadas sobre a interface do Kaspersky Security Center na *Ajuda do Kaspersky Security Center.*

Licenciamento do aplicativo

Esta seção fornece informações sobre os principais conceitos relacionados ao licenciamento do aplicativo.

Neste capítulo

Sobre o Contrato de Licença do Usuário Final....78
Sobre a licença....79
Sobre o certificado da licença....79
Sobre a chave....80
Sobre o arquivo de chave....80
Sobre o código de ativação....80
Sobre a coleta de dados....81
Ativar o aplicativo com uma chave de licença....83
Ativação do aplicativo com um código....84
Visualizando informações sobre a licença atual....84
Limitações funcionais quando a licença expira....86
Renovação da licença....87
Exclusão da chave....87

Sobre o Contrato de Licença do Usuário Final

O *Contrato de Licença do Usuário Final* é um contrato vinculativo entre o usuário e a AO Kaspersky Lab, que estipula os termos em que poderá usar o aplicativo.

Leia com atenção os termos do Contrato de Licença do Usuário Final antes de começar a usar o aplicativo.

Você pode rever os termos do Contrato de Licença do Usuário Final de várias formas:

- Durante a instalação do Kaspersky Embedded Systems Security
- Abrindo e lendo o arquivo license.txt. Esse documento é incluído no kit de distribuição do aplicativo

Ao confirmar que você aceita o Contrato de Licença do Usuário Final ao instalar o aplicativo, isso significa que você aceita e concorda com os termos do Contrato de Licença do Usuário Final. Se você não aceitar os termos do Contrato de Licença do Usuário Final, você deve cancelar a instalação do aplicativo e não usar o aplicativo.

Sobre a licença

Uma licença é um direito por tempo limitado de usar o aplicativo, concedido a você ao abrigo do Contrato de Licença do Usuário Final.

Uma licença válida dá a você o direito de receber os serviços seguintes:

- O uso do aplicativo de acordo com os termos do Contrato de Licença do Usuário Final
- Suporte técnico

O escopo do serviço e o período do uso do aplicativo dependem do tipo de licença usada para ativar o aplicativo.

O aplicativo é ativado usando um arquivo de chave ou um código de ativação para uma licença comercial adquirida.

Uma licença comercial é uma licença paga concedida após a compra do aplicativo.

O Kaspersky Embedded Systems Security implica as seguintes licenças comerciais:

- Licença padrão do Kaspersky Embedded Systems Security.
- A licença estendida do Kaspersky Embedded Systems Security Compliance Edition, que inclui dois componentes de inspeção do sistema adicionais: Monitor de Integridade de Arquivos e Inspeção de Log.

Quando a licença comercial expira, o aplicativo continua funcionando, mas alguns recursos se tornam inacessíveis (por exemplo, os bancos de dados do Kaspersky Embedded Systems Security não podem ser atualizados). Para continuar usando todos os recursos do Kaspersky Embedded Systems Security, você deve renovar sua licença.

Para garantir proteção máxima contra ameaças à segurança do seu computador, é recomendado renovar a licença antes que ela expire.

Certifique-se de que a chave adicional que você adiciona tem uma data de expiração posterior à da chave ativa.

Sobre o certificado da licença

Um *certificado da licença* é um documento fornecido a você junto com um arquivo de chave ou código de ativação (se aplicável).

Um certificado de licença contém as seguintes informações sobre a licença fornecida:

- Número de ordem
- Informações sobre o usuário a quem foi concedida a licença
- Informações sobre o aplicativo que pode ser ativado com a licença fornecida
- Limite do número de unidades de licenciamento (p. ex., dispositivos nos quais o aplicativo pode ser usado de acordo com a licença fornecida)
- Data inicial da validade da licença
- Data de expiração da licença ou período da licença
- Tipo de licença

Sobre a chave

Uma *chave* é uma sequência de bits com a qual você pode ativar e subsequentemente usar o aplicativo de acordo com os termos do Contrato de Licença do Usuário Final. Uma chave é criada pela Kaspersky Lab.

Você pode adicionar a chave ao aplicativo usando um arquivo de chave. Após adicionar uma chave ao aplicativo, a chave é exibida na interface do aplicativo como uma sequência alfanumérica exclusiva.

A Kaspersky Lab pode colocar na lista negra uma chave por violações do Contrato de Licença. Se sua chave estiver bloqueada, uma chave diferente deve ser adicionada para o aplicativo trabalhar.

Uma chave pode ser uma "chave ativa" ou uma "chave adicional".

Uma chave *ativa* é a chave que o aplicativo usa atualmente para funcionar. Uma chave para uma licença comercial ou de avaliação pode ser adicionada como a chave ativa. O aplicativo não pode ter mais de uma chave ativa.

Uma *chave adicional* é uma chave que confirma o direito de usar o aplicativo mas que não se encontra atualmente em uso. Uma chave adicional torna-se ativa automaticamente quando a licença associada com a chave ativa atual expira. Uma chave adicional pode ser adicionada somente se houver uma chave ativa.

Sobre o arquivo de chave

Um *arquivo de chave* é um arquivo com a extensão .key que você recebe da Kaspersky Lab. Os arquivos de chave destinam-se a ativar o aplicativo adicionando uma chave de licença.

Você recebe um arquivo de chave no endereço de e-mail fornecido ao comprar o Kaspersky Embedded Systems Security ou ao encomendar a versão de avaliação do Kaspersky Embedded Systems Security.

Você não precisa se conectar aos servidores de ativação da Kaspersky Lab para ativar o aplicativo com um arquivo de chave.

Você pode restaurar um arquivo de chave se ele for acidentalmente excluído. Você pode precisar de uma arquivo de chave para registrar um Kaspersky CompanyAccount, por exemplo.

Para restaurar seu arquivo de chave, execute uma das seguintes ações:

- Entre em contato com o vendedor da licença.
- Receba um arquivo de chave pelo site da Kaspersky Lab (https://keyfile.kaspersky.com/en/) usando o seu código de ativação disponível.

Sobre o código de ativação

Um *código de ativação* é uma sequência única de 20 letras e números. Você deve inserir um código de ativação para adicionar uma chave para ativar o Kaspersky Embedded Systems Security. Você recebe o código de ativação no endereço de e-mail fornecido ao adquirir o Kaspersky Embedded Systems Security.

Para ativar o aplicativo com um código de ativação, é preciso ter acesso à Internet para se conectar aos servidores de ativação da Kaspersky Lab.

Se você perdeu seu código de ativação após instalar o aplicativo, ele pode ser recuperado. Você pode precisar do código de ativação para registrar um Kaspersky CompanyAccount, por exemplo. Para recuperar seu código de

ativação, entre em contato com o Suporte Técnico da Kaspersky Lab.

Sobre a coleta de dados

O Contrato de Licença do Kaspersky Embedded Systems Security, especificamente a seção intitulada “Termos do processamento de dados”, especifica os termos, a responsabilidade e o procedimento para enviar e processar os dados indicados neste Manual. Antes de aceitar o Contrato de Licença, revise cuidadosamente os seus termos bem como todos os documentos referenciados em links no Contrato de Licença.

Os dados que a Kaspersky Lab recebe de você durante o uso do aplicativo são protegidos e processados conforme a Política de Privacidade disponível em www.kaspersky.com/Products-and-Services-Privacy-Policy.

Ao aceitar os termos do Contrato de Licença, você aceita enviar automaticamente os seguintes dados à Kaspersky Lab:

- Para apoiar o mecanismo de recepção de atualizações – informações sobre o aplicativo instalado e a sua ativação: o identificador do aplicativo a ser instalado e a sua versão completa, inclusive o número da compilação, tipo e identificador da licença, o identificador de instalação, o identificador de tarefa de atualização.
- Para usar a capacidade de navegar pelos artigos da Base de Dados de Conhecimento quando ocorrerem erros no aplicativo (serviço Redirecionador) – informações sobre o aplicativo e tipo de link, especificamente: o nome, localidade, e número da versão completa do aplicativo, tipo de link redirecionador e o identificador de erro.
- Para gerenciar confirmações para o processamento de dados – informações sobre o status da aceitação de contratos de licença e outros documentos que estipulam termos de transferência de dados: o identificador e a versão do Contrato de Licença ou outro documento, como parte do qual os termos de processamento de dados são aceitos ou recusados; um atributo, significando a ação do usuário (confirmação ou revogação da aceitação dos termos); data e hora de modificações de status da aceitação dos termos de processamento de dados.

Você pode rever os termos do Contrato de Licença do Usuário Final de várias formas:

- Durante a instalação do aplicativo, o Assistente de instalação do Kaspersky Embedded Systems Security exibe o texto completo do Contrato de Licença na etapa de solicitação de aceitação dos termos do Contrato de Licença.
- A qualquer momento no arquivo TXT (license.txt) que contém o texto completo do Contrato de Licença. O arquivo está incluído no kit de distribuição do Kaspersky Embedded Systems Security junto aos arquivos de instalação do aplicativo.

Processamento local de dados

Enquanto executa as funções principais do aplicativo descritas neste Manual, o Kaspersky Embedded Systems Security processa e armazena localmente uma sequência de tipos de dados no computador protegido. Os dados processados localmente pelo aplicativo não são enviados automaticamente à Kaspersky Lab ou a outros sistemas de terceiros.

O Kaspersky Embedded Systems Security processa e armazena os seguintes dados localmente:

- informações sobre arquivos verificados e objetos detectados, por exemplo, nomes e atributos de arquivos processados e caminhos completos deles na mídia verificada, tipos de arquivos, ações realizadas nos arquivos verificados, contas de usuários que executam qualquer ação na rede protegida ou no computador protegido, nomes e dados sobre dispositivos verificados, informações sobre processos executados no sistema, somas de verificação (MD5, SHA-256), carimbo de data/hora, atributos do certificado digital,

dados sobre scripts executados.

- Informações sobre atividades e configurações do sistema operacional, por exemplo, configurações do Firewall do Windows, entradas de Log de Eventos do Windows, nomes de contas de usuário, inicialização de arquivos executáveis, suas somas de verificação e seus atributos.

O Kaspersky Embedded Systems Security processa e armazena dados como parte da funcionalidade básica do aplicativo, inclusive para registrar em log eventos do aplicativo e receber dados de diagnósticos. Os dados processados localmente são protegidos conforme as configurações definidas e aplicadas do aplicativo.

O Kaspersky Embedded Systems Security permite configurar o nível da proteção de dados processados localmente: você pode alterar privilégios de usuários relativos a acesso de dados de processo, alterar o período de retenção de dados para tais dados, desativar inteira ou parcialmente a funcionalidade que envolve o registo de dados e alterar o caminho e os atributos da pasta em que os dados são registrados em log.

Informações detalhadas sobre a configuração da funcionalidade do aplicativo que relativa ao processamento de dados e as configurações padrão do armazenamento de dados processados podem ser encontradas nas seções correspondentes deste Manual.

Por padrão, todos os dados processados localmente pelo aplicativo durante a operação são removidos após a remoção do Kaspersky Embedded Systems Security do computador.

Uma exceção se aplica a arquivos com informações de diagnóstico (arquivos de rastreamento e despejo) e os aos eventos do aplicativo no Log de Eventos do Windows - recomenda-se remover manualmente esses arquivos.

Você pode encontrar as informações detalhadas sobre o trabalho com arquivos que contêm dados de diagnóstico do aplicativo nas seções correspondentes deste Guia.

É possível eliminar arquivos do Log de Eventos do Windows que contenham eventos de programa do Kaspersky Embedded Systems Security pelos meios padrão do sistema operacional.

Processamento local de dados por meio dos componentes auxiliares do aplicativo

O pacote de instalação do Kaspersky Embedded Systems Security contém os componentes auxiliares do aplicativo, que podem ser instalados no servidor ou computador mesmo se o Kaspersky Embedded Systems Security não estiver instalado nele. Esses componentes auxiliares são:

- O Console do Aplicativo. Este componente está incluído no conjunto de Ferramentas de Administração do Kaspersky Embedded Systems Security e é representado por um snap-in do Console de Gerenciamento da Microsoft.
- O Plug-in de Administração. Este componente fornece uma integração completa com o aplicativo do Kaspersky Security Service.

Ao executar as funções principais do aplicativo descrito neste Guia, os componentes auxiliares do aplicativo processam e armazenam localmente um conjunto de dados sobre o computador onde são instalados, mesmo se forem instalados separadamente do Kaspersky Embedded Systems Security.

Os componentes do aplicativo processam e armazenam localmente os seguintes dados:

- O Console do Aplicativo: o nome do computador com o Kaspersky Embedded Systems Security instalado (endereço IP ou nome do domínio) ao qual o Console do Aplicativo se conectou remotamente por último; parâmetros de exibição configurados no snap-in do Console de Gerenciamento da Microsoft; dados sobre a última pasta na qual o usuário selecionou objetos pelo Console do Aplicativo (por meio da caixa de diálogo do sistema aberta ao clicar no botão **Procurar**). Os arquivos de rastreamento do Console do Aplicativo também podem conter os seguintes dados: o nome do computador com o aplicativo do Kaspersky Embedded Systems Security instalado com o qual a conexão remota foi estabelecida, o nome da conta de usuário na qual a conexão remota foi estabelecida.

- O Plug-in de Administração pode processar e armazenar temporariamente dados processados pelo Kaspersky Embedded Systems Security; por exemplo, parâmetros configurados das tarefas e componentes do aplicativo, parâmetros das políticas do Kaspersky Security Center, dados enviados em listas de rede.

Os dados processados pelos componentes auxiliares não são automaticamente enviados à Kaspersky Lab ou outros sistemas de terceiros.

Por padrão, todos os dados processados localmente pelos componentes auxiliares do aplicativo durante a operação são excluídos após a remoção desses componentes.

As exceções são os arquivos de rastreamento dos componentes auxiliares do aplicativo, recomenda-se excluir esses arquivos manualmente.

Você pode encontrar informações detalhadas sobre o trabalho com arquivos que contêm dados de diagnóstico dos componentes auxiliares do aplicativo nas seções correspondentes deste Guia.

Ativar o aplicativo com uma chave de licença

Você pode ativar o Kaspersky Embedded Systems Security aplicando um arquivo de chave.

Se uma chave ativa já tiver sido adicionado ao Kaspersky Embedded Systems Security e você adicionar outra chave como a chave ativa, a nova chave substitui a chave adicionada anteriormente. A chave adicionada anteriormente é removida.

Se uma chave adicional já tiver sido adicionada ao Kaspersky Embedded Systems Security e você adicionar outra chave como uma chave adicional, a nova chave substitui a chave adicionada anteriormente. A chave adicional adicionada anteriormente é removida.

Se uma chave ativa e uma chave adicional já tiverem sido adicionadas ao Kaspersky Embedded Systems Security e você adicionar uma nova chave como a chave ativa, a nova chave substitui a chave ativa adicionada anteriormente; a chave adicional não é removida.

► *Para ativar o Kaspersky Embedded Systems Security usando um arquivo de chave, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Licenciamento**.
2. No painel de detalhes do nó **Licenciamento**, clique no link **Adicionar chave**.
3. Na janela exibida, clique no botão **Procurar** e selecione um arquivo de chave com a extensão .key.

   Você também pode adicionar uma chave como chave adicional. Para adicionar uma chave adicional, marque a caixa de seleção **Usar como chave adicional**.

4. Clique em **OK**.

O arquivo de chave selecionado será aplicado. As informações sobre a chave adicionada estarão disponíveis no nó **Licenciamento**.

Ativação do aplicativo com um código

Para ativar o aplicativo usando um código de ativação, o computador deve estar conectado à Internet.

Você pode ativar o Kaspersky Embedded Systems Security usando um código de ativação.

Com esse método, o Kaspersky Embedded Systems Security envia dados ao servidor de ativação para verificar o código inserido:

- Se a verificação do código de ativação for bem-sucedida, o aplicativo é ativado.
- Se a verificação do código de ativação falhar, a notificação correspondente será exibida. Nesse caso, você deve entrar em contato com o fornecedor de software de quem você comprou a licença do Kaspersky Embedded Systems Security.
- Se o número de ativações com o código de ativação for excedido, a notificação correspondente será exibida. O procedimento de ativação do aplicativo será interrompido e o aplicativo sugerirá que você entre em contato com o Suporte técnico da Kaspersky Lab.

► *Para obter uma chave para ativar o Kaspersky Embedded Systems Security usando um código de ativação, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Licenciamento**.
2. No painel de detalhes do nó **Licenciamento**, clique no link **Adicionar código de ativação**.
3. Na janela exibida, insira o código de ativação no campo **Código de ativação**.
   - Se desejar usar o código de ativação como uma chave adicional, ative a caixa de seleção **Usar como chave adicional**.
   - Se quiser visualizar as informações da licença, clique no botão **Mostrar informações da licença**; elas serão exibidas no grupo **Informações da licença**.
4. Clique em **OK**.

   O Kaspersky Embedded Systems Security envia informações sobre o código de ativação aplicado para o servidor de ativação.

Visualizando informações sobre a licença atual

Visualizando informações de licenciamento

As informações sobre a licença atual são exibidas no painel de detalhes do nó **Kaspersky Embedded Systems Security** do Console do Aplicativo. Uma chave pode ter os seguintes status:

- **Verificando o status da chave** – o Kaspersky Embedded Systems Security está verificando o arquivo de chave ou o código de ativação aplicado e aguardando uma resposta sobre o status da chave atual.
- **Data de expiração da licença** – o Kaspersky Embedded Systems Security foi ativado até a data e hora especificadas. O status da chave é realçado em amarelo nos seguintes casos:
  - A licença expirará em 14 dias e nenhuma chave adicional foi aplicada.
  - A chave adicionada foi colocada na lista negra e está prestes a ser bloqueada.
- **A licença expirou** – o Kaspersky Embedded Systems Security não está ativado porque a licença expirou.

O status é realçado em vermelho.

- **O Contrato de Licença do Usuário Final foi violado** – o Kaspersky Embedded Systems Security não está ativado porque os termos do Contrato de Licença do Usuário Final (consulte a seção "Sobre o Contrato de Licença do Usuário Final" na página 78) foram violados. O status é realçado em vermelho.
- **A chave está na lista negra** – a chave adicionada foi bloqueada e colocada na lista negra pela Kaspersky Lab, por exemplo, se a chave foi usada por terceiros para ativar o aplicativo ilegalmente. O status é realçado em vermelho.

Visualizando informações sobre a licença atual

► *Para visualizar informações sobre a licença atual,*

na árvore do Console do Aplicativo, expanda o nó **Licenciamento**.

As informações gerais sobre a licença atual são exibidas no painel de detalhes do nó **Licenciamento** (consulte a tabela abaixo).

Tabela 8. Informações gerais sobre a licença no nó Licenciamento

Campo	Descrição
Código de ativação	O código de ativação. Este campo é preenchido se você ativar o aplicativo usando um código de ativação.
Status da ativação	Informações sobre o status da ativação do aplicativo. A coluna **Ativação** do painel de detalhes do nó **Licenciamento** pode ter os seguintes status: • **Aplicado** – se você ativou o aplicativo usando um código de ativação ou arquivo de chave. **Ativação** – se você aplicou um código de ativação para ativar o aplicativo, mas o processo de ativação ainda não foi finalizado. O status muda para *Aplicado* quando a ativação do aplicativo é concluída e o conteúdo do painel de detalhes do nó é atualizado. • **Erro de ativação** – se a ativação do aplicativo falhou. Você pode visualizar a causa da ativação mal sucedida no log de tarefas.
Chave	A chave usada para ativar o aplicativo.
Tipo de licença	Tipo de licença: comercial ou de avaliação.
Data de expiração	Data e hora de expiração da licença associada à chave ativa.
Status do código de ativação ou da chave	Status do código de ativação ou da chave: Ativa ou Adicional.

► *Para visualizar informações detalhadas sobre a licença,*

no nó **Licenciamento**, abra o menu de contexto na linha com os dados de licença que deseja expandir e selecione **Propriedades**.

Na janela **Propriedades: <Status do código de ativação ou status da chave>**, a guia **Geral** exibe informações detalhadas sobre a licença atual, e a guia **Avançado** exibe informações sobre o cliente e os detalhes de contato da Kaspersky Lab ou do revendedor onde você adquiriu o Kaspersky Embedded Systems Security (consulte a tabela abaixo).

Tabela 9. Informações detalhadas da licença na janela Propriedades: <Status de Código de ativação ou status da chave>

Campo	Descrição
Guia Geral	
Chave	A chave usada para ativar o aplicativo.
Data de adição da chave	Data em que a chave foi adicionada ao aplicativo.
Tipo de licença	Tipo de licença: comercial ou de avaliação.
Dias até a expiração	Número de dias restantes até a expiração da licença associada à chave ativa.
Data de expiração	Data e hora de expiração da licença associada à chave ativa. Se você ativar o aplicativo com uma assinatura ilimitada, o valor do campo é *Ilimitado*. Se o Kaspersky Embedded Systems Security não for capaz de determinar a data de expiração da licença, o valor do campo é definido como *Desconhecido*.
Aplicativo	O nome do aplicativo ativado com o arquivo de chave ou código de ativação.
Restrição de uso da chave	Restrição de uso da chave (se houver).
Elegível para suporte técnico	Informações sobre se a Kaspersky Lab ou um de seus parceiros fornecerá Suporte técnico de acordo com os termos da licença.
Guia Avançado	
Informações sobre a licença	Número da licença atual.
Informações de suporte	Detalhes de contato da Kaspersky Lab ou de seu parceiro que fornece o Suporte técnico. Este campo pode ficar vazio se o suporte técnico não for fornecido.
Informações do proprietário	Informações sobre o proprietário da licença: o nome do cliente e o nome da organização para a qual a licença foi adquirida.

Limitações funcionais quando a licença expira

Quando a licença atual expira, as seguintes limitações são aplicadas aos componentes funcionais:

- Todas as tarefas serão interrompidas, exceto as tarefas de Proteção de Arquivos em Tempo Real, Verificação por Demanda e Controle de Integridade de Aplicativos.
- Não é possível iniciar nenhuma tarefa, exceto a Proteção de Arquivos em Tempo Real Verificação por Demanda e Controle de Integridade de Aplicativos. Essas tarefas continuam a ser executadas usando os bancos de dados de antivírus antigos.
- A funcionalidade de Prevenção de Exploits será limitada:

- Os processos serão protegidos até que sejam reiniciados.
- Os novos processos não podem ser adicionados ao escopo da proteção.

Outras funções (repositórios, logs, informações de diagnóstico) ainda estarão disponíveis.

Renovação da licença

Por padrão, quando a licença tem 14 dias restantes antes da expiração, o Kaspersky Embedded Systems Security notifica você sobre a data de expiração próxima. Nesse caso, o status **Data de expiração da licença** é realçado em amarelo no painel de detalhes do nó **Kaspersky Embedded Systems Security**.

Você pode renovar a licença antes da data de expiração usando um arquivo de chave adicional ou um código de ativação. Isto garante que seu computador permaneça protegido após a expiração da licença atual e antes que você ative o aplicativo com uma nova licença.

► *Para renovar uma licença, siga as etapas a seguir:*

1. Obtenha um novo código de ativação ou um arquivo de chave.
2. Na árvore do Console do Aplicativo, abra o nó **Licenciamento**.
3. Execute uma das ações seguintes no painel de detalhes do nó **Licenciamento**:
   - Caso deseje renovar uma licença usando uma chave adicional:
     a. Clique no link **Adicionar** chave.
     b. Na janela exibida, clique no botão **Procurar** e selecione um novo arquivo de chave com a extensão .key.
     c. Marque a caixa de seleção **Usar como chave adicional**.
   - Caso deseje renovar uma licença usando um código de ativação:
     a. Clique no link **Adicionar código de ativação**.
     b. Insira o código de ativação adquirido na janela que se abre.
     c. Marque a caixa de seleção **Usar como chave adicional**.

   É necessária uma conexão com a internet para aplicar um código de ativação.
4. Clique em **OK**.

   A chave adicional serão adicionados e automaticamente aplicados após a expiração da licença atual do Kaspersky Embedded Systems Security.

Exclusão da chave

Você pode remover a chave adicionada.

Se uma chave adicional tiver sido adicionada ao Kaspersky Embedded Systems Security e você remover a chave ativa, a chave adicional torna-se automaticamente a chave ativa.

Se você excluir uma chave adicionada, você pode restaurá-la aplicando novamente o arquivo de chave.

► *Para remover uma chave adicionada:*

1. Na árvore do Console do Aplicativo, selecione o nó **Licenciamento**.
2. No painel de detalhes do nó **Licenciamento**, na tabela contendo informações sobre chaves adicionadas, selecione a chave que deseja remover.
3. No menu de contexto da linha contendo informações sobre a chave selecionada, selecione **Remover**.
4. Clique no botão **Sim** na janela de confirmação para confirmar que você deseja excluir a chave.

A chave selecionada será removida.

Trabalhar como Plug-in de administração

Esta seção fornece informações sobre o Plug-in de Administração do Kaspersky Embedded Systems Security e descreve como gerenciar o aplicativo instalado em um computador protegido ou em um grupo de computadores.

Neste capítulo

Gerenciamento do Kaspersky Embedded Systems Security a partir do Kaspersky Security Center 89

Gerenciamento das configurações do aplicativo 91

Criação e configuração de políticas 108

Criando e configurando uma tarefa usando o Kaspersky Security Center 116

Relatórios do Kaspersky Security Center 133

Gerenciamento do Kaspersky Embedded Systems Security a partir do Kaspersky Security Center

É possível gerenciar de modo centralizado vários computadores com o Kaspersky Embedded Systems Security instalado e incluído em um grupo de administração por meio do Plug-in de Administração do programa. Com o Kaspersky Security Center, também é possível definir separadamente as configurações de operação de cada computador incluído no grupo de administração.

O grupo de administração é criado manualmente ao lado do Kaspersky Security Center e inclui vários computadores com o Kaspersky Embedded Systems Security instalado para os quais você deseja definir as mesmas configurações de controle e de proteção. Para obter mais detalhes sobre a utilização de grupos de administração, consulte a *Ajuda do Kaspersky Security Center*.

Não será possível configurar o aplicativo se a operação do Kaspersky Embedded Systems Security no computador for controlada por uma política ativa do Kaspersky Security Center.

O Kaspersky Embedded Systems Security pode ser gerenciado do Kaspersky Security Center das seguintes maneiras:

- **Usando políticas do Kaspersky Security Center**. As políticas do Kaspersky Security Center podem ser usadas para definir remotamente as mesmas configurações de proteção para um grupo de computadores. As configurações de tarefa especificadas na política ativa têm prioridade sobre configurações de tarefa definidas localmente no Console do Aplicativo ou remotamente na janela **Propriedades: <Nome do computador>** do Kaspersky Security Center.

  Você pode usar políticas para definir as configurações gerais do aplicativo, de tarefa de Proteção em Tempo Real, de tarefas de Controle de Atividades Locais, de inicialização de tarefas do sistema programadas e de uso de perfil.

- **Usando tarefas de grupo do Kaspersky Security Center**. Com as tarefas de grupo do Kaspersky

Security Center, é possível definir remotamente configurações comuns de tarefas com um período de validade para um grupo de computadores.

- É possível utilizar as tarefas de grupo para ativar o aplicativo, definir configurações da tarefa de Verificação por Demanda, atualizar configurações da tarefa e as configurações da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos.
- **Usando tarefas para um grupo de dispositivos**. Com as tarefas para um conjunto de dispositivos, é possível definir remotamente configurações de tarefa comuns com um período de execução limitado para computadores que não pertencem a nenhum dos grupos de administração.
- **Usando a janela de propriedades de um único computador**. Na janela **Propriedades: <Nome do computador>**, é possível definir remotamente as configurações de tarefa de um único computador incluído no grupo de administração. Você pode definir tanto as configurações gerais do aplicativo como as configurações de todas as tarefas do Kaspersky Embedded Systems Security se o computador selecionado não for controlado por uma política ativa do Kaspersky Security Center.

Com o Kaspersky Security Center, é possível definir configurações do aplicativo, recursos avançados e trabalhar com logs e notificações. É possível definir essas configurações para um grupo de computadores, bem como para um computador individual.

Gerenciamento das configurações do aplicativo

Esta seção contém informações sobre como definir as configurações gerais do Kaspersky Embedded Systems Security no Kaspersky Security Center.

Neste capítulo

Gerenciamento do Kaspersky Embedded Systems Security a partir do Kaspersky Security Center 91

Navegação 92

Definindo as configurações gerais do aplicativo no Kaspersky Security Center 93

Definindo as configurações de Quarentena e de Backup no Kaspersky Security Center 99

Configurações de logs e notificações 100

Gerenciamento do Kaspersky Embedded Systems Security a partir do Kaspersky Security Center

É possível gerenciar de modo centralizado vários computadores com o Kaspersky Embedded Systems Security instalado e incluído em um grupo de administração por meio do Plug-in de Administração do programa. Com o Kaspersky Security Center, também é possível definir separadamente as configurações de operação de cada computador incluído no grupo de administração.

O grupo de administração é criado manualmente ao lado do Kaspersky Security Center e inclui vários computadores com o Kaspersky Embedded Systems Security instalado para os quais você deseja definir as mesmas configurações de controle e de proteção. Para obter mais detalhes sobre a utilização de grupos de administração, consulte a *Ajuda do Kaspersky Security Center*.

Não será possível configurar o aplicativo se a operação do Kaspersky Embedded Systems Security no computador for controlada por uma política ativa do Kaspersky Security Center.

O Kaspersky Embedded Systems Security pode ser gerenciado do Kaspersky Security Center das seguintes maneiras:

- **Usando políticas do Kaspersky Security Center**. As políticas do Kaspersky Security Center podem ser usadas para definir remotamente as mesmas configurações de proteção para um grupo de computadores. As configurações de tarefa especificadas na política ativa têm prioridade sobre configurações de tarefa definidas localmente no Console do Aplicativo ou remotamente na janela **Propriedades: <Nome do computador>** do Kaspersky Security Center.

  Você pode usar políticas para definir as configurações gerais do aplicativo, de tarefa de Proteção em Tempo Real, de tarefas de Controle de Atividades Locais, de inicialização de tarefas do sistema programadas e de uso de perfil.

- **Usando tarefas de grupo do Kaspersky Security Center**. Com as tarefas de grupo do Kaspersky Security Center, é possível definir remotamente configurações comuns de tarefas com um período de validade para um grupo de computadores.

- É possível utilizar as tarefas de grupo para ativar o aplicativo, definir configurações da tarefa de Verificação por Demanda, atualizar configurações da tarefa e as configurações da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos.
- **Usando tarefas para um grupo de dispositivos**. Com as tarefas para um conjunto de dispositivos, é possível definir remotamente configurações de tarefa comuns com um período de execução limitado para computadores que não pertencem a nenhum dos grupos de administração.
- **Usando a janela de propriedades de um único computador**. Na janela **Propriedades: <Nome do computador>**, é possível definir remotamente as configurações de tarefa de um único computador incluído no grupo de administração. Você pode definir tanto as configurações gerais do aplicativo como as configurações de todas as tarefas do Kaspersky Embedded Systems Security se o computador selecionado não for controlado por uma política ativa do Kaspersky Security Center.

Com o Kaspersky Security Center, é possível definir configurações do aplicativo, recursos avançados e trabalhar com logs e notificações. É possível definir essas configurações para um grupo de computadores, bem como para um computador individual.

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface.

Nesta seção

Abrir as configurações gerais a partir da política 92

Abrir as configurações gerais na janela de propriedades do aplicativo 92

Abrir as configurações gerais a partir da política

► *Para abrir as configurações do aplicativo do Kaspersky Embedded Systems Security a partir da política:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Configurações do aplicativo**.
6. Clique no botão **Configurações** na subseção das configurações que você deseja definir.

Abrir as configurações gerais na janela de propriedades do aplicativo

► *Para abrir a janela de propriedades do Kaspersky Embedded Systems Security de um único computador:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Dispositivos**.
4. Abra a janela **Propriedades: <Nome do computador>** de uma das seguintes maneiras:
   - Clique duas vezes no nome do computador protegido.
   - Selecione o item **Propriedades** no menu de contexto do computador protegido.

   A janela **Propriedades: <Nome do computador>** é exibida.
5. Na seção **Aplicativos**, selecione **Kaspersky Embedded Systems Security**.
6. Clique no botão **Propriedades**.

   A janela de **configurações do aplicativo "Kaspersky Embedded Systems Security"** é exibida.
7. Selecione a seção **Configurações do aplicativo**.

Definindo as configurações gerais do aplicativo no Kaspersky Security Center

Você pode definir configurações gerais para o Kaspersky Embedded Systems Security através do Kaspersky Security Center para um grupo de computadores ou para um computador.

Nesta seção

Configuração de escalabilidade e interface no Kaspersky Security Center 93
Definição das configurações de segurança no Kaspersky Security Center 94
Definição das configurações de conexão usando o Kaspersky Security Center 96
Configuração da inicialização programada de tarefas locais do sistema 97

Configuração de escalabilidade e interface no Kaspersky Security Center

► *Para configurar configurações de escalabilidade e a interface do aplicativo:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

> Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

4. Na seção **Configurações do aplicativo**, no bloco **Escalabilidade e interface**, clique em **Configurações**.
5. Na janela **Configurações avançadas do aplicativo**, na guia **Geral**, defina as seguintes configurações:
   - Na seção **Configurações de escalabilidade**, defina as configurações que definem o número de processos usados pelo Kaspersky Embedded Systems Security:
     - **Detectar automaticamente as configurações de escalabilidade**.

       O Kaspersky Embedded Systems Security regulará automaticamente o número de processos utilizados.

       Este é o valor padrão.
     - **Definir o número de processos de trabalho manualmente**.

       O Kaspersky Embedded Systems Security regulará o número de processos de trabalho ativos de acordo com os valores especificados.

       - **Número máximo de processos ativos.**

         Número máximo de processos que o Kaspersky Embedded Systems Security usa. O campo de inserção de dados está disponível se a opção **Definir o número de processos de trabalho manualmente** estiver selecionada.
       - **Número de processos para a proteção em tempo real.**

         O número máximo de processos usados pelos componentes da tarefa de Proteção em Tempo Real. O campo de inserção de dados está disponível se a opção **Definir o número de processos de trabalho manualmente** estiver selecionada.
       - **Número de processos de tarefas de verificação por demanda em segundo plano.**

         Número máximo de processos utilizados pelo componente de Verificação por demanda ao executar tarefas de Verificação por Demanda em segundo plano. O campo de inserção de dados está disponível se a opção **Definir o número de processos de trabalho manualmente** estiver selecionada.
   - Na seção **Interação com o usuário**, configure a exibição do ícone do aplicativo da bandeja do sistema na área de notificação: desmarque ou selecione a caixa **Exibir o ícone da Bandeja do Sistema na barra de tarefas**.
6. Na guia **Armazenamento hierárquico**, selecione a opção para acessar o armazenamento hierárquico.
7. Clique em **OK**.

As configurações do aplicativo definidas são salvas.

Definição das configurações de segurança no Kaspersky Security Center

► *Para definir as configurações de segurança manualmente, siga as etapas a seguir:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.

3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
4. Na seção **Configurações do aplicativo**, clique no botão **Configurações** nas definições de **Segurança**.
5. Na janela **Configurações de segurança**, defina as seguintes configurações:
   - Na seção **Configurações de confiabilidade**, defina as configurações de recuperação de tarefas do Kaspersky Embedded Systems Security quando o aplicativo retornar um erro ou for encerrado.
     - **Executar recuperação da tarefa**

       Esta caixa de seleção ativa ou desativa a recuperação do Kaspersky Embedded Systems Security quando houver um erro ou o aplicativo for encerrado.

       Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security recuperará automaticamente as tarefas do Kaspersky Embedded Systems Security quando houver um erro ou o aplicativo for encerrado.

       Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não recuperará automaticamente as tarefas do Kaspersky Embedded Systems Security quando houver um erro ou o aplicativo for encerrado.

       A caixa de seleção é selecionada por padrão.
     - **Não recuperar tarefas de verificação por demanda mais do que (vezes)**

       O número de tentativas de recuperação de uma tarefa de Verificação por demanda após o Kaspersky Embedded Systems Security se recuperar de um erro. O campo de inserção estará disponível se a caixa de seleção **Executar recuperação da tarefa** estiver selecionada.
   - Na seção **Ações ao mudar para energia de backup UPS**, especifique as limitações na carga do computador criadas pelo Kaspersky Embedded Systems Security após mudar para uma fonte de energia UPS:
     - **Não iniciar tarefas de verificação programadas**

       Esta caixa de seleção ativa ou desativa a inicialização de uma tarefa de verificação programada após o computador mudar para uma fonte de energia UPS até que o modo de fornecimento de energia padrão seja restaurado.

       Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security não executará as tarefas de verificação programadas após o computador mudar para uma fonte UPS até que o modo de fornecimento de energia padrão seja restaurado.

       Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security executará as tarefas de verificação independentemente do modo de fornecimento de energia.

A caixa de seleção é selecionada por padrão.

- **Interromper tarefas de verificação atuais**

  A caixa de seleção ativa ou desativa a execução das tarefas de verificação após o computador mudar para uma fonte UPS.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security pausará as tarefas de verificação em execução após o computador mudar para uma fonte UPS.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security continuará as tarefas de verificação em execução após o computador mudar para uma fonte UPS.

  A caixa de seleção é selecionada por padrão.

- Na seção **Configurações de proteção de senha**, defina uma senha para proteger o acesso às funções do Kaspersky Embedded Systems Security.

6. Clique em **OK**.

As configurações de escalabilidade e de confiabilidade são salvas.

Definição das configurações de conexão usando o Kaspersky Security Center

As configurações de conexão definidas são usadas para conectar o Kaspersky Embedded Systems Security aos servidores de atualização e ativação e durante a integração de aplicativos com os serviços da KSN.

► *Para definir as configurações de conexão, siga as etapas a seguir:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
4. Na seção **Configurações do aplicativo**, clique no botão **Configurações** no bloco **Conexões**.

   A janela **Configurações de conexão** é aberta.
5. Na janela **Configurações de conexão**, defina as seguintes configurações:
   - Na seção **Configurações do servidor proxy**, selecione as configurações de uso do servidor proxy:
     - **Não usar o servidor proxy**.

Se esta opção estiver selecionada, o Kaspersky Embedded Systems Security conecta-se a serviços da KSN diretamente, sem usar nenhum servidor proxy.

- **Usar configurações especificadas de servidor proxy**.

  Se esta opção estiver selecionada, o Kaspersky Embedded Systems Security se conectará a KSN usando configurações de servidor proxy especificadas manualmente.

- Endereço IP ou o nome do símbolo do servidor proxy e o número da porta.
- **Ignorar servidor proxy para endereços locais**.

  A caixa ativa ou desativa o uso de um servidor proxy ao acessar computadores localizados na mesma rede que o computador com o Kaspersky Embedded Systems Security instalado.

  Se esta caixa estiver selecionada, os computadores serão acessados diretamente da rede, que hospeda o computador com o Kaspersky Embedded Systems Security instalado. Nenhum servidor proxy é usado.

  Se a caixa estiver desmarcada, o servidor proxy será aplicado para se conectar a computadores locais.

  A caixa de seleção é selecionada por padrão.

- Na seção **Configurações de autenticação do servidor proxy**, especifique as configurações de autenticação:
  - Selecione as configurações de autenticação na lista suspensa.
    - **Não usar autenticação** – a autenticação não é executada. Esse modo é selecionado por padrão.
    - **Usar autenticação NTLM** – a autenticação será executada com o protocolo de autenticação de rede NTLM desenvolvido pela Microsoft.
    - **Usar autenticação NTLM com nome de usuário e senha** – a autenticação será executada usando o nome e a senha através do protocolo de autenticação de rede NTLM desenvolvido pela Microsoft.
    - **Aplicar nome de usuário e senha** – a autenticação é executada com o uso de um nome de usuário e senha.
  - Insira o nome de usuário e a senha, se necessário.
- No bloco **Licenciamento** desmarque ou selecione **Usar o Kaspersky Security Center como servidor proxy ao ativar o aplicativo**.

6. Clique em **OK**.

As configurações de conexão definidas são salvas.

Configuração da inicialização programada de tarefas locais do sistema

É possível usar políticas para permitir ou bloquear a inicialização da tarefa de Verificação por Demanda e da tarefa de Atualização do sistema local de acordo com a seguinte programação configurada localmente em cada computador no grupo de administração:

- Se a inicialização programada de um tipo específico de tarefa local do sistema for proibida por uma política, essas tarefas não serão realizadas no computador local de acordo com a programação. É possível iniciar tarefas locais do sistema manualmente.

- Se a inicialização programada de um tipo específico de tarefa local do sistema for permitida por uma política, essas tarefas serão realizadas de acordo com os parâmetros programados configurados localmente para essa tarefa.

Por padrão, a inicialização de tarefas locais do sistema é proibida pela política.

Recomendamos que você não permita que tarefas locais do sistema sejam iniciadas se atualizações ou verificações por demanda estiverem sendo administradas por tarefas de grupo do Kaspersky Security Center.

Caso você não use as tarefas de atualização de grupo e verificação por demanda, permita que as tarefas locais do sistema sejam inicializadas na política: o Kaspersky Embedded Systems Security executará atualizações de banco de dados do aplicativo e de módulos, e iniciará todas as tarefas locais do sistema de verificação por demanda de acordo com a programação padrão.

Você pode usar políticas para permitir ou bloquear a inicialização programada das tarefas locais do sistema a seguir:

- Tarefas de Verificação por Demanda: Verificação de Áreas Críticas. Verificação da Quarentena, Verificação na Inicialização do Sistema Operacional, Controle de Integridade de Aplicativos.
- Tarefas de Atualização: Atualização do Banco de Dados, Atualização de módulos de software e Copiar Atualizações.

Se o computador protegido for excluído do grupo de administração, a programação de tarefas do sistema será ativada automaticamente.

► *Para permitir ou bloquear a inicialização programada de tarefas do sistema do Kaspersky Embedded Systems Security em uma política, siga as etapas a seguir:*

1. No nó **Dispositivos gerenciados** da árvore do Console de Administração, expanda o grupo requerido e selecione a guia **Políticas**.
2. Na guia **Políticas**, no menu de contexto da política para a qual você deseja configurar o início programado de tarefas do sistema do Kaspersky Embedded Systems Security nos computadores do grupo, selecione o item **Propriedades**
3. Na janela **Propriedades: <Nome da política>**, abra a seção **Configurações do aplicativo**. Na seção **Executar tarefas do sistema**, clique no botão **Configurações** e faça o seguinte:
   - Marque as caixas de seleção **Permitir inicialização de tarefas de verificação por demanda** e **Permitir tarefas de atualização e inicialização da tarefa de Cópia de atualização** para permitir a inicialização programada das tarefas listadas.
   - Desmarque as caixas **Permitir inicialização de tarefas de verificação por demanda** e **Permitir tarefas de atualização e inicialização da tarefa de Cópia de atualização** para desativar a inicialização programada das tarefas listadas.

   Marcar ou desmarcar a caixa de seleção não afetará as configurações de inicialização de quaisquer tarefas locais personalizadas desse tipo.
4. Certifique-se de que a política que você está configurando esteja ativa e seja aplicada ao grupo de

computadores selecionados.

5. Clique em **OK**.

As configurações de inicialização da tarefa programada são aplicadas às tarefas selecionadas.

Definindo as configurações de Quarentena e de Backup no Kaspersky Security Center

► *Para definir as configurações gerais do Backup no Kaspersky Security Center:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
4. Na seção **Suplementar**, clique no botão **Configurações** na subseção **Armazenamentos**.
5. Use a guia **Backup** da janela de configurações de **Armazenamentos** para especificar as configurações de Backup a seguir:
   - Para especificar a pasta de backup, use o campo **Pasta de backup** para selecionar a pasta requerida na unidade local do computador protegido ou insira o caminho completo.
   - Para configurar o tamanho máximo do Backup, selecione a caixa de seleção **Tamanho máximo do backup (MB)** e especifique o valor relevante em megabytes no campo de inserção de dados.
   - Para configurar o limite de espaço disponível no Backup, defina o valor da configuração **Tamanho máximo do backup (MB)**, selecione a caixa **Valor limite de espaço disponível (MB)** e especifique o valor mínimo de espaço disponível na pasta do Backup em megabytes.
   - Para especificar uma pasta para objetos restaurados, selecione a pasta relevante em uma unidade local do computador protegido na seção **Configurações de restauração** ou insira o nome e o caminho completo da pasta no campo **Pasta destino para a restauração de objetos**.
6. Na janela de configurações de **Armazenamentos**, na guia **Quarentena**, defina as seguintes configurações da Quarentena:
   - Para alterar a pasta da quarentena, no campo de inserção de dados da **Pasta da Quarentena**, especifique o caminho completo da pasta na unidade local do computador protegido.
   - Para configurar o tamanho máximo da Quarentena, selecione a caixa **Tamanho máximo da Quarentena (MB)** e especifique o valor desse parâmetro em megabytes no campo de inserção.

- Para configurar o volume mínimo de espaço disponível na Quarentena, selecione a caixa **Tamanho máximo da Quarentena (MB)** e a caixa **Valor limite de espaço disponível (MB)** e, em seguida, especifique o valor desse parâmetro em megabytes no campo de inserção.
- Para alterar a pasta onde os objetos são restaurados a partir da Quarentena, no campo de inserção **Pasta destino para a restauração de objetos**, especifique o caminho completo para a pasta na unidade local do computador protegido.

7. Clique em **OK**.

As configurações de Quarentena e Backup definidas são salvas.

Configurações de logs e notificações

O Console de Administração do Kaspersky Security Center pode ser usado para configurar notificações para administradores e usuários sobre os seguintes eventos relacionados ao Kaspersky Embedded Systems Security e ao status de proteção de antivírus no computador protegido:

- O administrador pode receber informações sobre eventos de tipos selecionados;
- Os usuários de LAN que acessam o computador protegido e os usuários do computador terminal podem receber informações sobre eventos do tipo *Objeto detectado*.

As notificações sobre os eventos do Kaspersky Embedded Systems Security podem ser configuradas para um único computador usando a janela **Propriedades: <Nome do computador>** do computador selecionado ou para um grupo de computadores na janela **Propriedades: <Nome da política>** do grupo de administração selecionado.

Na guia **Notificações de evento** ou na janela **Configurações de notificação**, você pode configurar os seguintes tipos de notificações:

- As notificações do administrador sobre eventos dos tipos selecionados podem ser configuradas na guia **Notificações de evento** (a guia padrão do aplicativo Kaspersky Security Center). Para obter mais detalhes sobre os métodos de notificação, consulte a *Ajuda do Kaspersky Security Center*.
- As notificações de administrador e usuário podem ser configuradas usando a janela **Configurações de notificação**.

Você pode configurar notificações para alguns tipos de eventos somente na janela ou na guia; você pode usar tanto a janela quanto a guia para configurar notificações para outros tipos de eventos.

Se você configurar notificações sobre eventos do mesmo tipo usando o mesmo modo na guia **Notificações de evento** e na janela **Configurações de notificação**, o administrador do sistema receberá notificações desses eventos duas vezes, mas no mesmo modo.

Nesta seção

Definição de configurações de log 101
Log de segurança 102
Definições das configurações de integração SIEM 102
Definição de configurações de notificação 105
Configuração de interações com o Servidor de Administração 106

Definição de configurações de log

► *Para configurar os logs do Kaspersky Embedded Systems Security, execute as seguintes etapas:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
4. Na seção **Logs e notificações**, clique no botão **Configurações** no bloco **Logs de tarefas**.
5. Na janela **Configurações de notificação** , defina as seguintes configurações do Kaspersky Embedded Systems Security de acordo com seus requisitos:
   - Configure o nível de detalhe de eventos em logs. Para isso, execute as seguintes ações:
     a. Na lista **Componente**, selecione o componente do Kaspersky Embedded Systems Security para o qual você deseja configurar o nível de detalhe.
     b. Para configurar o nível de detalhes nos logs de tarefas e no log de auditoria do sistema para o componente selecionado, selecione o nível requerido em **Nível de importância**.
   - Para alterar a localização padrão para logs, especifique o caminho completo para a pasta ou clique no botão **Procurar** para selecioná-la.
   - Especifique o número de dias em que os logs de tarefas serão armazenados.
   - Especifique o número de dias em que as informações exibidas no nó **Log de auditoria do sistema** serão armazenadas.
6. Clique em **OK**.

As configurações de log definidas são salvas.

Log de segurança

O Kaspersky Embedded Systems Security mantém um log de eventos associados a violações de segurança ou tentativas de violação no computador protegido. Os eventos a seguir são registrados nesse log:

- Eventos de Prevenção de Exploits.
- Eventos críticos de Inspeção de Log.
- Eventos críticos que indicam uma tentativa de violação de segurança (para as tarefas de Proteção do Computador em Tempo Real, Verificação por Demanda, Monitor de Integridade de Arquivos, Controle de Inicialização de Aplicativos e Controle de Dispositivos).

Você pode limpar o Log de segurança bem como o Log de auditoria do sistema (consulte a seção "Excluir eventos do log de auditoria do sistema" na página 203). Além disso, o Kaspersky Embedded Systems Security registra eventos de auditoria do sistema relativos à exclusão do Log de segurança.

Definições das configurações de integração SIEM

Para reduzir a carga nos dispositivos de baixo desempenho e reduzir o risco de degradação do sistema como resultado de maiores volumes de logs de aplicativo, é possível configurar a publicação de eventos de auditoria e de desempenho de tarefa para o *servidor syslog* por meio do protocolo Syslog.

Um servidor syslog é um servidor externo para eventos de agregação (SIEM). Ele coleta e analisa eventos recebidos e também executa outras ações de gerenciamento de logs.

É possível usar a integração SIEM de duas maneiras:

- Eventos duplicados no servidor syslog: este modo prescreve que todos os eventos de realização de tarefa cuja publicação esteja definida nas configurações de logs bem como todos os eventos de auditoria do sistema continuem a ser armazenados no computador local mesmo após terem sido enviados ao SIEM.

  Recomenda-se que esse modo seja utilizado para reduzir ao máximo a carga no computador protegido.

- Excluir cópias locais de eventos: este modo prescreve que todos os eventos registrados durante a operação do aplicativo e publicados no SIEM serão excluídos do computador local.

  > O aplicativo nunca exclui versões locais do log de segurança.

O Kaspersky Embedded Systems Security pode converter eventos em logs de aplicativo em formatos compatíveis com o servidor syslog para que esses eventos possam ser transmitidos e reconhecidos com sucesso pelo SIEM. O aplicativo é compatível com a conversão para um formato de dados estruturados e para o formato JSON.

Para reduzir o risco de transmissão mal sucedida de eventos ao SIEM, é possível definir as configurações para conectar ao servidor syslog de espelhamento.

Um servidor syslog de espelhamento adicional para o qual o aplicativo se alterna automaticamente se a conexão ao servidor principal syslog estiver indisponível ou se o servidor principal não puder ser utilizado.

Por padrão, a integração SIEM não é utilizada. É possível ativar e desativar a integração SIEM e definir as configurações de funcionalidade (consulte a tabela abaixo).

Tabela 10. Configurações de integração SIEM

Configuração	Valor padrão	Descrição
Enviar eventos para um servidor syslog remoto pelo protocolo syslog	Não aplicado	É possível ativar ou desativar a integração SIEM marcando ou desmarcando a caixa de seleção, respectivamente.
Remover cópias locais dos eventos que foram enviados para um servidor syslog remoto	Não aplicado	É possível definir as configurações para armazenar as cópias locais dos logs após eles terem sido enviados ao SIEM marcando ou desmarcando a caixa de seleção.
Formato dos eventos	Dados estruturados	É possível selecionar um de dois formatos nos quais o aplicativo converte seus eventos antes de enviá-los ao servidor syslog para um melhor reconhecimento desses eventos pelo SIEM.
Protocolo de conexão	TCP	Você pode usar a lista suspensa para configurar a conexão ao servidor syslog principal via protocolos UDP ou TCP; ao servidor syslog de espelhamento pelo protocolo TCP.
Configurações de conexão do servidor syslog principal	Endereço IP: 127.0.0.1 Porta: 514	Você pode usar os campos apropriados para configurar o endereço IP e a porta usados para conectar-se ao servidor syslog principal. É possível especificar o endereço IP somente no formato IPv4.
Use um servidor syslog de espelhamento se o servidor principal não estiver acessível	Não aplicado	É possível usar a caixa de seleção para ativar ou desativar o uso de um servidor syslog refletido.
Configurações de conexão do servidor syslog de espelhamento	Endereço IP: 127.0.0.1 Porta: 514	Você pode usar os campos apropriados para configurar o endereço IP e a porta usados para conectar-se ao servidor syslog de espelhamento. É possível especificar o endereço IP somente no formato IPv4.

► *Para definir as configurações de integração SIEM:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

> Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

4. Na seção **Logs e notificações**, clique no botão **Configurações** no bloco **Logs de tarefas**.

   A janela **Configurações de logs e notificações** é aberta.

5. Selecione a guia **Integração SIEM**.
6. Na seção **Configurações de integração**, marque a caixa de seleção **Enviar eventos para um servidor syslog remoto pelo protocolo syslog**.

   A caixa de seleção ativa ou desativa a funcionalidade de envio de eventos publicados a um servidor syslog externo.

   Se a caixa de seleção for selecionada, o aplicativo enviará eventos publicados ao SIEM de acordo com as configurações de integração SIEM definidas.

   Se a caixa de seleção for desmarcada, o aplicativo não executará a integração SIEM. Não é possível definir as configurações de integração SIEM se a caixa de seleção for desmarcada.

   Esta caixa é desmarcada por padrão.

7. Se necessário, na seção **Configurações de integração**, marque a caixa de seleção **Remover cópias locais dos eventos que foram enviados para um servidor syslog remoto**.

   A caixa de seleção ativa ou desativa a exclusão de cópias locais de logs quando eles são enviados para o SIEM.

   Se a caixa de seleção for marcada, o aplicativo exclui cópias locais de eventos depois que eles tiverem sido publicados com sucesso no SIEM. Este modo é recomendado em computadores com desempenho limitado.

   Se a caixa de seleção for desmarcada, o aplicativo apenas enviará os eventos para o SIEM. As cópias de logs continuam sendo armazenadas localmente.

   Esta caixa é desmarcada por padrão.

> O status da caixa de seleção **Remover cópias locais dos eventos que foram enviados para um servidor syslog remoto** não afeta as configurações de armazenamento de eventos do log de segurança: o aplicativo nunca exclui automaticamente os eventos de log de segurança.

8. Na seção **Formato dos eventos**, especifique o formato para o qual deseja converter eventos de operação do aplicativo para que sejam enviados ao SIEM.

   Por padrão, o aplicativo converte-os em um formato de dados estruturados.

9. Na seção **Configurações de conexão**:
   - Especifique o protocolo de conexão SIEM.
   - Especifique as configurações para a conexão com o servidor syslog principal.

     É possível especificar um endereço IP somente no formato IPv4.

   - Marque a caixa de seleção **Use um servidor syslog de espelhamento se o servidor principal não estiver acessível** se desejar que o aplicativo use outras configurações de conexão quando não for possível enviar eventos para o servidor syslog principal.

- Especifique as seguintes configurações para a conexão com o servidor syslog de espelhamento: **Endereço IP** e **Porta**.

  Os campos **endereço IP** e **Porta** do servidor syslog de espelhamento não poderão ser editados se a caixa de seleção **Use um servidor syslog de espelhamento se o servidor principal não estiver acessível** estiver desmarcada.

  É possível especificar um endereço IP somente no formato IPv4.

10. Clique em **OK**.

As configurações da integração SIEM definidas serão aplicadas.

Definição de configurações de notificação

► *Para configurar as notificações do Kaspersky Embedded Systems Security, execute as seguintes etapas:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
4. Na seção **Logs e notificações**, clique no botão **Configurações** na subseção **Notificações de evento**.
5. Na janela **Configurações de notificação** , defina as configurações seguintes do Kaspersky Embedded Systems Security de acordo com seus requisitos:
   - Na lista **Configurações de notificação**, selecione o tipo da notificação cujas configurações deseja definir.
   - Na seção **Notificar usuários**, configure o método de notificação do usuário. Se necessário, insira o texto da mensagem de notificação.
   - Na seção **Notificar administradores**, configure o método de notificação do administrador. Se necessário, insira o texto da mensagem de notificação. Se necessário, defina configurações adicionais de notificação clicando no botão **Configurações**.
   - Na seção **Limites de geração de evento**, especifique os intervalos de tempo após os quais o Kaspersky Embedded Systems Security registra os eventos *O banco de dados do aplicativo está desatualizado, O banco de dados do aplicativo está muito desatualizado* e *A verificação de Áreas Críticas não é realizada há muito tempo*.

- **O banco de dados do aplicativo está desatualizado (dias)**

  O número de dias decorridos desde a última Atualização do banco de dados.

  O valor padrão é 7 dias.

- **O banco de dados do aplicativo está muito desatualizado (dias)**

  O número de dias decorridos desde a última Atualização do banco de dados.

  O valor padrão é 14 dias.

- **A Verificação de áreas críticas não é executada há muito tempo (dias)**

  O número de dias após a última Verificação de áreas críticas concluída com êxito.

  O valor padrão é 30 dias.

6. Clique em **OK**.

As configurações de notificação definidas são salvas.

Configuração de interações com o Servidor de Administração

► *Para escolher os tipos de objetos sobre os quais o Kaspersky Embedded Systems Security envia informações ao Servidor de Administração do Kaspersky Security Center:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

4. Na seção **Logs e notificações**, clique no botão **Configurações** no bloco **Interação com o Servidor de Administração**.

   A janela **Listas da rede do Servidor de administração** é exibida.

5. Na janela **Listas da rede do Servidor de administração**, escolha os tipos de objetos sobre os quais o Kaspersky Embedded Systems Security enviará informações ao Servidor de Administração do Kaspersky Security Center:
   - Objetos em Quarentena.

- Objetos do Backup.

6. Clique em **OK**.

   O Kaspersky Embedded Systems Security enviará informações sobre os tipos de objetos selecionados para o Servidor de Administração.

Criação e configuração de políticas

Esta seção fornece informações sobre a utilização de políticas do Kaspersky Security Center para gerenciar o Kaspersky Embedded Systems Security em vários computadores.

As políticas globais do Kaspersky Security Center podem ser criadas para gerenciar a proteção em vários computadores onde o Kaspersky Embedded Systems Security está instalado.

Uma política impõe as configurações, funções e tarefas do Kaspersky Embedded Systems Security especificadas nela a todos os computadores protegidos de um grupo de administração.

Várias políticas podem ser criadas e impostas alternadamente para um grupo de administração. A política atualmente ativa para um grupo tem o status *ativo* no Console de Administração.

As informações sobre a imposição da política são registradas no log de auditoria do sistema do Kaspersky Embedded Systems Security. Essas informações podem ser visualizadas no Console do Aplicativo no nó **Log de auditoria do sistema**.

O Kaspersky Security Center oferece uma maneira para aplicar políticas em computadores locais: *Proibir a alteração das configurações*. Após uma política ter sido aplicada, o Kaspersky Embedded Systems Security usa os valores para as configurações junto dos quais você selecionou o ícone 🔒 nas propriedades de política em computadores locais ao invés dos valores para aquelas configurações que eram verdadeiras antes da política ser aplicada. O Kaspersky Embedded Systems Security não aplica os valores de configurações de política ativa junto dos quais o ícone 🔓 é selecionado nas propriedades de política.

Se uma política estiver ativa, os valores de configurações marcadas com o ícone 🔒 na política são exibidos no Console do Aplicativo, mas não podem ser editados. Os valores de outras configurações (marcados com o ícone 🔓 na política) podem ser editados no Console do Aplicativo.

As configurações definidas na política ativa e marcadas com o ícone 🔒 também bloqueiam alterações no Kaspersky Security Center para um computador na janela **Propriedades: <Nome do computador>**.

As configurações especificadas e enviadas para o computador local usando uma política ativa são salvas nas configurações de tarefas locais após a política ativa ser desativada.

Se a política definir as configurações para qualquer tarefa de Proteção do Computador em Tempo Real e se essa tarefa estiver em execução atualmente, as configurações definidas pela política serão modificadas assim que a política for aplicada. Se a tarefa não estiver sendo executada, as configurações serão aplicadas quando ela for iniciada.

Neste capítulo

Criando políticas 109

Seções de configurações de política do Kaspersky Embedded Systems Security 111

Configuração de políticas 115

Criando políticas

O processo de criação de uma política envolve as seguintes etapas:

1. Criando uma política usando o assistente de políticas. As configurações de tarefas de Proteção do Computador em Tempo Real podem ser definidas usando as caixas de diálogo do assistente.
2. Definindo as configurações de política. Na janela **Propriedades: <Nome da política>** da política criada, você pode definir as configurações de tarefas de Proteção do Computador em Tempo Real, as configurações gerais do Kaspersky Embedded Systems Security, as configurações de Quarentena e Backup, o nível de detalhe dos logs de tarefas, bem como notificações de administrador e de usuário sobre eventos do Kaspersky Embedded Systems Security.

► *Para criar uma política para um grupo de computadores que executam o Kaspersky Embedded Systems Security instalado, siga as etapas a seguir:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e, em seguida, selecione o grupo de administração que contém os computadores para os quais deseja criar uma política.
2. No painel de detalhes do grupo de administração selecionado, selecione a guia **Políticas** e clique no link **Criar uma política** para iniciar o assistente e criar uma política.

   A janela **Assistente de Nova Política** é exibida.
3. Na janela **Selecione o aplicativo para o qual deseja criar uma política de grupo**, selecione Kaspersky Embedded Systems Security e clique em **Avançar**.
4. Insira um nome de política de grupo no campo **Nome**.

   O nome da política não pode conter os seguintes símbolos: " * < : > ? \ | .
5. Para aplicar a configuração de política usada para a versão anterior do aplicativo:
   a. Marque a caixa de seleção **Usar configurações da política de versões anteriores do aplicativo**.
   b. Clique no botão **Selecionar**.
   c. Selecione a política que deseja aplicar.
   d. Clique em **Avançar**.
6. Na janela **Seleção do tipo de operação**, selecione uma das seguintes opções:
   - **Nova**, para criar uma nova política com configurações padrão.
   - **Importar política criada com a versão anterior do Kaspersky Embedded Systems Security** para usar tal versão da política como modelo.
   - Clique em **Procurar** e selecione um arquivo de configuração no qual uma política existente está armazenada.
7. Na janela **Proteção do Computador em Tempo Real**, configure a Proteção de Arquivos em Tempo Real, as tarefas de Uso da KSN e a funcionalidade de Prevenção de Exploits conforme necessário. Permita ou bloqueie o uso de tarefas de política configuradas em computadores locais na rede:
   - Clique no botão 🔒 para permitir alterações nas configurações de tarefa em computadores de rede e para bloquear a aplicação de configurações de tarefa definidas na política.
   - Clique no botão 🔓 para negar alterações nas configurações de tarefa em computadores de rede e

para permitir a aplicação de configurações de tarefa definidas na política.

A política recém-criada usa as configurações padrão das tarefas de Proteção do Computador em Tempo Real.

- Para editar as configurações padrão da tarefa de Proteção de Arquivos em Tempo Real, clique no botão **Configurações** na subseção **Proteção de Arquivos em Tempo Real**. Na janela exibida, configure a tarefa de acordo com as suas necessidades. Clique em **OK**.
- Para editar as configurações padrão da tarefa de Uso da KSN, clique no botão **Configurações** na subseção **Uso da KSN**. Na janela exibida, configure a tarefa de acordo com as suas necessidades. Clique em **OK**.

  Para iniciar a tarefa de Uso da KSN, é necessário aceitar a Declaração da KSN na janela Manuseio de dados (consulte a seção "Configurando o manuseio de dados por meio do Plug-in de Administração" na página 279).

- Para editar as configurações padrão do componente Prevenção de Exploits, clique no botão **Configurações** na subseção **Prevenção de Exploits**. Na janela exibida, configure a funcionalidade de acordo com a sua necessidade. Clique em **OK**.

8. Selecione um dos seguintes status de política na janela **Criar política de grupo para o aplicativo**:
   - **Política ativa** se quiser aplicar a política imediatamente após sua criação. Se uma política ativa já existir no grupo, ela será desativada e uma nova política será aplicada.
   - **Política inativa**, se não quiser aplicar a política criada imediatamente. Nesse caso, a política poderá ser ativada mais tarde.
   - Selecione caixa de seleção **Abrir propriedades da política imediatamente após serem criadas** para fechar automaticamente o **Assistente de Nova Política** e configurar a política recém-criada após clicar no botão **Avançar**.
9. Clique no botão **Concluir**.

A política criada é exibida na lista de políticas, na guia **Políticas** do grupo de administração selecionado. Na janela **Propriedades: <Nome da política>**, você pode definir outras configurações, tarefas e funções do Kaspersky Embedded Systems Security.

Seções de configurações de política do Kaspersky Embedded Systems Security

Geral

Na seção **Geral**, é possível definir as seguintes configurações de política:

- Indicar o status da política.
- Configurar a herança de configurações das políticas pais e políticas filhas.

Configuração de evento

Na seção **Configuração de evento**, é possível definir configurações para as seguintes categorias de evento:

- *Eventos críticos*
- *Falha funcional*
- *Aviso*
- *Mensagem informativa*

É possível usar o botão **Propriedades** para definir as seguintes configurações para os eventos selecionados:

- Indicar o local de armazenamento e o período de retenção das informações sobre os eventos registrados.
- Indicar o método de notificação sobre eventos registrados.

Configurações do aplicativo

Tabela 11. Configurações da seção Configurações do aplicativo

Seção	Opções
Escalabilidade e interface	Na subseção **Escalabilidade e interface**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Optar pela definição manual ou automática das configurações de escalabilidade. • Definir as configurações de exibição de ícone de aplicativo.
Segurança	Na subseção **Segurança**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Definir as configurações de execução de tarefa. • Especificar como o aplicativo deve se comportar quando o computador estiver funcionando com a fonte de energia UPS. • Ativar ou desativar a proteção de senha das funções do aplicativo.
Conexões	Na subseção **Conexões**, é possível usar o botão **Configurações** para definir os seguintes parâmetros de servidor proxy para se conectar a servidores de atualização, servidores de ativação e à KSN: • Definir as configurações do servidor proxy. • Especificar as configurações de autenticação do servidor proxy.
Executar tarefas do sistema	Na subseção **Executar tarefas do sistema**, é possível usar o botão **Configurações** para permitir ou bloquear a inicialização das seguintes tarefas do sistema de acordo com uma programação definida em computadores locais: • Tarefa de Verificação por Demanda. • Tarefas Atualização e Copiar atualizações.

Suplementar

Tabela 12. Configurações da seção Suplementar

Seção	Opções
Zona Confiável	Clique no botão **Configurações** na subseção **Zona Confiável** para definir as seguintes configurações da Zona Confiável do aplicativo: • Criar uma lista de exclusões da Zona Confiável. • Ativar ou desativar a verificação de operações de backup de arquivos. • Criar uma lista de processos confiáveis.
Verificação de unidades removíveis	Na subseção **Verificação de unidades removíveis**, é possível usar o botão **Configurações** para definir configurações de verificação para unidades USB removíveis.
Permissões de acesso do usuário para gerenciamento do aplicativo	Na subseção **Permissões de acesso do usuário para gerenciamento do aplicativo**, é possível configurar direitos de usuário e de grupos de usuários para gerenciar o Kaspersky Embedded Systems Security.
Permissões de acesso do usuário para gerenciamento do Security Service	Na subseção **Permissões de acesso do usuário para gerenciamento do Security Service**, é possível configurar direitos de usuário e de grupos de usuários para gerenciar o Kaspersky Security Service.
Armazenamentos	Na seção **Armazenamentos**, clique no botão **Configurações** para definir as seguintes configurações de Quarentena, Backup e Hosts Bloqueados: • Especificar o caminho da pasta na qual deseja colocar objetos em Quarentena ou de Backup. • Configurar o tamanho máximo do Backup e Quarentena e também especificar o limite de espaço livre. • Especificar o caminho da pasta na qual deseja colocar os objetos restaurados de Quarentena ou de Backup. • Configurar o período de bloqueio do host.

Proteção do Computador em Tempo Real

Tabela 13. Configurações da seção Proteção do Computador em Tempo Real

Seção	Opções
Proteção de Arquivos em Tempo Real	Na subseção **Proteção de Arquivos em Tempo Real**, é possível clicar no botão **Configurações** para definir as seguintes configurações de tarefa: • Indicar o modo de proteção. • Configurar o uso do Analisador Heurístico. • Configurar o uso da Zona Confiável. • Indicar o escopo da proteção. • Definir o nível de segurança para o escopo da proteção selecionado: você pode selecionar um nível de segurança predefinido ou definir manualmente as configurações de segurança. • Definir as configurações de inicialização da tarefa.

Uso da KSN	Na subseção **Uso da KSN**, é possível clicar no botão **Configurações** para definir as seguintes configurações de tarefa: • Indicar as ações a serem executadas em objetos não confiáveis da KSN. • Configurar a transferência de dados e o uso do Kaspersky Security Center como um servidor proxy da KSN. Clique no botão **Manuseio de dados** para aceitar ou rejeitar a Declaração da KSN e a declaração da KMP, e definir configurações de troca de dados seguras.
Prevenção de Exploits	Na subseção **Prevenção de Exploits**, é possível clicar no botão **Configurações** para definir as seguintes configurações de tarefa: • Selecionar o modo de proteção da memória do processo. • Indicar as ações para reduzir os riscos de exploit. • Adicionar e editar a lista de processos protegidos.

Controle de atividade local

Tabela 14. Configurações da seção Controle de atividade local

Seção	Opções
Controle de Inicialização de Aplicativos	Na subseção **Controle de Inicialização de Aplicativos**, é possível usar o botão **Configurações** para definir as seguintes configurações de tarefa: • Selecionar o modo de operação da tarefa. • Definir configurações para controlar as inicializações subsequentes de aplicativo. • Indicar o escopo para o aplicativo das regras de Controle de Inicialização de Aplicativos. • Configurar o uso da KSN. • Definir as configurações de inicialização da tarefa.
Controle de Dispositivos	Na subseção **Controle de Dispositivos**, é possível clicar no botão **Configurações** para definir as seguintes configurações de tarefa: • Selecionar o modo de operação da tarefa. • Definir as configurações de inicialização da tarefa.

Controle de atividade de rede

Tabela 15. Configurações da seção Controle de atividade de rede

Seção	Opções
Gerenciamento de Firewall	Na subseção **Gerenciamento de Firewall**, é possível clicar no botão **Configurações** para definir as seguintes configurações de tarefa: • Configurar as regras de Firewall. • Definir as configurações de inicialização da tarefa.

Inspeção do sistema

Tabela 16. Configurações da seção Inspeção do Sistema

Seção	Opções
Monitor de Integridade de Arquivos	Na subseção **Monitor de Integridade de Arquivos**, é possível configurar o controle sobre as modificações em arquivos que podem significar uma violação de segurança em um computador protegido.
Inspeção de Log	Na seção **Inspeção de Log**, é possível configurar um controle de integridade do computador protegido com base nos resultados da análise de Log de Eventos do Windows.

Logs e notificações

Tabela 17. Configurações da seção Logs e Notificações

Seção	Opções
Logs de tarefas	Na subseção **Logs de tarefas**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Especificar o nível de importância dos eventos registrados para os componentes de software selecionados. • Especificar as configurações de armazenamento do Log de tarefas. • Especificar a integração SIEM com configurações do Kaspersky Security Center.
Notificações de evento	Na subseção **Notificações de evento**, é possível clicar no botão **Configurações** para definir as seguintes configurações: • Especificar as configurações de notificação de usuário para os eventos *Objeto detectado*, *Armazenamento em massa não confiável detectado e restringido* e *Host listado como não confiável*. • Especificar as configurações de notificação de administrador para qualquer evento selecionado na lista de eventos na seção **Configurações de notificação**.
Interação com o Servidor de Administração	Na seção **Interação com o Servidor de Administração**, é possível clicar no botão **Configurações** para selecionar os tipos de objetos que o Kaspersky Embedded Systems Security relatará ao Servidor de Administração. Você também pode configurar a transmissão de informações sobre objetos de Quarentena e de Backup ao Servidor de Administração.

Para revisar informações detalhadas sobre tarefas de Proteção de Armazenamento Anexado de Rede, consulte o *Manual de Implementação do Kaspersky Embedded Systems Security para Proteção de Armazenamentos de Rede*.

Histórico de revisão

Na seção **Histórico de revisão**, é possível gerenciar revisões: comparar com a revisão atual ou outra política, adicionar descrições de revisões, salvar revisões em um arquivo ou realizar uma reversão.

Configuração de políticas

Na janela **Propriedades de <Nome da política>** de uma política existente, você pode definir as configurações gerais do Kaspersky Embedded Systems Security, configurações de Quarentena e de Backup, configurações da Zona Confiável, configurações da Proteção do Computador em Tempo Real, configurações de Controle de atividade local, o nível de detalhes para logs de tarefas, bem como notificações de usuários e de administrador sobre os eventos do Kaspersky Embedded Systems Security, privilégios de acesso para gerenciar o aplicativo e o Kaspersky Security Service e as configurações do aplicativo do perfil de política.

► *Para definir as configurações de política:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Expanda o grupo de administração para o qual deseja definir as configurações de política associadas e abra a guia **Políticas** no painel detalhes.
3. Selecione uma política que deseja configurar e abra a janela **Propriedades: <Nome de política>** usando um dos seguintes métodos:
   - Selecionando a opção **Propriedades** no menu de contexto de política.
   - Clicando no link **Configurar política** no painel de detalhes à direita da política selecionada.
   - Clicando duas vezes na política selecionada.
4. Na guia **Geral** na seção **Status de política**, ative ou desative a política. Para fazer isso, selecione uma das opções a seguir:
   - **Política ativa**, se deseja que a política seja aplicada a todos os computadores dentro do grupo de administração selecionado.
   - **Política inativa**, se desejar que a política seja aplicada posteriormente a todos os computadores dentro do grupo de administração selecionado.

   A configuração **Política de usuário ausente** não está disponível ao gerenciar o Kaspersky Embedded Systems Security.
5. Nas seções **Configuração de evento**, **Configurações do aplicativo**, **Suplementar**, **Logs e notificações** e **Histórico de revisão**, você pode modificar a configuração do aplicativo (consulte a tabela abaixo).
6. Nas seções **Proteção do Computador em Tempo Real**, **Controle de atividade local**, **Controle de atividade de rede** e **Inspeção do Sistema**, defina as configurações do aplicativo e de sua inicialização (consulte a tabela abaixo).

   Você pode ativar ou desativar a execução de qualquer tarefa em todos os computadores dentro do grupo de administração por meio de uma política do Kaspersky Security Center.
   Você pode configurar a aplicação de configurações de política em todos os computadores de rede para cada componente de software individual.
7. Clique em **OK**.

As configurações definidas são aplicadas na política.

Criando e configurando uma tarefa usando o Kaspersky Security Center

Esta seção contém informação sobre tarefas do Kaspersky Embedded Systems Security e como criá-las, definir suas configurações, iniciá-las e interrompê-las.

Neste capítulo

Sobre a criação de tarefa no Kaspersky Security Center 116

Criação de uma tarefa usando o Kaspersky Security Center 117

Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center 119

Configurando tarefas de grupo no Kaspersky Security Center 120

Definir configurações de diagnóstico de travamento no Kaspersky Security Center 128

Gerenciando programações de tarefas 130

Sobre a criação de tarefa no Kaspersky Security Center

Você pode criar tarefas de grupo para grupos de administração e conjuntos de computadores. Você pode criar os seguintes tipos de tarefa:

- Ativação do aplicativo
- Copiar atualizações
- Atualização do Banco de Dados
- Atualização de módulos de software
- Reversão da Atualização do Banco de Dados
- Verificação por Demanda
- Controle de Integridade de Aplicativos
- Gerador de Regras de Controle de Inicialização de Aplicativos
- Gerador de Regras de Controle de Dispositivos

Você pode criar tarefas de grupo e locais das seguintes maneiras:

- para um computador: na janela **Propriedades <Nome de computador>** na seção **Tarefas**.
- para um grupo de administração: no painel de detalhes do nó do grupo selecionado de computadores na guia **Tarefas**.
- para um conjunto de computadores: no painel de detalhes do nó **Seleções de dispositivo**.

Usando políticas é possível desativar programações para as tarefas locais do sistema de Atualização e Verificação por Demanda (consulte a seção "Configuração da inicialização programada de tarefas locais do sistema" na página 97) em todos os computadores protegidos do mesmo grupo de administração.

Informações gerais sobre tarefas no Kaspersky Security Center são fornecidas na *Ajuda do Kaspersky Security Center.*

Criação de uma tarefa usando o Kaspersky Security Center

► *Para criar uma nova tarefa no Console de Administração do Kaspersky Security Center:*

1. Inicie o assistente de tarefa de uma das seguintes maneiras:
   - Para criar uma tarefa local:
     a. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração e selecione o grupo ao qual o computador protegido pertence.
     b. No painel de detalhes, na guia **Dispositivos**, abra o menu de contexto do computador protegido e selecione **Propriedades**.
     c. Na janela exibida, clique no botão **Adicionar** na seção **Tarefas**.
   - Para criar uma tarefa de grupo:
     a. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
     b. Selecione o grupo de administração para o qual você deseja criar uma tarefa.
     c. No painel de detalhes, abra a guia **Tarefas** e selecione **Criar uma tarefa**.
   - Para criar uma tarefa para um conjunto personalizado de computadores:
     a. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
     b. Selecione o grupo de administração que contém o computador.
     c. Selecione um computador ou um conjunto personalizado de computadores.
     d. Na lista suspensa **Executar ação**, selecione a opção **Criar uma tarefa**.

   A janela do assistente de tarefa é exibida.
2. Na janela **Selecionar o tipo de tarefa**, sob o título **Kaspersky Embedded Systems Security**, selecione o tipo da tarefa a ser criada.
3. Se você tiver selecionado qualquer tipo de tarefa, exceto Reversão da Atualização do Banco de Dados, Controle de Integridade de Aplicativos ou Ativação do Aplicativo, a janela **Configurações** é exibida. Dependendo do tipo de tarefa, as configurações podem variar:
   - Crie uma tarefa de Verificação por demanda (consulte a seção "Criando uma tarefa de Verificação por Demanda" na página 411).
   - Para criar uma tarefa de atualização, defina as configurações da tarefa de acordo com suas necessidades:
     a. Selecione a fonte de atualizações na janela **Fonte de atualização**.

b. Clique no botão **Configurações de conexão**. A janela **Configurações de conexão** é aberta.

c. Na janela **Configurações de conexão**:

Especifique o modo do servidor FTP para conectar ao computador protegido.

Modifique o tempo limite de conexão ao conectar à fonte de atualização, se necessário.

Especifique as configurações de acesso do servidor proxy ao conectar com a fonte de atualização.

Especifique a localização dos computadores protegidos, para otimizar o download de atualizações.

- Para criar uma tarefa de Atualização de módulos de software, defina as configurações de atualização dos módulos de programa necessárias na janela **Configurações para atualizações de módulo de software do aplicativo**:

  a. Selecione Copiar e instalar atualizações críticas dos módulos de software ou apenas verificar a sua disponibilidade sem instalação.

  b. Se **Copiar e instalar atualizações críticas dos módulos de software** estiver selecionado, um reinício do computador poderá ser necessário para aplicar os módulos de software instalados. Se você desejar que o Kaspersky Embedded Systems Security reinicie o computador automaticamente após a conclusão da tarefa, selecione a caixa **Permitir reinício do sistema operacional**.

  c. Para obter informações sobre atualizações do módulo do Kaspersky Embedded Systems Security, selecione **Receber informações sobre as atualizações disponíveis programadas dos módulos de software**.

  A Kaspersky Lab não publica pacotes de atualizações planejados nos servidores de atualização para instalação automática; eles podem ser baixados manualmente no site da Kaspersky Lab. Pode ser configurada uma notificação do administrador sobre o evento **Nova atualização programada dos módulos de software disponível**. Isto conterá o URL do nosso site do qual as atualizações programadas podem ser baixadas.

- Para criar a tarefa Copiar atualizações, especifique o conjunto de atualizações e a pasta de destino na janela **Copiar configurações de atualizações**.

- Para criar a tarefa de Ativação do Aplicativo:

  a. Na janela **Configurações de Ativação**, especifique o arquivo de chave que você deseja usar para ativar o aplicativo.

  b. Marque a caixa de seleção **Usar como chave adicional** se desejar criar uma tarefa para renovar a licença.

- Crie a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos (consulte a seção "Criação de uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos" na página 316).

- Crie a tarefa do Gerador de Regras de Controle de Dispositivos (consulte a seção "Criação de regras usando a tarefa do Gerador de Regras de Controle de Dispositivos" na página 354).

4. Configure a programação da tarefa (ver a Seção "Definição das configurações da programação de inicialização da tarefa" na página 130) (você pode configurar uma programação para todos os tipos de tarefa exceto a tarefa de Reversão da Atualização do Banco de Dados).

5. Clique em **OK**.

6. Se a tarefa for criada para um conjunto de computadores, selecione a rede (ou grupo) de computadores na qual a tarefa será executada.

7. Na janela **Especificando uma conta para a execução da tarefa**, especifique a conta na qual você deseja

executar a tarefa.

8. Na janela **Definir nome da tarefa**, insira um nome para a tarefa (com menos de 100 caracteres) sem incluir os símbolos **" * < > ? \ | :** .

   Recomenda-se adicionar o tipo de tarefa ao seu nome (por exemplo, "Verificação por demanda de pastas compartilhadas").

9. Na janela **Conclusão da criação da tarefa**, selecione a caixa **Executar tarefa quando o assistente for concluído** se quiser que a tarefa seja iniciada logo após ser criada. Clique no botão **Concluir**.

A tarefa criada é exibida na lista de **Tarefas**.

Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center

► *Para configurar tarefas locais ou definir configurações gerais do aplicativo para um único computador da rede:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Servidor de Administração do Kaspersky Security Center e selecione o grupo ao qual o computador protegido pertence.
2. No painel de detalhes, selecione a guia **Dispositivos**.
3. Abra a janela **Propriedades: <Nome do computador>** de uma das seguintes maneiras:
   - Clique duas vezes no nome do computador protegido.
   - Abra o menu de contexto do nome do computador protegido e selecione o item **Propriedades**.

   A janela **Propriedades: <Nome do computador>** é exibida.
4. Para especificar as configurações da tarefa local, siga as etapas a seguir:
   a. Vá até a seção **Tarefas**.
      - Na lista de tarefas, selecione uma tarefa local para configurar.
      - Clique duas vezes no nome da tarefa na lista de tarefas.
      - Selecione o nome da tarefa e clique no botão **Propriedades**.
      - Selecione **Propriedades** no menu de contexto da tarefa selecionada.

        A janela **Propriedades: <Nome da tarefa>** é exibida.
5. Para definir as configurações do aplicativo, siga as etapas a seguir:
   a. Vá até a seção **Aplicativos**.
      - Na lista de aplicativos instalados, selecione um aplicativo para configurar.
      - Clique duas vezes no nome do aplicativo na lista de aplicativos instalados.
      - Selecione o nome do aplicativo na lista de aplicativos instalados e clique no botão **Propriedades**.
      - Abra o menu de contexto do nome do aplicativo na lista de aplicativos instalados e selecione o item **Propriedades**.

        A janela **Configurações do <Nome do aplicativo>** é exibida.

Se um aplicativo estiver sob a política do Kaspersky Security Center e essa política proibir a alteração das configurações do aplicativo, essas configurações não poderão ser editadas na janela **Configurações do <Nome do aplicativo>**.

Configurando tarefas de grupo no Kaspersky Security Center

► *Para configurar a tarefa de grupo para múltiplos computadores:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados** e seleciona o grupo de administração para o qual deseja configurar as tarefas de aplicativo.
2. No painel de detalhes de um grupo de administração selecionado, abra a guia **Tarefas**.
3. Na lista de tarefas de grupo criadas anteriormente, selecione uma tarefa que deseja configurar. Abra a janela **Propriedades: <Nome da tarefa>** de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa na lista de tarefas criadas.
   - Selecione o nome da tarefa na lista de tarefas criadas e clique no link **Configurar tarefa**.
   - Abra o menu de contexto do nome da tarefa na lista de tarefas criadas e selecione o item **Propriedades**.
4. Na seção **Notificações**, defina as configurações de notificação do evento da tarefa.

   Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.

5. Dependendo do tipo de tarefa configurada, execute uma das seguintes ações:
   - Para configurar uma tarefa de Verificação por Demanda:
     a. Na seção **Escopo da verificação**, configure um escopo de verificação.
     b. Na seção **Opções**, configure o nível de prioridade e integração de tarefa com outros componentes de software.
   - Para configurar uma tarefa de atualização, ajuste as configurações da tarefa de acordo com suas necessidades:
     a. Na seção **Configurações**, defina as configurações de fonte de atualização e otimização de uso de subsistema de disco.
     b. Clique no botão **Configurações de conexão** para definir as configurações de conexão da fonte de atualização.
   - Para configurar a tarefa de Atualização de módulos de software, na seção **Configurações para atualizações de módulo de software do aplicativo** selecione uma ação a ser executada: copiar e instalar atualizações críticas de módulos de software ou somente verificá-las.
   - Para configurar a tarefa Copiar atualizações, especifique o conjunto de atualizações e a pasta de destino na seção **Copiar configurações de atualizações**.
   - Para configurar a tarefa de Ativação do aplicativo, na seção **Configurações de ativação**, aplique o arquivo de chave que deseja usar para ativar o aplicativo. Selecione a caixa **Usar como chave adicional** se deseja adicionar um código de ativação ou arquivo de chave para renovar a licença.

- Para configurar a geração automática de regras de permissão para o controle do computador, na seção **Configurações** especifique as configurações com base nas quais a lista de regras de permissão será criada.

6. Configurar o agendamento de tarefa na seção **Programação** (você pode configurar um agendamento para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).
7. Na seção **Conta**, especifique a conta cujos direitos serão usados para a execução de tarefa. Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.
8. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**. Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.
9. Na janela **Propriedades: <Nome da tarefa>**, clique em **OK**.

As configurações de tarefas de grupo definidas recentemente são salvas.

As configurações de tarefas de grupo que estão disponíveis para configuração estão resumidas na tabela abaixo.

Tabela 18. Configurações de tarefas de grupo do Kaspersky Embedded Systems Security

Tipos de tarefas do Kaspersky Embedded Systems Security	Seção na janela Propriedades: <Nome da tarefa>	Configurações de tarefa
Gerador de Regras de Controle de Inicialização de Aplicativos	**Configurações**	Ao configurar a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos, você pode: • Criar regras de permissão com base nos aplicativos em execução; • Criar regras de permissão para aplicativos das pastas específicas.
	Opções	Você pode especificar ações para execução enquanto cria regras de permissão para o controle de inicialização de aplicativos: • **Usar certificado digital** • **Usar o requerente e a impressão digital do certificado digital** • **Se o certificado estiver ausente, use** • **Usar hash SHA256** • **Gerar regras para usuário ou grupo de usuários** Você pode definir as configurações para arquivos de configuração com listas de regras de permissão que o Kaspersky Embedded Systems Security cria após a conclusão da tarefa.
	Programação	Você pode definir as configurações de inicialização programada da tarefa.

Gerador de Regras de Controle de Dispositivos	**Configurações**	• Selecione o modo de operação: considere dados de sistema sobre todos os armazenamentos em massa que já estiveram conectados alguma vez ou considere somente os armazenamentos em massa conectados atualmente. • Defina as configurações para arquivos de configuração com listas de regras de permissão que o Kaspersky Embedded Systems Security cria após a conclusão da tarefa.
	Programação	Você pode definir as configurações de inicialização programada da tarefa.
A Ativação do Aplicativo (consulte a seção "Ativação da tarefa de Aplicativo" na página 125)	**Configurações de ativação**	Para ativar o aplicativo ou renovar a licença, você pode adicionar um arquivo de chave.
	Programação	Você pode definir as configurações de inicialização programada da tarefa.
Copiar atualizações (consulte a seção "Tarefas de atualização" na página 125)	**Fonte de atualização**	Você pode especificar o Servidor de Administração do Kaspersky Security Center ou os servidores de atualização da Kaspersky Lab como fonte de atualização do aplicativo. Você também pode criar uma lista personalizada de fontes de atualização: adicionando servidores HTTP ou FTP personalizados ou pastas de rede manualmente e definindo-os como fontes de atualização. Você pode especificar o uso dos servidores de atualização da Kaspersky Lab, se os servidores personalizados manualmente não estiverem disponíveis.
	Janela **Configurações de conexão**	Na janela **Configurações de conexão**,vinculada à seção **Fonte de atualização**, você pode especificar se a conexão a servidores de atualização da Kaspersky Lab ou a algum outro servidor deve ser estabelecida através do servidor proxy.
	Copiar configurações de atualizações	Você pode especificar o conjunto de atualizações destinado à cópia. No campo **Pasta para armazenamento local de atualizações copiadas**, especifique um caminho para uma pasta que será usada pelo Kaspersky Embedded Systems Security para armazenar atualizações copiadas.
	Programação	Você pode definir as configurações de inicialização programada da tarefa.

Atualização do Banco de Dados (consulte a seção "Tarefas de atualização" na página 125)	**Configurações**	Você pode especificar o Servidor de Administração do Kaspersky Security Center ou servidores de atualização da Kaspersky Lab como a fonte de atualização do aplicativo no grupo **Fonte de atualização**. Você também pode criar uma lista personalizada de fontes de atualização: adicionando servidores HTTP ou FTP personalizados ou pastas de rede manualmente e definindo-os como fontes de atualização. Você pode especificar o uso dos servidores de atualização da Kaspersky Lab, se os servidores personalizados manualmente não estiverem disponíveis. Na seção Otimização de uso da E/S de disco, é possível configurar o recurso que reduz a carga de trabalho no subsistema de disco: • **Diminuir a carga na E/S de disco** • **RAM usada para otimização (MB)**
	Janela **Configurações de conexão**	Na janela **Configurações de conexão**,vinculada à seção **Fonte de atualização**, você pode especificar se a conexão a servidores de atualização da Kaspersky Lab ou a algum outro servidor deve ser estabelecida através do servidor proxy.
	Programação	Você pode definir as configurações de inicialização programada da tarefa.
Atualização de módulos de software (consulte a seção "Tarefas de atualização" na página 125)	**Fonte de atualização**	Você pode especificar o Servidor de Administração do Kaspersky Security Center ou os servidores de atualização da Kaspersky Lab como fonte de atualização do aplicativo. Você também pode criar uma lista personalizada de fontes de atualização: adicionando servidores HTTP ou FTP personalizados ou pastas de rede manualmente e definindo-os como fontes de atualização. Você pode especificar o uso dos servidores de atualização da Kaspersky Lab, se os servidores personalizados manualmente não estiverem disponíveis.
	Janela **Configurações de conexão**	No grupo **Configurações de conexão da fonte de atualização** você pode especificar se a conexão a servidores de atualização da Kaspersky Lab ou a algum outro servidor deve ser estabelecida por meio do servidor proxy.
	Configurações para atualizações de módulo de software do aplicativo	Você pode especificar quais ações devem ser executadas pelo Kaspersky Embedded Systems Security quando as atualizações críticas dos módulos de software estão disponíveis ou já foram instaladas e também se o Kaspersky Embedded Systems Security tiver que receber informações com relação às atualizações programadas.
	Programação	Você pode definir as configurações de inicialização programada da tarefa.

Configurações de Verificação por demanda (consulte a seção "Criando uma tarefa de Verificação por Demanda" na página 411)	**Escopo da verificação**	É possível especificar um Escopo da verificação para a tarefa de Verificação por Demanda e definir configurações de nível de segurança.
	Janela **Configurações da verificação por demanda**	Na janela **Configurações da Verificação por demanda**, vinculada da seção **Escopo da verificação**, você pode selecionar um dos níveis de segurança predefinidos ou personalizar o nível de segurança manualmente.
	Opções	É possível ativar ou desativar o uso do analisador heurístico da tarefa de Verificação por Demanda e estabelecer o nível de análise usando um controle deslizante no grupo **Analisador heurístico**. No grupo **Integração com outros componentes** você pode definir as seguintes configurações: • Aplicar Zona Confiável para tarefas de Verificação por Demanda. • Aplicar o Uso da KSN para tarefas de Verificação por Demanda. • Defina uma prioridade para a tarefa de Verificação por Demanda: executar tarefa em segundo plano (prioridade baixa) ou considerar a tarefa como uma Verificação de áreas críticas.
	Programação	Você pode definir as configurações de inicialização programada da tarefa.
Controle de Integridade de Aplicativos (na página 127)	**Programação**	Você pode definir as configurações de inicialização programada da tarefa.

Para a tarefa de Reversão da Atualização do Banco de Dados, você pode definir somente configurações de tarefa padrão nas seções **Notificação** e **Exclusões do escopo de tarefa**, controladas pelo Kaspersky Security Center.

Para obter informações detalhadas sobre a definição das configurações destas seções, consulte a *Ajuda do Kaspersky Security Center*.

Nesta seção

Ativação da tarefa de Aplicativo 125
Tarefas de atualização 125
Controle de Integridade de Aplicativos 127

Ativação da tarefa de Aplicativo

► *Para configurar uma Ativação da tarefa de Aplicativo, siga as etapas a seguir:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados** e seleciona o grupo de administração para o qual deseja configurar as tarefas de aplicativo.
2. No painel de detalhes de um grupo de administração selecionado, abra a guia **Tarefas**.
3. Na lista de tarefas de grupo criadas anteriormente, selecione uma tarefa que deseja configurar. Abra a janela **Propriedades: <Nome da tarefa>** de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa na lista de tarefas criadas.
   - Selecione o nome da tarefa na lista de tarefas criadas e clique no link **Configurar tarefa**.
   - Abra o menu de contexto do nome da tarefa na lista de tarefas criadas e selecione o item **Propriedades**.
4. Na seção **Notificações**, defina as configurações de notificação do evento da tarefa.

   Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.

5. Na seção **Configurações de Ativação**, especifique o arquivo de chave que você deseja usar para ativar o aplicativo. Marque a caixa de seleção **Usar como chave adicional** se desejar adicionar uma chave para estender a licença.
6. Configurar o agendamento de tarefa na seção **Programação** (você pode configurar um agendamento para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).
7. Na seção **Conta**, especifique a conta cujos direitos serão usados para a execução de tarefa.
8. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**.

   Para obter informações detalhadas sobre a definição das configurações nestas seções, consulte a *Ajuda do Kaspersky Security Center*.

9. Na janela **Propriedades: <Nome da tarefa>**, clique em **OK**.

   As configurações de tarefas de grupo definidas recentemente são salvas.

Tarefas de atualização

► *Para configurar as tarefas Copiar Atualizações, Atualização do Banco de Dados ou de Atualização de módulos de software, faça o seguinte:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados** e seleciona o grupo de administração para o qual deseja configurar as tarefas de aplicativo.
2. No painel de detalhes de um grupo de administração selecionado, abra a guia **Tarefas**.
3. Na lista de tarefas de grupo criadas anteriormente, selecione uma tarefa que deseja configurar. Abra a janela **Propriedades: <Nome da tarefa>** de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa na lista de tarefas criadas.

- Selecione o nome da tarefa na lista de tarefas criadas e clique no link **Configurar tarefa**.
- Abra o menu de contexto do nome da tarefa na lista de tarefas criadas e selecione o item **Propriedades**.

4. Na seção **Notificações**, defina as configurações de notificação do evento da tarefa.

   Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.

5. Dependendo do tipo de tarefa configurada, execute uma das seguintes ações:

   - Na seção **Fonte de atualização**, defina as configurações de fonte de atualização e otimização de uso de subsistema de disco.

     a. Você pode especificar o Servidor de Administração do Kaspersky Security Center ou servidores de atualização da Kaspersky Lab como a fonte de atualização do aplicativo na seção **Fonte de atualização**. Você também pode criar uma lista personalizada de fontes de atualização: adicionando servidores HTTP ou FTP personalizados ou pastas de rede manualmente e definindo-os como fontes de atualização.

        Você pode especificar o uso dos servidores de atualização da Kaspersky Lab, se os servidores personalizados manualmente não estiverem disponíveis.

     b. Na seção **Otimização de uso da E/S de disco** para a tarefa de Atualização do Banco de Dados, é possível configurar o recurso que reduz a carga de trabalho no subsistema de disco:

        - **Diminuir a carga na E/S de disco**

          Esta caixa ativa ou desativa o recurso de otimização de subsistema de disco por meio do armazenamento de arquivos de atualização em uma unidade virtual na RAM.

          Se a caixa de seleção estiver selecionada, esta função será ativada.

          Esta caixa é desmarcada por padrão.

        - **RAM usada para otimização (MB)**

          O tamanho da RAM (em MB) que o aplicativo usa para armazenar arquivos de atualização. O tamanho de RAM padrão é 512 MB. O tamanho de RAM padrão é 400 MB.

     c. Clique no botão **Configurações de conexão** e, na janela **Configurações de conexão** exibida, configure o uso de servidor proxy para conexão com os servidores de atualização da Kaspersky Lab e outros servidores.

   - Na seção **Configurações para atualizações de módulo de software do aplicativo** para a tarefa Atualização de módulos de software, é possível especificar quais ações o Kaspersky Embedded Systems Security deve executar quando as atualizações dos módulos de software críticas ou as informações sobre as atualizações planejadas estiverem disponíveis, e também é possível especificar quais ações o Kaspersky Embedded Systems Security deve realizar quando as atualizações críticas forem instaladas.
   - Especifique o conjunto de atualizações e a pasta de destino na seção **Copiar configurações de atualizações** para a tarefa Copiar Atualizações.

6. Configurar o agendamento de tarefa na seção **Programação** (você pode configurar um agendamento para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).
7. Na seção **Conta**, especifique a conta cujos direitos serão usados para a execução de tarefa.

> Para obter informações detalhadas sobre a definição das configurações nestas seções, consulte a *Ajuda do Kaspersky Security Center*.

8. Na janela **Propriedades: <Nome da tarefa>**, clique em **OK**.

As configurações de tarefas de grupo definidas recentemente são salvas.

Para a tarefa de Reversão da Atualização do Banco de Dados, é possível definir somente configurações de tarefa padrão controladas pelo Kaspersky Security Center nas seções **Notificações** e **Exclusões do escopo da tarefa**. Para obter informações detalhadas sobre a definição das configurações nestas seções, consulte a *Ajuda do Kaspersky Security Center*.

Controle de Integridade de Aplicativos

► *Para configurar a tarefa de grupo de Controle de Integridade de Aplicativos:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados** e seleciona o grupo de administração para o qual deseja configurar as tarefas de aplicativo.
2. No painel de detalhes de um grupo de administração selecionado, abra a guia **Tarefas**.
3. Na lista de tarefas de grupo criadas anteriormente, selecione uma tarefa que deseja configurar. Abra a janela **Propriedades: <Nome da tarefa>** de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa na lista de tarefas criadas.
   - Selecione o nome da tarefa na lista de tarefas criadas e clique no link **Configurar tarefa**.
   - Abra o menu de contexto do nome da tarefa na lista de tarefas criadas e selecione o item **Propriedades**.
4. Na seção **Notificações**, defina as configurações de notificação do evento da tarefa.

> Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.

5. Na seção **Dispositivos**, selecione os dispositivos para os quais você deseja configurar a tarefa de Controle de Integridade de Aplicativos.
6. Configurar o agendamento de tarefa na seção **Programação** (você pode configurar um agendamento para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).
7. Na seção **Conta**, especifique a conta cujos direitos serão usados para a execução de tarefa.
8. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**.

> Para obter informações detalhadas sobre a definição das configurações nestas seções, consulte a *Ajuda do Kaspersky Security Center*.

9. Na janela **Propriedades: <Nome da tarefa>**, clique em **OK**.

   As configurações de tarefas de grupo definidas recentemente são salvas.

Definir configurações de diagnóstico de travamento no Kaspersky Security Center

Se um problema ocorrer durante a operação do Kaspersky Embedded Systems Security (por exemplo, travamentos do Kaspersky Embedded Systems Security) e você desejar diagnosticá-lo, é possível ativar a criação de arquivos de rastreamento e o arquivo de despejo do processo do Kaspersky Embedded Systems Security e enviar estes arquivos para análise ao Suporte Técnico da Kaspersky Lab.

O Kaspersky Embedded Systems Security não envia nenhum arquivo de rastreamento ou de despejo automaticamente. Os dados de diagnóstico só podem ser enviados pelo usuário com as permissões correspondentes.

O Kaspersky Embedded Systems Security grava as informações nos arquivos de rastreamento e no arquivo de despejo no formulário não criptografado. A pasta onde os arquivos são salvos é selecionada pelo usuário e gerenciada pela configuração do sistema operacional e do Kaspersky Embedded Systems Security. Você pode configurar permissões de acesso (consulte a seção "Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security" na página 226) e permitir o acesso a logs, arquivos de rastreamento e de despejo apenas para usuários necessários.

► *Para definir configurações de diagnóstico de travamento no Kaspersky Security Center:*

1. No Console de Administração do Kaspersky Security Center, abra a janela **Configurações do aplicativo** (consulte a seção **"Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center"** na página 119).
2. Na guia **Diagnóstico de funcionamento incorreto**, execute as ações seguintes:
   - Se você quiser que o aplicativo grave as informações de depuração no arquivo, marque a caixa de seleção **Gravar informações de depuração no arquivo de rastreamento**.
     - No campo abaixo especifique a pasta na qual o Kaspersky Embedded Systems Security salvará os arquivos rastreados.
     - Configure o nível de detalhe das informações de depuração.

       Esta lista suspensa permite a seleção do nível de detalhe das informações de depuração que o Kaspersky Embedded Systems Security salva no arquivo de rastreamento.

       Você pode selecionar um dos seguintes níveis de detalhe:

- **Eventos críticos** – O Kaspersky Embedded Systems Security salvará apenas as informações sobre eventos críticos relacionados ao arquivo de rastreamento.
- **Erros** – O Kaspersky Embedded Systems Security salvará as informações sobre eventos críticos e erros relacionados ao arquivo de rastreamento.
- **Eventos importantes** – O Kaspersky Embedded Systems Security salvará as informações sobre eventos críticos, erros e eventos importantes relacionados ao arquivo de rastreamento.
- **Eventos informativos** – O Kaspersky Embedded Systems Security salvará as informações sobre eventos críticos, erros, eventos importantes e eventos informativos relacionados ao arquivo de rastreamento.
- **Todas as informações da depuração** – O Kaspersky Embedded Systems Security salvará todas as informações da depuração no arquivo de rastreamento.

Um representante do Suporte Técnico determina o nível de detalhe que deve ser configurado para solucionar os problemas que ocorram.

O nível de detalhes padrão é configurado como **Todas as informações da depuração**.

A lista suspensa estará disponível se a caixa de seleção **Gravar informações de depuração no arquivo de rastreamento** estiver selecionada.

- Especifique o tamanho máximo dos arquivos de rastreamento.
- Especifique os componentes a serem depurados. Os códigos dos componentes devem ser separados por ponto e vírgula. Os códigos diferem entre maiúsculas e minúsculas (consulte a tabela abaixo).

Tabela 19. Códigos de subsistema do Kaspersky Embedded Systems Security

Código do componente	Nome do componente
*	Todos os componentes.
gui	Subsistema da interface de usuário, snap-in do Kaspersky Embedded Systems Security no Console de Gerenciamento da Microsoft.
ak_conn	Subsistema para a integração entre o Agente de rede e o Kaspersky Security Center.
bl	Processo de controle, implementa as tarefas de controle do Kaspersky Embedded Systems Security.
wp	Processo de trabalho, trata das tarefas de proteção do antivírus.
blgate	Processo de gerenciamento remoto do Kaspersky Embedded Systems Security.
ods	Subsistema de Verificação por Demanda.
oas	Subsistema de Proteção de Arquivos em Tempo Real.
qb	Subsistema da Quarentena e do Backup.
scandll	Módulo auxiliar para a verificação do antivírus.
core	Subsistema para a funcionalidade básica do antivírus.
avscan	Subsistema de processamento do antivírus.
avserv	Subsistema para controlar o kernel do antivírus.
prague	Subsistema para funcionalidade básica.
updater	Subsistema de atualização para bancos de dados e módulos do software.

snmp	Subsistema de suporte ao protocolo SNMP.
perfcount	Subsistema do contador de desempenho.

As configurações de rastreamento do snap-in (gui) do Kaspersky Embedded Systems Security e do Plug-in de Administração do Kaspersky Embedded Systems Security para o Kaspersky Security Center (ak_conn) serão aplicadas após estes componentes terem sido reiniciados. As configurações de rastreamento do subsistema de suporte de protocolo SNMP (snmp) serão aplicadas após o serviço SNMP ter sido reiniciado. As configurações de rastreamento do subsistema dos contadores de desempenho (perfcount) serão aplicadas após todos os processos que utilizam contadores de desempenho terem sido reiniciados. As configurações de rastreamento para outros subsistemas do Kaspersky Embedded Systems Security serão aplicadas assim que as configurações de diagnóstico de travamento forem salvas.

Por padrão, o Kaspersky Embedded Systems Security registra informações de depuração para todos os componentes do Kaspersky Embedded Systems Security.

O campo de inserção estará disponível se a caixa de seleção **Gravar informações de depuração no arquivo de rastreamento** estiver selecionada.

- Se desejar que o aplicativo crie um arquivo de despejo, selecione a caixa **Criar arquivo de despejo**.
  - No campo abaixo, especifique a pasta na qual o Kaspersky Embedded Systems Security salvará o arquivo de despejo.

3. Clique em **OK**.

As configurações do aplicativo definidas são aplicadas no computador protegido.

Gerenciando programações de tarefas

Você pode configurar a programação de inicialização para tarefas do Kaspersky Embedded Systems Security e definir as configurações para executar tarefas pela programação.

Nesta seção

Definição das configurações da programação de inicialização da tarefa 130
Ativando e desativando tarefas programadas 132

Definição das configurações da programação de inicialização da tarefa

É possível configurar a programação de inicialização de tarefas locais do sistema e tarefas personalizadas no Console do Aplicativo. Você não pode definir a programação de inicialização para tarefas de grupo.

► *Para definir as configurações da programação de inicialização da tarefa de grupo, execute as seguintes ações:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados**.
2. Selecione o grupo ao qual o servidor protegido pertence.

3. No painel de detalhes, selecione a guia **Tarefas**.
4. Abra a janela **Propriedades: <Nome da tarefa>** de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa.
   - Abra o menu de contexto do nome da tarefa e selecione o item Propriedades.
5. Selecione a seção **Programação**.
6. No bloco **Configurações de programação**, marque a caixa de seleção **Executar de acordo com o agendamento**.

   Os campos com as configurações de programação para as tarefas de Verificação por Demanda e de Atualização estarão indisponíveis se a inicialização da programação for bloqueada por uma política do Kaspersky Security Center.

7. Configure a programação de acordo com suas necessidades. Para isso, execute as seguintes ações:
   a. Na lista **Frequência**, selecione um dos seguintes valores:
      - **De hora em hora**, se desejar que a tarefa seja executada nos intervalos de um número especificado de horas; especifique o número de horas no campo **A cada <número> hora(s)**.
      - **Diariamente**, se desejar que a tarefa seja executada nos intervalos de um número especificado de dias; especifique o número de dias no campo **A cada <número> dia(s)**.
      - **Semanalmente**, se desejar que a tarefa seja executada nos intervalos de um número especificado de semanas; especifique o número de semanas no campo **A cada <número> semana(s)**. Especifique os dias da semana em que a tarefa será iniciada (por padrão, a tarefa é executada nas segundas-feiras).
      - **Ao iniciar o aplicativo**, se deseja que a tarefa seja executada a cada vez que iniciar o Kaspersky Embedded Systems Security.
      - **Após a atualização do banco de dados do aplicativo**, se desejar que a tarefa seja executada após cada atualização do banco de dados do aplicativo.
   b. Especifique a hora para a primeira inicialização da tarefa no campo **Hora inicial**.
   c. No campo **Data inicial**, especifique a data a partir da qual a programação se aplica.

      Após ter especificado a frequência de início da tarefa, a hora da primeira execução, a data a partir da qual se aplica a programação e informações sobre a hora estimada para a próxima execução da tarefa são exibidas na parte superior da janela, no campo **Próxima execução**. Informações atualizadas sobre a hora estimada da próxima execução da tarefa serão exibidas sempre que você abrir a janela **Configurações de tarefa** da guia **Agendar**.
      O valor **Bloqueado pela política** é exibido no campo **Próxima execução** se as configurações de política ativas do Kaspersky Security Center proibirem o início de tarefas programadas do sistema (consulte a seção "Configuração da inicialização programada de tarefas locais do sistema" na página 97).

8. Use a guia **Avançado** para definir as configurações de programação a seguir de acordo com os seus requisitos.
   - Na seção **Configurações de interrupção de tarefa**:
     a. Marque a caixa de seleção **Duração** e insira o número de horas e minutos necessários nos campos

à direita para especificar a duração máxima da execução da tarefa.

b. Marque a caixa de seleção **Pausar de** e insira os valores iniciais e finais do intervalo de tempo nos campos à direita para especificar o intervalo de tempo menor que 24 horas durante o qual a execução da tarefa será pausada.

- Na seção **Configurações avançadas**:

a. Marque a caixa de seleção **Cancelar agendamento a partir de** e especifique a data a partir da qual a programação será interrompida.

b. Marque a caixa de seleção **Executar tarefas ignoradas** para ativar a inicialização de tarefas ignoradas.

c. Marque a caixa de seleção **Randomizar a hora de início da tarefa no intervalo de** e especifique um valor em minutos.

9. Clique em **OK**.
10. Clique no botão **Aplicar** para salvar as configurações de início da tarefa.

Se desejar definir as configurações do aplicativo de uma única tarefa usando o Kaspersky Security Center, execute as etapas descritas em Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center (na página 119).

Ativando e desativando tarefas programadas

Você pode ativar e desativar tarefas programadas antes ou após a definição das configurações de programação.

► *Para ativar ou desativar a programação de inicialização da tarefa, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto no nome de tarefa para a qual deseja configurar a programação de inicialização.
2. Selecione **Propriedades**.

   A janela **Configurações de tarefa** é exibida.
3. Na janela exibida na guia **Programação**, faça uma das ações a seguir:
   - Marque a caixa de seleção **Executar de acordo com a programação** se desejar ativar o início da tarefa programada.
   - Desmarque a caixa de seleção **Executar de acordo com a programação** se desejar desativar o início da tarefa programada.

   As definições de programação de inicialização da tarefa configuradas não são excluídas e serão aplicadas no próximo início programado da tarefa.
4. Clique em **OK**.
5. Clique no botão **Aplicar**.

As definições de programação de inicialização da tarefa configuradas são salvas.

Relatórios do Kaspersky Security Center

Os relatórios do Kaspersky Security Center contêm informações sobre o status de dispositivos gerenciados. Os relatórios são baseados em informações armazenadas no Servidor de Administração.

A partir do Kaspersky Security Center 11, os seguintes tipos de relatórios estão disponíveis para o Kaspersky Embedded Systems Security:

- Relatório do status dos componentes do aplicativo
- Relatório de aplicativos proibidos
- Relatório de aplicativos proibidos em modo de teste

Consulte a *Ajuda do Kaspersky Security Center* para obter informações detalhadas sobre todos os relatórios do Kaspersky Security Center e como configurá-los.

Relatório do status dos componentes do aplicativo

É possível monitorar o status de proteção de todos os dispositivos da rede e obter um resumo estruturado do conjunto de componentes em cada dispositivo.

O relatório exibe um dos seguintes estados de cada componente: *Executando, Pausado, Interrompido, Mau funcionamento, Não instalado, Iniciando*.

O status *Não instalado* refere-se ao componente, não ao próprio aplicativo. Se o aplicativo não estiver instalado, o Kaspersky Security Center atribui o status N/A (Não disponível).

É possível criar seleções de componentes e usar filtros para exibir dispositivos de rede com o conjunto de componentes definidos e o estado deles.

Consulte a *Ajuda do Kaspersky Security Center* para obter informações detalhadas sobre a criação e o uso das seleções.

► *Para revisar o status dos componentes nas configurações do aplicativo:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center e selecione o grupo de administração para o qual você deseja definir as configurações do aplicativo.
2. Selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).
3. Selecione a seção **Componentes**.
4. Revise a tabela de status.

► *Para revisar um relatório padrão do Kaspersky Security Center:*

1. Selecione o nó **Servidor de Administração <Nome de computador>** na árvore do Console de

Administração.

2. Abra a guia **Relatórios**.
3. Clique duas vezes no item da lista **Relatório do status de componentes do aplicativo**.

   Um relatório é gerado.
4. Revise os seguintes detalhes do relatório:
   - Um diagrama gráfico.
   - Uma tabela de resumo de componentes e números agregados de dispositivos da rede em que cada componente está instalado, e grupos aos quais pertencem.
   - Uma tabela detalhada especificando o status, a versão, o dispositivo e o grupo do componente.

Relatórios de aplicativos bloqueados em modos ativo e de estatística

Com base nos resultados da execução da tarefa de Controle de Inicialização de Aplicativos, dois tipos de relatórios podem ser gerados: o relatório de aplicativos proibidos (se a tarefa for iniciada no modo Ativa) e o relatório de aplicativos proibidos no modo de teste (se a tarefa for iniciada no modo Somente estatísticas). Estes relatórios exibem informações sobre aplicativos bloqueados nos computadores protegidos da rede. Cada relatório é gerado para todos os grupos de administração e acumula dados de todos os aplicativos da Kaspersky Lab instalados nos dispositivos protegidos.

► *Para revisar um relatório de aplicativos proibidos no modo de teste:*

1. Inicie a tarefa de Controle de Aplicativos no modo Somente estatísticas (consulte a seção "Definição de configurações da tarefa de Controle de Inicialização de Aplicativos" na página 300).
2. Selecione o nó **Servidor de Administração <Nome de computador>** na árvore do Console de Administração.
3. Abra a guia **Relatórios**.
4. Clique duas vezes no item da lista **Relatório de aplicativos proibidos em modo de teste**.

   Um relatório é gerado.
5. Revise os seguintes detalhes do relatório:
   - Um diagrama gráfico exibe os dez principais aplicativos com o maior número de inicializações bloqueadas.
   - Uma tabela de resumo de bloqueios do aplicativo especificando o nome do arquivo executável, o motivo, o horário do bloqueio e o número de dispositivos em que o bloqueio ocorreu.
   - Uma tabela detalhada especificando dados do dispositivo, o caminho do arquivo e os critérios de bloqueio.

► *Para revisar um relatório de aplicativos proibidos no modo Ativo:*

1. Inicie a tarefa de Controle de Aplicativos no modo Ativa (consulte a seção "Definição de configurações da tarefa de Controle de Inicialização de Aplicativos" na página 300),
2. Selecione o nó **Servidor de Administração <Nome de computador>** na árvore do Console de Administração.
3. Abra a guia **Relatórios**.
4. Clique duas vezes no item da lista **Relatório de aplicativos proibidos**.

Um relatório é gerado.

Este relatório contém os mesmos blocos de dados que o relatório de aplicativos proibidos no modo de teste.

Trabalhar com o Console do Kaspersky Embedded Systems Security

Esta seção fornece informações sobre o Console do Kaspersky Embedded Systems Security e descreve como gerenciar o aplicativo usando o Console do Aplicativo instalado no computador protegido ou em outro computador.

Neste capítulo

Configurações do Kaspersky Embedded Systems Security no Console do Aplicativo 136

Sobre o Console do Kaspersky Embedded Systems Security 143

Interface do Console do Kaspersky Embedded Systems Security 143

Ícone da Bandeja do sistema na área de notificação 147

Gerenciando o Kaspersky Embedded Systems Security por meio do Console do Aplicativo em outro computador 148

Gerenciando as tarefas do Kaspersky Embedded Systems Security 148

Visualizando o status de proteção e as informações do Kaspersky Embedded Systems Security 161

Interface de Diagnóstico Compacta 166

Atualização de bancos de dados e módulos de software do Kaspersky Embedded Systems Security 171

Isolamento de objetos e cópia de backup 185

Registro de eventos. Logs do Kaspersky Embedded Systems Security 201

Configurações de notificação 215

Configurações do Kaspersky Embedded Systems Security no Console do Aplicativo

As configurações gerais e as configurações de diagnóstico de funcionamento incorreto das configurações do Kaspersky Embedded Systems Security estabelecem as condições gerais nas quais o aplicativo opera. Estas configurações permitem a você controlar o número de processos de trabalho usados pelo Kaspersky Embedded Systems Security, ativar a recuperação de tarefas do Kaspersky Embedded Systems Security após um encerramento anormal, manter o log de rastreamento, ativar a criação do arquivo de despejo dos processos do Kaspersky Embedded Systems Security no caso de um encerramento anormal e definir outras configurações gerais.

As configurações do aplicativo não podem ser definidas no Console do Aplicativo se a política ativa do Kaspersky Security Center bloquear alterações a essas configurações.

► *Para definir as configurações do Kaspersky Embedded Systems Security:*

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e execute uma das seguintes ações:
   - Clique no link **Propriedades do aplicativo** no painel de detalhes do nó.
   - Selecione **Propriedades** no menu de contexto do nó.

   A janela **Configurações do aplicativo** é exibida.
2. Na janela exibida, especifique as configurações gerais do Kaspersky Embedded Systems Security de acordo com suas preferências:
   - As configurações seguintes podem ser especificadas na guia **Escalabilidade e interface**:
     - Na seção **Configurações de escalabilidade**:
       - Número máximo de processos de trabalho que podem ser executados pelo Kaspersky Embedded Systems Security;

Tabela 20. Número máximo de processos ativos

<table>
<tr><th>Configuração</th><th>Número máximo de processos ativos</th></tr>
<tr><td>Descrição</td><td>Esta definição pertence ao grupo de Configurações de escalabilidade no Kaspersky Embedded Systems Security. Ela determina o número máximo de processos ativos que o aplicativo pode executar simultaneamente.
Aumentar o número de processos sendo executados em paralelo aumenta a velocidade da verificação de arquivos e melhora a segurança contra falhas do Kaspersky Embedded Systems Security. No entanto, se o valor desta definição for muito alto, ele pode reduzir o desempenho geral do computador e aumentar o uso de RAM.
No Console de Administração do aplicativo do Kaspersky Security Center você pode modificar a configuração do Número máximo de processos ativos somente para o Kaspersky Embedded Systems Security instalado em um computador independente (usando a caixa de diálogo Configurações do aplicativo); no entanto, você não pode modificar esta definição nas configurações de política para o grupo de computadores.</td></tr>
<tr><td>Valores possíveis</td><td>1 – 8</td></tr>
<tr><td>Valor padrão</td><td>O aplicativo controla automaticamente a escalabilidade dependendo do número de processadores no computador:
<table>
<tr><th>Número de processadores</th><th>Número máximo de processos ativos</th></tr>
<tr><td>1</td><td>1</td></tr>
<tr><td>1< número de processadores < 4</td><td>2</td></tr>
<tr><td>4 ou mais</td><td>4</td></tr>
</table></td></tr>
</table>

- Número de processos para a Proteção do Computador em Tempo Real

Tabela 21. Número de processos para a Proteção em tempo real

Configuração	Número de processos para a Proteção em tempo real

<table>
<tr><td>Descrição</td><td>Esta definição pertence ao grupo de Configurações de escalabilidade no Kaspersky Embedded Systems Security.
Ao usar esta definição você pode especificar o número fixo de processos nos quais o Kaspersky Embedded Systems Security executará as tarefas de Proteção em tempo real.
Um valor mais alto desta definição aumentará a velocidade de verificação nas tarefas de Proteção em tempo real. No entanto, quanto mais processos o Kaspersky Embedded Systems Security usar, maior será sua influência no desempenho geral do computador protegido e no uso dos recursos de RAM.
No Console de Administração do aplicativo do Kaspersky Security Center você pode modificar a configuração do Número de processos para a Proteção em tempo real somente para o Kaspersky Embedded Systems Security instalado em um computador independente (usando a janela Configurações do aplicativo); no entanto, você não pode modificar esta definição nas configurações de política para o grupo de computadores.</td></tr>
<tr><td>Valores possíveis</td><td>Valores possíveis: 1-N, em que N é o valor especificado usando a configuração do Número máximo de processos ativos.
Se você definir o valor da configuração do Número de processos para a Proteção em tempo real como igual ao número máximo de processos ativos, você reduzirá o impacto do Kaspersky Embedded Systems Security na taxa da troca de arquivos entre os computadores e o computador, dessa forma, melhorando ainda mais o desempenho durante a Proteção em tempo real. No entanto, tarefas de atualização e tarefas de Verificação por Demanda com a prioridade básica Médio (Normal) serão executadas nos processos do Kaspersky Embedded Systems Security que já estão em execução. As tarefas de Verificação por Demanda serão executadas com menos velocidade. Se a execução de uma tarefa causa um encerramento anormal de um processo, ele levará mais tempo para ser reiniciado.
Tarefas de Verificação por Demanda com a prioridade básica Baixa são sempre executadas em um processo ou processos separados.</td></tr>
<tr><td>Valor padrão</td><td>O Kaspersky Embedded Systems Security controla automaticamente a escalabilidade dependendo do número de processadores no computador:
<table>
<tr><th>Número de processadores</th><th>Número de processos para a Proteção em tempo real</th></tr>
<tr><td>=1</td><td>1</td></tr>
<tr><td>>1</td><td>2</td></tr>
</table>
</td></tr>
</table>

- Número de processos de trabalho para tarefas de Verificação por Demanda em segundo plano

Tabela 22. Número de processos de tarefas de verificação por demanda em segundo plano

Configuração	Número de processos de tarefas de verificação por demanda em segundo plano

Descrição	Esta definição pertence ao grupo de **Configurações de escalabilidade** no Kaspersky Embedded Systems Security. Você pode usar esta definição para especificar o número máximo de processos que o aplicativo usará para executar as tarefas de Verificação por Demanda em segundo plano. O número de processos especificados por esta definição não está incluído no número total de processos especificados do Kaspersky Embedded Systems Security pela configuração do **Número máximo de processos ativos**. Por exemplo, se você especificar os seguintes valores de configurações: • Número máximo de processos ativos – 3; • Número de processos para a Proteção em tempo real – 3; • Número de processos de trabalho para tarefas de Verificação por Demanda em segundo plano – 1; e, em seguida, inicie as tarefas de Proteção em tempo real e uma tarefa de Verificação por Demanda em segundo plano, o número total de processos kavfswp.exe do Kaspersky Embedded Systems Security será 4. Várias tarefas de Verificação por Demanda podem ser executadas em um processo com baixa prioridade. Você pode aumentar o número de processos, por exemplo, se executar várias tarefas em segundo plano para alocar um processo separado para cada tarefa. A alocação de processos separados para tarefas aumenta a confiabilidade e a velocidade da execução da tarefa.
Valores possíveis	1-4
Valor padrão	1

- Na seção **Interação com o usuário**, selecione se o Ícone da bandeja do sistema será exibido na barra de tarefas após a inicialização de cada aplicativo (consulte a seção "Ícone da bandeja do sistema na área de notificação" na página 147).

- As configurações seguintes podem ser especificadas na guia **Segurança e confiabilidade**:
  - Na seção **Configurações de confiabilidade**, especifique o número de tentativas para recuperar uma tarefa de Verificação por Demanda após o travamento.

Tabela 23. Recuperação de tarefa

Configuração	Recuperação da tarefa (**Executar recuperação da tarefa**)
Descrição	Esta configuração pertence ao grupo de **Configurações de confiabilidade** no Kaspersky Embedded Systems Security. Isso permite a recuperação de tarefas em caso de um encerramento de emergência e define o número de tentativas usadas para recuperar as tarefas de Verificação por Demanda. Quando uma tarefa trava, o processo kavfs.exe do Kaspersky Embedded Systems Security tenta reiniciar o processo no qual aquela tarefa executava no momento do travamento. Se a recuperação de tarefas estiver desativada, o aplicativo não restaurará as tarefas de Proteção em Tempo Real e de Verificação por Demanda. Se a recuperação de tarefas estiver ativada, o aplicativo tentará restaurar as tarefas de Proteção em Tempo Real até que elas sejam iniciadas com êxito e tentará restaurar as tarefas de Verificação por Demanda usando o número de tentativas especificado na configuração.

Valores possíveis	Ativado/Desativado. O número de tentativas de recuperação das tarefas de Verificação por Demanda: 1 - 10.
Valor padrão	A recuperação de tarefas está ativada. O número de tentativas de recuperação das tarefas de Verificação por Demanda: 2.

- Na seção **Ações ao mudar para energia de backup UPS**, especifique ações que o Kaspersky Embedded Systems Security realiza após alternar para a energia UPS:

Tabela 24. Uso de fonte de energia ininterrupta

Configuração	Ações ao mudar para energia de backup UPS.
Descrição	Esta configuração determina as ações que o Kaspersky Embedded Systems Security realiza quando o computador muda para uma fonte de energia ininterrupta.
Valores possíveis	Execute ou não tarefas de Verificação por Demanda a serem iniciadas de acordo com a programação. Execute ou pare todas as tarefas ativas de Verificação por Demanda.
Valor padrão	Por padrão, se a fonte de energia ininterrupta for usada para alimentar um computador, o Kaspersky Embedded Systems Security: • Não executará as tarefas de Verificação por Demanda executadas de acordo com a programação. • Interromperá automaticamente todas as tarefas ativas de Verificação por Demanda.

- Na seção **Configurações de proteção de senha**, defina as configurações de proteção de senha das funções do aplicativo (consulte a seção "Acesso protegido por senha às funções do Kaspersky Embedded Systems Security" na página 233).

- Na guia **Configurações de conexão**:
  - Na seção **Configurações do servidor proxy**, especifique as configurações de uso do servidor proxy.
  - Na seção **Configurações de autenticação do servidor proxy**, especifique o tipo de autenticação e detalhes exigidos para a autenticação no servidor proxy.
  - Na seção **Licenciamento**, indique se o Kaspersky Security Center será utilizado como um servidor proxy para a ativação do aplicativo.
- Na guia **Diagnóstico de funcionamento incorreto**:
  - Se você quiser que o aplicativo grave as informações de depuração no arquivo, marque a caixa de seleção **Gravar informações de depuração no arquivo de rastreamento**.
    - No campo abaixo especifique a pasta na qual o Kaspersky Embedded Systems Security salvará os arquivos rastreados.
    - Configure o nível de detalhe das informações de depuração.

      Esta lista suspensa permite a seleção do nível de detalhe das informações de depuração que o Kaspersky Embedded Systems Security salva no arquivo de rastreamento.

Você pode selecionar um dos seguintes níveis de detalhe:

- **Eventos críticos** – O Kaspersky Embedded Systems Security salvará apenas as informações sobre eventos críticos relacionados ao arquivo de rastreamento.
- **Erros** – O Kaspersky Embedded Systems Security salvará as informações sobre eventos críticos e erros relacionados ao arquivo de rastreamento.
- **Eventos importantes** – O Kaspersky Embedded Systems Security salvará as informações sobre eventos críticos, erros e eventos importantes relacionados ao arquivo de rastreamento.
- **Eventos informativos** – O Kaspersky Embedded Systems Security salvará as informações sobre eventos críticos, erros, eventos importantes e eventos informativos relacionados ao arquivo de rastreamento.
- **Todas as informações da depuração** – O Kaspersky Embedded Systems Security salvará todas as informações da depuração no arquivo de rastreamento.

Um representante do Suporte Técnico determina o nível de detalhe que deve ser configurado para solucionar os problemas que ocorram.

O nível de detalhes padrão é configurado como **Todas as informações da depuração**.

A lista suspensa estará disponível se a caixa de seleção **Gravar informações de depuração no arquivo de rastreamento** estiver selecionada.

- Especifique o tamanho máximo dos arquivos de rastreamento.
- Especifique os componentes a serem depurados.

Uma lista de códigos de componentes do Kaspersky Embedded Systems Security para os quais o aplicativo salva as informações de depuração no arquivo de rastreamento. Os códigos dos componentes devem ser separados por ponto e vírgula. Os códigos diferem entre maiúsculas e minúsculas (consulte a tabela abaixo).

Tabela 25. Códigos de subsistema do Kaspersky Embedded Systems Security

Código do componente	Nome do componente
*	Todos os componentes.
gui	Subsistema da interface de usuário, snap-in do Kaspersky Embedded Systems Security no Console de Gerenciamento da Microsoft.
ak_conn	Subsistema para a integração entre o Agente de rede e o Kaspersky Security Center.
bl	Processo de controle, implementa as tarefas de controle do Kaspersky Embedded Systems Security.
wp	Processo de trabalho, trata das tarefas de proteção do antivírus.
blgate	Processo de gerenciamento remoto do Kaspersky Embedded Systems Security.
ods	Subsistema de Verificação por Demanda.
oas	Subsistema de Proteção de Arquivos em Tempo Real.
qb	Subsistema da Quarentena e do Backup.
scandll	Módulo auxiliar para a verificação do antivírus.
core	Subsistema para a funcionalidade básica do antivírus.
avscan	Subsistema de processamento do antivírus.

avserv	Subsistema para controlar o kernel do antivírus.
prague	Subsistema para funcionalidade básica.
updater	Subsistema de atualização para bancos de dados e módulos do software.
snmp	Subsistema de suporte ao protocolo SNMP.
perfcount	Subsistema do contador de desempenho.

As configurações de rastreamento do snap-in (gui) do Kaspersky Embedded Systems Security e do Plug-in de Administração do Kaspersky Embedded Systems Security para o Kaspersky Security Center (ak_conn) serão aplicadas após estes componentes terem sido reiniciados. As configurações de rastreamento do subsistema de suporte de protocolo SNMP (snmp) serão aplicadas após o serviço SNMP ter sido reiniciado. As configurações de rastreamento do subsistema dos contadores de desempenho (perfcount) serão aplicadas após todos os processos que utilizam contadores de desempenho terem sido reiniciados. As configurações de rastreamento para outros subsistemas do Kaspersky Embedded Systems Security serão aplicadas assim que as configurações de diagnóstico de travamento forem salvas.

Por padrão, o Kaspersky Embedded Systems Security registra informações de depuração para todos os componentes do Kaspersky Embedded Systems Security.

O campo de inserção estará disponível se a caixa de seleção **Gravar informações de depuração no arquivo de rastreamento** estiver selecionada.

- Se desejar que o aplicativo crie um arquivo de despejo, selecione a caixa **Criar arquivo de despejo de travamento**.

O Kaspersky Embedded Systems Security não envia nenhum arquivo de rastreamento ou de despejo automaticamente. Os dados de diagnóstico só podem ser enviados pelo usuário com as permissões correspondentes.

- No campo abaixo, especifique a pasta na qual o Kaspersky Embedded Systems Security salvará os arquivos de despejo da memória.

O Kaspersky Embedded Systems Security grava as informações nos arquivos de rastreamento e nos arquivos de despejo no formulário não criptografado. A pasta em que os arquivos são salvos é selecionada pelo usuário e gerenciada pela configuração do sistema operacional e do Kaspersky Embedded Systems Security. Você pode configurar permissões de acesso (consulte a seção "Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security" na página 226) e permitir o acesso a logs, arquivos de rastreamento e de despejo apenas para usuários necessários.

3. Clique em **OK**.

As configurações do Kaspersky Embedded Systems Security são salvas.

Sobre o Console do Kaspersky Embedded Systems Security

O Console do Kaspersky Embedded Systems Security é um snap-in isolado adicionado ao Console de Gerenciamento da Microsoft.

O aplicativo pode ser gerenciado por meio do Console do Aplicativo instalado no computador protegido ou em outro computador na rede corporativa.

Depois que o Console do Aplicativo for instalado em outro computador, é necessária uma configuração avançada.

Se o Console do Aplicativo e o Kaspersky Embedded Systems Security forem instalados em computadores diferentes destinados a domínios diferentes, poderá haver limitações à entrega de informações do aplicativo ao Console do Aplicativo. Por exemplo, após o início de uma tarefa de aplicativo, seu status pode permanecer inalterado no Console do Aplicativo.

Durante a instalação do Console do Aplicativo, o assistente de instalação cria o arquivo kavfs.msc na pasta Instalação e adiciona o snap-in do Kaspersky Embedded Systems Security à lista de snap-ins isolados do Microsoft Windows.

Você pode iniciar o Console do Aplicativo do menu **Iniciar**. O arquivo msc do snap-in do Kaspersky Embedded Systems Security pode ser executado ou adicionado a um Console de Gerenciamento Microsoft existente como um novo elemento na árvore.

Em uma versão de 64 bits do Microsoft Windows, o snap-in do Kaspersky Embedded Systems Security pode ser adicionado somente na versão de 32 bits do Console de Gerenciamento Microsoft. Para isso, abra o Console de Gerenciamento da Microsoft a partir da linha de comando executando o comando: mmc.exe /32.

Vários snap-ins do Kaspersky Embedded Systems Security podem ser adicionados a um Console de Gerenciamento da Microsoft aberto no modo de autor para utilizá-lo para gerenciar a proteção de vários computadores nos quais o Kaspersky Embedded Systems Security está instalado.

Interface do Console do Kaspersky Embedded Systems Security

O Console do Kaspersky Embedded Systems Security é exibido na árvore do Console de Gerenciamento Microsoft na forma de um nó.

Após estabelecer uma conexão com o Kaspersky Embedded Systems Security instalado em um computador diferente, o nome do nó será complementado com o nome do computador no qual o aplicativo está instalado e o nome da conta de usuário em que a conexão foi estabelecida: **Kaspersky Embedded Systems Security <nome do computador> como <nome da conta>**. Após a conexão do Kaspersky Embedded Systems Security instalado no mesmo computador com o Console do Aplicativo, o nome do nó será **Kaspersky Embedded Systems Security**.

Por padrão, a janela do Console do Aplicativo inclui os seguintes elementos:

- Árvore do Console do Aplicativo
- Painel de detalhes
- Barra de ferramentas

A árvore do Console do Aplicativo

A árvore do Console do Aplicativo exibe o nó **Kaspersky Embedded Systems Security** e os subnós dos componentes funcionais do aplicativo.

O nó **Kaspersky Embedded Systems Security** inclui os seguintes subnós:

- **Proteção do Computador em Tempo Real**: gerencia tarefas de proteção em tempo real e serviços da KSN. O nó **Proteção do Computador em Tempo Real** permite configurar as seguintes tarefas:
  - **Proteção de Arquivos em Tempo Real**
  - **Uso da KSN**
- **Controle do Computador** controla as inicializações de aplicativos instalados em um computador protegido, bem como as conexões de dispositivos externos. O nó **Controle do Computador** permite configurar as seguintes tarefas:
  - **Controle de Inicialização de Aplicativos**
  - **Controle de Dispositivos**
  - **Gerenciamento de Firewall**
- **Geradores de regra automáticos**: a configuração de geração automática de regras de grupo e de sistema para as tarefas de Controle de Inicialização de Aplicativos e Controle de Dispositivos.
  - **Gerador de Regras de Controle de Inicialização de Aplicativos**
  - **Gerador de Regras de Controle de Dispositivos**
  - Tarefas de grupo de geração de regras **<Nomes da tarefa>** (se aplicável)

    As tarefas de grupo (consulte a seção "Categorias de tarefas do Kaspersky Embedded Systems Security" na página 149) são criadas usando o Kaspersky Security Center. Você não pode gerenciar tarefas de grupo pelo Console do Aplicativo.
- **Inspeção do sistema**: configuração do controle de operações de arquivos e configurações de inspeção de Log de Eventos do Windows.
  - **Monitor de Integridade de Arquivos**
  - **Inspeção de Log**
- **Verificação por Demanda**: gerencia tarefas de Verificação por Demanda. Existe um nó separado para cada tarefa:
  - **Verificação na Inicialização do Sistema Operacional**
  - **Verificação de Áreas Críticas**
  - **Verificação da Quarentena**
  - **Controle de Integridade de Aplicativos**
  - Tarefas personalizadas **<Nomes das tarefas>** (se aplicável)

  O nó exibe tarefas do sistema (consulte a seção "Categorias de tarefas do Kaspersky Embedded Systems Security" na página 149) criadas quando o aplicativo é instalado, tarefas personalizadas e de verificação

por demanda de grupo criadas e enviadas a um computador usando o Kaspersky Security Center.

- **Atualização**: gerencia as atualizações dos bancos de dados e dos módulos do Kaspersky Embedded Systems Security e copia as atualizações em uma pasta de fonte de atualização local. O nó contém nós filhos para administrar cada tarefa de atualização e a última tarefa de Reversão da Atualização do Banco de Dados:
  - **Atualização do Banco de Dados**
  - **Atualização de módulos de software**
  - **Copiar atualizações**
  - **Reversão da Atualização do Banco de Dados**

  O nó exibe todas as tarefas de atualização de grupo e personalizadas (consulte a seção "Categorias de tarefas do Kaspersky Embedded Systems Security" na página 149) criadas e enviadas a um computador usando o Kaspersky Security Center.
- **Armazenamentos**: Gerenciamento das configurações de Quarentena e de Backup.
  - **Quarentena**
  - **Backup**
- **Logs e notificações**: gerencia logs de tarefas locais, log de segurança e log de auditoria do Sistema Kaspersky Embedded Systems Security.
  - **Log de segurança**
  - **Log de auditoria do sistema**
  - **Logs de tarefas**
- **Licenciamento**: adiciona ou exclui as chaves e códigos de ativação do Kaspersky Embedded Systems Security, visualiza detalhes da licença.

Painel de detalhes

O painel de detalhes exibe informações sobre o nó selecionado. Se o nó **Kaspersky Embedded Systems Security** for selecionado, o painel de detalhes exibe informações sobre o status de proteção do computador atual (consulte a seção "Visualizando o status de proteção e as informações do Kaspersky Embedded Systems Security" na página 161) e informações sobre o Kaspersky Embedded Systems Security, o status de proteção dos seus componentes funcionais e a data de expiração da licença.

Menu de contexto do nó Kaspersky Embedded Systems Security

Você pode usar os itens do menu de contexto do nó **Kaspersky Embedded Systems Security** para executar as seguintes operações:

- **Conectar a outro computador**. Conectar a outro computador (consulte a seção "Gerenciando o Kaspersky Embedded Systems Security por meio do Console do Aplicativo em outro computador" na página 148) para gerenciar o Kaspersky Embedded Systems Security instalado nele. Você também pode executar esta operação clicando no link no canto inferior direito do painel de detalhes do nó **Kaspersky Embedded Systems Security**.
- **Iniciar o serviço** / **Interromper o serviço**. Iniciar ou interromper o aplicativo ou uma tarefa selecionada (consulte a seção "Executando / pausando / reiniciando / interrompendo tarefas manualmente" na página 150). Para executar essas operações, você também pode usar os botões da barra de ferramentas. Você também pode executar estas operações nos menus de contexto de tarefas do aplicativo.
- **Configurar verificação de unidades removíveis**. Configure a verificação de unidades removíveis

(consulte a seção "Sobre a Verificação de unidades removíveis" na página 406) conectadas ao computador protegido pela porta USB.

- **Prevenção de Exploits: configurações gerais**. Configure o modo de Prevenção de Exploits e define ações de prevenção.
- **Prevenção de Exploits: configurações de proteção de processos**. Adicione processos para proteção e selecione as técnicas de prevenção de exploits (ver a Seção "Técnicas de prevenção de exploits" na página 466).
- **Configurar a Zona Confiável**. Visualize e configure a Zona Confiável (consulte a seção "Sobre a Zona Confiável" na página 443).
- **Modificar direitos do usuário do gerenciamento de aplicativos**. Visualize e configure permissões de acesso a funções do Kaspersky Embedded Systems Security (consulte a seção "Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security" na página 226).
- **Modificar direitos de usuário de gerenciamento do Kaspersky Security Service**. Visualize e configure direitos de usuário para gerenciar Kaspersky Security Service (consulte a seção "Configuração de permissões de acesso para gerenciamento do Kaspersky Embedded Systems Security e do Kaspersky Security Service" na página 231).
- **Exportar configurações**. Salve as configurações do aplicativo em um arquivo de configuração no formato XML (consulte a seção "Exportando configurações" na página 155). Você também pode executar esta operação nos menus de contexto de tarefas do aplicativo.
- **Importar configurações**. Importe configuração do aplicativo de um arquivo de configuração no formato XML (consulte a seção "Importando configurações" na página 156). Você também pode executar esta operação nos menus de contexto de tarefas do aplicativo.
- **Informações sobre o aplicativo e atualizações de módulo disponíveis**. Consultar informações sobre o Kaspersky Embedded Systems Security e atualizações dos módulos do aplicativo atualmente disponíveis.
- **Atualizar**. Atualize o conteúdo da janela de Console do Aplicativo. Você também pode executar esta operação nos menus de contexto de tarefas do aplicativo.
- **Propriedades**. Visualize e defina as configurações do Kaspersky Embedded Systems Security ou uma tarefa selecionada. Você também pode executar esta operação nos menus de contexto de tarefas do aplicativo.

  Para fazer isso, você também pode usar o link **Propriedades do aplicativo** no painel de detalhes do nó **Kaspersky Embedded Systems Security** ou usar o botão na barra de ferramentas.

- **Ajuda**. Visualize as informações sobre a ajuda do Kaspersky Embedded Systems Security. Você também pode executar esta operação nos menus de contexto de tarefas do aplicativo.

Barra de ferramentas e menu de contexto das tarefas do Kaspersky Embedded Systems Security

Você pode gerenciar as tarefas do Kaspersky Embedded Systems Security usando os itens dos menus de contexto de cada tarefa na árvore do Console do Aplicativo.

Você pode usar os itens do menu de contexto para executar as seguintes operações:

- **Iniciar** / **Interromper**. Iniciar ou interromper a execução de uma tarefa (consulte a seção "Executando / pausando / reiniciando / interrompendo tarefas manualmente" na página 150). Para executar essas operações, você também pode usar os botões da barra de ferramentas.
- **Reiniciar** / **Pausar**. Reinicie ou pause a execução de uma tarefa (consulte a seção "Executando / pausando / reiniciando / interrompendo tarefas manualmente" na página 150). Para executar essas

operações, você também pode usar os botões da barra de ferramentas. Esta operação está disponível para as tarefas de Proteção em Tempo Real e tarefas de Verificação por Demanda.

- **Adicionar tarefa**. Crie uma nota tarefa personalizada (consulte a seção "Criação e configuração de uma tarefa de Verificação por Demanda" na página 427). Esta operação está disponível para tarefas de Verificação por Demanda.
- **Abrir log**. Visualize e gerencie um log de tarefas (consulte a seção "Sobre logs de tarefas" na página 204). Esta operação está disponível para todas as tarefas.
- **Remover tarefa**. Excluir tarefa personalizada. Esta operação está disponível para tarefas de Verificação por Demanda.
- **Modelos de configurações**. Gerencie modelos (consulte a seção "Usando os modelos de configurações de segurança" na página 157). Esta operação está disponível para a Proteção de Arquivos em Tempo Real e a Verificação por Demanda.

Ícone da bandeja do sistema na área de notificação

Cada vez que o Kaspersky Embedded Systems Security é iniciado automaticamente depois de uma reinicialização do computador, o ícone da bandeja do sistema é exibido na área de notificação da barra de ferramentas. Ele é exibido por padrão se o componente do ícone da bandeja do sistema tiver sido instalado durante a configuração do aplicativo.

A aparência do ícone da bandeja do sistema reflete o status atual da proteção do computador. Os dois status possíveis são:

ativa (ícone colorido) se pelo menos uma das tarefas está sendo executada no momento: Proteção de Arquivos em Tempo Real, Controle de Inicialização de Aplicativos

inativo (ícone em preto e branco) se nenhuma das tarefas está sendo executada no momento: Proteção de Arquivos em Tempo Real, Controle de Inicialização de Aplicativos

Você pode abrir o menu de contexto do ícone da bandeja de sistema clicando nele com o botão direito do mouse.

O menu de contexto oferece vários comandos que podem ser usados para exibir janelas do aplicativo (consulte a tabela abaixo).

Tabela 26. Comandos do menu de contexto exibidos no ícone da bandeja do sistema

Comando	Descrição
Abrir o Console do Aplicativo	Abre o Console do Kaspersky Embedded Systems Security (se instalado).
Abrir interface de diagnóstico compacta	Abre a interface de diagnóstico compacta.
Sobre o aplicativo	Abre a janela Sobre o aplicativo, que contém informações sobre o Kaspersky Embedded Systems Security. Para usuários registrados do Kaspersky Embedded Systems Security, a janela Sobre o aplicativo inclui informações sobre atualizações urgentes que tenham sido instaladas.

Comando	Descrição
Ocultar	Oculta o ícone da bandeja de sistema na área de notificação da barra de ferramentas.

Você pode exibir o ícone oculto da bandeja do sistema novamente a qualquer momento.

► *Para exibir o ícone do aplicativo novamente,*

no menu **Iniciar** do Microsoft Windows, selecione **Todos os Programas** > **Kaspersky Embedded Systems Security** > **Ícone da bandeja do sistema**.

Os nomes de configurações podem variar dependendo do sistema operacional instalado.

Nas configurações gerais do Kaspersky Embedded Systems Security, você pode ativar ou desativar a exibição do Ícone da bandeja do sistema sempre que o aplicativo for iniciado automaticamente após uma reinicialização do computador.

Gerenciando o Kaspersky Embedded Systems Security por meio do Console do Aplicativo em outro computador

Você pode gerenciar o Kaspersky Embedded Systems Security por meio do Console do Aplicativo instalado em um computador remoto.

Para gerenciar o aplicativo utilizando o Console do Kaspersky Embedded Systems Security em um computador remoto, certifique-se de que:

- Os usuários do Console do Aplicativo no computador remoto sejam adicionados ao grupo de Administradores de ESS no computador protegido.
- As conexões de rede são permitidas para o processo do Kaspersky Security Management Service (kavfsgt.exe) se o Firewall do Windows estiver ativado no computador protegido.
- Durante a instalação do Kaspersky Embedded Systems Security, a caixa **Permitir acesso remoto** foi selecionada na janela do Assistente de instalação.

Se o Kaspersky Embedded Systems Security no computador remoto for protegido por senha, insira a senha para acessar o gerenciamento do aplicativo por meio do Console do Aplicativo.

Gerenciando as tarefas do Kaspersky Embedded Systems Security

Esta seção contém informação sobre tarefas do Kaspersky Embedded Systems Security e como criá-las, definir suas configurações, iniciá-las e interrompê-las.

Nesta seção

Categorias de tarefa do Kaspersky Embedded Systems Security 149
Como salvar uma tarefa depois de alterar suas configurações 149
Executando / pausando / reiniciando / interrompendo tarefas manualmente 150
Gerenciando programações de tarefas 150
Uso de contas de usuário para iniciar tarefas 152
Configurações de importação e exportação 154
Usando os modelos de configurações de segurança 157

Categorias de tarefa do Kaspersky Embedded Systems Security

A Proteção do Computador em Tempo Real, o Controle do Computador, a Verificação por Demanda e as funções de Atualização no Kaspersky Embedded Systems Security são implementadas como tarefas.

Você pode gerenciar tarefas usando o menu de contexto da tarefa na árvore do Console do Aplicativo, na barra de ferramentas e na barra de acesso rápido. Você pode exibir informações de status de tarefa no painel de detalhes. As operações de gerenciamento da tarefa são gravadas no log de auditoria do sistema.

Há dois tipos de tarefas do Kaspersky Embedded Systems Security: *local* e *grupo*.

Tarefas locais

As tarefas locais são executadas somente no computador protegido para o qual elas são criadas. Dependendo do método de início, há os seguintes tipos de tarefas locais:

- **Tarefas locais do sistema**. Criadas automaticamente durante a instalação do Kaspersky Embedded Systems Security. Você pode editar as configurações de todas as tarefas do sistema, exceto as tarefas de Verificação da Quarentena e Reversão da Atualização do Banco de Dados. As tarefas do sistema não podem ser renomeadas ou excluídas. Você pode executar as tarefas de Verificação por Demanda do sistema e personalizadas simultaneamente.
- **Tarefas locais personalizadas**. No Console do Aplicativo, você pode criar tarefas de Verificação por Demanda. No Kaspersky Security Center, você pode criar tarefas de Verificação por Demanda, Atualização do Banco de Dados, Reversão da Atualização do Banco de Dados e Copiar Atualizações. Essas tarefas são chamadas tarefas personalizadas. As tarefas personalizadas podem ser renomeadas, configuradas e excluídas. É possível executar várias tarefas personalizadas simultaneamente.

Tarefas de grupo

As tarefas de grupo e as tarefas para conjuntos de computadores criadas usando o Kaspersky Security Center são exibidas no Console do Aplicativo. Estas tarefas são chamadas tarefas de grupo. Elas podem ser gerenciadas e configuradas no Kaspersky Security Center. No Console do Aplicativo, você pode visualizar somente o status de tarefas de grupo.

Como salvar uma tarefa depois de alterar suas configurações

As configurações de uma tarefa em execução ou interrompida (pausada) podem ser modificadas. As novas

configurações entram em vigor nas seguintes condições:

- Se você modificou as configurações de uma tarefa em execução, as novas configurações serão aplicadas imediatamente após salvar a tarefa.
- Se você se alterou as configurações de uma tarefa interrompida (pausada), as novas configurações serão aplicadas quando a tarefa for reiniciada.

► *Para salvar configurações de tarefas modificadas,*

no menu de contexto do nome da tarefa, selecione **Salvar tarefa**.

Se, após alterar as configurações da tarefa, outro nó for selecionado na árvore do Console do Aplicativo sem selecionar primeiramente o comando **Salvar tarefa**, a janela para salvar as configurações será exibida.

► *Para salvar as configurações modificadas ao alternar para outro nó do Console do Aplicativo,*

clique em **Sim** na janela Salvar configurações.

Executando / pausando / reiniciando / interrompendo tarefas manualmente

Você pode fazer uma pausa e reiniciar somente as tarefas de Proteção do Computador em Tempo Real e de Verificação por Demanda.

► *Para iniciar/pausar/reiniciar/interromper uma tarefa, siga as etapas a seguir:*

1. Abrir o menu de contexto da tarefa no Console do Aplicativo.
2. Selecione uma das seguintes opções: **Iniciar**, **Pausar**, **Reiniciar** ou **Interromper**.

A operação é executada e registrada no log de auditoria do sistema (na página 202).

Quando a tarefa de Verificação por Demanda é retomada, o Kaspersky Embedded Systems Security continua com o objeto estava sendo verificado quando a tarefa foi pausada.

Gerenciando programações de tarefas

Você pode configurar a programação de inicialização para tarefas do Kaspersky Embedded Systems Security e definir as configurações para executar tarefas pela programação.

Nesta seção

Definição das configurações da programação de inicialização da tarefa 151
Ativando e desativando tarefas programadas 152

Definição das configurações da programação de inicialização da tarefa

É possível configurar a programação de inicialização de tarefas locais do sistema e tarefas personalizadas no Console do Aplicativo. Você não pode definir a programação de inicialização para tarefas de grupo.

► *Para configurar a programação de inicialização da tarefa:*

1. Abra o menu de contexto da tarefa para a qual você deseja configurar a programação de inicialização.
2. Selecione **Propriedades**.

   A janela **Configurações de tarefa** é exibida.
3. Na janela exibida, na guia **Agendar**, marque a caixa de seleção **Executar de acordo com o agendamento**.
4. Configure a programação de acordo com suas necessidades. Para isso, execute as seguintes ações:
   a. Em **Frequência**, selecione um dos seguintes valores:
      - **De hora em hora**, se desejar que a tarefa seja executada nos intervalos de um número especificado de horas; especifique o número de horas no campo **A cada <número> hora(s)**.
      - **Diariamente**, se desejar que a tarefa seja executada nos intervalos de um número especificado de dias; especifique o número de dias no campo **A cada <número> dia(s)**.
      - **Semanalmente**, se desejar que a tarefa seja executada nos intervalos de um número especificado de semanas; especifique o número de semanas no campo **A cada <número> semana(s) em**. Especifique os dias da semana em que a tarefa será iniciada (por padrão, a tarefa é executada nas segundas-feiras).
      - **Ao iniciar o aplicativo**, se deseja que a tarefa seja executada a cada vez que iniciar o Kaspersky Embedded Systems Security.
      - **Após a atualização do banco de dados do aplicativo**, se desejar que a tarefa seja executada após cada atualização do banco de dados do aplicativo.

   b. Especifique a hora para a primeira inicialização da tarefa no campo **Hora inicial**.

   c. No campo **Data inicial**, especifique a data a partir da qual a programação se aplica.

   Após ter especificado a frequência de início da tarefa, a hora da primeira execução, a data a partir da qual se aplica a programação e informações sobre a hora estimada para a próxima execução da tarefa são exibidas na parte superior da janela, no campo **Próxima execução**. Informações atualizadas sobre a hora estimada da próxima execução da tarefa serão exibidas sempre que você abrir a janela **Configurações de tarefa** da guia **Agendar**.
   Bloqueado pela política será exibido no campo **Próxima execução** se as tarefas de inicialização do sistema em uma programação estiverem definidas nas configurações de política do Kaspersky Security Center.
5. Use a guia **Avançado** para definir as configurações de programação a seguir de acordo com os seus requisitos.
   - Na seção **Configurações de interrupção de tarefa**:
     a. Marque a caixa de seleção **Duração** e insira o número de horas e minutos necessários nos campos à direita para especificar a duração máxima da execução da tarefa.
     b. Marque a caixa de seleção **Pausar de** e insira os valores iniciais e finais do intervalo de tempo nos campos à direita para especificar o intervalo de tempo menor que 24 horas durante o qual a

execução da tarefa será pausada.

- Na seção **Configurações avançadas**:
  a. Marque a caixa de seleção **Cancelar agendamento a partir de** e especifique a data a partir da qual a programação será interrompida.
  b. Marque a caixa de seleção **Executar tarefas ignoradas** para ativar a inicialização de tarefas ignoradas.
  c. Marque a caixa de seleção **Aleatorizar o início da tarefa dentro do intervalo de** e especifique um valor em minutos.

6. Clique em **OK**.

As definições de inicialização de tarefa configuradas serão salvas.

Ativando e desativando tarefas programadas

Você pode ativar e desativar tarefas programadas antes ou após a definição das configurações de programação.

► *Para ativar ou desativar a programação de inicialização da tarefa, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto no nome de tarefa para a qual deseja configurar a programação de inicialização.
2. Selecione **Propriedades**.

   A janela **Configurações de tarefa** é exibida.
3. Na janela exibida na guia Programação, faça uma das ações a seguir:
   - Marque a caixa de seleção **Executar de acordo com a programação** se desejar ativar o início da tarefa programada.
   - Desmarque a caixa de seleção **Executar de acordo com a programação** se desejar desativar o início da tarefa programada.

   > As definições de programação de inicialização da tarefa configuradas não são excluídas e serão aplicadas no próximo início programado da tarefa.
4. Clique em **OK**.

As definições de programação de inicialização da tarefa configuradas são salvas.

Uso de contas de usuário para iniciar tarefas

É possível iniciar tarefas na conta do sistema ou especificar uma conta diferente.

Nesta seção

Sobre como usar contas para iniciar tarefas 153
Especificação de uma conta de usuário para iniciar uma tarefa 153

Sobre como usar contas para iniciar tarefas

Você pode especificar a conta sob a qual deseja executar a tarefa selecionada para os seguintes componentes funcionais do Kaspersky Embedded Systems Security:

- Tarefas do Gerador de Regras de Controle de Inicialização de Aplicativos e do Gerador de Regras de Controle de Dispositivos
- Tarefa de Verificação por Demanda
- Tarefas de atualização

Por padrão, essas tarefas são executadas usando as permissões de conta do sistema.

Uma conta diferente com as permissões de acesso apropriadas é recomendada nos seguintes casos:

- Na tarefa de Atualização, se você especificou uma pasta pública em outro computador na rede como fonte de atualização.
- Na tarefa de Atualização, se um servidor proxy com a autenticação NTLM incluída no Windows for utilizado para acessar a fonte de atualização.
- Em tarefas de Verificação por Demanda, se a conta do sistema não tiver as permissões para acessar qualquer um dos objetos verificados (por exemplo, aos arquivos nas pastas compartilhadas no computador).
- Na tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos, se após a conclusão da tarefa as regras geradas forem exportadas para um arquivo de configuração localizado em um caminho que a conta do sistema não possa acessar (por exemplo, em uma das pastas compartilhadas no computador).

Você pode executar as tarefas de Atualização, de Verificação por Demanda e do Gerador de Regras com permissões de conta do sistema. Durante a execução destas tarefas, o Kaspersky Embedded Systems Security acessa pastas compartilhadas em outro computador na rede se este computador estiver registrado no mesmo domínio que o computador protegido. Neste caso, a conta do sistema deve possuir permissões de acesso para estas pastas. O Kaspersky Embedded Systems Security acessará o computador usando permissões da conta **<nome do domínio \ computer_name>**.

Especificação de uma conta de usuário para iniciar uma tarefa

► *Para especificar uma conta para iniciar uma tarefa, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto da tarefa para a qual deseja configurar a inicialização com permissões de conta.
2. Selecione **Propriedades**.

   A janela **Configurações de tarefa** é exibida.
3. Na janela exibida, faça o seguinte na guia **Executar como**:
   a. Selecione **Nome de usuário**.
   b. Insira o nome de usuário e a senha para a conta que você deseja usar.

O usuário selecionado deve estar registrado no computador protegido ou no mesmo domínio que esse computador.

c. Confirme a senha inserida.

4. Clique em **OK**.

As configurações modificadas para executar a tarefa com as permissões de conta de usuário são salvas.

Configurações de importação e exportação

Essa seção fornece informações sobre como exportar as configurações do Kaspersky Embedded Systems Security ou as configurações de componentes específicos do software para um arquivo de configuração em formato XML e como importar essas configurações desse arquivo de configuração de volta ao aplicativo.

Nesta seção

Sobre a importação e exportação de configurações 154
Exportando configurações 155
Importando configurações 156

Sobre a importação e exportação de configurações

Você pode exportar as configurações do Kaspersky Embedded Systems Security para um arquivo de configuração XML e importar configurações para o Kaspersky Embedded Systems Security a partir do arquivo de configuração. É possível salvar todas as configurações do aplicativo ou apenas aquelas de componentes individuais como um arquivo de configuração.

Quando você exporta todas as configurações do Kaspersky Embedded Systems Security a um arquivo, as configurações gerais do aplicativo e as configurações dos seguintes componentes e funções do Kaspersky Embedded Systems Security são salvas:

- Proteção de Arquivos em Tempo Real
- Uso da KSN
- Controle de Dispositivos
- Controle de Inicialização de Aplicativos
- Gerador de Regras de Controle de Dispositivos
- Gerador de Regras de Controle de Inicialização de Aplicativos
- Tarefas de Verificação por Demanda
- Monitor de Integridade de Arquivos
- Inspetor do Log
- Atualização do banco de dados e dos módulos de software do Kaspersky Embedded Systems Security
- Quarentena

- Backup
- Logs
- Notificações do administrador e dos usuários
- Zona Confiável
- Prevenção de Exploits
- Proteção de senha

Além disso, você pode salvar as configurações gerais do Kaspersky Embedded Systems Security no arquivo, bem como os direitos das contas de usuário.

Não é possível exportar as configurações de tarefas de grupo.

O Kaspersky Embedded Systems Security exporta todas as senhas usadas pelo aplicativo, por exemplo, dados de conta para executar tarefas ou conectar-se a um servidor proxy. As senhas exportadas são salvas na forma criptografada do arquivo de configuração. Você pode importar senhas somente usando o Kaspersky Embedded Systems Security instalado neste computador se ele não tiver sido reinstalado ou atualizado.

Você não pode importar a utilização de senhas anteriormente salvas no Kaspersky Embedded Systems Security instalado em um computador diferente. Depois que as configurações tiverem sido importadas para outro computador, todas as senhas deverão ser inseridas manualmente.

Se uma política do Kaspersky Security Center estiver ativa no momento da exportação, o aplicativo exportará os valores especificados usados por essa política.

É possível importar as configurações de um arquivo de configuração que contém parâmetros de componentes individuais do Kaspersky Embedded Systems Security (por exemplo, de um arquivo criado no Kaspersky Embedded Systems Security instalado com um conjunto incompleto de componentes). Depois que as configurações são importadas, somente estas configurações do Kaspersky Embedded Systems Security que estavam contidas no arquivo de configuração serão alteradas. Todas as outras configurações permanecem iguais.

As configurações de uma política ativa do Kaspersky Security Center que tenham sido bloqueadas não são alteradas ao importar as configurações.

Exportando configurações

► *Para exportar configurações para um arquivo de configuração:, siga as etapas a seguir*

1. Na árvore do Console do Aplicativo, execute uma das seguintes ações:
   - No menu de contexto do nó **Kaspersky Embedded Systems Security**, selecione **Exportar configurações** para exportar todas as configurações do Kaspersky Embedded Systems Security.
   - No menu de contexto da tarefa cujas configurações você deseja exportar, selecione **Exportar configurações** para exportar as configurações de um componente funcional individual do aplicativo.
   - Para exportar as configurações do componente da Zona Confiável:
     a. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Kaspersky Embedded Systems Security**.
     b. Selecione **Configurar a Zona Confiável**.

A janela **Zona Confiável** é aberta.

c. Clique no botão **Exportar**.

A janela de boas-vindas do Assistente de exportação de configurações é aberta.

2. Siga as instruções do **Assistente**: especifique o nome do arquivo de configuração para salvar configurações e o caminho para ele.

As variáveis do ambiente do sistema podem ser usadas ao especificar o caminho; não são permitidas variáveis do ambiente do usuário.

Se uma política do Kaspersky Security Center estiver ativa no momento da exportação, o aplicativo exportará os valores das configurações usados por essa política.

3. Clique no botão **Fechar** na janela **Exportação de configurações do aplicativo concluída**.

As configurações exportadas são salvas quando o assistente fecha.

Importando configurações

► *Para importar configurações de um arquivo de configuração salvo, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, execute uma das seguintes ações:
   - No menu de contexto do nó **Kaspersky Embedded Systems Security**, selecione **Importar configurações** para importar todas as configurações do Kaspersky Embedded Systems Security.
   - No menu de contexto da tarefa cujas configurações você deseja importar, selecione **Importar configurações** para importar as configurações de um componente funcional individual do aplicativo.
   - Para importar as configurações do componente da Zona Confiável:
     a. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Kaspersky Embedded Systems Security**.
     b. Selecione **Configurar a Zona Confiável**.

     A janela **Zona Confiável** é aberta.

     c. Clique no botão **Importar**.

     A janela de boas-vindas do Assistente de importação de configurações é aberta.
2. Siga as instruções do Assistente: especifique o arquivo de configuração a partir do qual você deseja importar as configurações.

Depois de ter importado as configurações gerais do Kaspersky Embedded Systems Security ou de seus componentes funcionais no computador, você não poderá retornar para os valores das configurações anteriores.

3. Clique no botão **Fechar** na janela **Importação de configurações do aplicativo concluída**.

   As configurações importadas são salvas quando o assistente fecha.
4. Na barra de ferramentas do Console do Aplicativo, clique no botão **Atualizar**.

As configurações importadas são exibidas na janela do Console do Aplicativo.

O Kaspersky Embedded Systems Security não importa senhas (dados das contas para iniciar tarefas ou estabelecer a conexão com o servidor proxy) do arquivo criado em outro computador ou no mesmo computador depois que o Kaspersky Embedded Systems Security tiver sido reinstalado ou atualizado nele. Após a conclusão da operação de importação, as senhas deverão ser inseridas manualmente.

Usando os modelos de configurações de segurança

Esta seção contém informações sobre a utilização de modelos de configurações de segurança em tarefas de proteção e verificação do Kaspersky Embedded Systems Security.

Nesta seção

Sobre os modelos de configurações de segurança 157
Criação de um modelo de configurações de segurança 157
Exibindo configurações de segurança em um modelo 158
Aplicação de um modelo de configurações de segurança 158
Exclusão de um modelo de configurações de segurança 159

Sobre os modelos de configurações de segurança

É possível definir manualmente as configurações de segurança de um nó na árvore ou em uma lista dos recursos de arquivos de computador e salvar os valores das configurações definidas como um modelo. Esse modelo pode então ser usado para definir as configurações de segurança de outros nós nas tarefas de proteção e de verificação do Kaspersky Embedded Systems Security.

Os modelos podem ser usados para definir as configurações de segurança das seguintes tarefas do Kaspersky Embedded Systems Security:

- Proteção de Arquivos em Tempo Real
- Verificação na Inicialização do Sistema Operacional
- Verificação de Áreas Críticas
- Tarefas de Verificação por Demanda

As configurações de segurança de um modelo aplicadas a um nó pai na árvore de recursos de arquivos do computador são aplicadas a todos os nós filhos. Um modelo do nó pai não é aplicado aos nós filhos nos seguintes casos:

- Se as configurações de segurança dos nós filhos foram definidas separadamente (consulte a seção "Aplicação de um modelo de configurações de segurança" na página 158).
- Se os nós filhos forem virtuais. Você deve aplicar o modelo a cada nó virtual separadamente.

Criação de um modelo de configurações de segurança

► *Para salvar manualmente as configurações de segurança de um nó e salvar aquelas configurações*

em um modelo:

1. Na árvore do Console do Aplicativo, selecione a tarefa para a qual deseja aplicar o modelo de configurações de segurança.
2. No painel de detalhes da tarefa selecionada, clique no link **Configurar o escopo da proteção** ou **Configurar o escopo da verificação**.
3. Na árvore ou na lista dos recursos de arquivos de rede do computador, selecione o modelo que deseja exibir.
4. Na guia **Nível de segurança**, clique no botão **Salvar como modelo**.

   A janela **Propriedades do modelo** é exibida.
5. No campo **Nome do modelo**, digite o nome do modelo.
6. Insira informações adicionais do modelo no campo **Descrição**.
7. Clique em **OK**.

O modelo com o conjunto de configurações de segurança é salvo.

Exibindo configurações de segurança em um modelo

► *Para exibir configurações de segurança em um modelo que criou, execute as seguintes ações:*

1. Na árvore do Console do Aplicativo, selecione a tarefa para a qual deseja visualizar o modelo de segurança.
2. No menu de contexto da tarefa selecionada, selecione **Modelos de configurações**.

   A janela **Modelos** é exibida.
3. Na lista de modelos na janela exibida, selecione o modelo que deseja visualizar.
4. Clique no botão **Exibir**.

A janela **<Nome do modelo>** é exibida. A guia **Geral** exibe o nome e as informações adicionais do modelo; a guia **Opções** lista as configurações de segurança salvas no modelo.

Aplicação de um modelo de configurações de segurança

► *Para aplicar configurações de segurança de um modelo para um nó selecionado:*

1. Na árvore do Console do Aplicativo, selecione a tarefa para a qual deseja aplicar o modelo de configurações de segurança.
2. No painel de detalhes da tarefa selecionada, clique no link **Configurar o escopo da proteção** ou **Configurar o escopo da verificação**.
3. Na árvore ou lista de recursos de arquivos de rede do computador, abra o menu de contexto do nó ou item ao qual deseja aplicar o modelo.
4. Selecione **Aplicar modelo** → **<Nome do modelo>**.
5. Clique no botão **Salvar**.

O modelo de configurações de segurança é aplicado ao nó selecionado na árvore de recursos de arquivo do computador. A guia **Nível de segurança** do nó selecionado agora tem o valor **Personalizado**.

As configurações de segurança de um modelo aplicadas a um nó pai na árvore de recursos de arquivos do computador são aplicadas a todos os nós filhos.

Se o escopo da proteção ou o escopo da verificação dos nós filhos na árvore de recursos de arquivos do computador foi configurado separadamente, as configurações de segurança do modelo aplicadas ao nó pai não serão aplicadas automaticamente a esses nós filhos.

► *Para aplicar as configurações de segurança de um modelo para todos os nós selecionados, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, selecione a tarefa para a qual deseja aplicar o modelo de configurações de segurança.
2. No painel de detalhes da tarefa selecionada, clique no link **Configurar o escopo da proteção** ou **Configurar o escopo da verificação**.
3. Na árvore ou na lista de recursos de arquivos de rede do computador, selecione um nó pai para aplicar o modelo ao nó selecionado e a todos os nós filhos.
4. No menu de contexto, selecione **Aplicar modelo** → **<Nome do modelo>**.
5. Clique no botão **Salvar**.

O modelo de configurações de segurança é aplicado ao nó pai e a todos os nós filhos na árvore de recursos de arquivos do computador. A guia **Nível de segurança** do nó selecionado agora tem o valor **Personalizado**.

Exclusão de um modelo de configurações de segurança

► *Para excluir um modelo de configurações de segurança, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, selecione a tarefa para a qual não deseja mais usar um modelo de configurações de segurança para a configuração.
2. No menu de contexto da tarefa selecionada, selecione **Modelos de configurações**.

   Você pode visualizar modelos de configurações para tarefas de Verificação por Demanda a partir do painel de detalhes do nó pai **Verificação por Demanda**.

   A janela **Modelos** é exibida.
3. Na lista de modelos na janela exibida, selecione o modelo que você deseja excluir.
4. Clique no botão **Remover**.

   Uma janela é exibida para confirmar a exclusão.
5. Na janela exibida, clique em **Sim**.

O modelo selecionado é excluído.

Se o modelo de configurações de segurança tiver sido aplicado para proteger ou verificar nós de recursos de arquivos do computador, as configurações de segurança definidas para esses nós são conservadas após o modelo ser excluído.

Visualizando o status de proteção e as informações do Kaspersky Embedded Systems Security

► *Para visualizar informações sobre o status de proteção do computador do Kaspersky Embedded Systems Security,*

selecione o nó **Kaspersky Embedded Systems Security** na árvore do Console do Aplicativo.

Por padrão, as informações no painel de detalhes do Console do Aplicativo são atualizadas automaticamente:

- A cada 10 segundos, no caso de uma conexão local;
- A cada 15 segundos, no caso de uma conexão remota.

Você pode atualizar as informações manualmente.

► *Para atualizar as informações no nó **Kaspersky Embedded Systems Security** manualmente,*

selecione o comando **Atualizar** no menu de contexto do nó do **Kaspersky Embedded Systems Security**.

As seguintes informações do aplicativo são exibidas no painel de detalhes do Console do Aplicativo:

- Status de uso da Kaspersky Security Network.
- Status de proteção do computador.
- Informações sobre as atualizações do banco de dados e do módulo do aplicativo.
- Dados de diagnóstico reais.
- Dados sobre as tarefas de controle do computador.
- Informações da licença.
- Status da integração com o Kaspersky Security Center: os detalhes do computador com o Kaspersky Security Center instalado e ao qual o aplicativo está conectado; as informações sobre as tarefas do aplicativo controladas pela política ativa.

As cores diferentes são usadas para indicar o status de proteção:

- *Verde*. A tarefa está sendo executada de acordo com as configurações definidas. A proteção está ativa.
- *Amarelo*. A tarefa não foi iniciada, está em pausa ou foi interrompida. Podem ocorrer ameaças de segurança. Aconselha-se a configuração e inicialização da tarefa.
- *Vermelho*. Tarefa concluída com um erro ou uma ameaça de segurança foi detectada enquanto a tarefa estava sendo executada. Aconselha-se iniciar a tarefa ou tomar medidas para eliminar a ameaça de segurança detectada.

Alguns detalhes neste bloco (por exemplo, nomes de tarefa ou o número de ameaças detectadas) são links que, quando clicados, o levam ao nó da tarefa relevante ou abrem o log de tarefas.

A seção **Uso da Kaspersky Security Network** exibe o status de tarefa atual, por exemplo, *Executando*, *Interrompida* ou *Nunca foi executada*. O indicador pode ter os seguintes valores:

- A cor verde indica que a tarefa de Uso da KSN está em execução e as solicitações de arquivo para status

estão sendo enviadas à KSN.

- A cor amarela indica que uma das Declarações foi aceita, mas a tarefa não está em execução; ou a tarefa está em execução, mas as solicitações de arquivo não estão sendo enviadas à KSN.

Proteção do **computador**

A seção **Proteção do Computador** (consulte a tabela abaixo) exibe informações sobre o status de proteção atual do computador.

Tabela 27. Informações sobre o status de proteção do computador

Seção de Proteção	Informações
Indicador de status de proteção do computador	A cor do painel com o nome da seção reflete o status das tarefas sendo executadas na seção. O indicador pode ter os seguintes valores: • Verde – Esta cor é exibida por padrão e significa que o componente de Proteção de Arquivos em Tempo Real está instalado e a tarefa está em execução. • Amarelo – O componente de Proteção de Arquivos em Tempo Real não está instalado, e a tarefa de Verificação de Áreas Críticas. não é executada há muito tempo. • Vermelho – a tarefa de Proteção de Arquivos em Tempo Real não está em execução.
Proteção de Arquivos em Tempo Real	**Status da tarefa** – Status atual da tarefa, por exemplo, *Executando* ou *Interrompida*. **Detectado** – Número total de objetos detectados pelo Kaspersky Embedded Systems Security. Por exemplo, se o Kaspersky Embedded Systems Security detectar um malware em cinco arquivos, o valor desse campo aumentará em um. Se o número de malwares detectados exceder 0, o valor será realçado em vermelho.
Verificação de Áreas Críticas	**Data da última verificação** – Data e hora da última Verificação de Áreas Críticas para vírus e outras ameaças de segurança do computador. *Nunca foi executada* – Um evento que ocorre quando a tarefa de Verificação de Áreas Críticas não foi executada nos últimos 30 dias ou mais (valor padrão). Você pode alterar o limite para gerar esse evento.
Prevenção de Exploits	**Status** – o status atual de técnicas de prevenção de exploits, por exemplo, *Aplicada* ou *Não Aplicada*. **Modo de prevenção** - um dos dois modos disponíveis, selecionado durante a configuração da proteção da memória do processo: • Encerrar no exploit. • Somente estatísticas. **Processos protegidos** – o número total de processos adicionados ao escopo da proteção e tratado conforme o modo selecionado.
Objetos do backup	*Limite de espaço disponível no backup excedido* – Este evento ocorre quando o limite de espaço disponível no Backup está se aproximando do limite especificado. O Kaspersky Embedded Systems Security continua a mover objetos para o Backup. Nesse caso, o valor no campo **Espaço usado** é realçado em amarelo. *Tamanho máximo do Backup excedido* – Este evento ocorre quando o tamanho do Backup alcança o limite especificado. O Kaspersky Embedded Systems Security continua a mover objetos para o Backup. Nesse caso, o valor no campo **Espaço usado** é realçado em vermelho. **Objetos do backup** - o número de objetos atualmente no Backup. **Espaço usado** – volume de espaço usado no Backup.

Atualização

A seção **Atualização** (consulte a tabela abaixo) exibe informações sobre o quão atualizados estão os bancos de dados de antivírus e os módulos do aplicativo.

Tabela 28. Informações sobre o status dos bancos de dados e módulos do Kaspersky Embedded Systems Security

Seção Atualizações	Informações
Indicador de status para bancos de dados e de módulos de software	A cor do painel com o nome da seção reflete o status dos bancos de dados e módulos do aplicativo. O indicador pode ter os seguintes valores: • Verde – Esta cor é exibida por padrão e significa que o banco de dados do aplicativo está atualizado e que a última tarefa de atualização do banco de dados foi concluída com sucesso. • Amarelo – Os bancos de dados estão desatualizados ou a última tarefa de Atualização do Banco de Dados apresentou falha. • Vermelho – o evento *Os bancos de dados do aplicativo estão muito desatualizados* ou *Bancos de dados do aplicativo estão corrompidos* ocorreu.
Atualização do banco de dados e **Atualização de módulos de software**	**Status do banco de dados** – Uma avaliação do status de atualização do banco de dados. Ele pode ter os seguintes valores: • **O banco de dados do aplicativo está atualizado** - os bancos de dados do aplicativo foram atualizados há não mais que 7 dias (padrão). • **O banco de dados do aplicativo está desatualizado** – Os bancos de dados do aplicativo foram atualizados entre 7 e 14 dias atrás (padrão). • **O banco de dados do aplicativo está muito desatualizado** – Os bancos de dados do aplicativo foram atualizados há mais de 14 dias (padrão). Você pode alterar os limites para gerar os eventos *Os bancos de dados do aplicativo estão desatualizados* e *Os bancos de dados do aplicativo estão obsoletos.* **Data da versão do banco de dados do aplicativo** – a data e hora do lançamento da última atualização do banco de dados. A data e hora são especificadas em formato UTC. **Status da última tarefa de Atualização do banco de dados concluída** – data e hora da última atualização do banco de dados. A data e hora são especificadas de acordo com a hora local do computador protegido. O campo fica vermelho se o evento *Falhou* ocorreu. **Número de atualizações de módulo disponíveis** – o número de atualizações do módulo do Kaspersky Embedded Systems Security disponível para ser baixado e instalado. **Número de atualizações de módulo instaladas** – o número de atualizações do módulo do Kaspersky Embedded Systems Security instaladas.

Controle

A seção **Controle** (consulte a tabela abaixo) exibe informações sobre as tarefas de Controle de Inicialização de Aplicativos, Controle de Dispositivos e Gerenciamento de Firewall.

Tabela 29. Informações sobre o status do Controle do computador

Seção Controle	Informações
Indicador de status de Controle do computador	A cor do painel com o nome da seção reflete o status das tarefas sendo executadas na seção. O indicador pode ter os seguintes valores: • Verde – Esta cor é exibida por padrão e significa que o componente Controle de Inicialização de Aplicativos está instalado e a tarefa está em execução no modo **Ativa**. • Amarelo – o Controle de Inicialização de Aplicativos está em execução no modo **Somente estatísticas**. • Vermelho – a tarefa de Controle de Inicialização de Aplicativos não está em execução ou apresentou falha.
Controle de Inicialização de Aplicativos	**Status da tarefa** – Status atual da tarefa, por exemplo, *Executando* ou *Interrompida*. **Modo** - Um dos dois modos disponíveis para a tarefa de Controle de Inicialização de Aplicativos: • Ativa • Somente estatísticas **Inicializações de aplicativos negadas** – Número de tentativas de iniciar aplicativos bloqueados pelo Kaspersky Embedded Systems Security durante a tarefa de Controle de Inicialização de Aplicativos. Se o número de inicializações de aplicativo bloqueadas exceder 0, o campo ficará vermelho. **Tempo médio de processamento (ms)** – Tempo que levou para o Kaspersky Embedded Systems Security processar uma tentativa de iniciar aplicativos no computador protegido.
Controle de Dispositivos	**Status da tarefa** - Status atual da tarefa, por exemplo, *Executando* ou *Interrompida*. **Modo** – Um dos dois modos disponíveis para a tarefa Controle de Dispositivos: • **Ativa** • **Somente estatísticas** **Dispositivos bloqueados** – Número de tentativas de conectar um dispositivo de armazenamento em massa bloqueado pelo Kaspersky Embedded Systems Security durante a tarefa Controle de Dispositivos. Se o número de dispositivos de armazenamento em massa bloqueados exceder 0, o campo ficará vermelho.
Gerenciamento de Firewall	**Status da tarefa** – Status atual da tarefa, por exemplo, *Executando* ou *Interrompida*. **Tentativas de conexões bloqueadas** - Número de conexões a um dispositivo protegido bloqueadas pelas regras de firewall especificadas.

Diagnósticos

A seção **Diagnósticos** (consulte a tabela abaixo) exibe informações sobre as tarefas Monitor de Integridade de Arquivos e Inspeção de Log.

Tabela 30. Informação sobre o status de Inspeção do sistema

Seção Diagnósticos	Informações
Indicador de status de diagnóstico	A cor do painel com o nome da seção reflete o status das tarefas sendo executadas na seção. O indicador pode ter os seguintes valores: • Verde – Esta cor é exibida por padrão e significa que um ou ambos os componentes de inspeção de sistema estão instalados e as tarefas estão em execução. • Amarelo – Ambos os componentes estão instalados, mas uma das tarefas de inspeção do sistema não está em execução; ocorreu o evento *Não está em execução*. • Vermelho – Uma das tarefas falhou.
Monitor de Integridade de Arquivos	**Status da tarefa** – Status atual da tarefa, por exemplo, *Executando* ou *Interrompida*. **Operações de arquivos não sancionadas** – Número de modificações de arquivos dentro do escopo de monitoramento. Essas modificações podem indicar que a segurança de um computador protegido foi violada.
Inspeção de Log	**Status da tarefa** – Status atual da tarefa, por exemplo, *Executando* ou *Interrompida*. **Possíveis violações** – Número de violações registradas com base em dados do Log de Eventos do Windows. Este número é determinado com base nas regras de tarefa especificadas ou usando o analisador heurístico.

As informações sobre a licença do Kaspersky Embedded Systems Security são exibidas na linha no canto inferior esquerdo no painel de detalhes do nó do **Kaspersky Embedded Systems Security**.

Você pode configurar as propriedades do Kaspersky Embedded Systems Security seguindo o link Propriedades do aplicativo (consulte a seção "Configurações do Kaspersky Embedded Systems Security no Console do Aplicativo" na página 136).

Você pode se conectar a um computador diferente seguindo o link **Conectar a outro computador** (consulte a seção "Gerenciando o Kaspersky Embedded Systems Security por meio do Console do Aplicativo em outro computador" na página 148).

Interface de diagnóstico compacta

Esta seção descreve como usar a Interface de diagnóstico compacta para revisar o status do computador ou a atividade atual, e como configurar a escrita de arquivos de despejo e rastreamento.

Neste capítulo

Sobre a interface de diagnóstico compacta 166

Revisão do status do Kaspersky Embedded Systems Security por meio da Interface de diagnóstico compacta 167

Revisando estatística de evento de segurança 168

Revisando a atividade atual do aplicativo 168

Configuração da escrita de arquivos de despejo e de rastreamento 169

Sobre a interface de diagnóstico compacta

O componente Interface de diagnóstico compacta (também referido como "CDI") é instalado e desinstalado junto com o componente Ícone da bandeja do sistema, independentemente do Console do Aplicativo, e pode ser usado quando o Console do Aplicativo não estiver instalado no computador protegido. O CDI é iniciado a partir do Ícone da Bandeja do Sistema ou executando o arquivo kavfsmui.exe a partir da pasta aplicativo no computador.

Da janela CDI, você pode fazer o seguinte:

- Revisar informações sobre o status geral do aplicativo (consulte a seção "Revisar o Kaspersky Embedded Systems Security por meio da Interface de diagnóstico compacta" na página 167).
- Revisar incidentes de segurança que ocorreram (consulte a seção "Revisando estatística de evento de segurança" na página 168).
- Revisar a atividade atual no computador protegido (consulte a seção "Revisão de atividade atual do aplicativo" na página 168).
- Iniciar ou interromper a escrita de arquivos de despejo e de rastreamento (consulte a seção "Configuração da escrita de arquivos de despejo e de rastreamento" na página 169).
- Abrir o Console do Aplicativo.
- Abra a janela **Sobre o aplicativo** com a lista de atualizações instaladas e patches disponíveis.

A CDI está disponível mesmo se o acesso às funções do Kaspersky Embedded Systems Security for protegido por senha. Nenhuma senha é necessária.

O componente CDI não pode ser configurado por meio do Kaspersky Security Center.

Revisão do status do Kaspersky Embedded Systems Security por meio da Interface de diagnóstico compacta

► *Para abrir a janela da Interface de diagnóstico compacta, execute as seguintes ações:*

1. Clique com o botão direito do mouse no ícone da bandeja do sistema do Kaspersky Embedded Systems Security na área de notificação de barra de ferramentas.
2. Selecione a opção **Abrir Interface de diagnóstico compacta**.

   A janela **Interface de diagnóstico compacta** é exibida.

Revise o status atual da chave, as tarefas de Proteção do Computador em Tempo Real e as tarefas de Atualização na guia **Status de proteção**. As cores diferentes são usadas para notificar o usuário sobre o status de proteção (ver a tabela abaixo).

Tabela 31. Status de proteção na Interface de diagnóstico compacta.

Seção	Status

Proteção do Computador em Tempo Real	O painel fica *verde* para qualquer um dos seguintes cenários (qualquer número de condições pode ser atendido):
	• Configuração recomendada:
	  • A tarefa de Proteção de Arquivos em Tempo Real é iniciada com as configurações padrão.
	  • A tarefa de Controle de Inicialização de Aplicativos é iniciada no modo **Ativa** com as configurações padrão.
	• Configuração aceitável:
	  • A tarefa de Proteção de Arquivos em Tempo Real é configurada pelo usuário.
	  • As configurações da tarefa de Controle de Inicialização de Aplicativos são modificadas.

	O painel fica *amarelo* se uma ou mais das seguintes condições forem atendidas: • A tarefa de Proteção de Arquivos em Tempo Real é pausada (pelo usuário ou programação). • A tarefa de Controle de Inicialização de Aplicativos é iniciada no modo **Somente estatísticas**. • Proteção de Exploits e o Controle de Inicialização de Aplicativos são iniciados no modo **Somente estatísticas**.
	O painel fica *vermelho* se as seguintes condições forem atendidas: • O componente de Proteção de Arquivos em Tempo Real não está instalado ou a tarefa é interrompida ou pausada. • O componente Controle de Inicialização de Aplicativos não está instalado ou a atarefa é iniciada no modo **Somente estatísticas**.
Licenciamento	O painel fica *verde* se a licença atual for válida.

	Um painel *amarelo* significa que um dos seguintes eventos ocorreu: • **Verificação do status da licença**. • **A licença expirará em 14 dias e nenhuma chave adicional ou código de ativação foram adicionados**. • **A chave adicionada foi colocada na lista negra e está prestes a ser bloqueada**.
	Um painel *vermelho* significa que um dos seguintes eventos ocorreu: • **Aplicativo não ativado.** • **Licença expirou.** • **O Contrato de Licença do Usuário Final foi violado.** • **A chave está na lista negra.**
Atualização	O painel fica *verde* quando o banco de dados do aplicativo é atualizado.
	O painel fica *amarelo* quando os bancos de dados do aplicativo estão desatualizados.
	O painel fica *vermelho* quando os bancos de dados do aplicativo estão muito desatualizados.

Revisando estatística de evento de segurança

A guia **Estatísticas** exibe todos os eventos de segurança. Cada estatística de tarefa de proteção é exibida em um bloco separado que especifica o número de incidentes, a data e a hora quando o último incidente ocorreu. Quando um incidente é registrado em log, a cor do bloco se altera para vermelho.

► *Para revisar as estatísticas:*

1. Clique com o botão direito do mouse no ícone da bandeja do sistema do Kaspersky Embedded Systems Security na área de notificação de barra de ferramentas.
2. Selecione a opção **Abrir Interface de diagnóstico compacta**.

   A janela **Interface de diagnóstico compacta** é exibida.
3. Abra a guia **Estatísticas**.
4. Revise os incidentes de segurança para as tarefas de proteção.

Revisando a atividade atual do aplicativo

Nesta guia, é possível revisar o status das tarefas atuais e os processos do aplicativo, e receber notificações prontamente sobre eventos críticos que venham a ocorrer.

As cores diferentes são usadas para indicar o status de atividade do aplicativo:

- Na seção **Tarefas**:
  - *Verde*. Nenhuma condição para amarelo ou vermelho.
  - *Amarelo*. As áreas críticas não são verificadas há muito tempo.

- *Vermelho*. Alguma das seguintes condições é verdadeira:
  - Nenhuma tarefa foi iniciada e uma programação de início não foi configurada para nenhuma tarefa.
  - Os erros de inicialização de aplicativos são registrados como eventos críticos.
- Na seção **Kaspersky Security Network**:
  - *Verde*. A tarefa de Uso da KSN é iniciada.
  - *Amarelo*. A Declaração da KSN é aceita, mas a tarefa não é iniciada.

► *Para revisar a atividade atual do aplicativo no computador:*

1. Clique com o botão direito do mouse no ícone da bandeja do sistema do Kaspersky Embedded Systems Security na área de notificação de barra de ferramentas.
2. Selecione a opção **Abrir Interface de diagnóstico compacta**.

   A janela **Interface de diagnóstico compacta** é exibida.
3. Abrir a guia **Atividade do aplicativo atual**.
4. Revise as seguintes informações na seção **Tarefas**:
   - **Áreas críticas não verificadas há muito tempo.**

     Este campo é exibido apenas se o aplicativo retornar um aviso correspondente sobre verificações de áreas críticas.
   - **Executando agora**
   - **Falha de execução**
   - **Próxima execução definida por uma programação**
5. Revise as seguintes informações na seção **Kaspersky Security Network**:
   - **A KSN está ativa. Os serviços de reputação de arquivos estão ativados** ou **A Proteção está desligada**.
   - **As estatísticas de aplicativo estão sendo enviadas para a KSN**.

     O aplicativo envia informações sobre malware, inclusive software fraudulento, detectado durante a execução das tarefas de Proteção de Arquivos em Tempo Real e de Verificação por Demanda, bem como informações de depuração sobre erros durante a verificação.

     O campo é exibido se a caixa de seleção **Enviar as estatísticas da Kaspersky Security Network** for selecionada nas configurações de tarefa de Uso da KSN.
6. Revise as seguintes informações na seção **Integração com o Kaspersky Security Center**:
   - O gerenciamento local é permitido.
   - A política é aplicada: <nome do servidor do Kaspersky Security Center>.

Configuração da escrita de arquivos de despejo e de rastreamento

Você pode configurar a escrita de arquivos de despejo e de rastreamento via a CDI.

Você também pode configurar o diagnóstico de mau funcionamento via o Console do Aplicativo (consulte a seção "Configurações do Kaspersky Embedded Systems Security no Console do Aplicativo" na página 136).

► *Para iniciar a escrita em arquivos de despejo e de rastreamento, execute as seguintes ações:*

1. Clique com o botão direito do mouse no ícone da bandeja do sistema do Kaspersky Embedded Systems Security na área de notificação de barra de ferramentas.
2. Selecione a opção **Abrir Interface de diagnóstico compacta**.

   A janela **Interface de diagnóstico compacta** é exibida.
3. Abra a guia **Solução de problemas**.
4. Altere as seguintes configurações de rastreamento, conforme necessário:
   a. Selecione a caixa **Gravar informações de depuração no arquivo de rastreamento nesta pasta**.
   b. Clique no botão **Procurar** para especificar a pasta em que o Kaspersky Embedded Systems Security salvará arquivos de rastreamento.

      O rastreamento será ativado para todos os componentes com os parâmetros padrão, usando o nível de **Depuração** do detalhe e o tamanho de log de máximo padrão de 50 MB.
5. Altere as seguintes configurações do arquivo de despejo, conforme necessário:
   a. Selecione a caixa **Criar arquivo de despejo sobre mau funcionamento nesta pasta**.
   b. Clique no botão **Procurar** para especificar a pasta em que o Kaspersky Embedded Systems Security salvará o arquivo de despejo.
6. Clique no botão **Aplicar**.

   Uma nova configuração será aplicada.

Atualização de bancos de dados e módulos de software do Kaspersky Embedded Systems Security

Essa seção fornece informações sobre as tarefas de atualização dos bancos de dados e dos módulos de software do Kaspersky Embedded Systems Security, a cópia de atualizações e a reversão de atualizações dos bancos de dados do Kaspersky Embedded Systems Security, bem como instruções sobre como configurar as tarefas de atualização dos bancos de dados e dos módulos de software.

Neste capítulo

Sobre as tarefas de atualização 171

Sobre a atualização de módulos de software do Kaspersky Embedded Systems Security 172

Sobre a Atualização do Banco de Dados do Kaspersky Embedded Systems Security 173

Esquemas para atualizar bancos de dados e módulos de aplicativos antivírus usados em uma organização 173

Configurando tarefas de atualização 177

Revertendo atualizações do banco de dados do Kaspersky Embedded Systems Security 183

Revertendo atualizações dos módulos do aplicativo 183

Estatísticas da tarefa de atualização 184

Sobre as tarefas de atualização

O Kaspersky Embedded Systems Security fornece quatro tarefas de atualização do sistema: a Atualização do Banco de Dados, a Atualização de módulos de software, Copiar atualizações e Reversão da atualização do banco de dados.

Por padrão, o Kaspersky Embedded Systems Security conecta-se à fonte de atualizações (um dos computadores de atualização da Kaspersky Lab) a cada hora. Você pode configurar todas as tarefas de Atualização (consulte a seção "Configurando tarefas de atualização" na página 177), exceto a tarefa de Reversão da Atualização do Banco de Dados. Quando as configurações da tarefa forem modificadas, o Kaspersky Embedded Systems Security aplicará os novos valores na próxima execução da tarefa.

Não é permitido fazer uma pausa e reiniciar as tarefas de atualização.

Atualização do Banco de Dados

O Kaspersky Embedded Systems Security copia bancos de dados a partir da fonte de atualização para o computador protegido e começa a usá-los imediatamente na tarefa de Proteção do Computador em Tempo Real em execução. As tarefas de Verificação por Demanda começam a usar o banco de dados atualizado na próxima execução.

Por padrão, o Kaspersky Embedded Systems Security executa a tarefa de Atualização do banco de dados de hora em hora.

Atualização de módulos de software

Por padrão, o Kaspersky Embedded Systems Security verifica a disponibilidade de atualizações dos módulos de software na fonte de atualização. Para começar a usar os módulos de software instalados, é necessário reiniciar o

computador e/ou o Kaspersky Embedded Systems Security.

Por padrão, o Kaspersky Embedded Systems Security executa a tarefa de Atualização de módulos de software semanalmente às sextas-feiras às 16h00 (hora de acordo com as configurações regionais do computador protegido). Durante a execução da tarefa, o aplicativo verifica a disponibilidade de atualizações importantes e programas de módulos do Kaspersky Embedded Systems Security sem distribuí-las.

Copiar atualizações

Por padrão, durante a execução da tarefa, o Kaspersky Embedded Systems Security faz o download dos arquivos da Atualização do banco de dados e os salva na rede especificada ou pasta local sem aplicá-los.

A tarefa Copiar atualizações está desativada por padrão.

Reversão da Atualização do Banco de Dados

Durante a execução da tarefa, o Kaspersky Embedded Systems Security volta a utilizar os bancos de dados com atualizações instaladas previamente.

A tarefa de Reversão da atualização do banco de dados está desativada por padrão.

Sobre a Atualização de módulos de software do Kaspersky Embedded Systems Security

A Kaspersky Lab pode publicar pacotes de atualização para módulos do Kaspersky Embedded Systems Security. Os pacotes de atualização podem ser *urgentes* (ou *críticos*) e planejados. Os pacotes de atualização críticos corrigem vulnerabilidades e erros; os pacotes planejados adicionam novos recursos ou aprimoram recursos existentes.

Os pacotes de atualização urgentes (críticos) são carregados nos servidores de atualização da Kaspersky Lab. A sua instalação automática pode ser configurada usando a tarefa de Atualização de módulos de software. Por padrão, o Kaspersky Embedded Systems Security executa a tarefa de Atualização de módulos de software semanalmente às sextas-feiras às 16h00 (hora de acordo com as configurações regionais do computador protegido).

A Kaspersky Lab não publica pacotes de atualizações planejados nos servidores de atualização para atualização automática; eles podem ser baixados no site da Kaspersky Lab. A tarefa de Atualização de módulos de software pode ser usada para receber informações sobre a versão de atualizações programadas do Kaspersky Embedded Systems Security.

As atualizações críticas podem ser atualizadas pela Internet para cada computador protegido ou um computador pode ser usado como intermediário, copiando todas as atualizações nele e depois distribuindo-as aos computadores da rede. Para copiar e salvar atualizações sem instalá-las, use a tarefa Copiar atualizações.

Antes que as atualizações dos módulos sejam instaladas, o Kaspersky Embedded Systems Security cria cópias de backup dos módulos instalados anteriormente. Se o processo de atualização de módulos de software for interrompido ou resultar em erro, o Kaspersky Embedded Systems Security retornará automaticamente ao uso dos módulos de software instalados anteriormente. Os módulos do software podem ser revertidos manualmente para as atualizações instaladas anteriormente.

Durante a instalação das atualizações baixadas, o Kaspersky Security Service é interrompido e reiniciado automaticamente.

Sobre a Atualização do Banco de Dados do Kaspersky Embedded Systems Security

Os bancos de dados do Kaspersky Embedded Systems Security armazenados no computador protegido ficam desatualizados rapidamente. Os analistas de vírus da Kaspersky Lab detectam novas ameaças diariamente, criam registros para identificá-las e trabalham para incluí-las nas atualizações do banco de dados do aplicativo. As atualizações do banco de dados são um arquivo ou um conjunto de arquivos contendo registros que identificam as ameaças descobertas no período desde a criação da última atualização. Para manter o nível de proteção do computador desejado, é recomendado que atualizações do banco de dados sejam recebidas periodicamente.

Por padrão, se os bancos de dados do Kaspersky Embedded Systems Security não forem atualizados dentro de uma semana do tempo no qual as atualizações do banco de dados instaladas foram criadas pela última vez, ocorrerá o evento *O banco de dados do aplicativo está desatualizado*. Se os bancos de dados não forem atualizados durante um período de duas semanas, ocorrerá o evento *O banco de dados do aplicativo está muito desatualizado*. As informações sobre o status atualizado dos bancos de dados (consulte a seção "Visualizando o status de proteção e as informações do Kaspersky Embedded Systems Security" na página 161) são exibidas no painel de detalhes do nó **Kaspersky Embedded Systems Security** da árvore do Console do Aplicativo. Você pode usar as configurações gerais do Kaspersky Embedded Systems Security para indicar um número diferente de dias antes que estes eventos ocorram. Você também pode configurar notificações de administrador sobre estes eventos (consulte a seção "Configurando notificações do administrador e dos usuários" na página 216).

O Kaspersky Embedded Systems Security baixa atualizações para os bancos de dados e módulos do aplicativo a partir de servidores de atualização FTP ou HTTP da Kaspersky Lab, do Servidor de Administração do Kaspersky Security Center ou de outras fontes de atualização.

As atualizações podem ser baixadas para cada computador protegido ou um computador pode ser usado como intermediário, copiando todas as atualizações nele e depois distribuindo-as para os computadores. Se você usar o Kaspersky Security Center para administração centralizada da proteção dos computadores em uma organização, você pode usar o Servidor de Administração do Kaspersky Security Center como intermediário para baixar atualizações.

As tarefas de Atualização do banco de dados podem ser iniciadas manualmente ou com base em uma programação (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 151). Por padrão, o Kaspersky Embedded Systems Security executa a tarefa de Atualização do banco de dados de hora em hora.

Se o processo de download da atualização for interrompido ou resultar em erro, o Kaspersky Embedded Systems Security retornará automaticamente ao uso dos bancos de dados com as atualizações instaladas anteriormente. Se os bancos de dados do Kaspersky Embedded Systems Security ficarem corrompidos, eles podem ser revertidos manualmente (consulte a seção "Revertendo atualizações do banco de dados do Kaspersky Embedded Systems Security" na página 183) a atualizações instaladas anteriormente.

Esquemas para atualizar bancos de dados e módulos de aplicativos antivírus usados em uma organização

A seleção da fonte de atualizações nas tarefas de atualização depende do esquema de atualização dos bancos de dados e módulos do programa usado na organização.

Os bancos de dados e módulos do Kaspersky Embedded Systems Security podem ser atualizados nos computadores protegidos usando os seguintes esquemas:

- Baixar as atualizações diretamente da Internet para cada computador protegido (Esquema 1).
- Baixar as atualizações da Internet para um computador intermediário e distribuí-las para computadores a

partir do computador.

Qualquer computador com os softwares listados a seguir instalados pode ser usado como computador intermediário:

- Kaspersky Embedded Systems Security (Esquema 2).
- Servidor de Administração do Kaspersky Security Center (Esquema 3).

Atualizar usando um computador intermediário não só permitirá a diminuição do tráfego da Internet, mas também garantirá a segurança adicional dos computadores da rede.

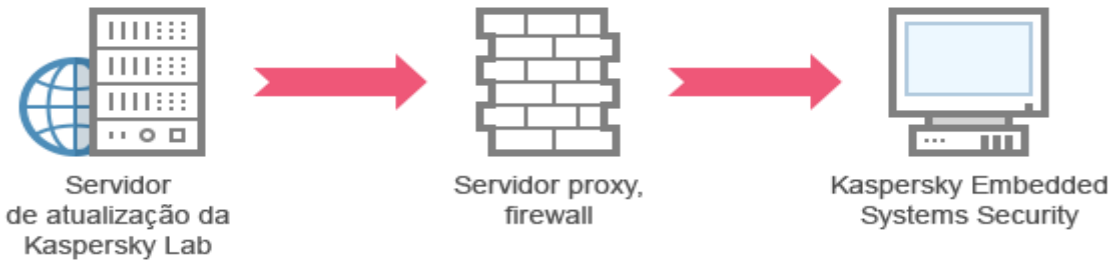
A descrição dos esquemas de atualização listados é fornecida a seguir.

Esquema 1. Atualização dos bancos de dados e módulos diretamente da Internet

► *Para configurar atualizações do Kaspersky Embedded Systems Security diretamente da Internet:*

em cada computador protegido nas configurações da tarefa de Atualização do banco de dados e na tarefa de Atualização de módulos de software, especifique os servidores de atualização da Kaspersky Lab como a fonte de atualização.

Outros servidores HTTP ou FTP que têm uma pasta de atualização podem ser configurados como fonte de atualizações.

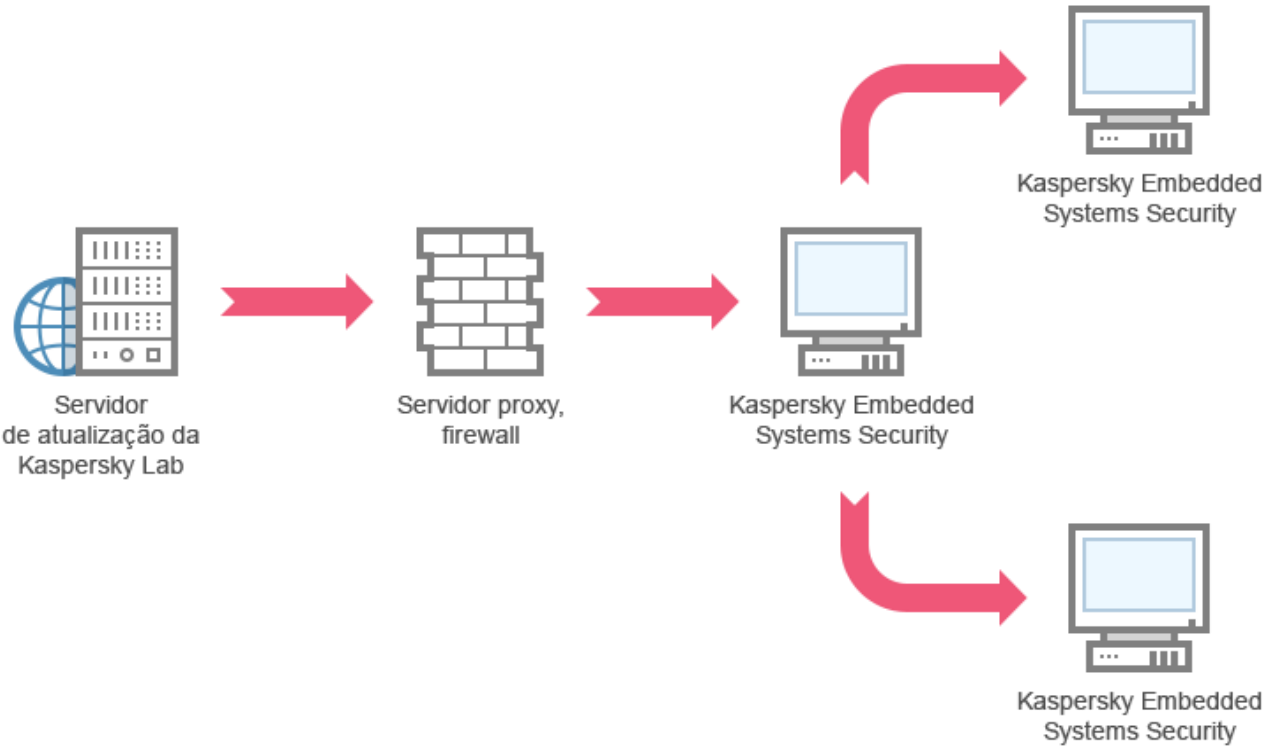


Esquema 2. Atualização dos bancos de dados e módulos através de um dos computadores protegidos

► *Para configurar atualizações do Kaspersky Embedded Systems Security através de um dos computadores protegidos:*

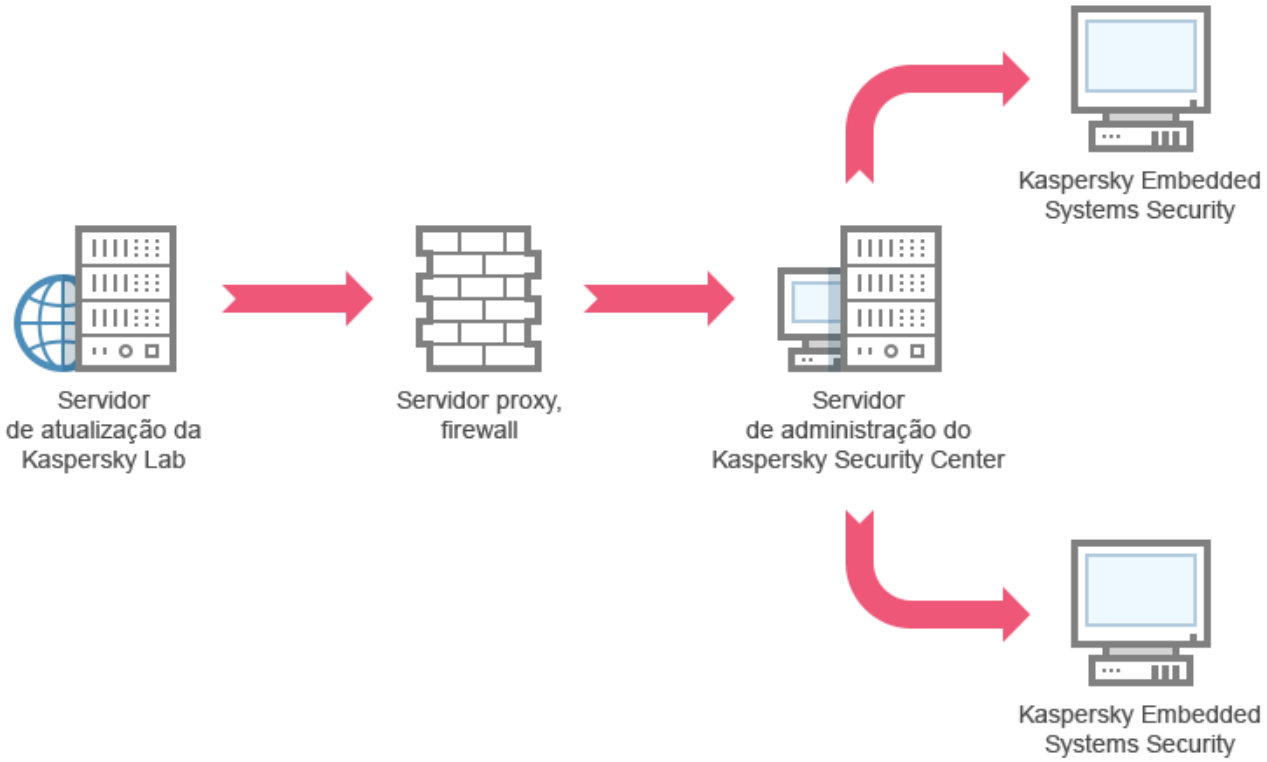
1. Copie as atualizações para o computador protegido selecionado. Para isso, execute as seguintes ações:
   - Configure a tarefa Copiar atualizações no computador selecionado:
     a. Especifique o servidor de atualização da Kaspersky Lab como fonte de atualizações.
     b. Especifique uma pasta compartilhada a ser usada como a pasta onde as atualizações são salvas.
2. Distribua as atualizações para outros computadores protegidos. Para isso, execute as seguintes ações:
   - Em cada computador protegido, defina as configurações para a tarefa de Atualização do banco de dados e para a tarefa de Atualização de módulos de software (consulte a figura abaixo).
     a. Para a fonte de atualização, especifique uma pasta na unidade do computador intermediário na qual as atualizações serão baixadas.

O Kaspersky Embedded Systems Security obterá atualizações através de um dos computadores protegidos.



Esquema 3. Atualização dos bancos de dados e módulos através do Servidor de Administração do Kaspersky Security Center

Se o aplicativo Kaspersky Security Center for usado para administração centralizada da proteção antivírus do computador, as atualizações podem ser baixadas através do Servidor de Administração do Kaspersky Security Center instalado na rede de área local (consulte a figura abaixo).



► *Para configurar atualizações do Kaspersky Embedded Systems Security através do Servidor de Administração do Kaspersky Security Center:*

1. Baixe atualizações dos servidores de atualização da Kaspersky Lab para o Servidor de Administração do Kaspersky Security Center. Para isso, execute as seguintes ações:
   - Configure a tarefa Recuperar atualizações pelo Servidor de administração para o conjunto de computadores especificado:
     a. Especifique os servidores de atualização da Kaspersky Lab como fonte de atualizações.
2. Distribuir atualizações para os computadores protegidos. Para fazer isso, execute uma das seguintes ações:
   - No Kaspersky Security Center configure uma tarefa de grupo de atualização (módulo do aplicativo) do banco de dados do antivírus para distribuir atualizações nos computadores protegidos:
     a. Na programação da tarefa, especifique **Após o Servidor de Administração ter recuperado as atualizações** como frequência de início.

        O Servidor de Administração executará a tarefa sempre que receber atualizações (método recomendado).

A frequência de início **Após o Servidor de Administração ter recuperado as atualizações** não pode ser especificada no Console do Aplicativo.

- Em cada computador protegido, configure a tarefa de Atualização do banco de dados e a tarefa de Atualização de módulos de software:
  a. Especifique o Servidor de Administração do Kaspersky Security Center como a fonte de atualização.
  b. Configure a programação da tarefa se necessário.

Se os bancos de dados de antivírus do Kaspersky Embedded Systems Security forem raramente atualizados (de uma vez por mês a uma vez por ano), a probabilidade da detecção de ameaças cai e a frequência de falsos positivos é elevada pelos aumentos dos componentes do aplicativo.

O Kaspersky Embedded Systems Security obterá atualizações através do Servidor de Administração do Kaspersky Security Center.

Se pretender usar o Servidor de Administração do Kaspersky Security Center para distribuir atualizações, instale o Agente de rede, um componente do aplicativo incluído no kit de distribuição do Kaspersky Security Center, em cada um dos computadores protegidos. Isso garante a interação entre o Servidor de Administração e o Kaspersky Embedded Systems Security no computador protegido. Informações detalhadas sobre o Agente de rede e a sua configuração usando o Kaspersky Security Center são fornecidas no *Ajuda do Kaspersky Security Center*.

Configurando tarefas de Atualização

Esta seção fornece instruções sobre como configurar tarefas de atualização do Kaspersky Embedded Systems Security.

Nesta seção

Definindo as configurações para trabalhar com fontes de atualização do Kaspersky Embedded Systems Security 177
Otimizando o uso da E/S de disco ao executar a tarefa de Atualização do banco de dados 180
Configurações da tarefa Copiar atualizações 181
Definindo as configurações da tarefa de Atualização de módulos de software 182

Definindo as configurações para trabalhar com fontes de atualização do Kaspersky Embedded Systems Security

Para cada tarefa de atualização exceto a tarefa de Reversão da atualização do banco de dados, você pode especificar uma ou várias fontes de atualização, adicionar fontes de atualização definidas pelo usuário e definir as configurações para a conexão com as fontes especificadas.

Após as configurações de tarefa de atualização serem modificadas, as novas configurações não serão imediatamente aplicadas nas tarefas de atualização em execução. As configurações definidas serão aplicadas somente quando a tarefa for reiniciada.

► *Para especificar o tipo de fonte de atualização:*

1. Na árvore do Console do Aplicativo, expanda o nó **Atualização**.
2. Selecione o nó filho que corresponde à tarefa de atualização que deseja configurar.
3. Clique no link **Propriedades** no painel de detalhes do nó selecionado.

   A janela **Configurações de tarefa** é exibida na guia **Geral**.
4. Na seção **Fonte de atualização**, selecione o tipo da fonte de atualização do Kaspersky Embedded Systems Security:
   - **Servidor de Administração do Kaspersky Security Center**

     O Kaspersky Embedded Systems Security usa o Servidor de Administração do Kaspersky Security Center como a fonte de atualização.

     Apenas será possível selecionar esta opção se os aplicativos da Kaspersky Lab em sua rede forem administrados usando o sistema de acesso remoto do Kaspersky Security Center e se o Agente de Rede (o componente do Kaspersky Security Center que fornece a conexão entre os computadores e o Servidor de Administração) estiver instalado no computador protegido.
   - **Servidores de atualização da Kaspersky Lab**

     O Kaspersky Embedded Systems Security utilizará os sites da Kaspersky Lab como fontes de atualização, hospedando atualizações para os bancos de dados e para os módulos de software para todos os produtos da empresa.

     Esta opção é selecionada por padrão.
   - **Servidores HTTP ou FTP ou pastas de rede personalizados**

     O Kaspersky Embedded Systems Security usa o servidor HTTP ou FTP especificado pelo administrador ou pastas na rede local como fonte de atualização.

     Você poderá criar uma lista de fontes com as atualizações atuais ao clicar no link **Servidores HTTP ou FTP ou pastas de rede personalizados**.
5. Se necessário, defina as configurações avançadas para as fontes de atualização definidas pelo usuário:
   a. Clique no link **Servidores HTTP ou FTP ou pastas de rede personalizados**.
      i. Na janela **Servidores de atualização** exibida, selecione ou desmarque as caixas ao lado das fontes de atualização definidas pelo usuário para começar ou encerrar seu uso.
      ii. Clique em **OK**.
   b. Na seção **Fonte de atualização** na guia **Geral**, selecione ou desmarque a caixa **Usar servidores de atualização da Kaspersky Lab se os servidores especificados não estiverem disponíveis**.

      Esta caixa de seleção ativa ou desativa a opção de uso dos servidores de atualização da Kaspersky Lab como a fonte de atualização se as fontes de atualização definidas pelo usuário estiverem indisponíveis.

      Se a caixa de seleção estiver selecionada, esta função será ativada.

A caixa de seleção é selecionada por padrão.

Você pode selecionar a caixa de seleção **Usar servidores de atualização da Kaspersky Lab se os servidores especificados não estiverem disponíveis** quando a opção **Servidores HTTP ou FTP ou pastas de rede personalizados** estiver ativada.

6. Na janela **Configurações de tarefa**, selecione a guia **Configurações de conexão** para definir as configurações para se conectar a fontes de atualização:
   - Desmarque ou selecione a caixa de seleção **Usar as configurações do servidor proxy para se conectar aos servidores de atualização da Kaspersky Lab**.

     A caixa de seleção ativa/desativa o uso de configurações do servidor proxy se as atualizações forem recebidas de servidores da Kaspersky Lab ou se a caixa de seleção **Usar servidores de atualização da Kaspersky Lab se os servidores especificados não estiverem disponíveis** estiver marcada.

     Se a caixa de seleção estiver selecionada, as configurações do servidor proxy serão usadas.

     Se a caixa de seleção estiver desmarcada, as configurações do servidor proxy não serão usadas.

     A caixa de seleção é selecionada por padrão.
   - Desmarque ou selecione a caixa **Usar configurações de servidor proxy para conectar a outros servidores**.

     As caixas de seleção ativam ou desativam o uso das configurações do servidor proxy se a opção **Servidores HTTP ou FTP ou pastas de rede personalizados** estiver selecionada como uma fonte de atualização.

     Se a caixa de seleção estiver selecionada, as configurações do servidor proxy serão usadas.

     Esta caixa é desmarcada por padrão.

   Para obter informações sobre a definição de configurações opcionais de servidor proxy e autenticação para acesso ao servidor proxy, consulte a seção Inicialização e configuração da tarefa de atualização dos bancos de dados do Kaspersky Embedded Systems Security.

7. Clique em **OK**.

As configurações definidas para a fonte de atualização do Kaspersky Embedded Systems Security serão salvas e aplicadas no momento da próxima inicialização da tarefa.

Você pode gerenciar a lista de fontes de atualização do Kaspersky Embedded Systems Security definida pelo usuário.

► *Para editar a lista de fontes de atualização de aplicativo definida pelo usuário:*

1. Na árvore do Console do Aplicativo, expanda o nó **Atualização**.
2. Selecione o nó filho que corresponde à tarefa de atualização que deseja configurar.
3. Clique no link **Propriedades** no painel de detalhes do nó selecionado.

   A janela **Configurações de tarefa** é exibida na guia **Geral**.
4. Clique no link **Servidores HTTP ou FTP ou pastas de rede personalizados**.

A janela **Servidores de atualização** é exibida.

5. Faça o seguinte:
   - Para adicionar uma fonte de atualização definida pelo usuário no campo de inserção, especifique o endereço da pasta que contém os arquivos de atualização no servidor FTP ou HTTP; especifique uma pasta local ou de rede no formato UNC (Universal Naming Convention). Pressione **ENTER**.

     Por padrão, a pasta adicionada é usada como a fonte de atualização.
   - Para desativar o uso de uma fonte definida pelo usuário, desmarque a caixa ao lado da fonte na lista.
   - Para ativar o uso de uma fonte definida pelo usuário, selecione a caixa ao lado da fonte na lista.
   - Para alterar a ordem na qual o Kaspersky Embedded Systems Security acessa fontes de atualização definidas pelo usuário, use os botões **Mover para cima** e **Mover para baixo** para mover a fonte selecionada para o início ou o final da lista, para que ela seja usada antes ou depois das outras fontes.
   - Para alterar o caminho para a fonte definida pelo usuário, selecione a fonte na lista e clique no botão **Editar**, efetue as alterações necessárias no campo de inserção e pressione a tecla **ENTER**.
   - Para remover uma fonte definida pelo usuário, selecione-a na lista e pressione o botão **Remover**.

     Não é possível excluir a única fonte definida pelo usuário da lista.
6. Clique em **OK**.

As modificações na lista de fontes de atualização de aplicativo definidas pelo usuário serão salvas.

Otimizando o uso da E/S de disco ao executar a tarefa de Atualização do banco de dados

Ao executar a tarefa de Atualização do banco de dados, o Kaspersky Embedded Systems Security armazena arquivos de atualização na unidade local do computador. Você pode diminuir a carga de trabalho no subsistema de E/S de disco do computador por meio do armazenamento de arquivos de atualização em uma unidade virtual na RAM ao executar a tarefa de atualização.

Este recurso está disponível para o Microsoft Windows 7 e sistemas operacionais posteriores.

Ao usar este recurso executando a tarefa de Atualização do banco de dados, uma unidade lógica extra pode aparecer no sistema operacional. Esta unidade lógica será removida do sistema operacional após a tarefa ser concluída.

► *Para diminuir a carga de trabalho no subsistema de E/S de disco do seu computador durante a tarefa de Atualização do banco de dados, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Atualização**.
2. Selecionar o nó filho **Atualização do Banco de Dados**.
3. Clique no link **Propriedades** no painel de detalhes do nó **Atualização do banco de dados**.

4. A janela **Configurações de tarefa** é exibida na guia **Geral**.
5. Na seção Otimização de uso da E/S de disco, defina as seguintes configurações:
   - Desmarque ou selecione a caixa **Diminuir a carga na E/S de disco**.

     Esta caixa ativa ou desativa o recurso de otimização de subsistema de disco por meio do armazenamento de arquivos de atualização em uma unidade virtual na RAM.

     Se a caixa de seleção estiver selecionada, esta função será ativada.

     Esta caixa é desmarcada por padrão.
   - No campo **RAM usada para otimização**, especifique o volume de RAM (em MB). O sistema operacional aloca temporariamente o volume de RAM especificado para armazenar arquivos de atualização ao executar a tarefa. O tamanho de RAM padrão é 512 MB. O tamanho de RAM padrão é 400 MB.
6. Clique em **OK**.

As configurações definidas serão salvas e aplicadas na próxima inicialização da tarefa.

Configurações da tarefa Copiar atualizações

► *Para configurar a tarefa Copiar atualizações:*

1. Na árvore do Console do Aplicativo, expanda o nó **Atualização**.
2. Selecione o nó filho **Copiar atualizações**.
3. Clique no link **Propriedades** no painel de detalhes do nó **Copiar atualizações**.

   A janela **Configurações de tarefa** é exibida.
4. Nas guias **Geral** e **Configurações de conexão**, defina as configurações para trabalhar com fontes de atualização (consulte a seção "Definindo as configurações para trabalhar com fontes de atualização do Kaspersky Embedded Systems Security" na página 177).
5. Na guia **Geral** na seção **Copiar configurações de atualizações**:
   - Especifique as condições para copiar atualizações:
     - **Copiar atualizações do banco de dados**.

       O Kaspersky Embedded Systems Security faz o download somente de atualizações do banco de dados do software.

       Esta opção é selecionada por padrão.
     - **Copiar atualizações críticas dos módulos de software**.

       O Kaspersky Embedded Systems Security faz o download somente de atualizações urgentes dos módulos de software do Kaspersky Embedded Systems Security.
     - **Copiar atualizações do banco de dados e atualizações críticas dos módulos de software**.

       O Kaspersky Embedded Systems Security faz o download somente de atualizações do banco de dados de software e atualizações críticas dos módulos de software do Kaspersky Embedded Systems Security.
   - Especifique a pasta local ou pasta de rede para a qual o Kaspersky Embedded Systems Security distribuirá as atualizações baixadas.
6. Nas guias **Programação** e **Avançado**, configure a programação de inicialização da tarefa (consulte a

seção "Definição das configurações da programação de inicialização da tarefa" na página 151).

7. Na guia **Executar como**, configure a tarefa a ser iniciada usando permissões de conta (consulte a seção "Especificação de uma conta de usuário para iniciar uma tarefa" na página 153).
8. Clique em **OK**.

As configurações definidas serão salvas e aplicadas na próxima inicialização da tarefa.

Definindo as configurações da tarefa de Atualização de módulos de software

► *Para configurar a tarefa de Atualização de módulos de software:*

1. Na árvore do Console do Aplicativo, expanda o nó **Atualização**.
2. Selecione o nó filho **Atualização de módulos de software**.
3. Clique no link **Propriedades** no painel de detalhes do nó **Atualização de módulos de software**.

   A janela **Configurações de tarefa** é exibida.
4. Nas guias **Geral** e **Configurações de conexão**, defina as configurações para trabalhar com fontes de atualização (consulte a seção "Definindo as configurações para trabalhar com fontes de atualização do Kaspersky Embedded Systems Security" na página 177).
5. Na guia **Geral** na seção **Configurações da atualização do aplicativo**, defina as configurações para atualizar módulos de aplicativo:
   - **Verificar somente atualizações críticas de software disponíveis**

     O Kaspersky Embedded Systems Security exibirá as notificações sobre atualizações urgentes dos módulos de software disponíveis na fonte de atualização sem fazer o download das atualizações. A notificação será exibida se as notificações sobre eventos desse tipo estiverem ativadas.

     Esta opção é selecionada por padrão.
   - **Copiar e instalar atualizações críticas dos módulos de software**

     O Kaspersky Embedded Systems Security baixa e instala atualizações críticas nos módulos de software.
   - **Permitir reinício do sistema operacional**

     O sistema operacional será reiniciado após a instalação das atualizações que necessitam de reinício.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security reiniciará o sistema operacional após instalar as atualizações que necessitam de reinicialização.

     Esta caixa de seleção estará ativa se a opção **Copiar e instalar atualizações críticas dos módulos de software** estiver selecionada.

     Esta caixa é desmarcada por padrão.
   - **Receber informações sobre as atualizações disponíveis programadas dos módulos de software**

     Serão exibidas as notificações sobre todas as atualizações programadas para os módulos de software do aplicativo do Kaspersky Embedded Systems Security disponíveis na fonte de atualização. O aplicativo exibirá a notificação se as notificações estiverem ativadas para eventos desse tipo.

Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security exibirá uma notificação sobre todas as atualizações programadas para os módulos de software disponíveis na fonte de atualização.

A caixa de seleção é selecionada por padrão.

6. Nas guias **Programação** e **Avançado**, configure a programação de inicialização da tarefa (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 151). Por padrão, o Kaspersky Embedded Systems Security executa a tarefa de Atualização de módulos de software semanalmente às sextas-feiras às 16h00 (hora de acordo com as configurações regionais do computador protegido).
7. Na guia **Executar como**, configure o início da tarefa usando permissões de conta (consulte a seção "Especificação de uma conta de usuário para iniciar uma tarefa" na página 153).
8. Clique em **OK**.

As configurações definidas serão salvas e aplicadas na próxima inicialização da tarefa.

A Kaspersky Lab não publica pacotes de atualizações planejados nos servidores de atualização para instalação automática; eles podem ser baixados manualmente no site da Kaspersky Lab. É possível configurar a notificação do administrador sobre o evento *Nova atualização programada dos módulos de software disponível*; ela conterá o URL da página no site na qual é possível baixar as atualizações programadas.

Revertendo atualizações do banco de dados do Kaspersky Embedded Systems Security

Antes que as atualizações do banco de dados sejam aplicadas, o Kaspersky Embedded Systems Security cria cópias de backup dos bancos de dados usados anteriormente. Se a atualização for interrompida ou resultar em erro, o Kaspersky Embedded Systems Security retornará automaticamente ao uso dos bancos de dados instalados anteriormente.

Se algum problema surgir após a atualização dos bancos de dados, eles poderão ser revertidos às atualizações instaladas anteriormente por meio da tarefa Reversão da atualização do banco de dados.

► *Para iniciar a tarefa Reversão da atualização do banco de dados:*

Clique no link **Iniciar** no painel de detalhes do nó **Reversão da atualização do banco de dados**.

Revertendo atualizações dos módulos do aplicativo

Os nomes de configurações podem variar em diferentes sistemas operacionais Windows.

Antes de aplicar as atualizações dos módulos de software, o Kaspersky Embedded Systems Security cria cópias de backup dos módulos atualmente em uso. Se o processo de atualização dos módulos for interrompido ou resultar em erro, o Kaspersky Embedded Systems Security retornará automaticamente ao uso dos módulos com as últimas atualizações instaladas.

Para reverter os módulos de software, use o componente do Microsoft Windows **Instalar e excluir aplicativos**.

Estatísticas da tarefa de atualização

Enquanto a tarefa de atualização está executando, é possível exibir informações em tempo real sobre a quantidade de dados baixados desde que a tarefa foi iniciada até o momento, além de outras estatísticas de execução da tarefa.

Quando a tarefa for concluída ou interrompida, você poderá visualizar esta informação no log de tarefas.

► *Para exibir estatísticas da tarefa de atualização, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Atualização**.
2. Selecione o nó filho que corresponde à tarefa cuja estatística deseja visualizar.

As estatísticas de tarefa são exibidas na seção **Estatísticas** do painel de detalhes do nó selecionado.

Se você estiver visualizando a tarefa de Atualização do banco de dados ou a tarefa Copiar atualizações, o bloco **Estatísticas** mostrará o volume de dados baixados pelo Kaspersky Embedded Systems Security no momento presente (**Dados recebidos**).

Se você estiver visualizando a tarefa de Atualização de módulos de software, você poderá exibir as informações descritas na tabela que se segue.

Tabela 32. Informações sobre a tarefa de Atualização de módulos de software

Campo	Descrição
Dados recebidos	Quantidade total de dados baixados.
Atualizações críticas disponíveis	Número de atualizações críticas disponíveis para instalação.
Atualizações programadas disponíveis	Número de atualizações planejadas disponíveis para instalação.
Erros ao aplicar atualizações	Se o valor deste campo for diferente de zero, a atualização não foi aplicada. O nome da atualização que causou um erro durante a aplicação pode ser exibido no log de tarefas (consulte a seção "Visualizando estatísticas e informações sobre uma tarefa do Kaspersky Embedded Systems Security em logs de tarefas" na página 206).

Isolamento de objetos e cópia de backup

Esta seção fornece informações sobre o backup de objetos maliciosos detectados antes que eles sejam desinfectados ou removidos e informações sobre a quarentena dos objetos possivelmente infectados.

Neste capítulo

Isolando objetos possivelmente infectados. Quarentena 185

Como fazer cópias de backup de objetos. Backup 194

Isolando objetos possivelmente infectados. Quarentena

Essa seção descreve como isolar objetos possivelmente infectados colocando-os na Quarentena e como especificar as configurações da Quarentena.

Nesta seção

Sobre a colocação na Quarentena de objetos possivelmente infectados 185

Exibindo objetos da Quarentena 185

Verificação da Quarentena 187

Restauração de objetos da quarentena 189

Movimentação de objetos para a Quarentena 191

Excluindo objetos da Quarentena 191

Enviando objetos possivelmente infectados à Kaspersky Lab para análise 191

Configurando a Quarentena 192

Estatísticas da Quarentena 193

Sobre a colocação na Quarentena de objetos possivelmente infectados

O Kaspersky Embedded Systems Security coloca em Quarentena objetos possivelmente infectados movendo esses objetos da sua localização original para a pasta da *Quarentena*. Por questões de segurança, os objetos são armazenados na pasta da Quarentena em formato criptografado.

Exibindo objetos da Quarentena

Os objetos da Quarentena podem ser exibidos no nó **Quarentena** do Console do Aplicativo.

► *Para visualizar objetos na quarentena, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Armazenamentos**.

2. Selecione o nó filho **Quarentena**.

As informações sobre objetos isolados em quarentena são exibidas no painel de detalhes do nó selecionado.

► *Para encontrar o objeto necessário na lista de objetos colocados na Quarentena,*

classifique os objetos (consulte a seção "Classificando objetos da Quarentena" na página 186) ou filtre os objetos (consulte a seção "Filtrando objetos da Quarentena" na página 186).

Nesta seção

Classificando objetos da Quarentena 186
Filtrando objetos da Quarentena 186

Classificando objetos da Quarentena

Por padrão, os objetos da lista de objetos da Quarentena são classificados por data de colocação na Quarentena em ordem cronológica inversa. Para localizar o objeto desejado, você pode classificar os objetos pelas colunas com informações sobre eles. Os resultados da classificação serão salvos se você sair e abrir novamente o nó **Quarentena**, ou se fechar o Console do Aplicativo, salvar o arquivo msc e abri-lo novamente a partir desse arquivo.

► *Para classificar os objetos, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Armazenamentos**.
2. Selecione o nó filho **Quarentena**.
3. No painel de detalhes do nó **Quarentena**, selecione o título da coluna que você deseja usar para classificar objetos na lista.

Os objetos na lista serão classificados com base na configuração selecionada.

Filtrando objetos da Quarentena

Para localizar o objeto da Quarentena desejado, você pode filtrar os objetos da lista e exibir apenas os objetos que atendem aos critérios de filtragem (filtros) especificados. Os resultados do filtro serão salvos se você sair e abrir novamente o nó **Quarentena** ou se fechar o Console do Aplicativo, salvar o arquivo msc e, em seguida, abri-lo novamente a partir desse arquivo.

► *Para especificar um ou mais filtros, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Armazenamentos**.
2. Selecione o nó filho **Quarentena**.
3. Selecione **Filtro** no menu de contexto do nome do nó.

   A janela **Configurações de filtro** é exibida.
4. Para adicionar um filtro, execute os passos que se seguem:
   a. Em **Nome do campo**, selecione um item ao qual o valor do filtro será comparado.
   b. Na lista **Operador**, selecione a condição de filtragem. Os valores das condições de filtragem na lista podem ser diferentes dependendo do valor que você selecionou na lista **Nome do campo**.

c. Insira o valor do filtro no campo **Valor do campo** ou o selecione na lista.

d. Clique no botão **Adicionar**.

O filtro que adicionou será exibido na lista de filtros, na janela **Configurações de filtro**. Repita essas etapas para cada filtro que adicionar. Use as seguintes diretrizes ao trabalhar com filtros:

- Para combinar vários filtros usando o operador lógico "AND", selecione **Se todas as condições forem atendidas**.
- Para combinar vários filtros usando o operador lógico "OR", selecione **Se alguma condição for atendida**.
- Para excluir um filtro, selecione o filtro que deseja excluir na lista de filtros e clique no botão **Remover**.
- Para editar um filtro, selecione o filtro na lista, na janela **Configurações de filtro**. Em seguida altere os valores requeridos nos campos **Nome do campo**, **Operador** ou **Valor do campo** e clique no botão **Substituir**.

5. Após todos os filtros serem adicionados, clique no botão **Aplicar**.

Os filtros criados serão salvos.

► *Para exibir novamente todos os objetos na lista de objetos da Quarentena,*

selecione **Remover** filtro no menu de contexto do nó **Quarentena**.

Verificação da quarentena

Por padrão, após cada atualização do banco de dados, o Kaspersky Embedded Systems Security executa a tarefa do sistema Verificação da quarentena. As configurações da tarefa estão descritas na tabela a seguir. As configurações da tarefa de Verificação da Quarentena não podem ser modificadas.

Você pode configurar a programação de inicialização da tarefa (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 151), iniciá-la manualmente e modificar as permissões da conta (consulte a seção "Especificação de uma conta de usuário para iniciar uma tarefa" na página 153) usada para iniciar a tarefa.

Após verificar objetos da Quarentena depois de atualizar os bancos de dados, o Kaspersky Embedded Systems Security poderá reconhecer alguns dos objetos como não infectados: o status desses objetos muda para **Falso positivo**. Outros objetos podem ser reclassificados como infectados e, nesse caso, o Kaspersky Embedded Systems Security trata tais objetos como especificados pela Verificação da Quarentena: desinfecta ou exclui se a desinfecção falhar.

Tabela 33. Configurações da tarefa de Verificação da Quarentena

Configuração da tarefa de Verificação da Quarentena	Valor
Escopo da verificação	Pasta da Quarentena
Configurações de segurança	Comum para toda a área de verificação; os valores são fornecidos na tabela que se segue

Tabela 34. Configurações de verificação na tarefa de Verificação da quarentena

Configuração de segurança	Valor
Verificar objetos	Todos os objetos incluídos no escopo da verificação
Otimização	Desativado
Ação a ser executada com objetos infectados e outros objetos detectados	Desinfectar; excluir se a desinfecção não for possível
Ação a ser executada com objetos infectados	Ignorar
Excluir objetos	Não
Não detectar	Não
Interromper a verificação se demorar mais que (s)	Não configurado
Não verificar objetos com mais de (MB)	Não configurado
Verificar fluxos NTFS alternativos	Ativado
Setores de inicialização de unidades e MBR	Desativado
Usando a tecnologia iChecker	Desativado
Usando a tecnologia iSwift	Desativado
Verificar objetos compostos	• Arquivos compactados* • Arquivos compactados SFX* • Objetos compactados* • Objetos OLE incorporados* *A opção Verificar apenas arquivos novos e modificados está desativada.
Verificando assinaturas da Microsoft nos arquivos	Não executado
Usar o analisador heurístico	Ativado com o nível de análise **Profundo**
Zona Confiável	Não aplicado

Restauração de objetos da quarentena

O Kaspersky Embedded Systems Security coloca os objetos possivelmente infectados na pasta da Quarentena em um formato criptografado, para proteger o computador contra qualquer possível efeito negativo.

Você pode restaurar qualquer objeto a partir da Quarentena. Isso poderá ser necessário nos seguintes casos:

- Se, após a verificação da quarentena usando o banco de dados atualizado, o status do objeto mudar para **Falso positivo** ou **Desinfectado**.
- Se você considerar o objeto inofensivo para o computador e desejar utilizá-lo. Se você não quiser que o Kaspersky Embedded Systems Security isole o objeto durante as verificações subsequentes, você poderá excluir esse objeto do processamento na tarefa Proteção de Arquivos em Tempo Real e nas tarefas de Verificação por Demanda. Para fazer isso, especifique o objeto como o valor das configurações de segurança **Excluir arquivos** (pelo nome de arquivo) ou **Não detectar** daquelas tarefas, ou adicione-o à Zona Confiável (na página 443).

Ao restaurar objetos, é possível selecionar onde o objeto restaurado será salvo: local original (por padrão), pasta especial para objetos restaurados no computador protegido ou pasta personalizada no computador em que o Console do Aplicativo está instalado, ou ainda em outro computador da rede.

A opção **Restaurar na pasta** é usada para armazenar objetos restaurados no computador protegido. Você pode definir configurações especiais de segurança para que ela seja verificada. O caminho dessa pasta é definido pelas configurações da Quarentena.

A restauração de objetos da Quarentena pode levar à infecção do computador.

Você pode restaurar o objeto e salvar sua cópia na pasta da Quarentena para usá-la posteriormente, por exemplo, para verificar novamente o objeto após o banco de dados ser atualizado.

Se um objeto colocado na Quarentena fizer parte de um objeto composto (por exemplo, em um arquivo compactado), o Kaspersky Embedded Systems Security não incluirá esse objeto no composto durante a restauração. Em vez disso, ele será salvo separadamente em uma pasta selecionada.

Você pode restaurar um ou vários objetos.

► *Para restaurar objetos colocados na quarentena, execute os passos a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Armazenamentos**.
2. Selecione o nó filho **Quarentena**.
3. Execute uma das ações seguintes no painel de detalhes do nó **Quarentena**:
   - Para restaurar um objeto, selecione **Restaurar** no menu de contexto do objeto que deseja restaurar.
   - Para restaurar vários objetos, selecione os objetos desejados usando a tecla **CTRL** ou **SHIFT**, clique com o botão direito do mouse em um dos objetos selecionados e selecione **Restaurar** no menu de contexto.

   A janela **Restauração de objeto** é aberta.
4. Na janela **Restauração de objeto**, especifique a pasta em que o objeto restaurado será salvo para cada

um dos objetos selecionados.

> O nome do objeto é exibido no campo **Objeto** na parte superior da janela. Se você selecionar vários objetos, o nome do primeiro objeto na lista de objetos selecionados será exibido.

5. Execute uma das seguintes etapas:
   - Para restaurar um objeto em seu local original, selecione **Restaurar na pasta de origem**.
   - Para restaurar um objeto na pasta especificada como a localização para objetos restaurados nas configurações, selecione **Restaurar na pasta padrão para restauração**.
   - Para salvar um objeto em uma pasta diferente no computador em que o Console do Aplicativo está instalado ou em uma pasta compartilhada, selecione **Restaurar na pasta em seu computador local ou no recurso de rede** e, em seguida, selecione a pasta requerida ou especifique o caminho para ela.
6. Se você desejar salvar uma cópia do objeto na pasta da Quarentena após esse objeto ser restaurado, desmarque a caixa de verificação **Remover objetos do armazenamento depois que forem restaurados**.
7. Para aplicar as condições de restauração especificadas ao resto dos objetos selecionados, marque a caixa **Aplicar a todos os objetos selecionados**.

   Todos os objetos selecionados são restaurados e salvos no local especificado: se você selecionou **Restaurar na pasta de origem**, cada um dos objetos será salvo em sua localização original; se você selecionou **Restaurar na pasta padrão para restauração** ou **Restaurar na pasta em seu computador local ou no recurso de rede**, todos os objetos serão salvos na pasta especificada.
8. Clique em **OK**.

   O Kaspersky Embedded Systems Security começará a restaurar o primeiro dos objetos selecionados.
9. Se um objeto com esse nome já existir na localização especificada, a janela **Já existe um objeto com este nome** é aberta.
   a. Selecione uma das seguintes ações para o Kaspersky Embedded Systems Security:
      - **Substituir**, para restaurar um objeto no lugar do existente.
      - **Renomear**, para salvar um objeto restaurado com outro nome. No campo de entrada, insira o novo nome de arquivo do objeto e seu caminho completo.
      - **Renomear adicionando um sufixo**, para renomear o objeto adicionando um sufixo ao nome do arquivo. Insira o sufixo no campo de entrada.
   b. Se você tiver selecionado vários objetos para restauração, selecione a caixa **Aplicar a todos os objetos selecionados** para poder aplicar a ação selecionada, como **Substituir** ou **Renomear** adicionando um sufixo ao resto dos objetos selecionados. (Se você tiver selecionado o valor **Renomear**, a caixa de seleção **Aplicar a todos os objetos selecionados** estará indisponível).
   c. Clique em **OK**.

   O objeto será restaurado. As informações sobre a operação de restauração serão registradas no log de auditoria do sistema.

   Se você não selecionar a opção **Aplicar a todos os objetos selecionados** na janela **Restauração de objeto**, a janela **Restauração de objeto** será novamente aberta. Usando essa janela você pode especificar a localização onde o próximo objeto selecionado será salvo (consulte a Etapa 4 desse procedimento).

Movimentação de objetos para a Quarentena

Você pode colocar arquivos na Quarentena manualmente.

► *Para colocar um arquivo na Quarentena, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Quarentena**.
2. Selecione **Adicionar**.
3. Na janela **Abrir**, selecione o arquivo no disco que deseja colocar na Quarentena.
4. Clique em **OK**.

O Kaspersky Embedded Systems Security isolará em quarentena o arquivo selecionado.

Excluindo objetos da Quarentena

De acordo com as configurações da tarefa Verificação da Quarentena, o Kaspersky Embedded Systems Security exclui automaticamente objetos da pasta Quarentena caso seu status tenha sido alterado para *Infectado* durante a verificação da Quarentena com os bancos de dados atualizados e caso o Kaspersky Embedded Systems Security não tenha conseguido desinfectar esses objetos. O Kaspersky Embedded Systems Security não remove outros objetos da Quarentena.

É possível excluir um ou mais objetos da Quarentena.

► *Para excluir um ou mais objetos da Quarentena, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Armazenamentos**.
2. Selecione o nó filho **Quarentena**.
3. Execute uma das seguintes etapas:
   - Para remover um objeto, selecione **Remover** no menu de contexto do nome do objeto.
   - Para excluir vários objetos, selecione os objetos que deseja excluir usando a tecla **Ctrl** ou **Shift**, abra o menu de contexto em um dos objetos selecionados e marque **Remover**.
4. Na janela de confirmação, clique no botão **Sim** para confirmar a operação.

Os objetos selecionados serão removidos da quarentena.

Enviando objetos possivelmente infectados à Kaspersky Lab para análise

Se o comportamento de um arquivo der um motivo a você para suspeitar que ele contém uma ameaça, e se o Kaspersky Embedded Systems Security considerar o arquivo como limpo, você poderá ter encontrado uma ameaça desconhecida cuja assinatura ainda não foi adicionada ao banco de dados. Você pode enviar esse arquivo à Kaspersky Lab para análise. Os analistas de Antivírus da Kaspersky Lab o examinarão e, se for detectada uma nova ameaça nele, será adicionado um registro aos bancos de dados identificando-a. É provável que, quando você verificar o objeto novamente após a atualização do banco de dados, o Kaspersky Embedded Systems Security considere esse objeto como infectado e possa desinfetá-lo. Além de poder manter o objeto, você também evitará um surto de vírus.

Somente os arquivos da Quarentena podem ser enviados para análise. Os arquivos da Quarentena são armazenados em forma criptografada e não são excluídos pelo aplicativo de Antivírus instalado no servidor de e-mail durante a transferência.

Os objetos da Quarentena não poderão ser enviados à Kaspersky Lab para análise depois que a licença expirar.

► *Para enviar um arquivo à Kaspersky Lab para análise, siga as etapas a seguir:*

1. Se o arquivo não foi adicionado à Quarentena, comece movendo-o para a **Quarentena**.
2. No nó **Quarentena**, abra o menu de contexto do arquivo que você deseja enviar para análise e selecione **Enviar objeto para análise**.
3. Na janela de confirmação exibida, clique em **Sim** se estiver seguro que deseja enviar o objeto selecionado para a análise.
4. Se houver um programa de e-mail configurado no computador em que o Console do Aplicativo está instalado, uma nova mensagem de e-mail será criada. Revise-a e clique no botão **Enviar**.

   O campo **Destinatário** conterá o endereço de e-mail da Kaspersky Lab, newvirus@kaspersky.com. O campo Assunto conterá o texto "Quarantined object".

   O corpo da mensagem conterá o seguinte texto: "Este arquivo será enviado à Kaspersky Lab para análise". Qualquer informação adicional sobre o arquivo, o motivo pelo qual foi considerado possivelmente infectado ou perigoso, como se comportou ou como afeta o sistema pode ser incluído no corpo da mensagem.

   O arquivo compactado <Nome do objeto>.cab será anexado à mensagem. Este arquivo comprimido conterá o arquivo <uuid>.klq com o objeto em formato criptografado, o arquivo <uuid>.txt com informações sobre o objeto extraído pelo Kaspersky Embedded Systems Security, além do arquivo Sysinfo.txt, que contém as seguintes informações sobre o Kaspersky Embedded Systems Security e o sistema operacional instalado no computador:

   - Nome e versão do sistema operacional.
   - Nome e versão do Kaspersky Embedded Systems Security.
   - Data de lançamento da atualização do banco de dados mais recente instalada.
   - Chave ativa.

   Essas informações são necessárias para que os analistas de Antivírus da Kaspersky Lab examinem seu arquivo de forma mais rápida e eficiente. Se, no entanto, você não desejar transferir essas informações, poderá excluir o arquivo Sysinfo.txt do arquivo comprimido.

Se um programa de e-mail não estiver instalado no computador com o Console do Aplicativo, o aplicativo solicitará que o objeto criptografado selecionado seja salvo no arquivo. Esse arquivo pode ser enviado à Kaspersky Lab manualmente.

► *Para salvar um objeto criptografado em um arquivo, siga as etapas a seguir:*

1. Na janela aberta com uma solicitação para salvar o objeto, clique em **OK**.
2. Selecione uma pasta na unidade do computador protegido ou uma pasta de rede na qual o arquivo que contém o objeto será salvo.

O objeto será salvo em um arquivo CAB.

Configurando a Quarentena

Você pode definir as configurações da Quarentena. As novas configurações da Quarentena são aplicadas

imediatamente após salvar.

► *Para configurar a Quarentena, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Armazenamentos**.
2. Abra o menu de contexto no nó filho **Quarentena**.
3. Selecione **Propriedades**.
4. Na janela **Propriedades da Quarentena**, defina as configurações da Quarentena necessárias de acordo com seus requisitos:
   - Na seção **Configurações da Quarentena**:
     - **Pasta da Quarentena**

       Caminho para a pasta da Quarentena em formato UNC (Universal Naming Convention).

       O caminho padrão é C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Quarantine\.
     - **Tamanho máximo da Quarentena**

       Esta caixa de seleção ativa ou desativa a função que monitora o tamanho total de objetos armazenados na pasta da quarentena. Se o valor especificado for excedido (o valor padrão sendo 200 MB), o Kaspersky Embedded Systems Security efetuará o log do evento *Tamanho máximo da quarentena excedido* e emitirá uma notificação de acordo com as configurações para notificações sobre eventos desse tipo.

       Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security monitorará o tamanho total dos objetos colocados na quarentena.

       Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não monitorará o tamanho total dos objetos colocados na quarentena.

       Esta caixa é desmarcada por padrão.
     - **Valor limite de espaço disponível**

     Se o tamanho dos objetos na Quarentena exceder o tamanho de máximo da Quarentena ou exceder o limite de espaço disponível, o Kaspersky Embedded Systems Security o notificará sobre isto enquanto continua colocando objetos na Quarentena.
   - Na seção **Configurações de restauração**:
     - **Pasta destino para a restauração de objetos**
5. Clique em **OK**.

As configurações definidas recentemente para a Quarentena serão salvas.

Estatísticas da Quarentena

Você pode exibir informações sobre o número de objetos da Quarentena, as estatísticas da Quarentena.

► *Para exibir as estatísticas da Quarentena,*

abra o menu de contexto do nó **Quarentena** na árvore do Console do Aplicativo e selecione **Estatísticas**.

A janela **Estatísticas** exibe informações sobre o número de objetos atualmente armazenados na Quarentena (consulte a tabela seguinte):

Campo	Descrição
Objetos possivelmente infectados	Número de objetos encontrados pelo Kaspersky Embedded Systems Security que estão possivelmente infectados.
Espaço usado da quarentena	Tamanho total dos dados na pasta Quarentena.
Falsos positivos	O número de objetos que receberam o status *Falso positivo* porque foram classificados como não infectados durante a verificação da Quarentena usando bancos de dados atualizados.
Objetos desinfectados	O número de objetos que receberam o status *Desinfectado* após a verificação da Quarentena.
Número total de objetos	Número total de objetos na Quarentena.

Como fazer cópias de backup de objetos. Backup

Essa seção fornece informações sobre o backup de objetos maliciosos detectados antes da desinfecção ou exclusão, bem como instruções para a configuração do Backup.

Nesta seção

Sobre o backup de objetos antes da desinfecção ou exclusão 194
Visualizando objetos armazenados no Backup 195
Restaurando arquivos do Backup 196
Excluindo arquivos do Backup 198
Configurando o Backup 199
Estatísticas do backup 200

Sobre o backup de objetos antes da desinfecção ou exclusão

O Kaspersky Embedded Systems Security armazena cópias criptografadas de objetos classificados como *Infectados* no *Backup* antes de desinfectá-los ou excluí-los.

Se o objeto fizer parte de um objeto composto (por exemplo, de um arquivo compactado), o Kaspersky Embedded Systems Security salvará esse objeto composto inteiro no Backup. Por exemplo, se o Kaspersky Embedded Systems Security tiver detectado que um dos objetos de um banco de dados de e-mail está infectado, ele fará backup de todo o banco de dados de e-mail.

Objetos grandes colocados no Backup pelo Kaspersky Embedded Systems Security podem tornar o sistema lento e reduzir o espaço no disco rígido.

É possível restaurar arquivos do Backup para sua pasta original ou para outra pasta do computador protegido ou de outro computador da rede local. Um arquivo poderá ser restaurado do Backup, por exemplo, se um arquivo infectado contiver informações importantes mas, durante sua desinfecção, o Kaspersky Embedded Systems Security não puder manter sua integridade e, portanto, as informações ficarem indisponíveis.

A restauração de arquivos do Backup pode levar à infecção do computador.

Visualizando objetos armazenados no Backup

Os objetos podem ser armazenados na pasta do Backup somente usando o Console do Aplicativo no nó **Backup**. Não é possível exibi-los usando os gerenciadores de arquivos do Microsoft Windows.

► *Para visualizar os objetos do Backup,*

1. Na árvore do Console do Aplicativo, expanda o nó **Armazenamentos**.
2. Selecione o nó filho **Backup**.

As informações sobre objetos colocados no Backup são exibidas no painel de detalhes do nó selecionado.

► *Para encontrar o objeto necessário na lista de objetos no Backup,*

classifique os objetos ou filtre os objetos.

Nesta seção

Classificando arquivos no Backup 195
Filtrando arquivos no Backup 196

Classificando arquivos no Backup

Por padrão, os arquivos do Backup são classificados pela data de salvamento, em ordem cronológica inversa. Para localizar o arquivo requerido, você pode ordenar arquivos de acordo com o conteúdo de qualquer coluna no painel de detalhes.

Os resultados de classificação serão salvos se você sair e abrir novamente o nó **Backup** ou se fechar o Console do Aplicativo, salvar o arquivo msc e, em seguida, abri-lo novamente a partir desse arquivo.

► *Para classificar os arquivos do Backup, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Armazenamentos**.
2. Selecione o nó filho **Backup**.
3. Na lista de arquivos do **Backup**, selecione o cabeçalho da coluna que você deseja usar para classificar os

objetos.

Os arquivos no Backup serão classificados com base no critério selecionado.

Filtrando arquivos no Backup

Para localizar o arquivo desejado no Backup, é possível filtrar os arquivos: exibir no nó **Backup** apenas os arquivos que atendem aos critérios de filtragem que você especificou (filtros).

Os resultados da classificação serão salvos se você sair e abrir novamente o nó **Backup**, ou se fechar o Console do Aplicativo, salvar o arquivo msc e abri-lo novamente desse arquivo.

► *Para filtrar os arquivos do Backup, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Backup** e selecione **Filtro**.

   A janela **Configurações de filtro** é exibida.

2. Para adicionar um filtro, execute os passos que se seguem:

   a. Na lista **Nome do campo**, selecione o campo cujos valores serão comparados aos valores do filtro durante a seleção.

   b. Na lista **Operador**, selecione a condição de filtragem. Os valores das condições de filtragem na lista podem ser diferentes dependendo do valor que você selecionou no campo **Nome do campo**.

   c. Insira o valor do filtro no campo **Valor do campo** ou selecione o valor do filtro.

   d. Clique no botão **Adicionar**.

   O filtro que adicionou será exibido na lista de filtros, na janela **Configurações de filtro**. Repita essas etapas para cada filtro que adicionar. As diretrizes seguintes podem ser usadas ao trabalhar com os filtros:

   - Para combinar vários filtros usando o operador lógico "AND", selecione **Se todas as condições forem atendidas**.
   - Para combinar vários filtros usando o operador lógico "OR", selecione **Se alguma condição for atendida**.
   - Para excluir um filtro, selecione o filtro que deseja excluir na lista de filtros e clique no botão **Remover**.
   - Para editar o filtro, selecione-o na lista de filtros, na janela **Configurações de filtro**, modifique os valores requeridos nos campos **Nome do campo**, **Operador** ou **Valor do campo** e clique no botão **Substituir**.

   Quando todos os filtros tiverem sido adicionados, clique no botão **Aplicar**. Então, somente os arquivos selecionados pelos filtros que você especificou serão exibidos na lista.

► *Para exibir todos os arquivos incluídos na lista de objetos armazenados no Backup,*

selecione **Remover filtro** no menu de contexto do nó **Backup**.

Restaurando arquivos do Backup

O Kaspersky Embedded Systems Security armazena arquivos na pasta Backup em formato criptografado para proteger o computador protegido contra seu possível efeito prejudicial.

Qualquer arquivo pode ser restaurado do Backup.

Talvez seja necessário restaurar um arquivo nos seguintes casos:

- Se o arquivo original, que aparenta estar infectado, incluísse informações importantes e o Kaspersky Embedded Systems Security não conseguisse manter a sua integridade, como resultado, a informação no arquivo ficaria indisponível.
- Se você considerar o arquivo inofensivo para o computador e desejar utilizá-lo. Se você não desejar que o Kaspersky Embedded Systems Security considere esse arquivo como infectado ou possivelmente infectado, durante verificações subsequentes você pode excluí-lo do processamento na tarefa Proteção de Arquivos em Tempo Real e nas tarefas de Verificação por Demanda. Para fazer isso, defina a configuração do arquivo como **Excluir arquivos** ou **Não detectar** nas tarefas correspondentes.

  A restauração de arquivos do Backup pode levar à infecção do computador.

Ao restaurar um arquivo, você pode escolher a localização onde deseja salvá-lo: na pasta original (por padrão), em uma pasta especial para objetos restaurados no computador protegido, em uma pasta personalizada em um computador em que o Console do Aplicativo está instalado ou em outro computador na rede.

A opção **Restaurar na pasta** é usada para armazenar objetos restaurados no computador protegido. Você pode definir configurações especiais de segurança para que ela seja verificada. O caminho para esta pasta é especificado por configurações de Backup (consulte a seção "Configurando o Backup" na página 199).

Por padrão, quando o Kaspersky Embedded Systems Security está restaurando um arquivo, ele faz uma cópia desse arquivo no Backup. A cópia do arquivo pode ser excluída do Backup depois de ser restaurada.

► *Para restaurar arquivos do Backup, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Armazenamentos**.
2. Selecione o nó filho **Backup**.
3. Execute uma das ações seguintes no painel de detalhes do nó **Backup**:
   - Para restaurar um objeto, selecione **Restaurar** no menu de contexto do objeto que deseja restaurar.
   - Para restaurar vários objetos, selecione os objetos que deseja restaurar usando a tecla **CTRL** ou **SHIFT**, clique com o botão direito do mouse em um dos objetos selecionados e selecione **Restaurar** no menu de contexto.

   A janela **Restauração de objeto** é aberta.
4. Na janela **Restauração de objeto**, especifique a pasta em que o objeto restaurado será salvo para cada um dos objetos selecionados.

   O nome do objeto é exibido no campo **Objeto** na parte superior da janela. Se você selecionar vários objetos, o nome do primeiro objeto na lista de objetos selecionados será exibido.
5. Execute uma das seguintes etapas:
   - Para restaurar um objeto em seu local original, selecione **Restaurar na pasta de origem**.
   - Para restaurar um objeto na pasta especificada como a localização para objetos restaurados nas configurações, selecione **Restaurar na pasta padrão para restauração**.
   - Para salvar um objeto em uma pasta diferente no computador em que o Console do Aplicativo está instalado ou em uma pasta compartilhada, selecione **Restaurar na pasta em seu computador local ou no recurso de rede** e, em seguida, selecione a pasta requerida ou especifique o caminho para ela.

6. Se você não desejar salvar uma cópia do arquivo na pasta do Backup após ele ser restaurado, selecione a caixa de seleção **Remover objetos do armazenamento depois que forem restaurados** (por padrão, esta caixa é desmarcada).
7. Para aplicar as condições de restauração especificadas ao resto dos objetos selecionados, marque a caixa **Aplicar a todos os objetos selecionados**.

   Todos os objetos selecionados são restaurados e salvos no local especificado: se você selecionou **Restaurar na pasta de origem**, cada um dos objetos será salvo em sua localização original; se você selecionou **Restaurar na pasta padrão para restauração** ou **Restaurar na pasta em seu computador local ou no recurso de rede**, todos os objetos serão salvos na pasta especificada.
8. Clique em **OK**.

   O Kaspersky Embedded Systems Security começará a restaurar o primeiro dos objetos selecionados.
9. Se um objeto com esse nome já existir na localização especificada, a janela **Já existe um objeto com este nome** é aberta.
   a. Selecione uma das seguintes ações para o Kaspersky Embedded Systems Security:
      - **Substituir**, para restaurar um objeto no lugar do existente.
      - **Renomear**, para salvar um objeto restaurado com outro nome. No campo de entrada, insira o novo nome de arquivo do objeto e seu caminho completo.
      - **Renomear adicionando um sufixo**, para renomear o objeto adicionando um sufixo ao seu nome de arquivo. Insira o sufixo no campo de entrada.
   b. Se você tiver selecionado vários objetos para restaurar, para poder aplicar a ação selecionada, como **Substituir** ou **Renomear** adicionando um sufixo ao resto dos objetos selecionados, selecione a caixa **Aplicar a todos os objetos selecionados**. (Se você tiver selecionado o valor **Renomear**, a caixa de seleção **Aplicar a todos os objetos selecionados** estará indisponível).
   c. Clique em **OK**.

   O objeto será restaurado. As informações sobre a operação de restauração serão registradas no log de auditoria do sistema.

Se você não selecionar a opção **Aplicar a todos os objetos selecionados** na janela **Restauração de objeto**, a janela **Restauração de objeto** será novamente aberta. Usando essa janela você pode especificar a localização onde o próximo objeto selecionado será salvo (consulte a Etapa 4 desse procedimento).

Excluindo arquivos do Backup

► *Para excluir um ou mais arquivos do Backup, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Armazenamentos**.
2. Selecione o nó filho **Backup**.
3. Execute uma das seguintes etapas:
   - Para remover um objeto, selecione **Remover** no menu de contexto do nome do objeto.
   - Para excluir vários objetos, selecione os objetos que deseja excluir usando a tecla **Ctrl** ou **Shift**, abra o menu de contexto em um dos objetos selecionados e marque **Remover**.
4. Na janela de confirmação, clique no botão **Sim** para confirmar a operação.

Os arquivos selecionados serão excluídos do Backup.

Configurando o Backup

► *Para configurar o Backup, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Armazenamentos**.
2. Abra o menu de contexto no nó **Backup**.
3. Selecione **Propriedades**.
4. Na janela **Propriedades de Backup**, defina as Configurações de backup necessárias, de acordo com os seus requisitos:

   Na seção **Configurações de backup**:

   - **Pasta de backup**

     Caminho para a pasta de Backup em formato UNC (Universal Naming Convention).

     O caminho padrão é C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Backup\.

   - **Tamanho máximo do backup (MB)**

     Esta caixa de seleção ativa ou desativa a função que monitora o tamanho total de objetos armazenados na pasta da Backup. Se o valor especificado for excedido (o valor padrão sendo 200 MB), o Kaspersky Embedded Systems Security registrará o evento *Tamanho máximo do Backup excedido* e emitirá uma notificação de acordo com as configurações para notificações sobre eventos desse tipo.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security monitorará o tamanho total dos objetos colocados no Backup.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não monitorará o tamanho total dos objetos colocados no Backup.

     Esta caixa é desmarcada por padrão.

   - **Valor limite de espaço disponível (MB)**

     A caixa de seleção ativa ou desativa a função que monitora a quantidade mínima de espaço livre no backup (o valor padrão sendo 50 MB). Se a quantidade de espaço livre cair para menos do que o limite especificado, o Kaspersky Embedded Systems Security efetuará registrará o evento *Limite de espaço livre no backup excedido* e emitirá uma notificação de acordo com as configurações para notificações sobre eventos desse tipo.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security monitorará a quantidade de espaço livre no backup.

     A caixa de seleção Valor limite de espaço disponível (MB) estará ativa se a caixa de seleção Tamanho máximo do backup (MB) estiver selecionada.

     A caixa de seleção é selecionada por padrão.

   Se o tamanho dos objetos no Backup exceder o tamanho máximo do Backup ou exceder o limite de espaço disponível, o Kaspersky Embedded Systems Security o notificará sobre isto enquanto continua colocando objetos no Backup.

   Na seção **Configurações de restauração**:

   - **Pasta destino para a restauração de objetos**

Caminho para a pasta de restauração de objetos em formato UNC (Universal Naming Convention).

Caminho padrão: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored\.

5. Clique em **OK**.

As definições de Backup configuradas serão salvas.

Estatísticas do backup

Você pode exibir informações sobre o status atual do Backup: Estatísticas do backup.

► *Para exibir as estatísticas do Backup,*

abra o menu de contexto do nó **Backup** na árvore do Console do Aplicativo e selecione **Estatísticas**. A janela **Estatísticas do Backup** é exibida.

A janela **Estatísticas do Backup** exibe informações sobre o status atual do Backup (consulte a tabela abaixo).

Tabela 35. Informações sobre o status atual do Backup

Campo	Descrição
Tamanho de Backup atual	Tamanho dos dados na pasta Backup; o aplicativo calcula o tamanho do arquivo em formato criptografado
Número total de objetos	Número atual total de objetos no Backup

Registro de eventos. Logs do Kaspersky Embedded Systems Security

Esta seção fornece informações sobre o trabalho com os logs do Kaspersky Embedded Systems Security: o log de auditoria do sistema, os logs de execução de tarefa e o log de evento.

Neste capítulo

Modos para registrar eventos do Kaspersky Embedded Systems Security 201

Log de auditoria do sistema..... 202

Logs de tarefas 204

Log de segurança 208

Visualizando o log de eventos do Kaspersky Embedded Systems Security no Visualizador de eventos 208

Definindo configurações de log no Console do Kaspersky Embedded Systems Security..... 209

Modos para registrar eventos do Kaspersky Embedded Systems Security

Os eventos do Kaspersky Embedded Systems Security são divididos em dois grupos:

- Os eventos relacionados com o processamento de objetos em tarefas do Kaspersky Embedded Systems Security.
- Os eventos relacionados à administração do Kaspersky Embedded Systems Security, como inicialização de aplicativo, criação ou exclusão de tarefas ou edição de configurações da tarefa.

O Kaspersky Embedded Systems Security usa os seguintes métodos de registro de eventos em log:

- **Logs de tarefas**. Um Log de tarefas contém informações sobre o status atual da tarefa e os eventos que ocorreram durante sua execução.
- **Log de auditoria do sistema**. O log de auditoria do sistema contém informações sobre eventos relacionados com a administração do Kaspersky Embedded Systems Security.
- **Log de Eventos**. O log de eventos contém informações sobre eventos requeridos para diagnóstico de falhas na operação do Kaspersky Embedded Systems Security. O log de eventos está disponível no Visualizador de Eventos do Microsoft Windows.
- **Log de segurança**. O Log de segurança contém informações sobre eventos associados a violações de segurança ou tentativas de violação de segurança no computador protegido.

Se ocorrer um problema durante a operação do Kaspersky Embedded Systems Security (por exemplo, se o Kaspersky Embedded Systems Security ou uma tarefa individual for encerrada de forma anormal ou não for executada), você poderá criar um arquivo de rastreamento e um despejo de memória de processos do Kaspersky Embedded Systems Security e enviar arquivos com essas informações para análise do Suporte Técnico da Kaspersky Lab para diagnosticar o problema encontrado.

O Kaspersky Embedded Systems Security não envia nenhum arquivo de rastreamento ou de despejo automaticamente. Os dados de diagnóstico só podem ser enviados pelo usuário com as permissões correspondentes.

O Kaspersky Embedded Systems Security grava as informações nos arquivos de rastreamento e no arquivo de despejo no formulário não criptografado. A pasta onde os arquivos são salvos é selecionada pelo usuário e gerenciada pela configuração do sistema operacional e do Kaspersky Embedded Systems Security. Você pode configurar permissões de acesso (consulte a seção "Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security" na página 226) e permitir o acesso a logs, arquivos de rastreamento e de despejo apenas para usuários necessários.

Log de auditoria do sistema

O Kaspersky Embedded Systems Security executa a auditoria de sistema de eventos relacionados à administração do Kaspersky Embedded Systems Security. O aplicativo registra informações sobre, por exemplo, o início do aplicativo, os inícios e interrupções de tarefas do Kaspersky Embedded Systems Security, alterações nas configurações da tarefa, criação e exclusão de tarefas de Verificação por Demanda. Os registros desses eventos são exibidos no painel de detalhes quando você seleciona o nó **Registro de auditoria do sistema** no Console do Aplicativo.

Por padrão, o Kaspersky Embedded Systems Security armazena registros no Log de auditoria do sistema durante um período ilimitado de tempo. Você especifica o período de armazenamento para registros no log de auditoria do sistema.

Você pode especificar uma pasta que será usada pelo Kaspersky Embedded Systems Security para armazenar os arquivos que contêm o Log de auditoria do sistema diferente da pasta padrão.

Nesta seção

Classificando eventos no Log de auditoria do sistema 202
Filtrando eventos no Log de auditoria do sistema 203
Excluir eventos do Log de auditoria do sistema 203

Classificando eventos no Log de auditoria do sistema

Por padrão, os eventos no nó Log de auditoria do sistema são exibidos em ordem cronológica inversa.

Os eventos podem ser classificados de acordo com o conteúdo de qualquer coluna, exceto da coluna **Evento** .

► *Para classificar eventos no Log de auditoria do sistema:*

1. Na árvore do Console do Aplicativo, expanda o nó **Logs e notificações**.
2. Selecione o nó filho **Log de auditoria do sistema**.

3. No painel de detalhes, selecione o título da coluna que você deseja usar para classificar eventos na lista.

   Os resultados classificados serão salvos até sua próxima sessão de visualização no Log de auditoria do sistema.

Filtrando eventos no Log de auditoria do sistema

Você pode configurar o Log de auditoria do sistema para exibir somente os registros de eventos que satisfazem as condições de filtragem (filtros) especificados.

► *Para filtrar eventos no Log de auditoria do sistema, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Logs e notificações**.
2. Abra o menu de contexto do nó filho **Log de auditoria do sistema** e selecione **Filtrar**.

   A janela **Configurações de filtro** é exibida.
3. Para adicionar um filtro, execute os passos que se seguem:
   a. Na lista **Nome do campo**, selecione uma coluna para filtrar os eventos.
   b. Na lista **Operador**, selecione a condição de filtragem. As condições de filtragem variam dependendo do item selecionado na lista **Nome do campo**.
   c. Na lista **Valor do campo**, selecione um valor para o filtro.
   d. Clique no botão **Adicionar**.

      O filtro que adicionou será exibido na lista de filtros, na janela **Configurações de filtro**.
4. Se necessário, execute uma das seguintes ações:
   - Se você desejar combinar vários filtros usando o operador lógico "AND", selecione **Se todas as condições forem atendidas**.
   - Se você desejar combinar vários filtros usando o operador lógico "OR", selecione **Se alguma condição for atendida**.
5. Clique no botão **Aplicar** para salvar as condições de filtragem no log de auditoria do sistema.

   A lista de eventos do Log de auditoria do sistema exibe somente os eventos que atendem às condições do filtro. Os resultados filtrados serão salvos até sua próxima sessão de visualização no Log de auditoria do sistema.

► *Para desativar o filtro:*

1. Na árvore do Console do Aplicativo, expanda o nó **Logs e notificações**.
2. Abra o menu de contexto do nó filho **Log de auditoria do sistema** e selecione **Remover filtro**.

   A lista de eventos do Log de auditoria do sistema exibirá então todos os eventos.

Excluir eventos do Log de auditoria do sistema

Por padrão, o Kaspersky Embedded Systems Security armazena registros no log de auditoria do sistema durante um período ilimitado de tempo. Você especifica o período de armazenamento para registros no log de auditoria do sistema.

É possível excluir manualmente todos os eventos do Log de auditoria do sistema.

► *Para excluir eventos do Log de auditoria do sistema:*

1. Na árvore do Console do Aplicativo, expanda o nó **Logs e notificações**.
2. Abra o menu de contexto do nó filho **Log de auditoria do sistema** e selecione **Limpar**.
3. Execute uma das seguintes etapas:
   - Se você desejar salvar o conteúdo do log como um arquivo em formato CSV ou TXT antes de excluir eventos do log de auditoria do sistema, clique no botão **Sim** na janela de confirmação de exclusão. Na janela que é exibida, especifique o nome e a localização do arquivo.
   - Se você não desejar salvar o conteúdo do log como um arquivo, clique no botão **Não** na janela de confirmação de exclusão.

O Log de auditoria do sistema será limpo.

Logs de tarefas

Essa seção fornece informações sobre logs de tarefas do Kaspersky Embedded Systems Security e instruções sobre como gerenciá-los.

Nesta seção

Sobre os Logs de tarefas....204
Visualizando a lista de eventos em Logs de tarefas....205
Classificando eventos em Logs de tarefas....205
Filtrar eventos em Logs de tarefas....205
Visualizando estatísticas e informações sobre uma tarefa do Kaspersky Embedded Systems Security em logs de tarefas....206
Exportando informações de um Log de tarefas....206
Excluindo eventos de Logs de tarefas....207

Sobre os Logs de tarefas

As informações sobre a execução de tarefas do Kaspersky Embedded Systems Security são exibidas no painel de detalhes ao selecionar o nó **Logs de tarefas** no Console do Aplicativo.

No log de cada tarefa, você pode exibir as estatísticas da execução da tarefa, os detalhes de cada um dos objetos que foram processados pelo aplicativo desde o início da tarefa até o momento atual e as configurações da tarefa.

Por padrão, o Kaspersky Embedded Systems Security armazena registros em logs de tarefas durante 30 dias a partir da conclusão da tarefa. Você pode alterar o período de armazenamento de registros em Logs de tarefas.

Você pode especificar uma pasta que será usada pelo Kaspersky Embedded Systems Security para armazenar os arquivos que contêm os logs de tarefas diferente da pasta padrão. Você pode também selecionar eventos que o Kaspersky Embedded Systems Security registrará nos logs de tarefas.

Visualizando a lista de eventos em Logs de tarefas

► *Para visualizar a lista de eventos em Logs de tarefas:*

1. Na árvore do Console do Aplicativo, expanda o nó **Logs e notificações**.
2. Selecione o subnó **Logs de tarefas**.

A lista de eventos salvos em Logs de tarefas do Kaspersky Embedded Systems Security será exibida no painel de resultados.

Os eventos podem ser classificados ou filtrados por qualquer outra coluna.

Classificando eventos em Logs de tarefas

Por padrão, os eventos em Logs de tarefas são exibidos por ordem cronológica inversa. Eles podem ser classificados por qualquer coluna.

► *Para classificar eventos em Logs de tarefas:*

1. Na árvore do Console do Aplicativo, expanda o nó **Logs e notificações**.
2. Selecione o subnó **Logs de tarefas**.
3. No painel de detalhes, selecione o título da coluna que deseja usar para classificar eventos nos Logs de tarefas do Kaspersky Embedded Systems Security.

Os resultados classificados serão salvos até sua próxima sessão de visualização nos Logs de tarefas.

Filtrar eventos em Logs de tarefas

Você pode configurar a lista de Logs de tarefas para que exiba somente os registros de eventos que correspondem às condições de filtragem (filtros) que você especificou.

► *Para filtrar eventos nos Logs de tarefas:*

1. Na árvore do Console do Aplicativo, expanda o nó **Logs e notificações**.
2. Abra o menu de contexto do nó filho **Logs de tarefas** e selecione **Filtrar**.

   A janela **Configurações de filtro** é exibida.
3. Para adicionar um filtro, execute os passos que se seguem:
   a. Na lista **Nome do campo**, selecione uma coluna para filtrar os eventos.
   b. Na lista **Operador**, selecione a condição de filtragem. As condições de filtragem variam dependendo do item selecionado na lista **Nome do campo**.
   c. Na lista **Valor do campo**, selecione um valor para o filtro.
   d. Clique no botão **Adicionar**.

      O filtro que adicionou será exibido na lista de filtros, na janela **Configurações de filtro**.
4. Se necessário, execute uma das seguintes ações:
   - Se você desejar combinar vários filtros usando o operador lógico "AND", selecione **Se todas as condições forem atendidas**.
   - Se você desejar combinar vários filtros usando o operador lógico "OR", selecione **Se alguma condição**

for atendida.

5. Clique no botão **Aplicar** para salvar as condições de filtragem na lista de Logs de tarefas.

A lista de eventos de logs de tarefas exibe somente os eventos que atendem às condições do filtro. Os resultados filtrados serão salvos até sua próxima sessão de visualização nos Logs de tarefas.

► *Para desativar o filtro:*

1. Na árvore do Console do Aplicativo, expanda o nó **Logs e notificações**.
2. Abra o menu de contexto do nó filho **Logs de tarefas** e selecione **Remover filtro**.

A lista de eventos dos Logs de tarefas exibirá então todos os eventos.

Visualizando estatísticas e informações sobre uma tarefa do Kaspersky Embedded Systems Security em logs de tarefas

Nos logs de tarefas, você pode visualizar informações detalhadas sobre todos os eventos que ocorreram em tarefas desde que foram iniciados até ao momento atual, bem como estatísticas de execução da tarefa e configurações da tarefa.

► *Para visualizar estatísticas e informações sobre uma tarefa do Kaspersky Embedded Systems Security:*

1. Na árvore do Console do Aplicativo, expanda o nó **Logs e notificações**.
2. Selecione o subnó **Logs de tarefas**.
3. No painel de resultados, abra a janela **Logs** usando um dos seguintes métodos:
   - Clique duas vezes no evento que ocorreu na tarefa cujo log você deseja visualizar.
   - Abra o menu de contexto do evento que ocorreu na tarefa cujo log você deseja visualizar e selecione **Exibir log**.
4. Na janela que é aberta, são exibidos os seguintes detalhes:
   - A guia **Estatísticas** exibe a hora de início e conclusão da tarefa, bem como as suas estatísticas.
   - A guia **Eventos** exibe uma lista de eventos que foram registrados durante a execução da tarefa.
   - A guia **Opções** exibe as configurações da tarefa.
5. Se necessário, clique no botão **Filtrar** para filtrar os eventos no log de tarefas.
6. Se necessário, clique no botão **Exportar** para exportar dados do log de tarefas para um arquivo em formato CSV ou TXT.
7. Pressione o botão **Fechar**.

A janela **Logs** será fechada.

Exportando informações de um Log de tarefas

Você pode exportar dados de um log de tarefas para um arquivo em formato CSV ou TXT.

► *Para exportar dados de um log de tarefas:*

1. Na árvore do Console do Aplicativo, expanda o nó **Logs e notificações**.
2. Selecione o subnó **Logs de tarefas**.
3. No painel de resultados, abra a janela **Logs** usando um dos seguintes métodos:
   - Clique duas vezes no evento que ocorreu na tarefa cujo log você deseja visualizar.
   - Abra o menu de contexto do evento que ocorreu na tarefa cujo log você deseja visualizar e selecione **Exibir log**.
4. Na parte inferior da janela **Logs**, clique no botão **Exportar**.

   A janela **Salvar como** é exibida.
5. Especifique o nome, a localização, o tipo e a codificação do arquivo para o qual você deseja exportar dados do log de tarefas.
6. Clique no botão **Salvar**.

As configurações especificadas são salvas.

Excluindo eventos de Logs de tarefas

Por padrão, o Kaspersky Embedded Systems Security armazena registros em logs de tarefas durante 30 dias a partir da conclusão da tarefa. Você pode alterar o período de armazenamento de registros em Logs de tarefas.

Você pode excluir manualmente todos os eventos de Logs de tarefas que já foram concluídas para o momento presente.

Eventos de Logs de tarefas em execução e tarefas usadas por outros usuários não serão excluídos.

► *Para excluir os eventos de Logs de tarefas:*

1. Na árvore do Console do Aplicativo, expanda o nó **Logs e notificações**.
2. Selecione o subnó **Logs de tarefas**.
3. Execute uma das seguintes etapas:
   - Se você desejar excluir os eventos dos logs de todas as tarefas que já foram concluídas para o momento atual, abra o menu de contexto do nó filho **Logs de tarefas** e selecione **Limpar**.
   - Se você quiser limpar o log de uma tarefa individual, no painel de detalhes, abra o menu de contexto de um evento que ocorreu na tarefa para a qual você deseja limpar o log e selecione **Remover**.
   - Se quiser limpar os logs de várias tarefas:
     a. No painel de detalhes, use as teclas **Ctrl** ou **Shift** para selecionar eventos que ocorreram nas tarefas para as quais você deseja limpar os logs.
     b. Abra o menu de contexto de qualquer evento selecionado e selecione **Remover**.
4. Clique no botão **Sim** na janela de confirmação de exclusão para confirmar que você deseja excluir os logs.

Os logs de tarefas selecionados serão limpos. A exclusão de eventos dos Logs de tarefas será registrada no Log de auditoria do sistema.

Log de segurança

O Kaspersky Embedded Systems Security mantém um log de eventos associados a violações de segurança ou tentativas de violação no computador protegido. Os eventos a seguir são registrados nesse log:

- Eventos de Prevenção de Exploits.
- Eventos críticos de Inspeção de Log.
- Eventos críticos que indicam uma tentativa de violação de segurança (para as tarefas de Proteção do Computador em Tempo Real, Verificação por Demanda, Monitor de Integridade de Arquivos, Controle de Inicialização de Aplicativos e Controle de Dispositivos).

Você pode limpar o Log de segurança bem como o Log de auditoria do sistema (consulte a seção "Para excluir eventos do Log de auditoria do sistema" na página 203). Além disso, o Kaspersky Embedded Systems Security registra eventos de auditoria do sistema relativos à exclusão do Log de segurança.

Visualizando o log de eventos do Kaspersky Embedded Systems Security no Visualizador de eventos

Você pode exibir o log de evento do Kaspersky Embedded Systems Security usando o snap-in Visualizador de Eventos do Microsoft Windows para o Console de Gerenciamento Microsoft. O log contém eventos registrados pelo Kaspersky Embedded Systems Security e requeridos para diagnóstico de falhas em sua operação.

Os eventos que serão registrados no Log de eventos podem ser selecionados de acordo com os seguintes critérios:

- **por tipos de eventos**
- **por nível de detalhamento**. O nível de detalhamento corresponde ao nível de importância dos eventos registrados no log (eventos informativos, importantes ou críticos). O mais detalhado é o nível de Eventos informativos, que registra todos os eventos, e o menos detalhado é o nível de Eventos críticos, que registra apenas os eventos críticos. Por padrão, todos os componentes, exceto o componente Atualização, têm o nível de detalhamento Eventos importantes selecionado (apenas os eventos importantes e críticos são registrados em log); para o componente Atualização, está selecionado o nível Eventos informativos.

► *Para visualizar o log de eventos do Kaspersky Embedded Systems Security:*

1. Clique no botão **Iniciar**, insira o comando `mmc` na barra de pesquisa e pressione **ENTER**.

   A janela do Console de Gerenciamento da Microsoft é exibida.

2. Selecione **Arquivo** > **Adicionar ou remover snap-in**.

   A janela **Adicionar ou remover snap-ins** é aberta.

3. Na lista de snap-ins disponíveis, selecione o snap-in **Visualizador de Eventos** e clique no botão **Adicionar**.

   A janela **Selecionar computador** é exibida.

4. Na janela **Selecionar computador**, especifique o computador no qual o Kaspersky Embedded Systems Security está instalado e clique em **OK**.

5. Na janela **Adicionar e remover snap-ins**, clique em **OK**.

   Na árvore do Console de Gerenciamento da Microsoft, o nó **Visualizador de Eventos** aparece.

6. Expanda o nó **Visualizador de Eventos** e selecione o nó filho **Logs de Aplicativos e Serviços** >

Kaspersky Embedded Systems Security.

O log de evento do Kaspersky Embedded Systems Security é exibido.

Definindo configurações de log no Console do Kaspersky Embedded Systems Security

Você pode editar as configurações seguintes de logs do Kaspersky Embedded Systems Security:

- Duração do período de armazenamento para eventos em logs de tarefas e no log de auditoria do sistema.
- Localização da pasta onde o Kaspersky Embedded Systems Security armazena arquivos de logs de tarefas e do log de auditoria do sistema.
- Limites de geração de evento para *O banco de dados do aplicativo está desatualizado*, *O banco de dados do aplicativo está muito desatualizado* e *A verificação de áreas críticas não é realizada há muito tempo*
- Eventos que o Kaspersky Embedded Systems Security salva em logs de tarefas, no log de auditoria do sistema e no log de eventos do Kaspersky Embedded Systems Security no Visualizador de eventos.
- Configurações para publicar eventos de auditoria e eventos de desempenho de tarefa para o servidor syslog através do protocolo Syslog.

► *Para configurar os logs do Kaspersky Embedded Systems Security, execute as seguintes etapas:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Logs e notificações** e selecione **Propriedades**.

   A janela **Configurações de logs e notificações** é aberta.

2. Na janela **Logs e notificações**, configure os logs de acordo com as suas necessidades. Para isso, execute as seguintes ações:

   - Na guia **Geral**, se necessário, selecione os eventos que o Kaspersky Embedded Systems Security salvará em logs de tarefas, no log de auditoria do sistema e no log de eventos do Kaspersky Embedded Systems Security no Visualizador de eventos. Para isso, execute as seguintes ações:

     - Na lista **Componente**, selecione o componente do Kaspersky Embedded Systems Security para o qual você deseja configurar o nível de detalhe.

       Para os componentes Proteção de Arquivos em Tempo Real, Verificação por Demanda e Atualização, é fornecido o registro de eventos por meio de logs de tarefas e do log de evento. Para esses componentes, a tabela de lista de eventos contém as colunas **Log de tarefas** e **Log de eventos do Windows**. Os eventos dos componentes Quarentena e Backup são registrados no log de auditoria do sistema e no log de eventos. Para esses componentes, a tabela de lista de eventos contém as colunas **Auditoria** e **Log de eventos do Windows**.

     - Na lista **Nível de importância**, selecione um nível de detalhe para eventos em logs de tarefas, no Log de auditoria do sistema e no log de eventos para o componente selecionado.

       Na tabela seguinte com uma lista de eventos, as caixas de seleção são marcadas junto de eventos registrados em logs de tarefas, no log de auditoria do sistema e no log de eventos, de acordo com o nível de detalhe atual.

     - Se você desejar apagar manualmente o registro de eventos específicos para um componente selecionado, execute as ações seguintes:

a. Na lista **Nível de importância**, selecione **Personalizado**.

b. Na tabela com a lista de eventos, selecione as caixas de seleção junto dos eventos que você deseja que sejam registrados em logs de tarefas, no log de auditoria do sistema e no log de eventos.

- Na guia **Avançado**, defina as configurações de armazenamento de logs e os Limites de geração de evento para o status de proteção do computador:
  - Na seção **Armazenamento de logs**:
    - **Pasta de logs**

      Caminho para a pasta de log em formato UNC (Universal Naming Convention).

      Caminho padrão: C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports\.

      Se o caminho padrão for alterado, uma pasta com nome correspondente é criada. Os novos logs serão armazenados na nova pasta. Os logs antigos serão mantidos.

    - **Remover logs de tarefas com mais de (dias)**

      A caixa de seleção ativa/desativa uma função que exclui os logs com os resultados da execução de tarefas concluídas e eventos publicados em logs de execução de tarefas após o período de tempo especificado (valor padrão: 30 dias).

      Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security excluirá os logs com os resultados da execução de tarefas completadas e eventos publicados nos logs de tarefas em execução após um período de tempo especificado.

      A caixa de seleção é selecionada por padrão.

    - **Remover do sistema eventos de log de auditoria com mais de (dias)**

      A caixa de seleção ativa/desativa uma função que exclui eventos gravados no log de auditoria do sistema após um período de tempo especificado (valor padrão: 60 dias).

      Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security excluirá os eventos gravados no log de auditoria do sistema após o período de tempo especificado.

      Esta caixa é desmarcada por padrão.

  - Na seção **Limites de geração de evento**:
    - Especifique o número de dias após os quais os eventos *O banco de dados do aplicativo está desatualizado*, *O banco de dados do aplicativo está muito desatualizado* e *A verificação de áreas críticas não é realizada há muito tempo* ocorrerão.

Tabela 36. Limites de geração de evento

Configuração	Limites de geração de evento.
Descrição	Você pode especificar limites para a geração dos seguintes tipos de evento: *O banco de dados do aplicativo está desatualizado* e *O banco de dados do aplicativo está muito desatualizado*. Este evento ocorrerá se o banco de dados do Kaspersky Embedded Systems Security não tiver sido atualizado durante o período (em dias) especificado pela configuração deste a data de lançamento das atualizações do banco de dados instaladas mais recentemente. Você pode configurar as notificações do administrador sobre este evento. *A verificação de áreas críticas não é realizada há muito tempo*. Este evento ocorre se nenhuma das tarefas marcadas com a caixa de seleção **Considerar tarefa como Verificação de Áreas Críticas** for executada durante o número especificado de dias.
Valores possíveis	Número de dias de 1 a 365.
Valor padrão	Os bancos de dados do aplicativo estão obsoletos – 7 dias. Os bancos de dados do aplicativo estão muito desatualizados – 14 dias. A verificação de áreas críticas não é realizada há muito tempo – 30 dias.

- Na guia **Integração SIEM**, defina as configurações para publicar eventos de auditoria e eventos de desempenho de tarefa no servidor syslog (consulte a seção "Definições das configurações de integração SIEM" na página 212).

3. Clique em **OK** para salvar as modificações.

Nesta seção

Sobre a integração SIEM.....211

Definições das configurações de integração SIEM.....212

Sobre a integração SIEM

Para reduzir a carga nos dispositivos de baixo desempenho e reduzir o risco de degradação do sistema como resultado de maiores volumes de logs de aplicativo, é possível configurar a publicação de eventos de auditoria e de desempenho de tarefa para o *servidor syslog* por meio do protocolo Syslog.

Um servidor syslog é um servidor externo para eventos de agregação (SIEM). Ele coleta e analisa eventos recebidos e também executa outras ações de gerenciamento de logs.

É possível usar a integração SIEM de duas maneiras:

- Eventos duplicados no servidor syslog: este modo prescreve que todos os eventos de realização de tarefa cuja publicação esteja definida nas configurações de logs bem como todos os eventos de auditoria do sistema continuem a ser armazenados no computador local mesmo após terem sido enviados ao SIEM.

  Recomenda-se que esse modo seja utilizado para reduzir ao máximo a carga no computador protegido.

- Excluir cópias locais de eventos: este modo prescreve que todos os eventos registrados durante a operação do aplicativo e publicados no SIEM serão excluídos do computador local.

O aplicativo nunca exclui versões locais do log de segurança.

O Kaspersky Embedded Systems Security pode converter eventos em logs de aplicativo em formatos compatíveis com o servidor syslog para que esses eventos possam ser transmitidos e reconhecidos com sucesso pelo SIEM. O aplicativo é compatível com a conversão para um formato de dados estruturados e para o formato JSON.

Recomenda-se selecionar o formato de eventos com base na configuração do SIEM utilizado.

Configurações de confiabilidade

É possível reduzir o risco de retransmissão malsucedida de eventos ao SIEM definindo as configurações para conectar ao servidor syslog espelho.

Um servidor syslog de espelhamento adicional para o qual o aplicativo se alterna automaticamente se a conexão ao servidor principal syslog estiver indisponível ou se o servidor principal não puder ser utilizado.

O Kaspersky Embedded Systems Security também notifica você sobre tentativas malsucedidas de conectar-se ao SIEM e sobre erros ao enviar eventos ao SIEM usando eventos de auditoria do sistema.

Definições das configurações de integração SIEM

Por padrão, a integração SIEM não é utilizada. É possível ativar e desativar a integração SIEM e definir as configurações de funcionalidade (consulte a tabela abaixo).

Tabela 37. Configurações de integração SIEM

Configuração	Valor padrão	Descrição
Enviar eventos para um servidor syslog remoto pelo protocolo syslog	Não aplicado	É possível ativar ou desativar a integração SIEM marcando ou desmarcando a caixa de seleção, respectivamente.
Remover cópias locais dos eventos que foram enviados para um servidor syslog remoto	Não aplicado	É possível definir as configurações para armazenar as cópias locais dos logs após eles terem sido enviados ao SIEM marcando ou desmarcando a caixa de seleção.
Formato dos eventos	Dados estruturados	É possível selecionar um de dois formatos nos quais o aplicativo converte seus eventos antes de enviá-los ao servidor syslog para um melhor reconhecimento desses eventos pelo SIEM.
Protocolo de conexão	TCP	É possível usar a lista suspensa para configurar a conexão com o servidor syslog principal e o refletido através dos protocolos UDP ou TCP.
Configurações de conexão do servidor syslog principal	Endereço IP: 127.0.0.1 Porta: 514	Você pode usar os campos apropriados para configurar o endereço IP e a porta usados para conectar-se ao servidor syslog principal. É possível especificar o endereço IP somente no formato IPv4.

Use um servidor syslog de espelhamento se o servidor principal não estiver acessível	Não aplicado	É possível usar a caixa de seleção para ativar ou desativar o uso de um servidor syslog refletido.
Configurações de conexão do servidor syslog de espelhamento	Endereço IP: 127.0.0.1 Porta: 514	Você pode usar os campos apropriados para configurar o endereço IP e a porta usados para conectar-se ao servidor syslog de espelhamento. É possível especificar o endereço IP somente no formato IPv4.

► *Para definir as configurações de integração SIEM:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Logs e notificações**.
2. Selecione **Propriedades**.

   A janela **Configurações de logs e notificações** é aberta.
3. Selecione a guia **Integração SIEM**.
4. Na seção **Configurações de integração**, marque a caixa de seleção **Enviar eventos para um servidor syslog remoto pelo protocolo syslog**.

   A caixa de seleção ativa ou desativa a funcionalidade de envio de eventos publicados a um servidor syslog externo.

   Se a caixa de seleção for selecionada, o aplicativo enviará eventos publicados ao SIEM de acordo com as configurações de integração SIEM definidas.

   Se a caixa de seleção for desmarcada, o aplicativo não executará a integração SIEM. Não é possível definir as configurações de integração SIEM se a caixa de seleção for desmarcada.

   Esta caixa é desmarcada por padrão.
5. Se necessário, na seção **Configurações de integração**, marque a caixa de seleção **Remover cópias locais dos eventos que foram enviados para um servidor syslog remoto**.

   A caixa de seleção ativa ou desativa a exclusão de cópias locais de logs quando eles são enviados para o SIEM.

   Se a caixa de seleção for marcada, o aplicativo exclui cópias locais de eventos depois que eles tiverem sido publicados com sucesso no SIEM. Este modo é recomendado em computadores com desempenho limitado.

   Se a caixa de seleção for desmarcada, o aplicativo apenas enviará os eventos para o SIEM. As cópias de logs continuam sendo armazenadas localmente.

   Esta caixa é desmarcada por padrão.

   O status da caixa de seleção **Remover cópias locais dos eventos que foram enviados para um servidor syslog remoto** não afeta as configurações de armazenamento de eventos do log de segurança: o aplicativo nunca exclui automaticamente os eventos de log de segurança.
6. Na seção **Formato dos eventos**, especifique o formato para o qual deseja converter eventos de operação do aplicativo para que sejam enviados ao SIEM.

   Por padrão, o aplicativo converte-os em um formato de dados estruturados.

7. Na seção **Configurações de conexão**:
   - Especifique o protocolo de conexão SIEM.
   - Especifique as configurações para a conexão com o servidor syslog principal.

     É possível especificar um endereço IP somente no formato IPv4.
   - Marque a caixa de seleção **Use um servidor syslog de espelhamento se o servidor principal não estiver acessível** se desejar que o aplicativo use outras configurações de conexão quando não for possível enviar eventos para o servidor syslog principal.
     - Especifique as seguintes configurações para a conexão com o servidor syslog de espelhamento: **Endereço IP** e **Porta**.

       Os campos **endereço IP** e **Porta** do servidor syslog de espelhamento não poderão ser editados se a caixa de seleção **Use um servidor syslog de espelhamento se o servidor principal não estiver acessível** estiver desmarcada.

       É possível especificar um endereço IP somente no formato IPv4.
8. Clique em **OK**.

   As configurações da integração SIEM definidas serão aplicadas.

Configurações de notificação

Essa seção fornece informações sobre as formas em que os usuários e administradores do Kaspersky Embedded Systems Security podem ser notificados sobre eventos do aplicativo e o status de proteção do computador, bem como instruções sobre como configurar notificações.

Neste capítulo

Métodos de notificação do administrador e dos usuários 215

Configurando notificações do administrador e dos usuários 216

Métodos de notificação do administrador e dos usuários

Você pode configurar o aplicativo para notificar o administrador e os usuários que acessam o computador protegido sobre eventos na operação do Kaspersky Embedded Systems Security e no status da proteção de antivírus no computador.

O aplicativo assegura o desempenho das seguintes tarefas:

- O administrador pode receber informações sobre eventos de tipos selecionados.
- Os usuários de LAN que acessam um computador protegido e os usuários do computador de terminal podem receber informações sobre eventos do tipo *Objeto detectado* na tarefa Proteção de Arquivos em Tempo Real.

No Console do Aplicativo, as notificações de administrador ou usuário podem ser ativadas usando vários métodos:

- Métodos de notificação do usuário:
  a. Ferramentas do serviço de terminal.

     Você pode aplicar esse método para notificar usuários do computador terminal se o computador protegido for usado como terminal.

  b. Ferramentas do serviço de mensagem.

     Você pode aplicar esse método para notificação através de serviços de mensagens do Microsoft Windows.
- Métodos de notificação do administrador:
  a. Ferramentas do serviço de mensagem.

     Você pode aplicar esse método para notificação através de serviços de mensagens do Microsoft Windows.

  b. Executando um arquivo executável.

     Esse método executa um arquivo executável armazenado na unidade local do computador protegido quando o evento ocorre.

  c. Enviar por e-mail.

     Esse método usa e-mail para transmitir mensagens.

Você pode criar mensagens para tipos de eventos individuais. Elas podem incluir um campo de informações para

descrever um evento. Por padrão, o aplicativo usa um texto predefinido para notificar os usuários.

Configurando notificações do administrador e dos usuários

As configurações de notificação de eventos oferecem opções de métodos para configurar e compor uma mensagem.

► *Para configurar a notificação de eventos, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Logs e notificações** e selecione **Propriedades**.

   A janela **Configurações de Logs e notificações** é aberta.

2. Na guia **Notificações**, selecione o modo de notificação:

   a. Selecione o evento para o qual você deseja selecionar um método de notificação na lista **Tipo de evento**.

   b. Nas configurações de grupo **Notificar administradores** ou **Notificar usuários** , selecione a caixa de seleção junto aos métodos de notificação que deseja configurar.

   > Você pode configurar notificações de usuário apenas para os eventos **Objeto detectado**, **Armazenamento em massa não confiável detectado e restringido** e **Host listado como não confiável**.

3. Para adicionar o texto de uma mensagem:

   a. Clique no botão **Texto da mensagem**.

   b. Na janela que se abre, insira o texto a ser exibido no evento de mensagem correspondente.

   > Você pode criar um texto de mensagem para vários tipos de eventos: após selecionar um método de notificação para um tipo de evento, selecione os outros tipos de eventos para os quais deseja usar o mesmo texto de mensagem usando a tecla **Ctrl** ou **Shift** e, em seguida, clique no botão **Texto da mensagem**.

   c. Para adicionar campos com informações sobre um evento, clique no botão **Macro** e selecione os campos relevantes na lista suspensa. Os campos com informações do evento estão descritos na tabela nesta seção.

   d. Para restaurar o texto padrão da mensagem de evento, clique no botão **Por padrão**.

4. Para configurar os métodos selecionados de notificação de administradores do evento selecionado, selecione a guia **Notificações**, clique no botão **Configurações** na seção **Notificar administradores** e configure os métodos selecionados na janela **Configurações avançadas**. Para isso, execute as seguintes ações:

   a. Para notificações por e-mail, abra a guia **E-mail** e especifique os endereços de e-mail de destinatários (separe os endereços com ponto e vírgula), nome ou endereço de rede do servidor SMTP e número da porta nos campos adequados. Se necessário, especifique o texto que será exibido nos campos **Assunto** e **De**. O texto no campo **Assunto** também pode incluir variáveis com informações sobre o evento (consulte a tabela abaixo).

   Se deseja aplicar a autenticação da conta ao se conectar ao servidor SMTP, selecione **Usar**

autenticação SMTP no grupo **Configurações de autenticação** e especifique o nome e a senha do usuário cuja conta de usuário será autenticada.

b. Para notificações usando **Windows Messenger Service**, crie uma lista de computadores destinatários de notificações na guia **Windows Messenger Service**: para cada computador que deseja adicionar, pressione o botão **Adicionar** e insira seu nome de rede no campo de entrada.

c. Para executar um arquivo executável, selecione o arquivo em uma unidade local do computador protegido que será executado no computador acionado pelo evento ou insira seu caminho completo na guia **Arquivo executável**. Insira o nome de usuário e a senha que serão usados para executar o arquivo.

   As variáveis de ambiente do sistema podem ser usadas ao especificar o caminho do arquivo executável; não são permitidas variáveis de ambiente do usuário.

   Se você desejar limitar o número de mensagens para um tipo de evento ao longo de um período de tempo, na guia **Avançado** selecione **Não enviar a mesma notificação mais de** e especifique o número de vezes e a unidade de tempo.

5. Clique em **OK**.

As configurações de notificação definidas são salvas.

Tabela 38. Campos com informações de eventos

Variável	Descrição
%EVENT_TYPE%	Tipo de evento.
%EVENT_TIME%	Hora do evento.
%EVENT_SEVERITY%	Nível de importância.
%OBJECT%	Nome do objeto (nas tarefas de Proteção do Computador em Tempo Real e de Verificação por Demanda). A tarefa de Atualização de módulos de software inclui o nome da atualização e o endereço da página da Web com as informações sobre a atualização.
%VIRUS_NAME%	O nome do objeto de acordo com a classificação da Enciclopédia de Vírus https://encyclopedia.kaspersky.com/knowledge/classification/. Esse nome é incluído no nome completo do objeto detectado que o Kaspersky Embedded Systems Security devolve ao detectar um objeto. Você pode visualizar o nome completo do objeto detectado no log de tarefas (consulte a seção "Visualizando estatísticas e informações sobre uma tarefa do Kaspersky Embedded Systems Security em Logs de tarefas" na página 206).
%VIRUS_TYPE%	O tipo de objeto detectado de acordo com a classificação da Kaspersky Lab, como "vírus" ou "Cavalo de troia". É incluído no nome completo do objeto detectado, o qual é devolvido pelo Kaspersky Embedded Systems Security quando identifica um objeto infectado ou possivelmente infectado. Você pode ver o nome completo do objeto excluído no log de tarefas.
%USER_COMPUTER%	Na tarefa de Proteção de arquivos em tempo real, o nome do computador do usuário que acessou o objeto no computador.
%USER_NAME%	Na tarefa Proteção de Arquivos em Tempo Real, o nome do usuário que acessou o objeto no computador.

Variável	Descrição
%FROM_COMPUTER%	Nome do computador protegido no qual a notificação foi gerada.
%EVENT_REASON%	Motivo do evento (alguns eventos não contêm este campo).
%ERROR_CODE%	Código de erro (usado somente para o evento "erro de tarefa interno").
%TASK_NAME%	Nome da tarefa (somente para eventos relacionados ao desempenho de tarefas).

Inicialização e interrupção do Kaspersky Embedded Systems Security

Esta seção contém informações sobre como iniciar o Console do Aplicativo e também como iniciar e interromper o Kaspersky Security Service.

Neste capítulo

Iniciando o Plug-in de Administração do Kaspersky Embedded Systems Security 219
Iniciando o Console do Kaspersky Embedded Systems Security a partir do menu Iniciar 219
Inicialização e interrupção do Kaspersky Security Service 220
Inicialização dos componentes do Kaspersky Embedded Systems Security no modo seguro do sistema operacional 222

Iniciando o Plug-in de Administração do Kaspersky Embedded Systems Security

Nenhuma ação adicional é necessária para iniciar o Plug-in de Administração do Kaspersky Embedded Systems Security no Kaspersky Security Center. Depois que o Plug-in for instalado no computador do administrador, ele é iniciado simultaneamente com o Kaspersky Security Center. Informações detalhadas sobre a inicialização do Kaspersky Security Center podem ser encontradas na *Ajuda do Kaspersky Security Center*.

Iniciando o Console do Kaspersky Embedded Systems Security a partir do menu Iniciar

Os nomes de configurações podem variar em diferentes sistemas operacionais Windows.

► *Para iniciar o Console do Aplicativo a partir do menu **Iniciar**:*

1. No menu **Iniciar**, selecione **Programas** > **Kaspersky Embedded Systems Security** > **Ferramentas de administração** > **Console do Kaspersky Embedded Systems Security**.

Para adicionar outros snap-ins ao Console do Aplicativo, inicie o Console do Aplicativo no modo de autor.

► *Para iniciar o Console do Aplicativo no modo de autor, siga as etapas a seguir:*

1. No menu **Iniciar**, selecione **Programas** > **Kaspersky Embedded Systems Security** > **Ferramentas de administração**.

2. No menu de contexto do Console do Aplicativo, selecione o comando **Autor**.

O Console do Aplicativo é iniciado no modo de autor.

Se o Console do Aplicativo for iniciado no computador protegido, a janela do Console do Aplicativo é exibida.

Se você tiver iniciado o Console do Aplicativo em um computador não protegido, mas em um computador diferente, conecte ao computador protegido.

► *Para conectar a um computador protegido:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Kaspersky Embedded Systems Security**.
2. Selecione o comando **Conectar a outro computador**.

   A janela **Selecionar computador** é exibida.
3. Selecione **Outro computador** na janela exibida.
4. Especifique o nome da rede do computador protegido no campo de inserção à direita.
5. Clique em **OK**.

O Console do Aplicativo será conectado a um computador protegido.

Se a conta de usuário que você está usando para iniciar a sessão no Microsoft Windows não tiver permissões suficientes para acessar o Kaspersky Security Management Service no computador, marque a caixa de seleção **Conectar como usuário** e especifique uma conta de usuário com essas permissões.

Inicialização e interrupção do Kaspersky Security Service

Por padrão, o Kaspersky Security Service é iniciado automaticamente no momento da inicialização do sistema operacional. O Kaspersky Security Service gerencia os processos de trabalho nos quais as tarefas de Proteção do Computador em Tempo Real, Controle do Computador, Verificação por Demanda e Atualização são executadas.

Por padrão, quando o Kaspersky Embedded Systems Security é iniciado, as tarefas de Proteção de Arquivos em Tempo Real e Verificação na Inicialização do Sistema Operacional são iniciadas, bem como outras tarefas que estejam programadas para serem iniciadas **Ao iniciar o aplicativo**.

Se o Kaspersky Security Service for interrompido, todas as tarefas em execução serão interrompidas. Quando você reinicia o Kaspersky Security Service, o aplicativo inicia automaticamente apenas as tarefas cuja programação tem uma frequência de inicialização definida como **Ao iniciar o aplicativo**, enquanto as outras tarefas devem ser iniciadas manualmente.

Você pode iniciar e interromper o Kaspersky Security Service usando o menu de contexto do nó **Kaspersky Embedded Systems Security** ou usando o snap-in do Microsoft Windows Services.

Você pode iniciar e interromper o Kaspersky Embedded Systems Security se for membro do grupo de Administradores no computador protegido.

► *Para interromper ou iniciar o aplicativo usando o Console do Aplicativo, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Kaspersky Embedded Systems**

Security.

2. Selecione um dos seguintes itens:
   - **Interromper o serviço**.
   - **Iniciar o serviço**.

O Kaspersky Security Service será iniciado ou interrompido.

Inicialização dos componentes do Kaspersky Embedded Systems Security no modo seguro do sistema operacional

Esta seção fornece informações sobre o funcionamento do Kaspersky Embedded Systems Security no modo seguro do sistema operacional.

Neste capítulo

Sobre o funcionamento do Kaspersky Embedded Systems Security no modo seguro do sistema operacional 222

Inicialização do Kaspersky Embedded Systems Security no modo seguro 223

Sobre o funcionamento do Kaspersky Embedded Systems Security no modo seguro do sistema operacional

Os componentes do Kaspersky Embedded Systems Security podem ser inicializados no carregamento do sistema operacional no modo seguro. Além do Kaspersky Security Service (kavfs.exe), o driver klam.sys é carregado e usado para registrar o Kaspersky Security Service como um serviço protegido durante a inicialização do sistema operacional. Para obter mais detalhes, consulte a seção Registrar o Kaspersky Security Service como um serviço protegido.

O Kaspersky Embedded Systems Security pode ser iniciado nos seguintes modos seguros do sistema operacional:

- Modo seguro Mínimo – este modo é inicializado quando a opção padrão do modo seguro do sistema operacional é selecionada. Nesse caso, o Kaspersky Embedded Systems Security pode iniciar os seguintes componentes:
  - Proteção de Arquivos em Tempo Real.
  - Verificação por Demanda.
  - Controle de Inicialização de Aplicativos e Gerador de Regras de Controle de Inicialização de Aplicativos.
  - Inspeção de Log.
  - Monitor de Integridade de Arquivos.
  - Controle de Integridade de Aplicativos.
- Modo seguro Rede – este modo é inicializado quando o sistema operacional é carregado no modo seguro com drivers de rede. Além dos componentes iniciados no Modo Seguro Mínimo, o Kaspersky Embedded Systems Security pode iniciar os seguintes componentes:
  - Atualização dos Bancos de Dados.
  - Atualização de módulos de software.

Inicialização do Kaspersky Embedded Systems Security no modo seguro

Por padrão, o Kaspersky Embedded Systems Security não é iniciado ao carregar o sistema operacional no modo seguro.

► *Para fazer com que o Kaspersky Embedded Systems Security seja inicializado no modo seguro do sistema operacional, execute as seguintes ações:*

1. Inicie o editor de registro do Windows (C:\Windows\regedit.exe).
2. Abra a chave [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] do registro de sistema.
3. Abra o parâmetro LoadInSafeMode.
4. Defina o valor `1`.
5. Clique em **OK**.

► *Para cancelar a inicialização do Kaspersky Embedded Systems Security no modo seguro do sistema operacional, execute as seguintes ações:*

1. Inicie o editor de registro do Windows (C:\Windows\regedit.exe).
2. Abra a chave [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] do registro de sistema.
3. Abra o parâmetro LoadInSafeMode.
4. Defina o valor `0`.
5. Clique em **OK**.

Autodefesa do Kaspersky Embedded Systems Security

Esta seção fornece informações sobre os mecanismos de autodefesa do Kaspersky Embedded Systems Security.

Neste capítulo

Sobre a autodefesa do Kaspersky Embedded Systems Security 224

Proteção contra alterações em pastas com componentes do Kaspersky Embedded Systems Security instalados 224

Proteção contra alterações em chaves de registro do Kaspersky Embedded Systems Security 224

Registrar o Kaspersky Security Service como um serviço protegido 225

Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security 226

Sobre a autodefesa do Kaspersky Embedded Systems Security

O Kaspersky Embedded Systems Security contém mecanismos de autodefesa que protegem o aplicativo contra modificação ou exclusão de sua pasta no disco rígido, processos de memória e entradas de registro de sistema.

Proteção contra alterações em pastas com componentes do Kaspersky Embedded Systems Security instalados

O Kaspersky Embedded Systems Security restringe a renomeação e a exclusão de pastas com os componentes do aplicativo instalado para qualquer conta de usuário. Por padrão, os caminhos das pastas de instalação do aplicativo são os seguintes:

- Na versão de 32 bits do Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- Na versão de 64 bits do Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

Proteção contra alterações em chaves de registro do Kaspersky Embedded Systems Security

O Kaspersky Embedded Systems Security restringe direitos de acesso às seguintes chaves e bifurcações de registro, que fornecem o carregamento dos drivers e serviços do aplicativo:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [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] (na versão de 64 bits do Microsoft Windows)
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\Trace]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Trace] (na versão de 64 bits do Microsoft Windows)

Os direitos de alterar essas chaves e bifurcações de registro são concedidos apenas à conta Sistema Local (SYSTEM). As contas de usuário e Administrador são concedidas com direitos somente-leitura.

Registrar o Kaspersky Security Service como um serviço protegido

A tecnologia Processo protegido Superficial (também referido como "PPL") assegura que o sistema operacional só carregue serviços e processos confiáveis. Para um serviço ser executado como serviço protegido, um driver *Early Launch Antimalware* deve ser instalado no computador protegido.

Um driver *Early Launch Antimalware* (também referido como "ELAM") fornece a proteção para os computadores na sua rede quando eles iniciam e antes que drivers de terceiros sejam inicializados.

O driver ELAM é instalado automaticamente durante a instalação do Kaspersky Embedded Systems Security e é usado para registrar o Kaspersky Security Service como PPL quando o sistema operacional é inicializado. Quando o Kaspersky Security Service (KAVFS) é iniciado como um processo protegido do sistema, outros processos não protegidos no sistema não são capazes de injetar threads, gravar na memória virtual do processo protegido ou interromper o serviço.

Quando um processo é iniciado como PPL, ele não pode ser gerenciado pelo usuário desconsiderando as permissões de usuário configuradas. O registro do Kaspersky Security Service como PPL usando o driver ELAM é compatível com o Microsoft Windows 10 e sistemas operacionais posteriores. Se você instalar o Kaspersky Embedded Systems Security em um servidor executando um sistema operacional compatível com PPL, o gerenciamento de permissões para o Kaspersky Security Service (KAVFS) não estará disponível.

► *Para instalar o Kaspersky Embedded Systems Security como PPL, execute o seguinte comando:*

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security

Esta seção contém informações sobre permissões para gerenciar o Kaspersky Embedded Systems Security e os serviços Windows registrados pelo aplicativo, bom como as instruções sobre como configurar essas permissões.

Neste capítulo

Sobre permissões para gerenciar o Kaspersky Embedded Systems Security 226

Sobre permissões de gerenciamento de serviços registrados 228

Sobre permissões para gerenciar o Kaspersky Security Service 228

Sobre permissões de acesso para o Kaspersky Security Management Service 230

Configurando permissões de acesso para gerenciar o Kaspersky Embedded Systems Security e o Kaspersky Security Service 231

Acesso protegido por senha às funções do Kaspersky Embedded Systems Security 233

Configurando permissões de acesso no Kaspersky Security Center 234

Sobre permissões para gerenciar o Kaspersky Embedded Systems Security

Por padrão, o acesso a todas as funções do Kaspersky Embedded Systems Security é concedido aos usuários do grupo Administradores no computador protegido, aos usuários do grupo Administradores de ESS criado no computador protegido durante a instalação do Kaspersky Embedded Systems Security e ao grupo SYSTEM.

Os usuários com acesso à função de Permissões de **Edição** permissões do Kaspersky Embedded Systems Security podem conceder acesso às funções do Kaspersky Embedded Systems Security a outros usuários registrados no computador protegido ou incluídos no domínio.

Os usuários que não estiverem registrados na lista de usuários do Kaspersky Embedded Systems Security não poderão abrir o Console do Aplicativo.

Você pode escolher um dos seguintes níveis predefinidos de acesso para um usuário ou grupo de usuários:

- **Controle total** – acesso a todas as funções do aplicativo: capacidade de visualizar e editar configurações gerais do Kaspersky Embedded Systems Security, configurações de componentes e permissões de usuários do Kaspersky Embedded Systems Security; além de capacidade de visualizar estatísticas do Kaspersky Embedded Systems Security.
- **Editar** - acesso a todas as funções do aplicativo, exceto à edição das permissões de usuário: capacidade de visualizar e editar as configurações gerais do Kaspersky Embedded Systems Security e de componentes do Kaspersky Embedded Systems Security.
- **Ler** – capacidade de visualizar as configurações gerais do Kaspersky Embedded Systems Security, configurações de componentes do Kaspersky Embedded Systems Security, estatísticas do Kaspersky Embedded Systems Security e permissões de usuário do Kaspersky Embedded Systems Security.

Também é possível configurar permissões de acesso avançadas: permitir ou bloquear acesso a funções

específicas do Kaspersky Embedded Systems Security.

Se você tiver configurado manualmente as permissões de acesso para um usuário ou grupo, o nível de acesso **Permissões especiais** será definido para este usuário ou grupo.

Tabela 39. Sobre permissões de acesso para funções do Kaspersky Embedded Systems Security

Direitos de usuário	Descrição
Gerenciamento da tarefa	Capacidade para iniciar/interromper/pausar/reiniciar tarefas do Kaspersky Embedded Systems Security.
Criar e excluir tarefas de Verificação por Demanda	Capacidade para criar e excluir tarefas de Verificação por Demanda.
Editar configurações	Capacidade para: • Importar as configurações do Kaspersky Embedded Systems Security a partir de um arquivo de configuração. • Editar as configurações do aplicativo.
Configurações de leitura	Capacidade para: • Visualizar as configurações gerais e configurações de tarefas do Kaspersky Embedded Systems Security. • Exportar as configurações do Kaspersky Embedded Systems Security para um arquivo de configuração. • Visualizar configurações para logs de tarefas, log de auditoria do sistema e notificações.
Gerenciar repositórios	Capacidade para: • Colocar objetos na Quarentena. • Remover objetos da Quarentena e do Backup. • Restaurar objetos da Quarentena e do Backup.
Gerenciar logs	Capacidade para excluir logs de tarefas e limpar o log de auditoria do sistema.
Ler logs	Capacidade para visualizar eventos do Antivírus em logs de tarefas e no log de auditoria do sistema.
Ler estatísticas	Capacidade de visualizar estatísticas de cada tarefa do Kaspersky Embedded Systems Security.
Licenciamento do aplicativo	Capacidade de ativar o Kaspersky Embedded Systems Security.
Desinstalar o aplicativo	Capacidade de desinstalar o Kaspersky Embedded Systems Security.
Permissões de leitura	Capacidade de visualizar a lista de usuários do Kaspersky Embedded Systems Security e privilégios de acesso dos usuários.
Permissões de edição	Capacidade para: • Editar a lista de usuários com acesso ao gerenciamento de aplicativos. • Editar permissões de acesso de usuário às funções do Kaspersky Embedded Systems Security.

Sobre permissões de gerenciamento de serviços registrados

Durante a instalação, o Kaspersky Embedded Systems Security registra no Windows o Kaspersky Security Service (KAVFS), o Kaspersky Security Management Service (KAVFSGT) e o Kaspersky Security Exploit Prevention (KAVFSSLP).

O registro do Kaspersky Security Service como um processo protegido Superficial usando o driver ELAM é compatível com o Microsoft Windows 10 e sistemas operacionais posteriores. Quando um processo é iniciado como PPL, ele não pode ser gerenciado pelo usuário desconsiderando as permissões de usuário configuradas. Se você instalar o Kaspersky Embedded Systems Security em um computador executando um sistema operacional compatível com PPL, o gerenciamento de permissões para o Kaspersky Security Service (KAVFS) não estará disponível.

Kaspersky Security Service

Por padrão, as permissões de acesso para gerenciar o Kaspersky Security Service são concedidas a usuários no grupo de Administradores no computador protegido, bem como aos grupos SERVICE e INTERACTIVE com permissões de leitura e ao grupo SYSTEM com permissões de leitura e execução.

Os usuários com acesso a funções do nível de permissões de edição (consulte a seção "Acesso protegido por senha às funções do Kaspersky Embedded Systems Security" na página 233) podem conceder permissões de acesso para gerenciar o Kaspersky Security Service a outros usuários registrados no computador protegido ou incluídos no domínio.

Kaspersky Security Management Service

Para gerenciar o aplicativo por meio do Console do Aplicativo instalado em um computador diferente, a conta cujas permissões são usadas para conectar ao Kaspersky Embedded Systems Security deve ter acesso total ao Kaspersky Security Management Service no computador protegido.

Por padrão, o acesso ao Kaspersky Security Management Service é concedido aos usuários do grupo Administradores no computador protegido e aos usuários do grupo Administradores do ESS criado no computador protegido durante a instalação do Kaspersky Embedded Systems Security.

Só é possível gerenciar o Kaspersky Security Management Service por meio do snap-in Serviços do Microsoft Windows.

Kaspersky Security Exploit Prevention

Por padrão, as permissões de acesso para gerenciar o Serviço Security Broker Host Kaspersky são concedidas a usuários no grupo de Administradores no computador protegido, bem como ao grupo SYSTEM com permissões de leitura e execução.

Sobre permissões para gerenciar o Kaspersky Security Service

Durante a instalação, o Kaspersky Embedded Systems Security registra o Kaspersky Security Service (KAVFS) no Windows e ativa internamente componentes funcionais iniciados durante a inicialização do sistema operacional. Para reduzir o risco de acesso de terceiros às funções do aplicativo e configurações de segurança em um computador protegido por meio do gerenciamento do Kaspersky Security Service, você pode restringir as permissões de gerenciamento do Kaspersky Security Service a partir do Console do Aplicativo ou do Plug-in de

Administração.

Por padrão, as permissões de acesso para gerenciar o Kaspersky Security Service são concedidas a usuários no grupo de Administradores no computador protegido. Permissões de leitura são concedidas aos grupos SERVICE e INTERACTIVE e permissões de leitura e execução são concedidas ao grupo SYSTEM.

Não é possível excluir a conta de usuário SYSTEM ou editar permissões para esta conta. Se as permissões da conta SYSTEM forem editadas, os privilégios máximos são restaurados para esta conta ao salvar as alterações.

Os usuários com acesso a funções (consulte a seção "Sobre permissões para gerenciar o Kaspersky Embedded Systems Security" na página 226) que requerem Permissões de edição podem conceder permissões de acesso para gerenciar o Kaspersky Security Service a outros usuários registrados no computador protegido ou incluídos no domínio.

Você pode selecionar um dos seguintes níveis predefinidos de permissões para um usuário ou grupo de usuários do Kaspersky Embedded Systems Security para gerenciar o Kaspersky Security Service:

- **Controle total**: capacidade de visualizar e editar configurações gerais e permissões de usuário para o Kaspersky Security Service e de iniciar e interromper o Kaspersky Security Service.
- **Ler**: capacidade de visualizar as configurações gerais e as permissões de usuário do Kaspersky Security Service.
- **Modificação**: capacidade de visualizar e editar as configurações gerais e as permissões de usuário do Kaspersky Security Service.
- **Execução**: capacidade de iniciar e interromper o Kaspersky Security Service.

É possível configurar as permissões de acesso avançadas: permitir ou negar acesso a funções específicas do Kaspersky Embedded Systems Security (consulte a tabela abaixo).

Se você tiver configurado manualmente as permissões de acesso para um usuário ou grupo, o nível de acesso **Permissões especiais** será definido para este usuário ou grupo.

Tabela 40. Permissões de acesso para as funções do Kaspersky Security Service

Recurso	Descrição
Visualizar configurações de serviço	Capacidade de visualizar as configurações gerais e as permissões de usuário do Kaspersky Security Service.
Solicitar status de serviço do Gerenciador de Controle de Serviço	Capacidade de solicitar o status de execução do Kaspersky Security Service a partir do Gerenciador de Controle de Serviço do Microsoft Windows.
Solicitação de status de serviço	Capacidade de solicitar o status de execução do Kaspersky Security Service.
Ler lista de serviços dependentes	Capacidade de visualizar uma lista de serviços dos quais o Kaspersky Security Service depende e que dependem do Kaspersky Security Service.
Editar configurações de serviço	Capacidade de visualizar e editar as configurações gerais e as permissões de usuário do Kaspersky Security Service.
Iniciar o serviço	Capacidade de iniciar o Kaspersky Security Service.

Recurso	Descrição
Interromper o serviço	Capacidade de interromper o Kaspersky Security Service.
Pausar/Reiniciar o serviço	Capacidade de pausar e reiniciar o Kaspersky Security Service.
Permissões de leitura	Capacidade de visualizar a lista de usuários do Kaspersky Security Service e os privilégios de acesso de cada usuário.
Permissões de edição	Capacidade para: • Adicionar e remover usuários do Kaspersky Security Service. • Editar permissões de acesso de usuários ao Kaspersky Security Service.
Excluir o serviço	Capacidade de anular o registro do Kaspersky Security Service no Gerenciador de Controle de Serviço do Microsoft Windows.
Solicitações ao serviço definidas pelo usuário	Capacidade de criar e enviar solicitações de usuário ao Kaspersky Security Service.

Sobre permissões de acesso para o Kaspersky Security Management Service

Você pode revisar a lista de serviços do Kaspersky Embedded Systems Security.

Durante a instalação, o Kaspersky Embedded Systems Security registra o Kaspersky Security Management Service (KAVFSGT). Para gerenciar o aplicativo por meio do Console do Aplicativo instalado em um computador diferente, a conta usada para conectar ao Kaspersky Embedded Systems Security deve ter acesso total ao Kaspersky Security Management Service no computador protegido.

Por padrão, o acesso ao Kaspersky Security Management Service é concedido aos usuários do grupo Administradores no computador protegido e aos usuários do grupo Administradores de ESS criado no computador protegido durante a instalação do Kaspersky Embedded Systems Security.

Só é possível gerenciar o Kaspersky Security Management Service por meio do snap-in do Microsoft Windows Services.

Você não pode permitir ou bloquear o acesso ao Kaspersky Security Management Service configurando o Kaspersky Embedded Systems Security.

Você pode conectar ao Kaspersky Embedded Systems Security a partir de uma conta local se existir uma conta com o mesmo nome de usuário e senha registrada no computador protegido.

Configurando permissões de acesso para gerenciar o Kaspersky Embedded Systems Security e o Kaspersky Security Service

É possível editar a lista de usuários e grupos de usuário com permissão para acessar as funções do Kaspersky Embedded Systems Security e gerenciar o Kaspersky Security Service. Também é possível editar as permissões de acesso desses usuários e grupos de usuário.

► *Para adicionar ou remover um usuário ou grupo da lista:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e ela bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
4. Na seção **Suplementar**, execute uma das seguintes etapas:
   - Clique em **Configurações** na subseção **Permissões de acesso do usuário para gerenciamento do aplicativo** se desejar editar a lista de usuários que têm permissões de acesso para gerenciar as funções do Kaspersky Embedded Systems Security.
   - Clique em **Configurações**, na subseção **Permissões de acesso do usuário para o Kaspersky Security Management Service** se desejar editar a lista de usuários com permissões de acesso para gerenciar o Kaspersky Security Service.

     A janela **Permissões para o grupo do Kaspersky Embedded Systems Security** é exibida.
5. Na janela exibida, execute as seguintes operações:
   - Para adicionar um usuário ou grupo à lista, clique no botão **Adicionar** e selecione o usuário ou grupo ao qual deseja conceder privilégios.
   - Para remover um usuário ou grupo da lista, selecione o usuário ou grupo cujo acesso deseja restringir e clique no botão **Remover**.
6. Clique no botão **Aplicar**.

Os usuários selecionados (grupos) são adicionados ou removidos.

► *Para editar permissões de um usuário ou grupo para gerenciar o Kaspersky Embedded Systems Security ou o Kaspersky Security Service:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.

2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
4. Na seção **Suplementar**, execute uma das seguintes etapas:
   - Clique em **Configurações** na subseção **Modificar direitos de gerenciamento de aplicativos do usuário** se desejar editar a lista de usuários que têm permissões de acesso para gerenciar as funções do Kaspersky Embedded Systems Security.
   - Clique em **Configurações** na subseção **Modificar direitos do usuário de gerenciamento do Kaspersky Security Service** se desejar editar a lista de usuários que têm permissões de acesso para gerenciar o aplicativo por meio do Kaspersky Security Service.

     A janela **Permissões para o grupo do Kaspersky Embedded Systems Security** é exibida.
5. Na janela exibida, na lista **Grupo ou nomes de usuário**, selecione o usuário ou grupo de usuários de quem você deseja alterar as permissões.
6. Na seção **Permissões para <Usuário (Grupo)>**, selecione as caixas de seleção **Permitir** ou **Negar** para os seguintes níveis de acesso:
   - **Controle total**: conjunto completo de permissões para gerenciar o Kaspersky Embedded Systems Security ou o Kaspersky Security Service.
   - **Ler**:
     - As seguintes permissões para gerenciar o Kaspersky Embedded Systems Security: **Recuperar estatísticas**, **Configurações de leitura**, **Logs de leitura** e **Permissões de leitura**.
     - As seguintes permissões para gerenciar o Kaspersky Security Service: **Ler as configurações de serviço**, **Solicitar status de serviço do Service Control Manager**, **Solicitar status do serviço**, **Ler lista de serviços dependentes**, **Permissões de leitura**.
   - **Modificação**:
     - Todas as permissões para gerenciar o Kaspersky Embedded Systems Security, exceto **Permissões de edição**.
     - As seguintes permissões para gerenciar o Kaspersky Security Service: **Modificar configurações do serviço**, **Permissões de leitura**.
   - **Permissões especiais**: as seguintes permissões para gerenciar o Kaspersky Security Service: **Inicializar serviço**, **Interromper serviço**, **Pausar/Reiniciar serviço**, **Permissões de leitura**, **Solicitações de serviço definidas pelo usuário**.
7. Para configurar permissões avançadas para um usuário ou grupo (**Permissões especiais**), clique no botão **Avançado**.

a. Na janela **Configurações avançadas de segurança para o Kaspersky Embedded Systems Security** exibida, selecione o usuário ou grupo desejado.

b. Clique no botão **Editar**.

c. Na lista suspensa na parte superior da janela, selecione o tipo do controle de acesso (**Permitir** ou **Bloquear**).

d. Selecione as caixas de seleção ao lado das funções que deseja permitir ou bloquear para o usuário ou grupo selecionado.

e. Clique em **OK**.

f. Na janela **Configurações de segurança avançadas para o Kaspersky Embedded Systems Security**, clique em **OK**.

8. Na janela **Permissões para o grupo do Kaspersky Embedded Systems Security**, clique no botão **Aplicar**.
9. As permissões configuradas para o gerenciamento do Kaspersky Embedded Systems Security ou do Kaspersky Security Service são salvas.

Acesso protegido por senha às funções do Kaspersky Embedded Systems Security

Você pode restringir o acesso ao gerenciamento do aplicativo e aos serviços registrados configurando permissões de usuário (consulte a seção "Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security" na página 226). Também é possível estabelecer uma proteção de senha nas configurações do Kaspersky Embedded Systems Security para proteção adicional. A Proteção de senha permite limitar adicionalmente o acesso ao gerenciamento de Console do Aplicativo e a execução de comandos de linha de comando. Se a proteção de senha for aplicada, o Kaspersky Embedded Systems Security determina que todos os usuários insiram a senha ao iniciar o Console do Aplicativo ou executar comandos na linha de comando.

► *Para proteger o acesso às funções do Kaspersky Embedded Systems Security:*

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security** e execute uma das seguintes ações:
   - Clique no link **Propriedades do aplicativo** no painel de detalhes do nó.
   - Selecione **Propriedades** no menu de contexto do nó.

   A janela **Configurações do aplicativo** é exibida.
2. Na guia **Segurança e confiabilidade** em **Configurações de proteção de senha** clique na caixa **Aplicar proteção de senha**.

   Os campos **Senha** e **Confirmar senha** ficam ativos.
3. No campo **Senha**, insira o valor que você deseja utilizar para proteger o acesso às funções do Kaspersky Embedded Systems Security.
4. No campo **Confirmar senha**, insira a sua senha novamente.
5. Clique em **OK**.

Esta senha não pode ser recuperada. A perda da senha resulta na perda completa do controle do aplicativo. Além disso, será impossível desinstalar o aplicativo do computador protegido.

Você pode redefinir a senha a qualquer momento. Para isso, desmarque a caixa **Aplicar proteção de senha** e salve as alterações. A proteção de senha será desativada e a soma de verificação da senha antiga será removida. Repita o processo de entrada de senha com uma senha nova.

Configurando permissões de acesso no Kaspersky Security Center

Você pode configurar permissões de acesso para gerenciar o aplicativo e o Kaspersky Security Service no Kaspersky Security Center para um grupo de computadores ou para um computador separado.

► *Para acessar permissões para gerenciar o aplicativo e o Kaspersky Security Service:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
4. Na seção **Suplementar**, execute as seguintes ações:
   - Para configurar permissões de acesso para gerenciar o Kaspersky Embedded Systems Security para um usuário ou grupo de usuários, na seção **Permissões de acesso do usuário para gerenciamento do aplicativo**, clique no botão **Configurações**.
   - Para configurar permissões de acesso para gerenciar o Kaspersky Security Service para um usuário ou grupo de usuários, na seção **Permissões de acesso do usuário para gerenciamento do Security Service**, clique no botão **Configurações**.
5. Na janela que se abre, configure os privilégios de acesso (consulte a seção "Gerenciamento das permissões de acesso para funções do Kaspersky Embedded Systems Security" na página 226) segundo as suas necessidades.

As configurações especificadas são salvas.

Proteção de Arquivos em Tempo Real

Esta seção contém informações sobre a tarefa de Proteção de Arquivos em Tempo Real e como configurá-la.

Neste capítulo

Sobre a tarefa de Proteção de Arquivos em Tempo Real 235
Sobre o escopo de proteção da tarefa e configurações de segurança 236
Sobre o escopo da proteção virtual 237
Escopos da proteção predefinidos 237
Níveis de segurança predefinidos 238
Extensões de arquivos verificadas por padrão na tarefa de Proteção de Arquivos em Tempo Real 240
Configurações padrão da tarefa de Proteção de arquivos em tempo real 241
Gerenciamento da tarefa de Proteção de Arquivos em Tempo Real por meio do Plug-in de Administração 241
Gerenciamento da tarefa de Proteção de Arquivos em Tempo Real por meio do Console do Aplicativo 256

Sobre a tarefa de Proteção de Arquivos em Tempo Real

Quando a tarefa de Proteção de arquivos em tempo real é executada, o Kaspersky Embedded Systems Security verifica os seguintes objetos do computador protegido quando eles são acessados:

- Arquivos.
- Fluxos alternativos do sistema de arquivos (fluxos NTFS).
- Registros mestre de inicialização e setores de inicialização nos discos rígidos locais e dispositivos externos.

Quando um aplicativo grava um arquivo em um computador ou lê um arquivo a partir dele, o Kaspersky Embedded Systems Security intercepta esse arquivo, verifica se existem ameaças e, se uma ameaça for detectada, executa uma ação padrão ou uma ação especificada por você: tenta desinfectá-lo, move-o para a Quarentena ou o exclui, se a desinfecção não for possível. Antes da desinfecção ou exclusão, o Kaspersky Embedded Systems Security salvará uma cópia criptografada do arquivo fonte na pasta de Backup. O Kaspersky Embedded Systems Security restaura o arquivo da Quarentena na pasta original se ele tiver sido desinfectado com êxito.

O Kaspersky Embedded Systems Security também detecta malware em processos executados sob o Subsistema Windows para Linux®. Para tais processos, a tarefa de Proteção de Arquivos em Tempo Real aplica a ação definida pela configuração atual.

Sobre o escopo de proteção da tarefa e configurações de segurança

Por padrão, a tarefa de Proteção de Arquivos em Tempo Real protege todos os objetos do sistema de arquivos do computador. Se não houver requisito de segurança para proteger todos os objetos do sistema de arquivos ou se você deseja excluir qualquer objeto do escopo de tarefa, é possível limitar o escopo da proteção.

No Console do Aplicativo, o escopo da proteção é exibido como uma árvore ou na lista dos recursos de arquivos de computador que o Kaspersky Embedded Systems Security pode controlar. Por padrão, os recursos de arquivos de rede do computador protegido são exibidos em um modo de visualização em lista.

No Plug-in de Administração, apenas a visão de lista está disponível.

► *Para exibir recursos de arquivos de rede no modo de visualização em árvore no Console do Aplicativo,*

abra a lista suspensa no setor superior esquerdo da janela **Configurações do escopo da proteção** e selecione **Visualização em árvore**.

Os itens ou nós são exibidos em um modo de visualização de lista ou em árvore dos recursos de arquivos de computador, como se segue:

☑ O nó é incluído no escopo da proteção.

☐ O nó é excluído do escopo da proteção.

☑ Pelo menos um dos nós filhos deste nó é excluído do escopo da proteção ou as configurações de segurança dos nós filhos são diferentes da configuração de um nó pai (somente para um modo de visualização em árvore).

O ícone ☑ é exibido se todos os nós filhos forem selecionados, mas se o nó pai não for selecionado. Neste caso, as modificações na composição de arquivos e das pastas do nó pai são desconsideradas automaticamente quando o escopo da proteção para o nó filho selecionado está sendo criado.

Usando o Console do Aplicativo, você também pode acrescentar unidades virtuais (consulte a seção "Criação de escopo da proteção virtual" na página 264) ao escopo de proteção. Os nomes dos nós virtuais são exibidos em azul.

Configurações de segurança

As configurações de segurança de tarefas podem ser definidas como configurações em comum para todos os nós ou itens incluídos no escopo da proteção ou como configurações distintas para cada nó ou item na árvore ou lista de recursos de arquivos do computador.

As configurações de segurança definidas para o nó pai selecionado são automaticamente aplicadas a todos os nós filhos. As configurações de segurança do nó pai não são aplicadas a nós filhos configurados separadamente.

As configurações de um escopo de proteção selecionado podem ser definidas usando um dos seguintes métodos:

- Selecionar um dos três níveis de segurança pré-definidos (na página 238).
- Definição do manual de configurações de segurança (ver a seção "Configuração do manual de

configurações de segurança" na página 249) para os nós ou itens selecionados na árvore de recursos de arquivo ou lista (o nível de segurança é alterado para **Personalizado**).

Um conjunto de configurações de um nó ou item pode ser salvo em um modelo para ser aplicado posteriormente a outros nós ou itens.

Sobre o escopo da proteção virtual

O Kaspersky Embedded Systems Security pode verificar não apenas as pastas e arquivos existentes em discos rígidos e unidades removíveis, mas também unidades criadas dinamicamente no computador por vários aplicativos e serviços.

Se todos os objetos do computador forem incluídos no escopo da proteção, esses nós dinâmicos serão incluídos automaticamente no escopo da proteção. No entanto, se desejar especificar valores especiais para as configurações de segurança desses nós dinâmicos ou se não tiver selecionado o computador inteiro para a proteção, mas apenas algumas áreas dele, para incluir unidades, arquivos ou pastas dinâmicos no escopo da proteção, primeiro será necessário criá-los no Console do Aplicativo, ou seja, especificar o escopo da proteção virtual. As unidades, os arquivos e as pastas criados existirão apenas no Console do Aplicativo e não na estrutura de arquivos do computador protegido.

Se, ao criar um escopo da proteção, todas as subpastas ou arquivos forem selecionados sem que a pasta pai seja selecionada, todas as pastas ou os arquivos dinâmicos que serão exibidos nela não serão incluídos automaticamente no escopo da proteção. "Cópias virtuais" deles devem ser criadas no Console do Aplicativo e adicionadas ao escopo da proteção.

Escopos da proteção predefinidos

A árvore ou a lista de recursos de arquivos exibem os nós aos quais você tem o acesso à leitura com base nas configurações de segurança definidas do Microsoft Windows.

O Kaspersky Embedded Systems Security abrange os seguintes escopos de proteção predefinidos:

- **Discos rígidos locais**. O Kaspersky Embedded Systems Security protege arquivos nos discos rígidos de computador.
- **Unidades removíveis**. O Kaspersky Embedded Systems Security protege arquivos em dispositivos externos, como unidades USB ou em CDs. É possível incluir ou excluir do escopo da proteção todos os discos removíveis, discos, pastas ou arquivos individuais.
- **Rede**. O Kaspersky Embedded Systems Security verifica os arquivos gravados em pastas de redes ou lidos nelas por aplicativos em execução no computador. O Kaspersky Embedded Systems Security não protege os arquivos quando eles são acessados por aplicativos de outros computadores.
- **Unidades virtuais**. Pastas e arquivos dinâmicos, e unidades que são temporariamente conectadas ao computador podem ser incluídos no escopo da proteção, por exemplo, unidades de cluster comuns.

Por padrão, você pode visualizar e configurar escopos da proteção predefinidos na lista de escopo; você também pode adicionar escopos predefinidos à lista durante sua formação nas configurações do escopo da proteção.

Por padrão, o escopo da proteção inclui todas as áreas predefinidas, exceto unidades virtuais.

As unidades virtuais criadas usando o comando SUBST não são exibidas na árvore de recursos de arquivos do computador no Console do Aplicativo. Para incluir objetos da unidade virtual no escopo da proteção, inclua a pasta do computador à qual essa unidade virtual está associada no escopo da proteção.

As unidades de rede conectadas também não serão exibidas na lista de recursos de arquivos do computador. Para incluir objetos das unidades de rede no escopo da proteção, especifique o caminho da pasta que corresponde a essa unidade de rede no formato UNC.

Níveis de segurança predefinidos

Um dos seguintes níveis de segurança predefinidos para os nós selecionados na árvore ou na lista de recursos de arquivo do computador pode ser aplicado: **Desempenho máximo**, **Recomendado** e **Proteção máxima**. Cada um desses níveis contém seu próprio conjunto de configurações de segurança predefinido (veja a tabela abaixo).

Desempenho máximo

O nível de segurança **Desempenho máximo** é recomendado se, além de usar o Kaspersky Embedded Systems Security nos computadores, existirem medidas de segurança adicionais nos computadores da rede como, por exemplo, firewalls e políticas de segurança existentes.

Recomendado

O nível de segurança **Recomendado** assegura uma combinação ideal de impacto de proteção e desempenho nos computadores protegidos. Esse nível é recomendado pelos especialistas da Kaspersky Lab como suficiente para proteger computadores na maioria das redes corporativas. O nível de segurança **Recomendado** é configurado por padrão.

Proteção máxima

O nível de segurança de **Proteção máxima** é recomendado se a rede da sua organização tiver requisitos elevados de segurança para seus computadores.

Tabela 41. Níveis de segurança predefinidos e valores de configurações correspondentes

Opções	Nível de segurança		
	Desempenho máximo	Recomendado	Proteção máxima
Proteção de objetos	Por extensão	Por formato	Por formato
Proteger somente arquivos novos e modificados	Ativado	Ativado	Desativado

Opções	Nível de segurança		
Ação a ser executada em objetos infectados e outros	Bloquear acesso e desinfectar. Remover se a desinfecção falhar	Bloquear acesso e executar ação recomendada	Bloquear acesso e desinfectar. Remover se a desinfecção falhar
Ação a ser executada em objetos possivelmente infectados	Bloquear acesso e colocar na quarentena	Bloquear acesso e executar ação recomendada	Bloquear acesso e colocar na quarentena
Excluir arquivos	Não	Não	Não
Não detectar	Não	Não	Não
Parar a verificação se demorar mais que (s)	60 seg.	60 seg.	60 seg.
Não verificar obj. compostos com mais de (MB)	8 MB	8 MB	Não definido
Verificar fluxos NTFS alternativos	Sim	Sim	Sim
Verificar setores de inicialização do disco e MBR	Sim	Sim	Sim
Proteção de objetos compostos	• Objetos compactados* *Somente objetos novos e modificados	• Arquivos compactados SFX* • Objetos compactados* • Objetos OLE incorporados* *Somente objetos novos e modificados	• Arquivos compactados SFX* • Objetos compactados* • Objetos OLE incorporados* *Todos os objetos
Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte objeto incorporado	Não	Não	Sim

As configurações **Proteção de objetos**, **Usar a tecnologia iChecker**, **Usar a tecnologia iSwift** e **Usar o analisador heurístico** não estão incluídas nas configurações dos níveis de segurança predefinidos. Se você editar as configurações de segurança **Proteção de objetos**, **Usar a tecnologia iChecker**, **Usar a tecnologia iSwift** ou **Usar o analisador heurístico** após selecionar um dos níveis de segurança predefinidos, o nível de segurança que selecionou não será alterado.

Extensões de arquivos verificadas por padrão na tarefa de Proteção de Arquivos em Tempo Real

O Kaspersky Embedded Systems Security verifica arquivos das seguintes extensões por padrão:

- *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?.*

Configurações padrão da tarefa de Proteção de arquivos em tempo real

Por padrão, a tarefa de Proteção de Arquivos em Tempo Real usa as configurações descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Tabela 42. Configurações padrão da tarefa de Proteção de arquivos em tempo real

Configuração	Valor padrão	Descrição
Escopo da proteção	O computador inteiro, excluindo unidades virtuais.	Você pode limitar o escopo da proteção.
Modo de proteção dos objetos	**Ao acessar e modificar**	Você pode selecionar o modo de proteção, ou seja, definir o tipo de acesso usado pelo Kaspersky Embedded Systems Security para verificar objetos.
Analisador heurístico	O nível de segurança **Médio** é aplicado.	É possível ativar ou desativar o Analisador Heurístico, e configurar o nível de análise.
Aplicar à Zona Confiável	Aplicada.	Lista geral de exclusões que podem ser usadas em tarefas selecionadas.
Usar a KSN para proteção	Aplicada.	Você pode melhorar a proteção do servidor usando a infraestrutura dos serviços na nuvem da Kaspersky Security Network (disponível se a Declaração da KSN for aceita).
Programação de inicialização da tarefa	Na inicialização do aplicativo.	Você pode configurar a programação de inicialização da tarefa.
Bloquear acesso a recursos compartilhados de rede para hosts que exibem atividade maliciosa	Não aplicado.	Você pode adicionar hosts que mostram atividade maliciosa à lista de hosts bloqueados.

Gerenciamento da tarefa de Proteção de Arquivos em Tempo Real por meio do Plug-in de Administração

Nesta seção, aprenda como navegar pela interface do Plug-in de Administração e definir configurações de tarefa para um ou todos os computadores na rede.

Nesta seção

Navegação 242
Configuração da tarefa de Proteção de Arquivos em Tempo Real 243
Criação e configuração do escopo de proteção da tarefa 248
Definição manual de configurações de segurança 249

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface.

Nesta seção

Abertura das definições de política para a tarefa de proteção de Arquivos em Tempo Real 242
Abertura das propriedades da tarefa de Proteção de Arquivos em Tempo Real 243

Abertura das definições de política para a tarefa de proteção de Arquivos em Tempo Real

► *Para abrir as definições da tarefa de Proteção de Arquivos em Tempo Real por meio da política do Kaspersky Security Center:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Proteção de computador em tempo real**.
6. Clique no botão **Configurações** na subseção **Proteção de Arquivos em Tempo Real**.

   A janela **Proteção de arquivos em tempo real** é aberta.

Se um computador estiver sendo gerenciado por uma política ativa do Kaspersky Security Center e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas por meio do Console do Aplicativo.

Abertura das propriedades da tarefa de Proteção de Arquivos em Tempo Real

► *Para abrir as configurações da tarefa de Proteção de Arquivos em Tempo Real para um único computador da rede:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Dispositivos**.
4. Abra a janela **Propriedades: <Nome do computador>** de uma das seguintes maneiras:
   - Clique duas vezes no nome do computador protegido.
   - Selecione o item **Propriedades** no menu de contexto do computador protegido.

   A janela **Propriedades: <Nome do computador>** é exibida.
5. Na seção **Tarefas**, selecione a tarefa **Proteção de Arquivos em Tempo Real**.
6. Clique no botão **Propriedades**.

   A janela **Propriedades: Proteção de Arquivos em Tempo Real** é aberta.

Configuração da tarefa de Proteção de Arquivos em Tempo Real

► *Para configurar a tarefa de Proteção de arquivos em tempo real:*

1. Abra a janela **Proteção de arquivos em tempo real** (consulte a seção "Abertura das definições de políticas para a tarefa de Proteção de Arquivos em Tempo Real" na página 242).
2. Defina as seguintes configurações da tarefa:
   - Na guia **Geral**:
     - **Modo de proteção dos objetos**(consulte a seção "**Selecionar o modo de proteção**" na página 244)
     - **Analisador heurístico**
     - **Integração com outros componentes** (consulte a seção "**Configuração do Analisador Heurístico e integração com outros componentes**" na página 245)
   - Na guia **Gerenciamento da tarefa**:
     - Configurações de inicialização da tarefa programada (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 130).
3. Selecione a guia **Escopo da proteção** e faça o seguinte:
   - Clique no botão **Adicionar** ou **Editar** para editar o escopo da proteção (consulte a seção "Criação do escopo da proteção" na página 261).
     - Na janela aberta, escolha o que você deseja incluir no escopo da proteção da tarefa:
       - **Escopo predefinido**
       - **Disco, pasta ou local de rede**
       - **Arquivo**

- Selecione um dos níveis de segurança predefinidos (na página 238) ou defina manualmente as configurações de proteção (consulte a seção "Definição manual de configuração de segurança" na página 249).

4. Clique em **OK** na janela **Proteção de arquivos em tempo real**.

O Kaspersky Embedded Systems Security aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

Nesta seção

Selecionando o modo de proteção 244

Configuração do Analisador Heurístico e integração com outros componentes do aplicativo 245

Definição das configurações da programação de inicialização da tarefa 246

Selecionando o modo de proteção

Na tarefa Proteção de Arquivos em Tempo Real, o modo de proteção pode ser selecionado. A seção **Modo de proteção dos objetos** permite a especificação do tipo do acesso aos objetos sobre os quais o Kaspersky Embedded Systems Security deve realizar a verificação.

A configuração **Modo de proteção dos objetos** tem o valor comum para o escopo da proteção inteiro especificado na tarefa. Você não pode especificar valores diferentes para a configuração de nós individuais dentro do escopo da proteção.

► *Para selecionar o modo de proteção:*

1. Abra a janela **Proteção de arquivos em tempo real** (consulte a seção "Abertura das definições de políticas para a tarefa de Proteção de Arquivos em Tempo Real" na página 242).
2. Na janela exibida, abra a guia **Geral** e selecione o modo de proteção que deseja definir:
   - **Modo inteligente**

     O Kaspersky Embedded Systems Security seleciona objetos a serem verificados de maneira independente. O objeto é verificado ao ser aberto e novamente depois de ser salvo, caso tenha sido modificado. Se várias chamadas ao objeto foram feitas pelo processo enquanto ele estava em execução e se o processo o modificou, o Kaspersky Embedded Systems Security verifica o objeto novamente somente após o objeto ter sido salvo pelo processo pela última vez.
   - **Ao acessar e modificar**

     O Kaspersky Embedded Systems Security verifica o objeto quando é aberto e verifica-o novamente após ele ser salvo se o objeto foi modificado.

     Esta opção é selecionada por padrão.
   - **Ao acessar**

     O Kaspersky Embedded Systems Security verifica todos os objetos quando eles são abertos para a leitura ou para execução ou modificação.
   - **Ao executar**

O Kaspersky Embedded Systems Security verificará o arquivo apenas quando ele for acessado para ser executado.

3. Clique em **OK**.

O modo de proteção selecionado entrará em vigor.

Configuração do Analisador Heurístico e integração com outros componentes do aplicativo

Para iniciar a tarefa de Uso da KSN, você deve aceitar a Declaração da Kaspersky Security Network.

► *Para configurar o Analisador Heurístico e a integração com outros componentes:*

1. Abra a janela **Proteção de arquivos em tempo real** (consulte a seção "Abertura das definições de políticas para a tarefa de Proteção de Arquivos em Tempo Real" na página 242).
2. Na guia **Geral**, selecione ou desmarque a caixa de seleção **Usar o analisador heurístico**.

   Esta caixa ativa/desativa o analisador heurístico durante a verificação do objeto.

   Se a caixa de seleção estiver selecionada, o Analisador Heurístico será ativado.

   Se a caixa de seleção estiver desmarcada, o Analisador Heurístico será desativado.

   A caixa de seleção é selecionada por padrão.
3. Se necessário, ajuste o nível da análise usando o controle deslizante.

   O controle deslizante permite o ajuste do nível de análise heurística. O nível de intensidade da verificação define o equilíbrio entre a profundidade das pesquisas de ameaças, a carga sobre os recursos do sistema operacional e o tempo necessário para a verificação.

   Estão disponíveis os seguintes níveis de intensidade da verificação:

   - **Superficial**. O analisador heurístico executa menos operações encontradas nos arquivos executáveis. A probabilidade de detectar ameaças nesse modo é um pouco menor. A verificação é mais rápida e utiliza menos recursos.
   - **Médio**. O Analisador Heurístico executa a quantidade de instruções encontradas nos arquivos executáveis recomendada pelos especialistas da Kaspersky Lab.

     Este nível é selecionado por padrão.
   - **Profundo**. O analisador heurístico executa mais operações encontradas nos arquivos executáveis. De certa forma, a probabilidade de detectar ameaças nesse modo é maior. A verificação esgota mais recursos do sistema, leva mais tempo e pode causar um número mais alto de falsos positivos.

     O controle deslizante estará disponível se a caixa de seleção **Usar o analisador heurístico** estiver selecionada.
4. Na seção **Integração com outros componentes**, defina as seguintes configurações:
   - Selecione ou desmarque a caixa de seleção **Aplicar Zona Confiável**.

     Esta caixa de seleção ativa/desativa o uso da zona confiável em uma tarefa.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security adiciona operações de arquivos de processos confiáveis às exclusões da verificação

definidas nas configurações de tarefa.

Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security desconsiderará as operações de arquivos de processos confiáveis ao formar o escopo da proteção para a tarefa.

A caixa de seleção é selecionada por padrão.

- Selecione ou desmarque a caixa de seleção **Usar a KSN para proteção**.

  Esta caixa ativa ou desativa o uso de serviços da KSN.

  Se a caixa for selecionada, o aplicativo usa dados da Kaspersky Security Network para assegurar que o aplicativo responde mais rapidamente a novas ameaças e reduza a probabilidade de falsos positivos.

  Se a caixa estiver desmarcada, a tarefa não usará serviços da KSN.

  A caixa de seleção é selecionada por padrão.

  A caixa de seleção **Enviar dados dos arquivos verificados** deve estar selecionada na configuração da tarefa de Uso da KSN.

- Selecione ou desmarque a caixa de seleção **Bloquear acesso a recursos compartilhados de rede para hosts que exibem atividade maliciosa**.

5. Clique em **OK**.

As configurações de tarefa definidas são aplicadas imediatamente à tarefa sendo executada. Se a tarefa não estiver sendo executada, as configurações modificadas serão aplicadas na próxima execução.

Definição das configurações da programação de inicialização da tarefa

É possível configurar a programação de inicialização de tarefas locais do sistema e tarefas personalizadas no Console do Aplicativo. Você não pode definir a programação de inicialização para tarefas de grupo.

► *Para definir as configurações da programação de inicialização da tarefa de grupo, execute as seguintes ações:*

1. Na árvore do Console de Administração do Kaspersky Security Center, expanda o nó **Dispositivos gerenciados**.
2. Selecione o grupo ao qual o servidor protegido pertence.
3. No painel de detalhes, selecione a guia **Tarefas**.
4. Abra a janela **Propriedades: <Nome da tarefa>** de uma das seguintes maneiras:
   - Clique duas vezes no nome da tarefa.
   - Abra o menu de contexto do nome da tarefa e selecione o item Propriedades.
5. Selecione a seção **Programação**.
6. No bloco **Configurações de programação**, marque a caixa de seleção **Executar de acordo com o agendamento**.

Os campos com as configurações de programação para as tarefas de Verificação por Demanda e de Atualização estarão indisponíveis se a inicialização da programação for bloqueada por uma política do Kaspersky Security Center.

7. Configure a programação de acordo com suas necessidades. Para isso, execute as seguintes ações:
   a. Na lista **Frequência**, selecione um dos seguintes valores:
      - **De hora em hora**, se desejar que a tarefa seja executada nos intervalos de um número especificado de horas; especifique o número de horas no campo **A cada <número> hora(s)**.
      - **Diariamente**, se desejar que a tarefa seja executada nos intervalos de um número especificado de dias; especifique o número de dias no campo **A cada <número> dia(s)**.
      - **Semanalmente**, se desejar que a tarefa seja executada nos intervalos de um número especificado de semanas; especifique o número de semanas no campo **A cada <número> semana(s)**. Especifique os dias da semana em que a tarefa será iniciada (por padrão, a tarefa é executada nas segundas-feiras).
      - **Ao iniciar o aplicativo**, se deseja que a tarefa seja executada a cada vez que iniciar o Kaspersky Embedded Systems Security.
      - **Após a atualização do banco de dados do aplicativo**, se desejar que a tarefa seja executada após cada atualização do banco de dados do aplicativo.
   b. Especifique a hora para a primeira inicialização da tarefa no campo **Hora inicial**.
   c. No campo **Data inicial**, especifique a data a partir da qual a programação se aplica.

   Após ter especificado a frequência de início da tarefa, a hora da primeira execução, a data a partir da qual se aplica a programação e informações sobre a hora estimada para a próxima execução da tarefa são exibidas na parte superior da janela, no campo **Próxima execução**. Informações atualizadas sobre a hora estimada da próxima execução da tarefa serão exibidas sempre que você abrir a janela **Configurações de tarefa** da guia **Agendar**.
   O valor **Bloqueado pela política** é exibido no campo **Próxima execução** se as configurações de política ativas do Kaspersky Security Center proibirem o início de tarefas programadas do sistema (consulte a seção "Configuração da inicialização programada de tarefas locais do sistema" na página 97).

8. Use a guia **Avançado** para definir as configurações de programação a seguir de acordo com os seus requisitos.
   - Na seção **Configurações de interrupção de tarefa**:
     a. Marque a caixa de seleção **Duração** e insira o número de horas e minutos necessários nos campos à direita para especificar a duração máxima da execução da tarefa.
     b. Marque a caixa de seleção **Pausar de** e insira os valores iniciais e finais do intervalo de tempo nos campos à direita para especificar o intervalo de tempo menor que 24 horas durante o qual a execução da tarefa será pausada.
   - Na seção **Configurações avançadas**:
     a. Marque a caixa de seleção **Cancelar agendamento a partir de** e especifique a data a partir da qual a programação será interrompida.
     b. Marque a caixa de seleção **Executar tarefas ignoradas** para ativar a inicialização de tarefas

ignoradas.

c. Marque a caixa de seleção **Randomizar a hora de início da tarefa no intervalo de** e especifique um valor em minutos.

9. Clique em **OK**.
10. Clique no botão **Aplicar** para salvar as configurações de início da tarefa.

Se desejar definir as configurações do aplicativo de uma única tarefa usando o Kaspersky Security Center, execute as etapas descritas em Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center (na página 119).

Criação e configuração do escopo de proteção da tarefa

► *Para criar e configurar o escopo de proteção da tarefa por meio do Kaspersky Security Center:*

1. Abra a janela **Proteção de arquivos em tempo real** (consulte a seção "Abertura das definições de políticas para a tarefa de Proteção de Arquivos em Tempo Real" na página 242).
2. Selecione a guia **Escopo da proteção**.
3. Todos os itens já protegidos pela tarefa são listados na tabela **Escopo da proteção**.
4. Clique no botão **Adicionar** para adicionar um novo item à lista.

   A janela **Adicionar objetos ao escopo da proteção** será aberta.
5. Selecione um tipo de objeto para adicioná-lo a um escopo de proteção:
   - **Escopo predefinido** para incluir um dos escopos predefinidos no escopo da proteção no servidor. Em seguida, na lista suspensa, selecione um escopo de proteção necessário.
   - **Disco, pasta ou local de rede** para incluir um objeto individual de unidade, pasta ou rede em um escopo da proteção. Em seguida, selecione um escopo de proteção necessário clicando no botão **Procurar**.
   - **Arquivo** para incluir um arquivo individual no escopo da proteção. Em seguida, selecione um escopo de proteção necessário clicando no botão **Procurar**.

     Você não pode adicionar um objeto no escopo da proteção se ele já foi adicionado como uma exclusão fora de um escopo da proteção.
6. Para excluir itens individuais do escopo da proteção, desmarque as caixas de seleção ao lado dos nomes desses itens ou siga as etapas a seguir:
   a. Abra o menu de contexto no escopo da verificação clicando nele com o botão direito.
   b. No menu de contexto selecione a opção **Adicionar exclusão**.
   c. Na janela **Adicionar exclusão**, selecione um tipo de objeto que deseja adicionar como uma exclusão fora do escopo da proteção seguindo a lógica de adicionar o objeto a um procedimento de escopo da proteção.
7. Para modificar o escopo da proteção ou uma exclusão adicionada, selecione a opção **Editar escopo** no menu de contexto do escopo de proteção necessário.
8. Para ocultar o escopo da proteção adicionado anteriormente ou uma exclusão na lista de recursos de

arquivos de rede, selecione a opção **Remover escopo** no menu de contexto do escopo de proteção necessário.

O escopo da proteção é excluído fora do escopo da tarefa de Proteção de arquivos em tempo real na sua remoção da lista de recursos de arquivos de rede.

9. Clique no botão **Salvar**.

A janela de configuração do escopo da proteção será fechada. As configurações recém-definidas foram salvas.

A tarefa **Proteção de Arquivos em Tempo Real** pode ser iniciada somente se pelo menos um dos nós de recursos de arquivos do computador for incluído no escopo da proteção.

Definição manual de configurações de segurança

Por padrão, a tarefa de Proteção de Arquivos em Tempo Real usa as configurações de segurança comuns para todo o escopo da proteção. Estas configurações correspondem ao nível de segurança predefinido **Recomendado** (consulte a seção "Níveis de segurança predefinidos" na página 238).

Os valores padrão das configurações de segurança podem ser modificados, definindo-os como configurações em comum para todo o escopo da proteção ou como configurações distintas para diferentes itens na lista de recursos de arquivos de computador ou nós da árvore.

► *Para definir as configurações de segurança do nó selecionado manualmente:*

1. Abra a janela **Proteção de arquivos em tempo real** (consulte a seção "Abertura das definições de políticas para a tarefa de Proteção de Arquivos em Tempo Real" na página 242).
2. Na guia **Escopo da proteção**, selecione o nó cujas configurações de segurança você deseja definir e clique em **Configurar**.

   A janela **Configurações de Proteção de Arquivos em Tempo Real** é aberta.
3. Na guia **Nível de segurança**, clique no botão **Configurações** para definir a configuração personalizada.
4. É possível definir configurações de segurança personalizadas do nó selecionado, de acordo com os seus requisitos:
   - As configurações gerais (consulte a seção "Definir configurações gerais de tarefas" na página 250)
   - Ações (consulte a seção "Configurar ações" na página 252)
   - Desempenho (consulte a seção "Configurar o desempenho" na página 254)
5. Clique em **OK** na janela **Proteção de arquivos em tempo real**.

As novas configurações de escopo da proteção são salvas.

Nesta seção

Definir configurações gerais de tarefas 250
Configurar ações 252
Configurar o desempenho 254

Definir configurações gerais de tarefas

► *Para definir as configurações gerais da tarefa de Proteção de Arquivos em Tempo Real:*

1. Abra a janela **Configurações de Proteção de Arquivos em Tempo Real** (consulte a seção "Abertura das definições de políticas para a tarefa de Proteção de Arquivos em Tempo Real" na página 242).
2. Selecione a guia **Geral**.
3. Na seção **Proteção de objetos**, especifique os tipos de objetos que deseja incluir no escopo da proteção:
   - **Todos os objetos**

     O Kaspersky Embedded Systems Security verifica todos os objetos.
   - **Objetos verificados por formato**

     O Kaspersky Embedded Systems Security verificará somente objetos infectáveis com base no formato do arquivo.

     A lista de formatos é compilada pela Kaspersky Lab. Ela está incluída nos bancos de dados do Kaspersky Embedded Systems Security.
   - **Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus**

     O Kaspersky Embedded Systems Security verificará somente objetos infectáveis com base na extensão do arquivo.

     A lista de extensões é compilada pela Kaspersky Lab. Ela está incluída nos bancos de dados do Kaspersky Embedded Systems Security.
   - **Objetos verificados pela lista de extensões especificada**

     O Kaspersky Embedded Systems Security verificará os arquivos baseados em suas extensões. A lista de extensões de arquivo pode ser personalizada manualmente na janela **Lista de extensões**, que pode ser aberta clicando no botão **Editar**.
   - **Verificar setores de inicialização do disco e MBR**

     Ativa a proteção dos setores de inicialização e dos registros mestres de inicialização.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os setores de inicialização e os registros mestres de inicialização nos discos rígidos e unidades removíveis do computador.

     A caixa de seleção é selecionada por padrão.
   - **Verificar fluxos NTFS alternativos**

     Verificação de fluxos alternativos de arquivos e pastas nas unidades do sistema de arquivos NTFS.

Se a caixa estiver selecionada, o aplicativo verifica um objeto possivelmente infectado e todos os fluxos NTFS associados àquele objeto.

Se a caixa estiver desmarcada, o aplicativo verifica apenas o objeto detectado e considerado possivelmente infectado.

A caixa de seleção é selecionada por padrão.

4. Na seção **Desempenho**, selecione ou desmarque a caixa **Proteger somente arquivos novos e modificados**.

   Esta caixa de seleção ativa/desativa a verificação e a proteção de arquivos que foram reconhecidos pelo Kaspersky Embedded Systems Security como novos ou modificados desde a última verificação.

   Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará e protegerá apenas os arquivos reconhecidos como novos ou modificados desde a última verificação.

   Se a caixa estiver desmarcada, você poderá selecioná-la se quiser verificar e proteger apenas arquivos novos ou todos os arquivos, desconsiderando o status de modificação.

   Por padrão, a caixa de seleção está selecionada para o nível de segurança **Desempenho máximo**. Se os níveis de segurança **Proteção máxima** ou **Recomendado** estiverem definidos, a caixa estará desmarcada.

> Para alternar entre as opções disponíveis quando a caixa estiver desmarcada, clique no link **Todos** / **Apenas novos** para cada um dos tipos de objetos compostos.

5. Na seção **Proteção de objetos compostos**, especifique os objetos compostos que deseja incluir no escopo da proteção:

   - **Todos / Apenas novos arquivos compactados**

     Verificação dos arquivos compactados ZIP, CAB, RAR, ARJ e de outros formatos.

     Se essa a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos compactados.

     Se essa caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos compactados durante a verificação.

     O valor padrão depende do nível de proteção selecionado.

   - **Todos / Apenas novos arquivos compactados SFX**

     Verificação de arquivos compactados autoextraíveis.

     Se essa caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos compactados durante a verificação.

     Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos compactados SFX durante a verificação.

     O valor padrão depende do nível de proteção selecionado.

     Essa opção fica ativa quando a caixa de seleção **Arquivos compactados** é desmarcada.

   - **Todos / Apenas novos bancos de dados de e-mail**

     Verificação de arquivos de banco de dados de correio do Microsoft Outlook e Microsoft Outlook Express.

Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos de bancos de dados de e-mail.

Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos de bancos de dados de e-mail durante a verificação.

O valor padrão depende do nível de segurança selecionado.

- **Todos / Apenas novos objetos compactados**

  Verificação de arquivos executáveis compactados por compactadores de código binário, como UPX ou ASPack.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos executáveis compactados por compactadores de código binário.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos executáveis compactados por compactadores de código binário durante a verificação.

  O valor padrão depende do nível de proteção selecionado.

- **Todos / Apenas novos e-mails sem formatação**

  Verificação de arquivos de formato de e-mail, como mensagens do Microsoft Outlook e Microsoft Outlook Express.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos de formato de e-mail.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos de formato de e-mail durante a verificação.

  O valor padrão depende do nível de segurança selecionado.

- **Todos / Apenas novos objetos OLE incorporados**

  Verificação de objetos incorporados em arquivos (como macros do Microsoft Word ou anexos de e-mail).

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os objetos inseridos em arquivos.

  Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os objetos inseridos em arquivos durante a verificação.

  O valor padrão depende do nível de proteção selecionado.

6. Clique em **Salvar**.

A nova configuração de tarefa será salva.

Configurar ações

► *Para configurar as ações em objetos infectados e outros objetos detectados da tarefa Proteção de Arquivos em Tempo Real:*

1. Abra a janela **Configurações de Proteção de Arquivos em Tempo Real** (consulte a seção "**Abertura das definições de políticas para a tarefa de Proteção de Arquivos em Tempo Real**" na página 242).
2. Selecione a guia **Ações**.
3. Selecione a ação a ser executada em objetos infectados e outros objetos detectados.

- **Notificar somente**.

  Quando esse modo estiver selecionado, o Kaspersky Embedded Systems Security não bloqueará o acesso a objetos infectados ou outros objetos detectados, nem executará qualquer ação sobre eles. O seguinte evento é registrado no log de tarefas: *Objeto não desinfectado. Motivo: nenhuma ação foi executada para neutralizar o objeto detectado devido a configurações definidas pelos usuários.* O evento especifica todas as informações disponíveis sobre o objeto detectado.

  O modo **Notificar somente** deve ser configurado separadamente para cada área de verificação. Este modo não é usado por padrão para qualquer um dos níveis de segurança. Se você selecionar esse modo, o Kaspersky Embedded Systems Security alterará automaticamente o nível de segurança para **Personalizado**.

- **Bloquear acesso**.

  Quando esta opção estiver selecionada o Kaspersky Embedded Systems Security bloqueará o acesso ao objeto detectado ou possivelmente infectado. É possível selecionar ação adicional para objetos bloqueados na lista suspensa.

- **Executar ação adicional**.

  Selecionar ação da lista suspensa:

  - **Desinfectar**.
  - **Desinfectar. Desinfectar. Remover se a desinfecção falhar**.
  - **Remover**.
  - **Recomendado**.

4. Selecione a ação a ser executada em objetos possivelmente infectados:

- **Notificar somente**.

  Quando esse modo estiver selecionado, o Kaspersky Embedded Systems Security não bloqueará o acesso a objetos infectados ou outros objetos detectados, nem executará qualquer ação sobre eles. O seguinte evento é registrado no log de tarefas: *Objeto não desinfectado. Motivo: nenhuma ação foi executada para neutralizar o objeto detectado devido a configurações definidas pelos usuários.* O evento especifica todas as informações disponíveis sobre o objeto detectado.

  O modo **Notificar somente** deve ser configurado separadamente para cada área de verificação. Este modo não é usado por padrão para qualquer um dos níveis de segurança. Se você selecionar esse modo, o Kaspersky Embedded Systems Security alterará automaticamente o nível de segurança para **Personalizado**.

- **Bloquear acesso**.

  Quando esta opção estiver selecionada o Kaspersky Embedded Systems Security bloqueará o acesso ao objeto detectado ou possivelmente infectado. É possível selecionar ação adicional para objetos bloqueados na lista suspensa.

- **Executar ação adicional**.

  Selecionar ação da lista suspensa:

  - **Quarentena**.
  - **Remover**.
  - **Recomendado**.

5. Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:
   a. Desmarque ou selecione a caixa **Executar ações dependendo do tipo de objeto detectado**.

      Se a caixa for selecionada, você pode definir a ação primária e secundária independentemente para cada tipo de objeto detectado clicando no botão **Configurações** ao lado da caixa. Nesse caso, o Kaspersky Embedded Systems Security não permitirá que um objeto infectado seja aberto ou executado independentemente da sua escolha.

      Se a caixa de seleção for desmarcada, o Kaspersky Embedded Systems Security executará as ações selecionadas nas seções **Ação a ser executada em objetos infectados e outros** e **Ação a ser executada em objetos possivelmente infectados** para os tipos de objetos indicados, respectivamente.

      Esta caixa é desmarcada por padrão.

   b. Clique no botão **Configurações**.
   c. Na janela que se abre, selecione a ação primária e secundária (se a primeira ação falhar) para cada tipo do objeto detectado.
   d. Clique em **OK**.
6. Selecione a ação a ser executada em arquivos compostos não modificáveis: selecione ou desmarque a caixa **Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte objeto incorporado**.

   Esta caixa ativa ou desativa a remoção forçada do arquivo composto pai quando um objeto malicioso, possivelmente infectado ou outro objeto filho incorporado for detectado.

   Se a caixa estiver selecionada e a tarefa for configurada para remover objetos infectados e possivelmente infectados, o Kaspersky Embedded Systems Security forçosamente removerá todo o objeto composto pai quando um objeto incorporado malicioso ou outro objeto for detectado. A remoção forçada de um arquivo pai juntamente com todo o seu conteúdo ocorrerá se o aplicativo não puder remover apenas o objeto filho detectado (por exemplo, se o objeto pai não puder ser modificado).

   Se esta caixa estiver desmarcada e a tarefa for configurada para remover objetos infectados e possivelmente infectados, o Kaspersky Embedded Systems Security não executará a ação selecionada se o objeto pai não puder ser modificado.
7. Clique em **Salvar**.

A nova configuração de tarefa será salva.

Configurar o desempenho

► *Para configurar o desempenho da tarefa de Proteção de Arquivos em Tempo Real:*

1. Abra a janela **Configurações de Proteção de Arquivos em Tempo Real (consulte a seção "Abertura das definições de políticas para a tarefa de Proteção de Arquivos em Tempo Real" na página** 242**)**.
2. Selecione a guia **Desempenho**.
3. Na seção **Exclusões**:
   - Desmarque ou selecione a caixa **Excluir arquivos**.

     Excluindo arquivos da verificação pelo nome de arquivo ou pela máscara de nome de arquivo.

     Se esta caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security

ignorará os objetos especificados durante a verificação.

Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará todos os objetos.

Esta caixa é desmarcada por padrão.

- Desmarque ou selecione a caixa **Não detectar**.

  Os objetos são excluídos da verificação pelo nome ou pela máscara de nome do objeto detectável. A lista de nomes de objetos detectáveis está disponível no site da Enciclopédia de Vírus https://encyclopedia.kaspersky.com/knowledge/classification/.

  Se esta caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará os objetos detectáveis especificados durante a verificação.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security detectará todos os objetos especificados no aplicativo por padrão.

  Esta caixa é desmarcada por padrão.

- Clique no botão **Editar** de cada configuração para adicionar exclusões.

4. Na seção **Configurações avançadas**:

   - **Parar a verificação se demorar mais que (s)**

     Limita a duração da verificação do objeto. O valor padrão é 60 segundos.

     Se a caixa de seleção estiver selecionada, a duração da verificação será limitada ao valor especificado.

     Se a caixa de seleção estiver desmarcada, a duração da verificação será ilimitada.

     Por padrão, a caixa de seleção está selecionada para o nível de segurança **Desempenho máximo**.

   - **Não verificar obj. compostos com mais de (MB)**

     Exclui objetos maiores do que o tamanho especificado na verificação.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará objetos compostos cujo tamanho exceda o limite especificado durante a verificação de vírus.

     Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará os objetos compostos de qualquer tamanho.

     Por padrão, a caixa de seleção está selecionada para o nível de segurança **Desempenho máximo**.

   - **Usar a tecnologia iSwift**

     A tecnologia iSwift compara o identificador NTFS do arquivo armazenado em um banco de dados com um identificador atual. A verificação é executada apenas para arquivos cujos identificadores foram alterados (novos arquivos e arquivos modificados desde a última verificação dos objetos do sistema NTFS).

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará apenas os novos arquivos ou aqueles modificados desde a última verificação dos objetos do sistema NTFS.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará objetos do sistema de arquivos NTFS sem considerar a data de criação ou

modificação do arquivo, exceto em arquivos das pastas de rede.

A caixa de seleção é selecionada por padrão.

- **Usar a tecnologia iChecker**

  A tecnologia iChecker calcula e lembra de somas de verificação de arquivos verificados. Se um objeto for modificado a soma de verificação é alterada. O aplicativo compara todas as somas de verificação durante a tarefa de verificação e verifica apenas objetos novos e modificados desde a última verificação de arquivos.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará apenas arquivos novos e modificados.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará os arquivos sem considerar a data de criação ou modificação do arquivo.

  A caixa de seleção é selecionada por padrão.

Gerenciamento da tarefa de Proteção de Arquivos em Tempo Real por meio do Console do Aplicativo

Nesta seção, aprenda como navegar pela interface do Console do Aplicativo e definir configurações de tarefa em um computador local.

Nesta seção

Navegação 256
Abertura das configurações de escopo da Proteção de Arquivos em Tempo Real 257
Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real 257
Configuração da tarefa de Proteção de Arquivos em Tempo Real 257
Criando um escopo da proteção 261
Definição manual de configurações de segurança 264
Estatísticas da tarefa de Proteção de Arquivos em Tempo Real 271

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface.

Abertura das configurações de escopo da Proteção de Arquivos em Tempo Real

► *Para abrir a janela Configurações do escopo da proteção para a tarefa de Proteção de Arquivos em Tempo Real:*

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.
2. Selecione o nó filho **Proteção de Arquivos em Tempo Real**.
3. Clique no link **Configurar o escopo da proteção** no painel de detalhes.

   A janela **Configurações do escopo da proteção** é exibida.

Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real

► *Para abrir a janela de configurações gerais da tarefa:*

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.
2. Selecione o nó filho **Proteção de Arquivos em Tempo Real**.
3. Clique no link **Propriedades** no painel de detalhes.

   A janela **Configurações de tarefa** é exibida.

Configuração da tarefa de Proteção de Arquivos em Tempo Real

► *Para configurar a tarefa de Proteção de arquivos em tempo real:*

1. Abra a janela **Configurações de tarefa** (consulte a seção "Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real" na página 257).
2. Na guia **Geral**, defina as seguintes configurações de tarefa:
   - **Modo de proteção dos objetos**(consulte a seção "**Selecionar o modo de proteção**" na página 258)
   - **Analisador heurístico**
   - **Integração com outros componentes** (consulte a seção "**Configuração do Analisador Heurístico e integração com outros componentes**" na página 259)
3. Nas guias **Agendar** e **Avançado**, especifique as configurações de inicialização programada (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 151).
4. Clique em **OK** na janela **Configurações de tarefa**.

   As configurações modificadas são salvas.
5. No painel de detalhes do nó **Proteção de Arquivos em Tempo Real**, clique no link **Configurar o escopo da proteção**.
6. Faça o seguinte:
   - Na lista ou na árvore de recursos de arquivos de computador, selecione os nós ou itens que você deseja incluir no escopo da proteção de tarefa.
   - Selecione um dos níveis de segurança predefinidos ou configure as definições de proteção do objeto

manualmente (consulte a seção "Definição manual de configurações de segurança" na página 433).

7. Na janela **Configurações do escopo da proteção**, clique no botão **Salvar**.

O Kaspersky Embedded Systems Security aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora das modificações feitas nas configurações e os valores de configurações de tarefa antes e depois da modificação são salvos no log de auditoria do sistema.

Nesta seção

Selecionando o modo de proteção 258

Configuração do Analisador Heurístico e integração com outros componentes do aplicativo 259

Definição das configurações da programação de inicialização da tarefa 260

Selecionando o modo de proteção

Na tarefa Proteção de Arquivos em Tempo Real, o modo de proteção pode ser selecionado. A seção **Modo de proteção dos objetos** permite a especificação do tipo do acesso aos objetos sobre os quais o Kaspersky Embedded Systems Security deve realizar a verificação.

A configuração **Modo de proteção dos objetos** tem o valor comum para o escopo da proteção inteiro especificado na tarefa. Você não pode especificar valores diferentes para a configuração de nós individuais dentro do escopo da proteção.

► *Para selecionar o modo de proteção, siga as etapas a seguir:*

1. Abra a janela **Configurações de tarefa** (consulte a seção "Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real" na página 257).
2. Na janela exibida, abra a guia **Geral** e selecione o modo de proteção que deseja definir:
   - **Modo inteligente**

     O Kaspersky Embedded Systems Security seleciona objetos a serem verificados de maneira independente. O objeto é verificado ao ser aberto e novamente depois de ser salvo, caso tenha sido modificado. Se várias chamadas ao objeto foram feitas pelo processo enquanto ele estava em execução e se o processo o modificou, o Kaspersky Embedded Systems Security verifica o objeto novamente somente após o objeto ter sido salvo pelo processo pela última vez.
   - **Ao acessar e modificar**

     O Kaspersky Embedded Systems Security verifica o objeto quando é aberto e verifica-o novamente após ele ser salvo se o objeto foi modificado.

     Esta opção é selecionada por padrão.
   - **Ao acessar**

     O Kaspersky Embedded Systems Security verifica todos os objetos quando eles são abertos para a leitura ou para execução ou modificação.
   - **Ao executar**

     O Kaspersky Embedded Systems Security verificará o arquivo apenas quando ele for acessado para ser executado.

3. Clique em **OK**.

O modo de proteção selecionado entrará em vigor.

Configuração do Analisador Heurístico e integração com outros componentes do aplicativo

Para iniciar a tarefa de Uso da KSN, você deve aceitar a Declaração da Kaspersky Security Network.

► *Para configurar o Analisador Heurístico e a integração com outros componentes:*

1. Abra a janela **Configurações de tarefa** (consulte a seção "**Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real**" na página 257).
2. Na guia **Geral**, selecione ou desmarque a caixa de seleção **Usar o analisador heurístico**.

   Esta caixa ativa/desativa o analisador heurístico durante a verificação do objeto.

   Se a caixa de seleção estiver selecionada, o Analisador Heurístico será ativado.

   Se a caixa de seleção estiver desmarcada, o Analisador Heurístico será desativado.

   A caixa de seleção é selecionada por padrão.
3. Se necessário, ajuste o nível da análise usando o controle deslizante.

   O controle deslizante permite o ajuste do nível de análise heurística. O nível de intensidade da verificação define o equilíbrio entre a profundidade das pesquisas de ameaças, a carga sobre os recursos do sistema operacional e o tempo necessário para a verificação.

   Estão disponíveis os seguintes níveis de intensidade da verificação:

   - **Superficial**. O analisador heurístico executa menos operações encontradas nos arquivos executáveis. A probabilidade de detectar ameaças nesse modo é um pouco menor. A verificação é mais rápida e utiliza menos recursos.
   - **Médio**. O Analisador Heurístico executa a quantidade de instruções encontradas nos arquivos executáveis recomendada pelos especialistas da Kaspersky Lab.

     Este nível é selecionado por padrão.
   - **Profundo**. O analisador heurístico executa mais operações encontradas nos arquivos executáveis. De certa forma, a probabilidade de detectar ameaças nesse modo é maior. A verificação esgota mais recursos do sistema, leva mais tempo e pode causar um número mais alto de falsos positivos.

     O controle deslizante estará disponível se a caixa de seleção **Usar o analisador heurístico** estiver selecionada.
4. Na seção **Integração com outros componentes**, defina as seguintes configurações:
   - Selecione ou desmarque a caixa de seleção **Aplicar à Zona Confiável**.

     Esta caixa de seleção ativa/desativa o uso da zona confiável em uma tarefa.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security adiciona operações de arquivos de processos confiáveis às exclusões da verificação definidas nas configurações de tarefa.

     Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security desconsiderará

as operações de arquivos de processos confiáveis ao formar o escopo da proteção para a tarefa.

A caixa de seleção é selecionada por padrão.

Clique no link **Zona Confiável** para abrir as configurações da Zona Confiável.

- Selecione ou desmarque a caixa de seleção **Usar a KSN para proteção**.

  Esta caixa ativa ou desativa o uso de serviços da KSN.

  Se a caixa for selecionada, o aplicativo usa dados da Kaspersky Security Network para assegurar que o aplicativo responde mais rapidamente a novas ameaças e reduza a probabilidade de falsos positivos.

  Se a caixa estiver desmarcada, a tarefa não usará serviços da KSN.

  A caixa de seleção é selecionada por padrão.

  A caixa de seleção **Enviar dados dos arquivos verificados** deve estar selecionada na configuração da tarefa de Uso da KSN.

- Selecione ou desmarque a caixa de seleção **Bloquear acesso a recursos compartilhados de rede para hosts que exibem atividade maliciosa**.

5. Clique em **OK**.

As configurações recém-definidas serão aplicadas.

Definição das configurações da programação de inicialização da tarefa

É possível configurar a programação de inicialização de tarefas locais do sistema e tarefas personalizadas no Console do Aplicativo. Você não pode definir a programação de inicialização para tarefas de grupo.

► *Para configurar a programação de inicialização da tarefa:*

1. Abra o menu de contexto da tarefa para a qual você deseja configurar a programação de inicialização.
2. Selecione **Propriedades**.

   A janela **Configurações de tarefa** é exibida.
3. Na janela exibida, na guia **Agendar**, marque a caixa de seleção **Executar de acordo com o agendamento**.
4. Configure a programação de acordo com suas necessidades. Para isso, execute as seguintes ações:

   a. Em **Frequência**, selecione um dos seguintes valores:

   - **De hora em hora**, se desejar que a tarefa seja executada nos intervalos de um número especificado de horas; especifique o número de horas no campo **A cada <número> hora(s)**.
   - **Diariamente**, se desejar que a tarefa seja executada nos intervalos de um número especificado de dias; especifique o número de dias no campo **A cada <número> dia(s)**.
   - **Semanalmente**, se desejar que a tarefa seja executada nos intervalos de um número especificado de semanas; especifique o número de semanas no campo **A cada <número> semana(s) em**. Especifique os dias da semana em que a tarefa será iniciada (por padrão, a tarefa é executada nas segundas-feiras).
   - **Ao iniciar o aplicativo**, se deseja que a tarefa seja executada a cada vez que iniciar o Kaspersky

Embedded Systems Security.

- **Após a atualização do banco de dados do aplicativo**, se desejar que a tarefa seja executada após cada atualização do banco de dados do aplicativo.

b. Especifique a hora para a primeira inicialização da tarefa no campo **Hora inicial**.

c. No campo **Data inicial**, especifique a data a partir da qual a programação se aplica.

Após ter especificado a frequência de início da tarefa, a hora da primeira execução, a data a partir da qual se aplica a programação e informações sobre a hora estimada para a próxima execução da tarefa são exibidas na parte superior da janela, no campo **Próxima execução**. Informações atualizadas sobre a hora estimada da próxima execução da tarefa serão exibidas sempre que você abrir a janela **Configurações de tarefa** da guia **Agendar**.
Bloqueado pela política será exibido no campo **Próxima execução** se as tarefas de inicialização do sistema em uma programação estiverem definidas nas configurações de política do Kaspersky Security Center.

5. Use a guia **Avançado** para definir as configurações de programação a seguir de acordo com os seus requisitos.

- Na seção **Configurações de interrupção de tarefa**:

a. Marque a caixa de seleção **Duração** e insira o número de horas e minutos necessários nos campos à direita para especificar a duração máxima da execução da tarefa.

b. Marque a caixa de seleção **Pausar de** e insira os valores iniciais e finais do intervalo de tempo nos campos à direita para especificar o intervalo de tempo menor que 24 horas durante o qual a execução da tarefa será pausada.

- Na seção **Configurações avançadas**:

a. Marque a caixa de seleção **Cancelar agendamento a partir de** e especifique a data a partir da qual a programação será interrompida.

b. Marque a caixa de seleção **Executar tarefas ignoradas** para ativar a inicialização de tarefas ignoradas.

c. Marque a caixa de seleção **Aleatorizar o início da tarefa dentro do intervalo de** e especifique um valor em minutos.

6. Clique em **OK**.

As definições de inicialização de tarefa configuradas serão salvas.

Criando um escopo da proteção

Esta seção fornece instruções sobre a criação e o gerenciamento de um escopo da proteção na tarefa de Proteção de Arquivos em Tempo Real.

Nesta seção

Criando um escopo da proteção.....262
Criando o escopo da proteção virtual.....264

Criando um escopo da proteção

O procedimento para criar o escopo da tarefa de Proteção de Arquivos em Tempo Real depende do modo de visualização de recursos de arquivo de rede (consulte a seção "Sobre o escopo de proteção da tarefa e configurações de segurança" na página 236). Você pode configurar o modo de visualização de recursos de arquivos de rede como uma árvore ou como uma lista (definir como padrão).

Para aplicar à tarefa as novas configurações do escopo da proteção, a tarefa de Proteção de Arquivos em Tempo real deve ser reiniciada.

► *Para criar um escopo da proteção usando a árvore de recursos de arquivos de rede:*

1. Abra a janela **Configurações do escopo da proteção** (consulte a seção "Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real" na página 257).
2. Na seção esquerda da janela, abra a árvore de recursos de arquivos de rede para exibir todos os nós e os nós filhos.
3. Faça o seguinte:
   - Para excluir os nós individuais do escopo da proteção, desmarque as caixas ao lado dos nomes destes nós.
   - Para incluir nós individuais no escopo da proteção, desmarque a caixa de seleção **Meu Computador** e faça o seguinte:
     - Se todas as unidades de um tipo forem incluídas no escopo da proteção, selecione a caixa de seleção junto do nome do tipo de disco requerido (por exemplo, para adicionar todas as unidades removíveis no computador, selecione a caixa **Unidades removíveis**).
     - Para incluir um disco individual de um determinado tipo no escopo da proteção, expanda o nó que contém a lista de unidades desse tipo e marque a caixa ao lado do nome da unidade desejada. Por exemplo, para selecionar a unidade removível F:, expanda o nó **Unidades removíveis** e marque a caixa da unidade **F:**.
     - Se deseja incluir somente uma única pasta ou arquivo na unidade, selecione a caixa ao lado do nome daquela pasta ou arquivo.
4. Clique no botão **Salvar**.

A janela de configuração do escopo da proteção será fechada. As configurações recém-definidas foram salvas.

► *Para criar um escopo da proteção usando a lista de recursos de arquivos de rede:*

1. Abra a janela **Configurações do escopo da proteção** (consulte a seção "Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real" na página 257).
2. Para incluir nós individuais no escopo da proteção, desmarque a caixa de seleção **Meu Computador** e faça o seguinte:
   a. Abra o menu de contexto no escopo da verificação clicando nele com o botão direito.
   b. No menu de contexto do botão, selecione **Adicionar escopo da proteção**.
   c. Na janela **Adicionar escopo da proteção**, selecione um tipo de objeto para adicioná-lo a um escopo da proteção:
      - **Escopo predefinido** para incluir um dos escopos predefinidos no escopo da proteção do

computador. Em seguida, na lista suspensa, selecione um escopo de proteção necessário.

- **Disco, pasta ou local de rede** para incluir um objeto individual de unidade, pasta ou rede em um escopo da proteção. Em seguida, selecione um escopo necessário clicando no botão **Procurar**.
- **Arquivo** para incluir um arquivo individual no escopo da proteção. Em seguida, selecione um escopo necessário clicando no botão **Procurar**.

Você não pode adicionar um objeto no escopo da proteção se ele já foi adicionado como uma exclusão fora de um escopo da proteção.

3. Para excluir nós individuais do escopo da proteção, desmarque as caixas ao lado dos nomes destes nós ou siga as etapas a seguir:
   a. Abra o menu de contexto no escopo da verificação clicando nele com o botão direito.
   b. No menu de contexto selecione a opção **Adicionar exclusão**.
   c. Na janela **Adicionar exclusão**, selecione um tipo de objeto que deseja adicionar como uma exclusão fora do escopo da proteção seguindo a lógica de adicionar o objeto a um procedimento de escopo da proteção.
4. Para modificar o escopo da proteção ou uma exclusão adicionada, selecione a opção **Editar escopo** no menu de contexto do escopo de proteção necessário.
5. Para ocultar o escopo da proteção adicionado anteriormente ou uma exclusão na lista de recursos de arquivos de rede, selecione a opção **Remover da lista** no menu de contexto do escopo de proteção necessário.

   O escopo da proteção é excluído fora do escopo da tarefa de Proteção de arquivos em tempo real na sua remoção da lista de recursos de arquivos de rede.

6. Clique no botão **Salvar**.

A janela de configuração do escopo da proteção será fechada. As configurações recém-definidas foram salvas.

A tarefa *Proteção de arquivos em tempo real* pode ser iniciada somente se pelo menos um dos nós de recursos de arquivos do computador for incluído no escopo da proteção.

Se for especificado um escopo da proteção complexo, por exemplo, se forem especificados valores de configurações de segurança diferentes para vários nós da árvore de recursos de arquivos do computador, isso poderá deixar a verificação dos objetos mais lenta quando eles forem acessados.

Criando o escopo da proteção virtual

Você pode expandir o escopo da proteção/verificação adicionando unidades virtuais individuais, pastas ou arquivos somente se o escopo da proteção/verificação for apresentado como uma árvore de recursos de arquivos (consulte a seção "Configurando o modo de visualização de recursos de arquivos de rede" na página 429).

► *Para adicionar uma unidade virtual ao escopo da proteção:*

1. Abra a janela **Configurações do escopo da proteção** (consulte a seção "Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real" na página 257).
2. Abra a lista suspensa no setor esquerdo superior da janela e selecione **Visualização em árvore**.
3. Abra o menu de contexto das **Unidades virtuais**.
4. Selecione a opção **Adicionar unidade virtual**.
5. Na lista de nomes disponíveis, selecione o nome da unidade virtual que está sendo criada.
6. Ative a caixa ao lado da unidade adicionada para incluí-la no escopo da proteção.
7. Na janela **Configurações do escopo da proteção**, clique no botão **Salvar**.

As configurações recém-definidas foram salvas.

► *Para adicionar uma pasta ou um arquivo virtual ao escopo da proteção:*

1. Abra a janela **Configurações do escopo da proteção** (consulte a seção "Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real" na página 257).
2. Abra a lista suspensa no setor esquerdo superior da janela e selecione **Visualização em árvore**.
3. Abra o menu de contexto da unidade virtual à qual você deseja adicionar uma pasta ou arquivo e selecione uma das seguintes opções:
   - **Adicionar pasta virtual** se você deseja adicionar uma pasta virtual ao escopo da proteção.
   - **Adicionar arquivo virtual** se você deseja adicionar um arquivo virtual ao escopo da proteção.
4. No campo de entrada, especifique o nome da pasta ou arquivo.
5. Na linha que contém o nome da pasta ou arquivo criado, selecione a caixa de seleção para incluir essa pasta ou arquivo no escopo da proteção.
6. Na janela **Configurações do escopo da proteção**, clique no botão **Salvar**.

As configurações de tarefa modificadas são salvas.

Definição manual de configurações de segurança

Por padrão, a tarefa de Proteção do Computador em Tempo Real usa as configurações de segurança comuns para todo o escopo da proteção. Estas configurações correspondem ao nível de segurança predefinido **Recomendado** (consulte a seção "Níveis de segurança predefinidos" na página 238).

Os valores padrão das configurações de segurança podem ser modificados, definindo-os como configurações em comum para todo o escopo da proteção ou como configurações distintas para diferentes itens na lista de recursos

de arquivos de computador ou nós da árvore.

Ao trabalhar com a árvore de recursos de arquivo de servidor, as configurações de segurança definidas para o nó pai selecionado são automaticamente aplicadas a todos os nós filhos. As configurações de segurança do nó pai não são aplicadas a nós filhos configurados separadamente.

► *Para definir as configurações de segurança manualmente:*

1. Abra a janela **Configurações do escopo da proteção** (consulte a seção "Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real" na página 257).
2. Na seção esquerda da janela, selecione o nó para definir as configurações de segurança.

   Um modelo predefinido contendo configurações de segurança (consulte a seção "Sobre modelos de configurações de segurança" na página 157) pode ser aplicado a um nó ou item selecionado no escopo da proteção.

3. Defina as configurações de segurança necessárias para o nó ou item selecionado de acordo com seus requisitos:
   - As **Geral** (consulte a seção "**Definir configurações gerais de tarefas**" na página 265)
   - **Ações** (consulte a seção "**Configurar ações**" na página 268)
   - **Desempenho** (consulte a seção "**Configurar o desempenho**" na página 270)
4. Na janela **Configurações do escopo da proteção**, clique no botão **Salvar**.

As novas configurações de escopo da proteção são salvas.

Nesta seção

Definir configurações gerais de tarefas 265
Configurar ações 268
Configurar o desempenho 270

Definir configurações gerais de tarefas

► *Para definir as configurações gerais da tarefa de Proteção de Arquivos em Tempo Real:*

1. Abra a janela **Configurações do escopo da proteção** (consulte a seção "Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real" na página 257).
2. Selecione a guia **Geral**.
3. Na seção **Proteção de objetos**, especifique os objetos que deseja incluir no escopo da proteção:
   - **Todos os objetos**

     O Kaspersky Embedded Systems Security verifica todos os objetos.
   - **Objetos verificados por formato**

     O Kaspersky Embedded Systems Security verificará somente objetos infectáveis com base no formato do arquivo.

A lista de formatos é compilada pela Kaspersky Lab. Ela está incluída nos bancos de dados do Kaspersky Embedded Systems Security.

- **Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus**

  O Kaspersky Embedded Systems Security verificará somente objetos infectáveis com base na extensão do arquivo.

  A lista de extensões é compilada pela Kaspersky Lab. Ela está incluída nos bancos de dados do Kaspersky Embedded Systems Security.

- **Objetos verificados pela lista de extensões especificada**

  O Kaspersky Embedded Systems Security verificará os arquivos baseados em suas extensões. A lista de extensões de arquivo pode ser personalizada manualmente na janela **Lista de extensões**, que pode ser aberta clicando no botão **Editar**.

- **Verificar setores de inicialização do disco e MBR**

  Ativa a proteção dos setores de inicialização e dos registros mestres de inicialização.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os setores de inicialização e os registros mestres de inicialização nos discos rígidos e unidades removíveis do computador.

  A caixa de seleção é selecionada por padrão.

- **Verificar fluxos NTFS alternativos**

  Verificação de fluxos alternativos de arquivos e pastas nas unidades do sistema de arquivos NTFS.

  Se a caixa estiver selecionada, o aplicativo verifica um objeto possivelmente infectado e todos os fluxos NTFS associados àquele objeto.

  Se a caixa estiver desmarcada, o aplicativo verifica apenas o objeto detectado e considerado possivelmente infectado.

  A caixa de seleção é selecionada por padrão.

4. Na seção **Desempenho**, selecione ou desmarque a caixa **Proteger somente arquivos novos e modificados**.

   Esta caixa de seleção ativa/desativa a verificação e a proteção de arquivos que foram reconhecidos pelo Kaspersky Embedded Systems Security como novos ou modificados desde a última verificação.

   Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará e protegerá apenas os arquivos reconhecidos como novos ou modificados desde a última verificação.

   Se a caixa estiver desmarcada, você poderá selecioná-la se quiser verificar e proteger apenas arquivos novos ou todos os arquivos, desconsiderando o status de modificação.

   Por padrão, a caixa de seleção está selecionada para o nível de segurança **Desempenho máximo**. Se os níveis de segurança **Proteção máxima** ou **Recomendado** estiverem definidos, a caixa estará desmarcada.

> Para alternar entre as opções disponíveis quando a caixa estiver desmarcada, clique no link **Todos** / **Apenas novos** para cada um dos tipos de objetos compostos.

5. Na seção **Proteção de objetos compostos**, especifique os objetos compostos que deseja incluir no escopo da proteção:

   - **Todos / Apenas novos arquivos compactados**

     Verificação dos arquivos compactados ZIP, CAB, RAR, ARJ e de outros formatos.

     Se essa a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos compactados.

     Se essa caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos compactados durante a verificação.

     O valor padrão depende do nível de proteção selecionado.

   - **Todos / Apenas novos arquivos compactados SFX**

     Verificação de arquivos compactados autoextraíveis.

     Se essa caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos compactados durante a verificação.

     Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos compactados SFX durante a verificação.

     O valor padrão depende do nível de proteção selecionado.

     Essa opção fica ativa quando a caixa de seleção **Arquivos compactados** é desmarcada.

   - **Todos / Apenas novos bancos de dados de e-mail**

     Verificação de arquivos de banco de dados de correio do Microsoft Outlook e Microsoft Outlook Express.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos de bancos de dados de e-mail.

     Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos de bancos de dados de e-mail durante a verificação.

     O valor padrão depende do nível de segurança selecionado.

   - **Todos / Apenas novos objetos compactados**

     Verificação de arquivos executáveis compactados por compactadores de código binário, como UPX ou ASPack.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos executáveis compactados por compactadores de código binário.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos executáveis compactados por compactadores de código binário durante a verificação.

     O valor padrão depende do nível de proteção selecionado.

   - **Todos / Apenas novos e-mails sem formatação**

     Verificação de arquivos de formato de e-mail, como mensagens do Microsoft Outlook e Microsoft Outlook Express.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos de formato de e-mail.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos de formato de e-mail durante a verificação.

O valor padrão depende do nível de segurança selecionado.

- **Todos / Apenas novos objetos OLE incorporados**

  Verificação de objetos incorporados em arquivos (como macros do Microsoft Word ou anexos de e-mail).

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os objetos inseridos em arquivos.

  Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os objetos inseridos em arquivos durante a verificação.

  O valor padrão depende do nível de proteção selecionado.

6. Clique em **Salvar**.

A nova configuração de tarefa será salva.

Configurar ações

► *Para configurar as ações em objetos infectados e outros objetos detectados da tarefa Proteção de Arquivos em Tempo Real:*

1. Abra a janela **Configurações do escopo da proteção** (consulte a seção "Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real" na página 257).
2. Selecione a guia **Ações**.
3. Selecione a ação a ser executada em objetos infectados e outros objetos detectados.
   - **Notificar somente**.

     Quando esse modo estiver selecionado, o Kaspersky Embedded Systems Security não bloqueará o acesso a objetos infectados ou outros objetos detectados, nem executará qualquer ação sobre eles. O seguinte evento é registrado no log de tarefas: *Objeto não desinfectado. Motivo: nenhuma ação foi executada para neutralizar o objeto detectado devido a configurações definidas pelos usuários.* O evento especifica todas as informações disponíveis sobre o objeto detectado.

     O modo **Notificar somente** deve ser configurado separadamente para cada área de verificação. Este modo não é usado por padrão para qualquer um dos níveis de segurança. Se você selecionar esse modo, o Kaspersky Embedded Systems Security alterará automaticamente o nível de segurança para **Personalizado**.
   - **Bloquear acesso**.

     Quando esta opção estiver selecionada o Kaspersky Embedded Systems Security bloqueará o acesso ao objeto detectado ou possivelmente infectado. É possível selecionar ação adicional para objetos bloqueados na lista suspensa.
   - **Executar ação adicional**.

     Selecionar ação da lista suspensa:

     - **Desinfectar**.
     - **Desinfectar. Desinfectar. Remover se a desinfecção falhar**.
     - **Remover**.
     - **Recomendado**.

4. Selecione a ação a ser executada em objetos possivelmente infectados:

   - **Notificar somente**.

     Quando esse modo estiver selecionado, o Kaspersky Embedded Systems Security não bloqueará o acesso a objetos infectados ou outros objetos detectados, nem executará qualquer ação sobre eles. O seguinte evento é registrado no log de tarefas: *Objeto não desinfectado. Motivo: nenhuma ação foi executada para neutralizar o objeto detectado devido a configurações definidas pelos usuários.* O evento especifica todas as informações disponíveis sobre o objeto detectado.

     O modo **Notificar somente** deve ser configurado separadamente para cada área de verificação. Este modo não é usado por padrão para qualquer um dos níveis de segurança. Se você selecionar esse modo, o Kaspersky Embedded Systems Security alterará automaticamente o nível de segurança para **Personalizado**.

   - **Bloquear acesso**.

     Quando esta opção estiver selecionada o Kaspersky Embedded Systems Security bloqueará o acesso ao objeto detectado ou possivelmente infectado. É possível selecionar ação adicional para objetos bloqueados na lista suspensa.

   - **Executar ação adicional**.

     Selecionar ação da lista suspensa:

     - **Quarentena**.
     - **Remover**.
     - **Recomendado**.

5. Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:

   a. Desmarque ou selecione a caixa **Executar ações dependendo do tipo de objeto detectado**.

      Se a caixa for selecionada, você pode definir a ação primária e secundária independentemente para cada tipo de objeto detectado clicando no botão **Configurações** ao lado da caixa. Nesse caso, o Kaspersky Embedded Systems Security não permitirá que um objeto infectado seja aberto ou executado independentemente da sua escolha.

      Se a caixa de seleção for desmarcada, o Kaspersky Embedded Systems Security executará as ações selecionadas nas seções **Ação a ser executada em objetos infectados e outros** e **Ação a ser executada em objetos possivelmente infectados** para os tipos de objetos indicados, respectivamente.

      Esta caixa é desmarcada por padrão.

   b. Clique no botão **Configurações**.

   c. Na janela que se abre, selecione a ação primária e secundária (se a primeira ação falhar) para cada tipo do objeto detectado.

   d. Clique em **OK**.

6. Selecione a ação a ser executada em arquivos compostos não modificáveis: selecione ou desmarque a caixa **Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte objeto incorporado**.

   Esta caixa ativa ou desativa a remoção forçada do arquivo composto pai quando um objeto malicioso, possivelmente infectado ou outro objeto filho incorporado for detectado.

   Se a caixa estiver selecionada e a tarefa for configurada para remover objetos infectados e possivelmente infectados, o Kaspersky Embedded Systems Security forçosamente

removerá todo o objeto composto pai quando um objeto incorporado malicioso ou outro objeto for detectado. A remoção forçada de um arquivo pai juntamente com todo o seu conteúdo ocorrerá se o aplicativo não puder remover apenas o objeto filho detectado (por exemplo, se o objeto pai não puder ser modificado).

Se esta caixa estiver desmarcada e a tarefa for configurada para remover objetos infectados e possivelmente infectados, o Kaspersky Embedded Systems Security não executará a ação selecionada se o objeto pai não puder ser modificado.

7. Clique em **Salvar**.

A nova configuração de tarefa será salva.

Configurar o desempenho

► *Para configurar o desempenho da tarefa de Proteção de Arquivos em Tempo Real:*

1. Abra a janela **Configurações do escopo da proteção** (consulte a seção "Abertura das configurações da tarefa de Proteção de Arquivos em Tempo Real" na página 257).
2. Selecione a guia **Desempenho**.
3. Na seção **Exclusões**:
   - Desmarque ou selecione a caixa **Excluir arquivos**.

     Excluindo arquivos da verificação pelo nome de arquivo ou pela máscara de nome de arquivo.

     Se esta caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará os objetos especificados durante a verificação.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará todos os objetos.

     Esta caixa é desmarcada por padrão.

   - Desmarque ou selecione a caixa **Não detectar**.

     Os objetos são excluídos da verificação pelo nome ou pela máscara de nome do objeto detectável. A lista de nomes de objetos detectáveis está disponível no site da Enciclopédia de Vírus https://encyclopedia.kaspersky.com/knowledge/classification/.

     Se esta caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará os objetos detectáveis especificados durante a verificação.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security detectará todos os objetos especificados no aplicativo por padrão.

     Esta caixa é desmarcada por padrão.

   - Clique no botão **Editar** de cada configuração para adicionar exclusões.
4. Na seção **Configurações avançadas**:
   - **Parar a verificação se demorar mais que (s)**

     Limita a duração da verificação do objeto. O valor padrão é 60 segundos.

     Se a caixa de seleção estiver selecionada, a duração da verificação será limitada ao valor especificado.

     Se a caixa de seleção estiver desmarcada, a duração da verificação será ilimitada.

Por padrão, a caixa de seleção está selecionada para o nível de segurança **Desempenho máximo**.

- **Não verificar obj. compostos com mais de (MB)**

  Exclui objetos maiores do que o tamanho especificado na verificação.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará objetos compostos cujo tamanho exceda o limite especificado durante a verificação de vírus.

  Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará os objetos compostos de qualquer tamanho.

  Por padrão, a caixa de seleção está selecionada para o nível de segurança **Desempenho máximo**.

- **Usar a tecnologia iSwift**

  A tecnologia iSwift compara o identificador NTFS do arquivo armazenado em um banco de dados com um identificador atual. A verificação é executada apenas para arquivos cujos identificadores foram alterados (novos arquivos e arquivos modificados desde a última verificação dos objetos do sistema NTFS).

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará apenas os novos arquivos ou aqueles modificados desde a última verificação dos objetos do sistema NTFS.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará objetos do sistema de arquivos NTFS sem considerar a data de criação ou modificação do arquivo, exceto em arquivos das pastas de rede.

  A caixa de seleção é selecionada por padrão.

- **Usar a tecnologia iChecker**

  A tecnologia iChecker calcula e lembra de somas de verificação de arquivos verificados. Se um objeto for modificado a soma de verificação é alterada. O aplicativo compara todas as somas de verificação durante a tarefa de verificação e verifica apenas objetos novos e modificados desde a última verificação de arquivos.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará apenas arquivos novos e modificados.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará os arquivos sem considerar a data de criação ou modificação do arquivo.

  A caixa de seleção é selecionada por padrão.

Estatísticas da tarefa de Proteção de Arquivos em Tempo Real

Enquanto uma tarefa de Proteção de arquivos em tempo real está sendo executada, é possível visualizar informações detalhadas em tempo real sobre o número de objetos processados pelo Kaspersky Embedded Systems Security desde que a tarefa tenha sido iniciada até o momento atual.

► *Para exibir as estatísticas de uma tarefa de Proteção de Arquivos em Tempo Real, siga as etapas a*

seguir:

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.
2. Selecione o nó filho **Proteção de Arquivos em Tempo Real**.

As estatísticas de tarefa são exibidas na seção **Estatísticas** do painel de detalhes do nó selecionado.

É possível visualizar informações sobre os objetos processados pelo Kaspersky Embedded Systems Security desde que ele foi iniciado até o momento atual (veja a tabela abaixo):

Tabela 43. Estatísticas da tarefa de Proteção de Arquivos em Tempo Real

Campo	Descrição
Detectado	Número total de objetos detectados pelo Kaspersky Embedded Systems Security. Por exemplo, se o Kaspersky Embedded Systems Security detectar um malware em cinco arquivos, o valor desse campo aumentará em um.
Objetos infectados e outros detectados	O número de objetos que o Kaspersky Embedded Systems Security encontrou e classificou como infeccionado ou o número de arquivos de software legítimos encontrados que podem ser usados por invasores para danificar o seu computador ou dados pessoais.
Objetos detectados possivelmente suspeitos	Número de objetos encontrados pelo Kaspersky Embedded Systems Security que estão possivelmente infectados.
Objetos não desinfectados	Número de objetos que o Kaspersky Embedded Systems Security não desinfetou pelos seguintes motivos: • O tipo de objeto detectado não pode ser desinfectado. • Ocorreu um erro durante a desinfecção.
Objetos não movidos para a Quarentena	O número de objetos que o Kaspersky Embedded Systems Security tentou colocar na Quarentena mas que não conseguiu, devido a espaço insuficiente no disco.
Objetos não removidos	O número de objetos que o Kaspersky Embedded Systems Security tentou excluir mas não conseguiu, devido, por exemplo, a um bloqueio no acesso ao objeto por parte de outro aplicativo.
Objetos não verificados	O número de objetos no escopo de proteção que o Kaspersky Embedded Systems Security não verificou devido, por exemplo, ao acesso ao objeto estar bloqueado por outro aplicativo.
Objetos sem backup	O número de objetos cujas cópias o Kaspersky Embedded Systems Security tentou salvar no Backup mas não conseguiu, por exemplo, devido a espaço de disco insuficiente.
Erros de processamento	Número de objetos cujo processamento resultou em um erro.
Objetos desinfectados	Número de objetos desinfectados pelo Kaspersky Embedded Systems Security.
Movidos para a Quarentena	Número de objetos colocados na Quarentena pelo Kaspersky Embedded Systems Security.
Movidos para o backup	O número de cópias de objetos salvas pelo Kaspersky Embedded Systems Security no Backup.

Campo	Descrição
Objetos removidos	Número de objetos removidos pelo Kaspersky Embedded Systems Security.
Objetos protegidos por senha	Número de objetos (arquivos compactados, por exemplo) que o Kaspersky Embedded Systems Security ignorou porque estavam protegidos por senha.
Objetos corrompidos	O número de objetos ignorados pelo Kaspersky Embedded Systems Security devido a corrupção do formato.
Objetos processados	Número total de objetos processados pelo Kaspersky Embedded Systems Security.

Você pode visualizar as estatísticas da tarefa de Proteção de Arquivos em Tempo Real no log de tarefas clicando em **Abrir log da tarefa** na seção **Gerenciamento** no painel de detalhes.

Se o valor do campo **Total de eventos:** na janela do log de tarefas de Proteção em Tempo Real exceder 0, recomenda-se processar os eventos encontrados no log de tarefa manualmente na guia **Eventos**.

Uso da KSN

Esta seção contém informações sobre a tarefa de Uso da KSN e como configurá-la.

Neste capítulo

Sobre a tarefa de Uso da KSN 274
Configurações padrão da tarefa de Uso da KSN 276
Gerenciando o Uso da KSN por meio do Plug-in de Administração 277
Gerenciando o Uso da KSN por meio do Console do Aplicativo 280
Configurando a transferência de dados adicionais 283
Estatísticas da tarefa de Uso da KSN 285

Sobre a tarefa de Uso da KSN

A *Kaspersky Security Network* (também referida como “KSN”) é uma infraestrutura de serviços on-line que fornece acesso à base de conhecimentos operacionais da Kaspersky Lab sobre a reputação de arquivos, de recursos da web e de programas. A Kaspersky Security Network permite ao Kaspersky Embedded Systems Security reagir muito rapidamente a novas ameaças, melhora o desempenho de vários componentes de proteção e reduz a probabilidade de falsos positivos.

Para iniciar a tarefa de Uso da KSN, você deve aceitar a Declaração da Kaspersky Security Network.

As informações recebidas pelo Kaspersky Embedded Systems Security da Kaspersky Security Network referem-se apenas à reputação de programas.

A participação na KSN permite que a Kaspersky Lab receba informações em tempo real sobre os tipos e fontes de novas ameaças, desenvolva modos de neutralizá-las e reduza o número de falsos positivos em componentes de aplicativo.

Mais informações detalhadas sobre transferência, processamento, armazenamento e destruição de informações sobre o uso do aplicativo estão disponíveis na janela **Manuseio de dados** da tarefa de Uso da KSN e na Política de Privacidade no site da Kaspersky Lab.

A participação na Kaspersky Security Network é voluntária. A decisão quanto à participação na Kaspersky Security Network é tomada durante ou após a instalação do Kaspersky Embedded Systems Security. É possível modificar a sua decisão sobre a participação na Kaspersky Security Network a qualquer momento.

O Kaspersky Security Network pode ser usado nas seguintes tarefas do Kaspersky Embedded Systems Security:

- Proteção de Arquivos em Tempo Real.
- Verificação por Demanda.
- Controle de Inicialização de Aplicativos.

Kaspersky Private Security Network

> Veja detalhes sobre como configurar a Kaspersky Private Security Network (também referida como “KSN Particular”) no *Kaspersky Security Center*.

Se você usar a KSN Particular no computador protegido, na janela **Manuseio de dados** (consulte a seção "Configurando o Manuseio de dados por meio do Plug-in de Administração" na página 279) da tarefa de Uso da KSN, é possível ler a Declaração da KSN e ativar a tarefa selecionando **Eu aceito a Declaração da Kaspersky Private Security Network**. Ao aceitar os termos, você aceita enviar todos os tipos de dados mencionados na Declaração da KSN (solicitações de segurança, dados estatísticos) aos serviços da KSN.

> Depois de aceitar os termos da KSN Particular, as caixas que ajustam o uso da KSN Global não estarão disponíveis.

Se você desativar a KSN Particular quando a tarefa de Uso da KSN estiver em execução, o erro *Violação da licença* ocorrerá e a tarefa será interrompida. Para continuar protegendo o computador, será necessário aceitar a Declaração da KSN na janela **Manuseio de dados** e reiniciar a tarefa.

Cancelar a aceitação da Declaração da KSN

Você pode cancelar a aceitação e interromper qualquer troca de dados com a Kaspersky Security Network a qualquer momento. As seguintes ações são consideradas como o cancelamento total ou parcial da Declaração da KSN:

- Desmarcar a caixa **Enviar dados dos arquivos verificados**: o aplicativo deixa de enviar somas de verificação de arquivos verificados ao serviço KSN para análise.
- Desmarcar a caixa **Enviar as estatísticas da Kaspersky Security Network**: o aplicativo deixa de processar dados com estatísticas adicionais da KSN.
- Desmarcar a caixa **Eu aceito os termos da Declaração da Kaspersky Security Network**: o aplicativo interrompe todo o processamento de dados relacionado à KSN e também interrompe a tarefa de Uso da KSN.
- Desinstalar o componente Uso da KSN: todo processamento de dados relacionado à KSN é interrompido.
- Desinstalar o Kaspersky Embedded Systems Security: todo processamento de dados relacionado à KSN é interrompido.

Configurações padrão da tarefa de Uso da KSN

É possível alterar as configurações padrão da tarefa de Uso da KSN (consulte a tabela abaixo).

Tabela 44. Configurações padrão da tarefa de Uso da KSN

Configuração	Valor padrão	Descrição
Ação a ser executada nos objetos não confiáveis da KSN	Remover	Você pode especificar ações que o Kaspersky Embedded Systems Security executará em objetos identificados pela KSN como não confiáveis.
Transferência de dados	A soma de verificação de arquivo (hash MD5) é calculada para arquivos que não excedam 2 MB de tamanho.	Você pode especificar o tamanho máximo de arquivos para os quais uma soma de verificação é calculada usando o algoritmo MD5 para a entrega à KSN. Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security calculará o hash MD5 para arquivos de qualquer tamanho.
Programação de inicialização da tarefa	A primeira execução não está programada.	É possível iniciar a tarefa manualmente ou configurar um início programado.
Usar o Kaspersky Security Center como Proxy da KSN	Selecionado	Por padrão, os dados são enviados à KSN por meio do Kaspersky Security Center. Só é possível alterar essa configuração por meio do Plug-in de Administração.
Eu aceito os termos da Declaração da Kaspersky Security Network	Desmarcada	Se selecionado, a participação na KSN depois da instalação é aceita. Você pode alterar a sua decisão a qualquer momento.
Enviar as estatísticas da Kaspersky Security Network	Selecionado (aplica-se apenas se a Declaração da KSN for aceita)	Se a Declaração da KSN for aceita, as estatísticas da KSN serão enviadas automaticamente, a menos que você desmarque a caixa.
Enviar dados dos arquivos verificados	Selecionado (aplica-se apenas se a Declaração da KSN for aceita)	Se a Declaração do KSN for aceita, os dados dos arquivos verificados e analisados desde que a tarefa foi iniciada são enviados Você pode desmarcar a caixa a qualquer momento.
Enviar dados sobre URLs verificados	Selecionado (aplica-se apenas se a Declaração da KSN for aceita)	Se a Declaração da KSN for aceita, o aplicativo envia informações sobre URLs acessados à Kaspersky Lab.
Aceitar os termos da Declaração da Kaspersky Managed Protection	Desmarcada	Você pode ativar ou desativar o serviço KMP. O serviço fica disponível apenas se o acordo adicional tiver sido assinado durante o processo de compra do aplicativo.

Gerenciando o Uso da KSN por meio do Plug-in de Administração

Nesta seção, aprenda a configurar a tarefa de Uso da KSN e o Gerenciamento de dados por meio do Plug-in de Administração.

Nesta seção

Configurando a tarefa de Uso da KSN por meio do Plug-in de Administração.....277
Configurando o Manuseio de Dados por meio do Plug-in de Administração.....279

Configurando a tarefa de Uso da KSN por meio do Plug-in de Administração

► *Para configurar a tarefa de Uso da KSN, siga as etapas a seguir:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
4. Na seção **Proteção do Computador em Tempo Real**, clique no botão **Configurações** no bloco **Uso da KSN**.

   A janela **Uso da KSN** é exibida.
5. Na guia **Geral**, defina as seguintes configurações de tarefa:
   - Na seção **Ação a ser executada nos objetos não confiáveis da KSN**, especifique a ação que o Kaspersky Embedded Systems Security deverá executar se detectar um objeto identificado pela KSN como infectado:
     - **Remover**

       O Kaspersky Embedded Systems Security exclui o objeto com o status não confiável da KSN e coloca uma cópia dele no Backup.

       Esta opção é selecionada por padrão.
     - **Informações de log**

O Kaspersky Embedded Systems Security registra informações sobre o objeto com o status não confiável da KSN no log de tarefas. O Kaspersky Embedded Systems Security não exclui o objeto não confiável.

- Na seção **Transferência de dados**, restrinja o tamanho dos arquivos para que a soma de verificação seja calculada:
  - Desmarque ou selecione a caixa **Não calcular a soma de verificação antes de enviar à KSN se o tamanho do arquivo ultrapassar (MB)**.

    Esta caixa ativa ou desativa o cálculo da soma de verificação para arquivos do tamanho especificado para a entrega destas informações ao serviço da KSN.

    A duração do cálculo de soma de verificação depende do tamanho do arquivo.

    Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security não calculará a soma de verificação de arquivos que excedam o tamanho especificado (em MB).

    Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security calculará a soma de verificação para arquivos de qualquer tamanho.

    A caixa de seleção é selecionada por padrão.
  - Se necessário, no campo à direita, altere o tamanho máximo de arquivos para os quais o Kaspersky Embedded Systems Security calcula a soma de verificação.
- Na seção **Proxy da KSN**, desmarque ou selecione a caixa **Usar o Kaspersky Security Center como Proxy da KSN**.

  A caixa permite gerenciar a transferência de dados entre os computadores protegidos e a KSN.

  Se a caixa for desmarcada os dados do Servidor de Administração e dos computadores protegidos são enviados à KSN diretamente (não via o Kaspersky Security Center). A política ativa define que tipo de dados pode ser enviado à KSN diretamente.

  Se a caixa for selecionada, todos os dados são enviados à KSN via o Kaspersky Security Center.

  A caixa de seleção é selecionada por padrão.

Para ativar o Proxy da KSN a Declaração da KSN deve ser aceita e o Kaspersky Security Center propriamente configurado. Consulte a *Ajuda do Kaspersky Security Center* para mais detalhes.

6. Se necessário, configure a programação de inicialização da tarefa na guia **Gerenciamento da tarefa**. Por exemplo, você pode ativar o início da tarefa por programação e especificar a frequência de início da tarefa **Ao iniciar o aplicativo** se desejar que a tarefa seja executada automaticamente quando o servidor for reiniciado.

   O aplicativo iniciará automaticamente a tarefa de Uso da KSN de acordo com a programação.
7. Configure o manuseio de dados (consulte a seção "Configurando o Manuseio de Dados por meio do Plug-in de Administração" na página 279) antes de iniciar a tarefa.
8. Clique em **OK**.

As configurações modificadas são aplicadas. A data e hora da modificação das configurações, bem como informações sobre as configurações de tarefa antes e depois da modificação, são salvas no log de auditoria do sistema.

Configurando o Manuseio de Dados por meio do Plug-in de Administração

► *Para configurar quais dados serão processados pelos serviços da KSN e aceitar a Declaração da KSN:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
4. Na seção **Proteção do Computador em Tempo Real** clique no botão **Manuseio de dados** no bloco **Uso da KSN**.

   A janela **Manuseio de dados** é exibida.
5. Na guia **Estatísticas e serviços**, leia a Declaração e selecione a caixa **Eu aceito os termos da Declaração da Kaspersky Security Network**.
6. Para aumentar o nível de proteção, as seguintes caixas são selecionadas automaticamente:
   - **Enviar dados dos arquivos verificados**.

     Se a caixa for selecionada, o Kaspersky Embedded Systems Security envia a soma de verificação dos arquivos verificados para a Kaspersky Lab. A conclusão sobre a segurança de cada arquivo baseia-se na reputação recebida da KSN.

     Se a caixa for desmarcada, o Kaspersky Embedded Systems Security não envia a soma de verificação dos arquivos à KSN.

     Note que as solicitações de reputação de arquivos poderiam ser enviadas em um modo limitado. As limitações são usadas para proteger os servidores de reputação da Kaspersky Lab de ataques DDoS. Neste cenário, os parâmetros das solicitações de reputação de arquivos sendo enviados são definidos pelas regras e pelos métodos estabelecidos por especialistas da Kaspersky Lab, e não podem ser configurados pelo usuário em um computador protegido. As atualizações dessas regras e métodos são recebidas juntamente com as atualizações do banco de dados do aplicativo. Se as limitações forem aplicadas, o status *Ativado pela Kaspersky Lab para proteger os servidores KSN contra DDoS* é exibido na estatística da tarefa de Uso da KSN.

     A caixa de seleção é selecionada por padrão.
   - **Enviar as estatísticas da Kaspersky Security Network.**

     Se a caixa for selecionada o Kaspersky Embedded Systems Security envia estatísticas

adicionais que podem conter dados pessoais. A lista de todos os dados enviados como estatística da KSN é especificada na Declaração da KSN. Os dados recebidos pela Kaspersky Lab são usados para melhorar a qualidade dos aplicativos e as taxas de detecção de ameaças.

Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não enviará estatísticas adicionais.

A caixa de seleção é selecionada por padrão.

Você pode desmarcar estas caixas e deixar de enviar dados adicionais a qualquer momento.

7. Na guia **Kaspersky Managed Protection**, leia a Declaração e selecione a caixa **Eu aceito os termos da Kaspersky Managed Protection**.

   Se a caixa for selecionada, você aceita enviar estatísticas das atividades do computador protegido aos especialistas da Kaspersky Lab. Os dados recebidos serão usados para análise e reporte contínuos, necessários para impedir incidentes de violação de segurança.

   Esta caixa é desmarcada por padrão.

   Alterações no status da caixa **Eu aceito os termos da Kaspersky Managed Protection** não iniciam ou interrompem o processamento de dados imediatamente. Para aplicar as alterações, é necessário reiniciar o Kaspersky Embedded Systems Security.

   Para usar o serviço KMP, é necessário assinar o acordo correspondente e executar os arquivos de configuração em um computador protegido.

   Para usar o serviço KMP os termos de processamento de dados da Declaração da KSN na guia **Estatísticas e serviços** devem ser aceitos.

8. Clique em **OK**.

   A configuração de processamento de dados será salva.

Gerenciando o Uso da KSN por meio do Console do Aplicativo

Nesta seção, aprenda como configurar a tarefa de Uso da KSN e Manuseio de dados por meio do Console do Aplicativo.

Nesta seção

Configurando a tarefa de Uso da KSN por meio do Console do Aplicativo 281

Configurando o Manuseio de Dados por meio do Console do Aplicativo 282

Configurando a tarefa de Uso da KSN por meio do Console do Aplicativo

► *Para configurar a tarefa de Uso da KSN, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.
2. Selecione o nó filho **Uso da KSN**.
3. Clique no link **Propriedades** no painel de detalhes.

   A janela **Configurações de tarefa** é exibida na guia **Geral**.
4. Configure a tarefa:
   - Na seção **Ação a ser executada nos objetos não confiáveis da KSN**, especifique a ação que o Kaspersky Embedded Systems Security deverá executar se detectar um objeto identificado pela KSN como infectado:
     - **Remover**

       O Kaspersky Embedded Systems Security exclui o objeto com o status não confiável da KSN e coloca uma cópia dele no Backup.

       Esta opção é selecionada por padrão.
     - **Informações de log**

       O Kaspersky Embedded Systems Security registra informações sobre o objeto com o status não confiável da KSN no log de tarefas. O Kaspersky Embedded Systems Security não exclui o objeto não confiável.
   - Na seção **Transferência de dados**, restrinja o tamanho dos arquivos para que a soma de verificação seja calculada:
     - Desmarque ou selecione a caixa **Não calcular a soma de verificação antes de enviar à KSN se o tamanho do arquivo ultrapassar (MB)**.

       Esta caixa ativa ou desativa o cálculo da soma de verificação para arquivos do tamanho especificado para a entrega destas informações ao serviço da KSN.

       A duração do cálculo de soma de verificação depende do tamanho do arquivo.

       Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security não calculará a soma de verificação de arquivos que excedam o tamanho especificado (em MB).

       Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security calculará a soma de verificação para arquivos de qualquer tamanho.

       A caixa de seleção é selecionada por padrão.
     - Se necessário, no campo à direita, altere o tamanho máximo de arquivos para os quais o Kaspersky Embedded Systems Security calcula a soma de verificação.
5. Se necessário, configure a programação de inicialização da tarefa nas guias **Programação** e **Avançado**. Por exemplo, você pode ativar a inicialização de tarefa por programação e especificar a frequência da inicialização da tarefa **Ao iniciar o aplicativo** se desejar que a tarefa seja executada automaticamente quando o computador for reiniciado.

   O aplicativo iniciará automaticamente a tarefa de Uso da KSN de acordo com a programação.
6. Configure o Manuseio de dados (consulte a seção "Configurando o Manuseio de dados por meio por meio

do Console do Aplicativo" na página 282) antes de iniciar a tarefa.

7. Clique em **OK**.

As configurações modificadas são aplicadas. A data e hora da modificação das configurações, bem como informações sobre as configurações de tarefa antes e depois da modificação, são salvas no log de auditoria do sistema.

Configurando o Manuseio de dados por meio do Console do Aplicativo

► *Para configurar quais dados serão processados pelos serviços da KSN e aceitar a Declaração da KSN:*

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.
2. Selecione o nó filho **Uso da KSN**.
3. Clique no link **Manuseio de dados** no painel de detalhes.

   A janela **Manuseio de dados** é exibida.
4. Na guia **Estatísticas e serviços**, leia a Declaração e selecione a caixa **Eu aceito os termos da Declaração da Kaspersky Security Network**.
5. Para aumentar o nível de proteção, as seguintes caixas são selecionadas automaticamente:

   - **Enviar dados dos arquivos verificados**.

     Se a caixa for selecionada, o Kaspersky Embedded Systems Security envia a soma de verificação dos arquivos verificados para a Kaspersky Lab. A conclusão sobre a segurança de cada arquivo baseia-se na reputação recebida da KSN.

     Se a caixa for desmarcada, o Kaspersky Embedded Systems Security não envia a soma de verificação dos arquivos à KSN.

     Note que as solicitações de reputação de arquivos poderiam ser enviadas em um modo limitado. As limitações são usadas para proteger os servidores de reputação da Kaspersky Lab de ataques DDoS. Neste cenário, os parâmetros das solicitações de reputação de arquivos sendo enviados são definidos pelas regras e pelos métodos estabelecidos por especialistas da Kaspersky Lab, e não podem ser configurados pelo usuário em um computador protegido. As atualizações dessas regras e métodos são recebidas juntamente com as atualizações do banco de dados do aplicativo. Se as limitações forem aplicadas, o status *Ativado pela Kaspersky Lab para proteger os servidores KSN contra DDoS* é exibido na estatística da tarefa de Uso da KSN.

     A caixa de seleção é selecionada por padrão.

   - **Enviar as estatísticas da Kaspersky Security Network.**

     Se a caixa for selecionada o Kaspersky Embedded Systems Security envia estatísticas adicionais que podem conter dados pessoais. A lista de todos os dados enviados como estatística da KSN é especificada na Declaração da KSN. Os dados recebidos pela Kaspersky Lab são usados para melhorar a qualidade dos aplicativos e as taxas de detecção de ameaças.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não enviará estatísticas adicionais.

A caixa de seleção é selecionada por padrão.

Você pode desmarcar estas caixas e deixar de enviar dados adicionais a qualquer momento.

6. Na guia **Kaspersky Managed Protection**, leia a Declaração e selecione a caixa **Eu aceito os termos da Kaspersky Managed Protection**.

   Se a caixa for selecionada, você aceita enviar estatísticas das atividades do computador protegido aos especialistas da Kaspersky Lab. Os dados recebidos serão usados para análise e reporte contínuos, necessários para impedir incidentes de violação de segurança.

   Esta caixa é desmarcada por padrão.

   Alterações no status da caixa **Eu aceito os termos da Kaspersky Managed Protection** não iniciam ou interrompem o processamento de dados imediatamente. Para aplicar as alterações, é necessário reiniciar o Kaspersky Embedded Systems Security.

   Para usar o serviço KMP, é necessário assinar o acordo correspondente e executar os arquivos de configuração em um computador protegido.

   Para usar o serviço KMP os termos de processamento de dados da Declaração da KSN na guia **Estatísticas e serviços** devem ser aceitos.

7. Clique em **OK**.

A configuração de processamento de dados será salva.

Configurando a transferência de dados adicionais

O Kaspersky Embedded Systems Security pode ser configurado para enviar os seguintes dados à Kaspersky Lab:

- Somas de verificação de arquivos verificados (caixa de seleção **Enviar dados dos arquivos verificados**).
- Estatísticas adicionais, inclusive dados pessoais (caixa de seleção **Enviar as estatísticas da Kaspersky Security Network**).

Consulta a seção "Tratamento local de dados" neste manual para obter informações detalhadas sobre dados enviados à Kaspersky Lab.

As caixas correspondentes podem ser selecionadas ou desmarcadas (consulte a seção "Configurando o Manuseio de dados por meio do Console do Aplicativo" na página 282) apenas se a caixa **Eu aceito os termos da Declaração da Kaspersky Security Network** for selecionada.

Por padrão, o Kaspersky Embedded Systems Security envia somas de verificação de arquivos e estatísticas adicionais após aceitar a Declaração da KSN.

Tabela 45. Estados possíveis de caixas de seleção e condições correspondentes

Estado da caixa	**Condições de estado da caixa** Enviar dados dos arquivos verificados	**Condições de estado da caixa** Enviar as estatísticas da Kaspersky Security Network	**Condições de estado da caixa de seleção** Enviar dados dos URLs verificados	**Condições de estado da caixa de seleção** Aceito os termos da Declaração da Kaspersky Managed Protection	**Condições de estado da caixa** Eu aceito os termos da Declaração da Kaspersky Security Network
☑	• solicitações de reputação são enviadas • a caixa pode ser editada	• estatísticas adicionais são enviadas • a caixa pode ser editada	• os dados sobre URLs verificados são enviados • a caixa pode ser editada	• os termos da Declaração da Kaspersky Managed Protection são aceitos • a caixa pode ser editada	• os termos da Declaração da Kaspersky Security Network são aceitos • a caixa pode ser editada
☑	• solicitações de reputação são enviadas • a caixa não pode ser editada	• estatísticas adicionais são enviadas • a caixa não pode ser editada	• os dados sobre URLs verificados são enviados • a caixa não pode ser editada	• os termos da Declaração da Kaspersky Managed Protection são aceitos • a caixa não pode ser editada	• os termos da Declaração da Kaspersky Security Network são aceitos • a caixa não pode ser editada
☐	• solicitações de reputação não são enviadas • a caixa pode ser editada	• estatísticas adicionais não são enviadas • a caixa pode ser editada	• os dados sobre URLs verificados não são enviados • a caixa pode ser editada	• os termos da Declaração da Kaspersky Managed Protection não são aceitos • a caixa pode ser editada	• os termos da Declaração da Kaspersky Security Network não são aceitos • a caixa pode ser editada
☐	• solicitações de reputação não são enviadas • a caixa não pode ser editada	• estatísticas adicionais não são enviadas • a caixa não pode ser editada	• os dados sobre URLs verificados não são enviados • a caixa não pode ser editada	• os termos da Declaração da Kaspersky Managed Protection não são aceitos • a caixa não pode ser editada	• os termos da Declaração da Kaspersky Security Network não são aceitos • a caixa não pode ser editada

Estatísticas da tarefa de Uso da KSN

Enquanto uma tarefa de Uso da KSN está sendo executada, é possível visualizar informações detalhadas sobre o número de objetos processados pelo Kaspersky Embedded Systems Security desde de foi iniciado até o momento atual. As informações sobre todos os eventos que ocorrem durante a execução da tarefa são registradas no log de tarefas (consulte a seção "Sobre logs de tarefa" na página 204).

► *Para exibir estatísticas da tarefa de Uso da KSN, siga as etapas a seguir:*

1. Na árvore do Console do Aplicativo, expanda o nó **Proteção do Computador em Tempo Real**.
2. Selecione o nó filho **Uso da KSN**.

As estatísticas de tarefa são exibidas na seção **Estatísticas** do painel de detalhes do nó selecionado.

Você pode visualizar informações sobre objetos processados pelo Kaspersky Embedded Systems Security desde quando a tarefa foi iniciada (consulte a tabela abaixo).

Tabela 46. Estatísticas da tarefa de Uso da KSN

Campo	Descrição
Erros no envio de solicitações	Número de solicitações da KSN cujo processamento resultou em um erro de tarefa.
Estatísticas formadas	Número de pacotes estatísticos gerados e enviados à KSN.
Objetos removidos	Número de objetos que o Kaspersky Embedded Systems Security excluiu ao executar a tarefa de Uso da KSN.
Movidos para o backup	O número de cópias de objetos salvas pelo Kaspersky Embedded Systems Security no Backup.
Objetos não removidos	O número de objetos que o Kaspersky Embedded Systems Security tentou excluir mas não conseguiu, devido, por exemplo, a um bloqueio no acesso ao objeto por parte de outro aplicativo. As informações sobre tais objetos são registradas no log de tarefas.
Objetos dos quais não foi feito backup	O número de objetos cujas cópias o Kaspersky Embedded Systems Security tentou salvar no Backup mas não conseguiu, por exemplo, devido a espaço de disco insuficiente. O aplicativo não desinfecta ou exclui arquivos que não podem ser movidos para o Backup. As informações sobre tais objetos são registradas no log de tarefas.
Modo limitado	O status indica se o aplicativo envia solicitações de reputação de arquivo em um modo limitado.

Controle de Inicialização de Aplicativos

Esta seção contém informações sobre a tarefa de Controle de Inicialização de Aplicativos e como configurá-la.

Neste capítulo

Sobre a tarefa de Controle de Inicialização de Aplicativos 286
Sobre as regras de Controle de inicialização de aplicativos 287
Sobre o Controle de Distribuição de Software 289
Sobre o uso da KSN para a tarefa de Controle de Inicialização de Aplicativos 292
Geração de regras de Controle de Inicialização de Aplicativos 293
Configurações padrão da tarefa de Controle de Inicialização de Aplicativos 295
Gerenciamento do Controle de Inicialização de Aplicativos por meio do Plug-in de Administração 298
Gerenciamento do Controle de Inicialização de Aplicativos por meio do Console do Aplicativo 320

Sobre a tarefa de Controle de Inicialização de Aplicativos

Durante a execução da tarefa de Controle de Inicialização de Aplicativos, o Kaspersky Embedded Systems Security monitora as tentativas de inicialização de aplicativos por usuários e permite ou nega a inicialização desses aplicativos. A tarefa de Controle de Inicialização de Aplicativos baseia-se no princípio de Negação Padrão, o que significa que qualquer aplicativo que não tenha permissão configurada na tarefa será automaticamente bloqueado.

Você pode permitir a inicialização de aplicativos usando um dos seguintes métodos:

- Definir regras de permissão para aplicativos confiáveis.
- Verificar a reputação de aplicativos confiáveis na KSN na inicialização.

A tarefa dá a prioridade máxima à negação da inicialização de aplicativos. Por exemplo, se um aplicativo for impedido de iniciar por uma das regras de bloqueio, a inicialização do aplicativo será negada independentemente da conclusão confiável da KSN. Nesse caso, se o aplicativo for considerado não confiável pelos serviços da KSN, mas estiver incluído no escopo de uma regra de permissão, sua inicialização será negada.

Todas as tentativas de iniciar aplicativos são registradas no log de tarefas (consulte a seção "Sobre logs de tarefas" na página 204).

A tarefa de Controle de Inicialização de Aplicativos pode operar em um de dois modos:

- **Ativa**. O Kaspersky Embedded Systems Security usa um conjunto de regras para controlar a inicialização de aplicativos que se enquadram no escopo das regras de Controle de inicialização de aplicativos. O escopo das regras de Controle de inicialização de aplicativos é especificado nas configurações dessa tarefa. Se um aplicativo se enquadrar no escopo das regras de Controle de inicialização de aplicativos, e as configurações da tarefa não satisfizerem alguma regra especificada, a inicialização do aplicativo será

negada.

A inicialização dos aplicativos que não se enquadram no escopo de nenhuma regra especificada nas configurações de tarefa de Controle de inicialização de aplicativos é permitida, independentemente das configurações de tarefa de Controle de inicialização de aplicativos.

A tarefa de **Controle de Inicialização de Aplicativos** não pode ser iniciada no modo Ativa se nenhuma regra tiver sido criada ou se houver mais de 65.535 regras para um computador.

- **Somente Estatísticas**. O Kaspersky Embedded Systems Security não usa as regras de Controle de Inicialização de Aplicativos para permitir ou negar a inicialização de aplicativos. Em vez disso, ele apenas registra informações sobre a inicialização de aplicativos, sobre as regras atendidas pelos aplicativos em execução e ações que seriam executadas se a tarefa estivesse sendo executada no modo **Ativa**. Todos os aplicativos podem ser inicializados. Este modo está definido por padrão.

  Você pode usar esse modo para criar regras de Controle de inicialização de aplicativos (consulte a seção "Criação de regras de permissão a partir de eventos da tarefa de Controle de Inicialização de Aplicativos" na página 332) com base nas informações registradas no log de tarefas.

Você pode configurar a tarefa de Controle de Inicialização de Aplicativos de acordo com um dos seguintes cenários:

- Configuração avançada de regras (consulte a seção "Sobre regras de Controle de inicialização de aplicativos" na página 287) e seu uso para Controle de inicialização de aplicativos.
- Configuração básica de regras e uso da KSN (consulte a seção "Configuração do uso da KSN" na página 325) para o Controle de inicialização de aplicativos.

Se os arquivos do sistema operacional estiverem enquadrados no escopo da tarefa de Controle de inicialização de aplicativos, recomendamos que, ao criar as regras de Controle de inicialização de aplicativos, você se certifique de tais aplicativos devem ser permitidos pela criação de novas regras. Caso contrário, o sistema operacional pode não conseguir ser iniciado.

O Kaspersky Embedded Systems Security também intercepta processos iniciados sob o Subsistema do Windows para Linux (exceto scripts executados no shell do UNIX™ ou interpretadores da linha de comando). Para tais processos, a tarefa de Controle de Inicialização de Aplicativos aplica a ação definida pela configuração atual. A tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos reconhece a inicialização do aplicativo e gera regras correspondentes para aplicativos executados sob o Subsistema do Windows para Linux.

Sobre as regras de Controle de inicialização de aplicativos

Como funcionam as regras de Controle de inicialização de aplicativos

A operação das regras de Controle de inicialização de aplicativos é baseada nos seguintes componentes:

- Tipo de regra.

  As regras de Controle de Inicialização de Aplicativos podem permitir ou negar a inicialização de um aplicativo. Consequentemente, elas são chamadas de regras de *permissão* ou *negação*. Para criar uma lista de regras de permissão para o Controle de inicialização de aplicativos, você pode usar o Gerador de Regras para gerar regras de permissão ou usar a tarefa de Controle de Inicialização de Aplicativos no

modo **Somente Estatísticas**. Você também pode adicionar regras de permissão manualmente.

- Usuário e/ou grupo de usuário.

  As regras de Controle de Inicialização de Aplicativos podem controlar a inicialização de aplicativos específicos por um usuário e/ou grupo de usuários.

- Escopo de uso da regra.

  As regras de Controle de Inicialização de Aplicativos podem ser aplicadas à inicialização de *arquivos executáveis*, *scripts* e *pacotes MSI*.

- Critério para acionamento de regras.

  As regras de Controle de inicialização de aplicativos controlam a inicialização de arquivos que satisfazem um dos critérios especificados nas configurações da regra: assinados pelo *certificado digital* especificado, correspondem ao *hash SHA256* especificado ou estão localizados no *caminho* especificado.

  Se o **Certificado digital** for estabelecido como critério para acionamento de regras, a regra criada controla a inicialização de todos os aplicativos confiáveis no sistema operacional. Você pode estabelecer condições mais estritas para este critério selecionando as caixas de seleção a seguir:

  - **Usar assunto**

    A caixa de seleção ativa ou desativa o uso do requerente do certificado digital como critério para acionamento de regras.

    Se a caixa estiver selecionada, o requerente especificado do certificado digital será usado como critério para acionamento de regras. A regra criada controlará a inicialização de aplicativos somente para o fornecedor especificado no requerente.

    Se a caixa estiver desmarcada, o aplicativo não usará o requerente do certificado digital como critério para acionamento de regras. Se o critério do **Certificado digital** for selecionado, a regra criada controlará a inicialização de aplicativos assinados com um certificado digital que contenha qualquer requerente.

    O requerente do certificado digital usado para assinar o arquivo pode ser especificado somente a partir das propriedades do arquivo selecionado usando o botão **Definir critério disponíveis de regra a partir das propriedades do arquivo** localizado acima da seção **Critério para acionamento de regras**.

    Esta caixa é desmarcada por padrão.

  - **Usar miniatura**

    A caixa de seleção ativa ou desativa o uso da impressão digital do certificado digital como critério para acionamento de regras.

    Se a caixa estiver selecionada, a impressão digital especificada do certificado digital será usada como critério para acionamento de regras. A regra criada controlará a inicialização de aplicativos assinados com um certificado digital com a impressão digital especificada.

    Se a caixa estiver desmarcada, o aplicativo não usará a impressão digital do certificado digital como critério para acionamento de regras. Se o critério do **Certificado digital** for selecionado, o aplicativo controlará a inicialização de aplicativos assinados com um certificado digital que contenha qualquer impressão digital.

    A impressão digital do certificado digital usada para assinar o arquivo pode ser especificada somente a partir das propriedades do arquivo selecionado usando o botão **Definir critério disponíveis de regra a partir das propriedades do arquivo** localizado acima da seção **Critério para acionamento de regras**.

Esta caixa é desmarcada por padrão.

O uso de impressões digitais permite o acionamento mais restrito das regras de inicialização de aplicativos com base em um certificado digital, pois uma impressão digital é um identificador único de um certificado digital e não pode ser forjada, diferentemente do requerente de um certificado digital.

Você pode especificar exclusões das regras de Controle de inicialização de aplicativos. As exclusões das regras de Controle de inicialização de aplicativos são baseadas nos mesmos critérios usados para acionar as regras: certificado digital, hash SHA256 e caminho do arquivo. As exclusões das regras de Controle de inicialização de aplicativos podem ser necessárias para especificar certas regras de permissão: por exemplo, se você quiser permitir que os usuários iniciem aplicativos no caminho C:\Windows, enquanto bloqueia a inicialização do arquivo Regedit.exe.

Se os arquivos do sistema operacional estiverem enquadrados no escopo da tarefa de Controle de inicialização de aplicativos, recomendamos que, ao criar as regras de Controle de inicialização de aplicativos, você se certifique de tais aplicativos devem ser permitidos pela criação de novas regras. Caso contrário, o sistema operacional pode não conseguir ser iniciado.

Gerenciando regras de Controle de inicialização de aplicativos

Você pode executar as seguintes ações com as regras de Controle de inicialização de aplicativos:

- Adicionar regras manualmente.
- Gerar e adicionar regras automaticamente.
- Remover regras.
- Exportar regras para o arquivo.
- Verificar arquivos selecionados para regras que permitam a execução desses arquivos.
- Filtrar as regras na lista segundo o critério especificado.

Sobre o Controle de Distribuição de Software

Gerar regras de Controle de Inicialização de Aplicativos pode ser complicado se você também tiver que controlar a distribuição de software em um computador protegido, por exemplo, em computadores onde o software instalado é atualizado automaticamente de maneira periódica. Nesse caso, a lista de regras de permissão deve ser atualizada após cada atualização de software para que arquivos recém-criados sejam considerados nas configurações da tarefa de Controle de Inicialização de Aplicativos. Para simplificar o controle de inicialização nos cenários de distribuição de software, você pode usar o subsistema de Controle de Distribuição de Software.

Um pacote de distribuição de software (a partir de agora referido como “pacote”) representa um aplicativo de software a ser instalado em um computador. Cada pacote contém pelo menos um aplicativo e também pode conter arquivos individuais, atualizações, ou até mesmo um comando individual, além dos aplicativos, particularmente ao instalar um aplicativo de software ou atualização.

O subsistema de Controle de Distribuição de Software é implementado como uma lista adicional de exclusões. Quando você adiciona um pacote de distribuição de software a essa lista, o aplicativo permitirá a descompactação desses pacotes confiáveis e permitir que softwares instalados ou modificados por um pacote confiável sejam inicializados automaticamente. Os arquivos extraídos podem herdar o atributo de confiabilidade do pacote primário

de distribuição. *Um pacote primário de distribuição* é um pacote que foi adicionado à lista de exclusões de Controle de Distribuição de Software por um usuário e se tornou um pacote confiável.

O Kaspersky Embedded Systems Security controla apenas ciclos completos de distribuição de software. O aplicativo não pode processar corretamente a inicialização de arquivos modificados por um pacote confiável se, quando o pacote for iniciado pela primeira vez, o controle de distribuição de software estiver desativado ou o componente de Controle de Inicialização de Aplicativos não estiver instalado.

O controle de distribuição de software não está disponível se a caixa **Aplicar regras a arquivos executáveis** estiver desmarcada nas configurações da tarefa de Controle de Inicialização de Aplicativos.

Cache de distribuição de software

O Kaspersky Embedded Systems Security usa um cache de distribuição de software gerado dinamicamente ("cache de distribuição") para estabelecer a relação entre pacotes confiáveis e arquivos criados durante a distribuição de software. Quando o pacote é iniciado pela primeira vez, o Kaspersky Embedded Systems Security detecta todos os arquivos criados pelo pacote durante o processo de distribuição de software e armazena as somas de verificação dos arquivos e os caminhos no cache de distribuição. Então todos os arquivos no cache de distribuição podem ser inicializados por padrão.

Você não pode analisar, limpar ou modificar manualmente o cache de distribuição por meio da interface de usuário. O cache é preenchido e controlado pelo Kaspersky Embedded Systems Security.

Você pode exportar o cache de distribuição para um arquivo de configuração (no formato XML) e limpar o cache usando opções de linha de comando.

► *Para exportar o cache de distribuição para um arquivo de configuração, execute o seguinte comando:*

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

► *Para limpar o cache de distribuição, execute o seguinte comando:*

```
kavshell appcontrol /config /clearsdc
```

O Kaspersky Embedded Systems Security atualiza o cache de distribuição a cada 24 horas. Se a soma de verificação de um arquivo permitido anteriormente forem alterados, o aplicativo exclui o registro desse arquivo do cache de distribuição. Se a tarefa de Controle de Inicialização de Aplicativos for iniciada no modo Ativa, tentativas subsequentes de inicialização desse arquivo serão bloqueadas. Se o caminho completo do arquivo anteriormente permitido for alterado, as tentativas subsequentes de iniciar esse arquivo não serão bloqueadas, porque a soma de verificação é armazenada dentro do cache de distribuição.

Processamento dos arquivos extraídos

Todos os arquivos extraídos de um pacote confiável herdam o atributo de confiabilidade na primeira execução do pacote. Se você desmarcar a caixa de seleção após a primeira inicialização, todos os arquivos extraídos do pacote reterão o atributo herdado. Para reinicializar o atributo herdado em todos os arquivos extraídos, você precisará limpar o cache de distribuição e desmarcar a caixa **Permitir a inicialização para todos os arquivos desta cadeia de extração do pacote de distribuição** antes de iniciar o pacote de distribuição confiável novamente.

Os arquivos e pacotes extraídos criados por um pacote primário de distribuição confiável herdam o atributo de confiabilidade quando as suas somas de verificação são adicionadas ao cache de distribuição quando o pacote de distribuição de software na lista de exclusão é aberto pela primeira vez. Portanto, o próprio pacote de distribuição e todos os arquivos extraídos desse pacote também serão confiáveis. Por padrão, o número de níveis de herança do atributo de confiabilidade é ilimitado.

Os arquivos extraídos manterão o atributo de confiabilidade após a reinicialização do sistema operacional.

O processamento de arquivos é definido nas configurações de Controle de Distribuição de Software (consulte a seção "Configuração do controle de distribuição de software" na página 303) selecionando ou desmarcando a caixa **Permitir a inicialização para todos os arquivos desta cadeia de extração do pacote de distribuição**.

Por exemplo, suponha que você adicione um pacote test.msi contendo vários outros pacotes e aplicativos à lista de exclusões selecione a caixa. Nesse caso, todos os pacotes e aplicativos contidos no pacote test.msi podem ser executados ou extraídos se contiverem outros arquivos. Este cenário funciona para arquivos extraídos em todos os níveis aninhados.

Se você adicionar um pacote test.msi à lista de exclusões e desmarcar a caixa **Permitir a inicialização para todos os arquivos desta cadeia de extração do pacote de distribuição**, o aplicativo definirá o atributo de confiabilidade apenas aos pacotes e arquivos executáveis extraídos diretamente do pacote confiável primário (aninhado no primeiro nível). As somas de verificação de tais arquivos são armazenadas em cache de distribuição. Todos os arquivos aninhados ao segundo nível e além serão bloqueados pelo princípio de Negação padrão.

Trabalhando com a lista de regras de Controle de inicialização de aplicativos

A lista de pacotes confiáveis do subsistema de controle de distribuição de software é uma lista de exclusões que amplifica, mas não substitui a lista geral de regras de controle de inicialização de aplicativos.

As regras de negação de controle de inicialização de aplicativos têm a prioridade mais alta: a descompressão de pacotes confiáveis e a inicialização de arquivos novos ou modificados serão bloqueadas caso tais pacotes e arquivos forem afetados pelas regras de negação de controle de inicialização de aplicativos.

As exclusões do controle de distribuição de software são aplicadas tanto para pacotes confiáveis quanto para arquivos criados ou modificados por tais pacotes, caso nenhuma regra de negação de controle de inicialização de aplicativos seja aplicada àqueles pacotes e arquivos.

Uso das conclusões do KSN

As conclusões da KSN de que um arquivo não é confiável têm uma prioridade mais alta do que as exclusões do controle de distribuição de software: a descompactação de pacotes confiáveis e a inicialização de arquivos criados e modificados por esses pacotes serão bloqueadas se a KSN reportar que esses arquivos não são confiáveis.

Depois de serem descompactados de um pacote confiável, será permitido que todos os arquivos filhos sejam executados independentemente do uso da KSN no escopo do Controle de Inicialização de Aplicativos. Nesse caso, os estados das caixas de seleção **Proibir aplicativos não confiáveis pela KSN** e **Permitir aplicativos confiáveis pela KSN** não afetam a operação da caixa de seleção **Permitir a inicialização para todos os arquivos desta**

cadeia de extração do pacote de distribuição.

Sobre o uso da KSN para a tarefa de Controle de inicialização de aplicativos

Para iniciar a tarefa de Uso da KSN, você deve aceitar a Declaração da KSN.

Se os dados da KSN sobre a reputação de um aplicativo forem usados pela tarefa de Controle de Inicialização de Aplicativos, a reputação do aplicativo na KSN será considerada um critério para permitir ou negar a inicialização desse aplicativo. Se a KSN reportar para o Kaspersky Embedded Systems Security que um aplicativo não é confiável, quando o usuário tentar iniciar o aplicativo, a inicialização do aplicativo será negada. Se a KSN reportar para o Kaspersky Embedded Systems Security que um aplicativo é confiável, quando o usuário tentar iniciar o aplicativo, a inicialização do aplicativo será permitida. A KSN pode ser usada junto com as regras de Controle de inicialização de aplicativos ou como um critério independente para negar a inicialização de aplicativos.

Usar conclusões da KSN como critério independente para negar a inicialização do aplicativo

Este cenário permite que você controle com segurança inicializações de aplicativos em um computador protegido sem a necessidade de configuração avançada da lista de regras.

É possível aplicar conclusões da KSN ao Kaspersky Embedded Systems Security em conjunto com a única regra especificada. O aplicativo só permitirá a inicialização de aplicativos confiáveis na KSN ou os permitidos por uma regra específica.

Para esse cenário, recomendamos definir uma regra que permita a inicialização do aplicativo com base em um certificado digital.

Todos os outros aplicativos serão negados conforme a política de Negação padrão. Usar a KSN quando nenhuma regra é aplicada protege um computador de aplicativos que a KSN considera como uma ameaça.

Usar conclusões da KSN simultaneamente com regras de Controle de inicialização de aplicativos

Ao usar as conclusões da KSN simultaneamente com regras de Controle de inicialização de aplicativos, as seguintes condições se aplicam:

- O Kaspersky Embedded Systems Security sempre nega a inicialização de um aplicativo se este estiver incluído no escopo de ao menos uma regra de negação. Se o aplicativo for considerado confiável pela KSN, a conclusão correspondente terá uma prioridade mais baixa e não será considerada; a inicialização do aplicativo ainda será negada. Isso permite que você expanda a lista de aplicativos indesejados.
- O Kaspersky Embedded Systems Security sempre nega a inicialização de um aplicativo se a inicialização de aplicativos não confiáveis na KSN for proibida e o aplicativo não for confiável na KSN. Se uma regra de permissão for definida para o aplicativo, ela terá uma prioridade mais baixa e não será considerada; a inicialização do aplicativo ainda será negada. Isso protege o computador de aplicativos que a KSN considera como ameaças, mas que não foram considerados durante a configuração inicial das regras.

Geração de regras de Controle de inicialização de aplicativos

Você pode criar listas de regras de Controle de inicialização de aplicativos usando tarefas e políticas do Kaspersky Security Center simultaneamente para todos os computadores e para grupos de computadores na rede corporativa. Este cenário é recomendado se a rede corporativa não tiver uma máquina de referência e você não puder criar uma lista de regras de permissão com base nos aplicativos instalados na máquina de referência. Você também pode executar a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos localmente por meio do Console do Aplicativo para criar uma lista de regras com base nos aplicativos em execução em um único computador.

O componente de Controle de Inicialização de Aplicativos é instalado com duas regras de permissão predefinidas:

- Regra de permissão para scripts e arquivos MSI com certificado confiável pelo sistema operacional.
- Regra de permissão para arquivos executáveis com certificado confiável pelo sistema operacional.

Você pode criar listas de regras de Controle de inicialização de aplicativos no lado do Kaspersky Security Center de duas maneiras:

- Usando uma tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos.

  Nesse cenário, uma tarefa de grupo gera sua própria lista de regras de Controle de inicialização de aplicativos para cada computador na rede e salva essas listas em um arquivo XML na pasta compartilhada especificada. O arquivo XML gerado pela tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos contém as regras de permissão especificadas nas configurações da tarefa antes que a tarefa seja iniciada. Nenhuma regra será criada para aplicativos que não têm permissão para inicializar nas configurações da tarefa especificada. A inicialização desses aplicativos é negada por padrão. Você pode então importar manualmente a lista de regras criada para tarefa de Controle de inicialização de aplicativos da política do Kaspersky Security Center. Você pode configurar uma política do Kaspersky Security Center para adicionar automaticamente as regras criadas à lista de regras de Controle de Inicialização de Aplicativos quando tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos for concluída.

  Você pode configurar a importação automática das regras geradas para a lista de regras da tarefa de Controle de inicialização de aplicativos.

  Este cenário é recomendado quando você precisar criar listas de regras de Controle de inicialização de aplicativos rapidamente. Recomendamos que você configure a inicialização programada da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos somente se as regras de permissão aplicadas incluírem pastas e arquivos que você sabe que são seguros.

  > Antes de usar a tarefa de Controle de inicialização de aplicativos na rede, certifique-se de que todos os computadores protegidos tenham acesso a uma pasta compartilhada. Se a política da organização não prevê o uso de uma pasta compartilhada na rede, recomendamos que você inicie a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos em um computador em um grupo de computadores de teste ou em uma máquina de referência.

- Com base em um relatório dos eventos de tarefa gerados no Kaspersky Security Center pela execução da tarefa de Controle de inicialização de aplicativos no modo **Somente Estatísticas**.

  Nesse cenário, o Kaspersky Embedded Systems Security não nega a inicialização de aplicativos. Em vez disso, com a execução do Controle de Inicialização de Aplicativos no modo **Somente Estatísticas**, ele reporta todas as inicializações de aplicativos permitidas e negadas em todos os computadores da rede na guia **Eventos** da área de trabalho do nó Servidor de Administração no Kaspersky Security Center. O Kaspersky Security Center usa o log de tarefas para gerar uma lista única de eventos nos quais a

inicialização de aplicativos foi negada.

Você precisa configurar o período de execução da tarefa para que todos os cenários possíveis envolvendo computadores protegidos e grupos de computadores e, ao menos uma reinicialização de computador sejam executados durante o período de tempo especificado. Depois que as regras tiverem sido adicionadas à tarefa de Controle de Inicialização de Aplicativos, você pode importar dados de inicialização do relatório de eventos do Kaspersky Security Center (no formato TXT) e gerar regras de permissão para o Controle de Inicialização de Aplicativos para esses aplicativos com base nesses dados.

Este cenário é recomendado se uma rede corporativa incluir um grande número de computadores de tipo diferente (com um software diferente instalado).

- Com base nos eventos de inicialização de aplicativos negados recebidos pelo Kaspersky Security Center, sem criar e importar um arquivo de configuração.

  Para usar esse recurso, a tarefa de Controle de Inicialização de Aplicativos no computador local deve estar em execução segundo uma política ativa do Kaspersky Security Center. Neste caso, todos os eventos no computador local são enviados para o Servidor de administração.

Recomendamos que você atualize a lista de regras quando houver alterações no conjunto de aplicativos instalado nos computadores da rede (por exemplo, quando as atualizações são instaladas ou os sistemas operacionais são reinstalados). Recomendamos que você gere uma lista atualizada de regras executando a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos ou a tarefa de Controle de Inicialização de Aplicativos no modo **Somente Estatísticas** em computadores no grupo de administração de teste. O grupo de administração de teste inclui computadores necessários para testar a inicialização de novos aplicativos antes que eles sejam instalados em computadores da rede.

Os arquivos de XML contendo listas de regras de permissão são criados com base em uma análise das tarefas iniciadas no computador protegido. Para considerar todos os aplicativos utilizados na rede ao gerar listas de regras, aconselha-se a inicialização da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos e a tarefa de Controle de Inicialização de Aplicativos no modo **Somente estatísticas** em uma máquina de referência.

Antes de iniciar a geração das regras de permissão com base nos aplicativos iniciados em uma máquina de referência, certifique-se de que a máquina de referência esteja segura e que não contenha nenhum malware.

Antes de acrescentar regras de permissão, selecione um dos modos de aplicação de regras disponíveis. A lista das regras da política do Kaspersky Security Center exibe apenas as regras especificadas pela política, independentemente do modo de aplicação da regra. A lista de regras locais inclui todas as regras aplicadas - tanto as regras locais como as regras adicionadas através de uma política.

Configurações padrão da tarefa de Controle de Inicialização de Aplicativos

Por padrão, a tarefa de Controle de inicialização de aplicativos possui as configurações descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Tabela 47. Configurações padrão da tarefa de Controle de Inicialização de Aplicativos

Configuração	Valor padrão	Descrição
Modo da tarefa	**Somente Estatísticas**. A tarefa registra eventos de inicialização negados e permitidos com base nas regras definidas. A inicialização do aplicativo não é de fato negada.	Você pode selecionar o modo **Ativa** depois que a lista final de regras for gerada.
Repetir ação da primeira inicialização de arquivo em todas as inicializações subsequentes deste arquivo	Aplicada	Você pode repetir ações executadas na primeira inicialização do arquivo em todas as inicializações subsequentes desse arquivo.
Negar a inicialização de interpretadores da linha de comando sem o comando para executar	Não aplicado.	Você pode negar a inicialização de interpretadores de comando sem comando a ser executado.
Gerenciamento de regras	**Substituir regras locais por regras de política**	Você pode selecionar um modo em que regras especificadas em uma política sejam aplicadas em conjunto com as regras no computador local.
Escopo de uso das regras	A tarefa controla a inicialização de arquivos executáveis, scripts e pacotes MSI. Ela também monitora o carregamento de módulos DLL.	Você pode especificar os tipos de arquivos para os quais a inicialização será controlada por regras.
Uso da KSN	Os dados de reputação do aplicativo na KSN não serão utilizados.	É possível usar os dados da reputação do aplicativo da KSN ao executar uma tarefa de Controle de Inicialização de Aplicativos.

Configuração	Valor padrão	Descrição
Permitir distribuição automática de software para aplicativos e pacotes listados	Não aplicado.	É possível permitir a distribuição de software usando os instaladores e aplicativos especificados nas configurações. Por padrão, a distribuição de software só é permitida com a utilização do serviço do Windows Installer.
Sempre permitir distribuição de software via Windows Installer	Aplicado (pode ser alterado apenas quando a configuração **Permitir distribuição automática de software para aplicativos e pacotes listados** está ativa).	É possível permitir qualquer instalação ou atualização de software se as operações forem executadas por meio do Windows Installer.
Sempre permitir distribuição de software via SCCM usando o Background Intelligent Transfer Service	Não aplicado (pode ser alterado apenas quando a configuração **Permitir distribuição automática de software para aplicativos e pacotes listados** está ativa).	Você pode ativar ou desativar a distribuição automática de software usando o System Center Configuration Manager.
Início da tarefa	A primeira execução não está programada.	A tarefa de Controle de Inicialização de Aplicativos não é iniciada automaticamente no momento da inicialização do Kaspersky Embedded Systems Security. É possível iniciar a tarefa manualmente ou configurar um início programado.

Tabela 48. Configurações padrão da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos

Configuração	Valor padrão	Descrição
Prefixo para nomes de regras de permissão	Idêntico ao nome do computador no qual o Kaspersky Embedded Systems Security está instalado.	Você pode modificar o prefixo dos nomes de regras de permissão.

Configuração	Valor padrão	Descrição
Escopo de uso das regras de permissão	O escopo de regras de permissão inclui as seguintes categorias de arquivo por padrão: • Arquivos com a extensão EXE localizados nas pastas C:\Windows, C:\Program Files (x86) e C:\Program Files • Pacotes MSI armazenados na pasta C:\Windows • Scripts armazenados na pasta C:\Windows A tarefa também cria regras para todos os aplicativos em execução, independente de seu local e formato.	Você pode modificar o escopo de proteção adicionando ou removendo caminhos de pastas e especificando tipos de arquivo que poderão ser inicializados pelas regras geradas automaticamente. Você também pode ignorar os aplicativos em execução ao criar regras de permissão.
Critérios para a geração de regras de permissão	O requerente e a impressão digital do certificado digital serão usados; as regras serão geradas para todos os usuários e grupos de usuários.	Você pode usar o Hash SHA256 gerando regras de permissão. Você pode selecionar um usuário e grupo de usuários para os quais as regras de permissão devem ser geradas automaticamente.
Ações após a conclusão da tarefa	As regras de permissão são adicionadas à lista de regras de Controle de Inicialização de Aplicativos; as novas regras serão agregadas às existentes; as regras duplicadas serão removidas.	Você pode adicionar regras às regras existentes sem agregá-las e sem excluir regras duplicadas, ou substituir as regras existentes por regras novas de permissão ou configurar a exportação de regras de permissão para um arquivo.
Configurações de inicialização de tarefa com permissões	A tarefa é iniciada em uma conta do sistema.	Você pode permitir a inicialização da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos através de uma conta do sistema ou das permissões de um usuário especificado.
Programação de inicialização da tarefa	A primeira execução não está programada.	A tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos não é iniciada automaticamente no momento da inicialização do Kaspersky Embedded Systems Security. É possível iniciar a tarefa manualmente ou configurar um início programado.

Gerenciamento do Controle de Inicialização de Aplicativos por meio do Plug-in de Administração

Nesta seção, aprenda como navegar pela interface do Plug-in de Administração e definir configurações de tarefa para um ou todos os computadores na rede.

Nesta seção

Navegação 298
Definição de configurações da tarefa de Controle de Inicialização de Aplicativos 300
Configuração do Controle de Distribuição de Software 303
Configuração da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos 305
Configuração de regras de Controle de inicialização de Aplicativos por meio do Kaspersky Security Center ... 307
Criação de uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos 316

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface.

Nesta seção

Abertura das definições de política para a tarefa de Controle de Inicialização de Aplicativos 298
Abertura da lista de regras de Controle de Inicialização de Aplicativos 299
Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos 299

Abertura das definições de política para a tarefa de Controle de Inicialização de Aplicativos

► *Para abrir as configurações da tarefa de Controle de Inicialização de Aplicativos por meio da política no Kaspersky Security Center:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Controle de atividade local**.
6. Clique no botão **Configurações** na subseção **Controle de inicialização de aplicativos**.

   A janela **Controle de Inicialização de Aplicativos** é exibida.

Configure a política conforme necessário.

Abertura da lista de regras de Controle de Inicialização de Aplicativos

► *Para abrir a lista de regras de Controle de Inicialização de Aplicativos por meio do Kaspersky Security Center:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Controle de atividade local**.
6. Clique no botão **Configurações** na subseção **Controle de inicialização de aplicativos**.

   A janela **Controle de Inicialização de Aplicativos** é exibida.
7. Na guia **Geral**, clique no botão **Lista de regras**.

   A janela **Regras de Controle de Inicialização de Aplicativos** é exibida.

Configure a lista de regras conforme necessário.

Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos

► *Para criar uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Tarefas**.
4. Clique no botão **Criar uma tarefa**.

   A janela **Assistente de Nova Tarefa** será aberta.
5. Selecione a tarefa **Gerador de Regras de Controle de Inicialização de Aplicativos**.
6. Clique em **Avançar**.

   A janela **Configurações** é exibida.

► *Para configurar a tarefa existente do Gerador de Regras de Controle de Inicialização de Aplicativos:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Tarefas**.
4. Clique duas vezes no nome da tarefa na lista de tarefas no Kaspersky Security Center.

A janela **Propriedades: Gerador de Regras de Controle de Inicialização de Aplicativos** será aberta.

Consulte a seção Configuração da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos para detalhes sobre a configuração da tarefa.

Definição de configurações da tarefa de Controle de Inicialização de Aplicativos

► *Para definir as configurações gerais da tarefa de Controle de Inicialização de Aplicativos:*

1. Abra o **Controle de Inicialização de Aplicativos** (consulte a seção "**Abertura das configurações de política para a tarefa de Controle de Inicialização de Aplicativos**" na página 298).
2. Na guia **Geral**, selecione as seguintes configurações na seção **Modo da tarefa**:
   - Na lista suspensa **Modo da tarefa**, especifique o modo da tarefa.

     Nessa lista suspensa você pode selecionar um modo para tarefa de Controle de inicialização de aplicativos:

     - **Ativa**. O Kaspersky Embedded Systems Security usa as regras especificadas para controlar a inicialização de qualquer aplicativo.
     - **Somente Estatísticas**. O Kaspersky Embedded Systems Security não usa as regras especificadas para controlar a inicialização de aplicativos. Em vez disso, ele simplesmente registra as informações sobre eventos de inicialização no log de tarefas. Todos os aplicativos podem ser inicializados. Você pode usar esse modo para gerar uma lista de regras de Controle de inicialização de aplicativos com base nas informações sobre inicializações negadas registradas no log de tarefas.

     Por padrão, a tarefa de Controle de Inicialização de Aplicativos é executada no modo **Somente Estatísticas**.

   - Desmarque ou selecione a caixa de seleção **Repetir ação da primeira inicialização de arquivo em todas as inicializações subsequentes deste arquivo**.

     A caixa de seleção ativa ou desativa o controle de inicialização para a segunda tentativa e todas as tentativas subsequentes de inicialização de aplicativos com base nas informações de eventos armazenadas em cache.

     Se a caixa estiver selecionada, o Kaspersky Embedded Systems Security permitirá ou negará uma inicialização subsequente do aplicativo com base na conclusão da tarefa referente à primeira inicialização do aplicativo. Por exemplo, se a primeira inicialização de aplicativo foi permitida pelas regras, as informações sobre essa decisão serão armazenadas em cache e a segunda e todas as inicializações subsequentes também serão permitidas, sem qualquer verificação adicional.

     Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security analisará o aplicativo a cada tentativa de inicialização.

     A caixa de seleção é selecionada por padrão.

   - Desmarque ou selecione a caixa **Negar a inicialização de interpretadores da linha de comando sem o comando para executar**.

     Se a caixa estiver selecionada, o Kaspersky Embedded Systems Security negará a inicialização de interpretadores da linha de comando, mesmo que a inicialização de interpretadores seja permitida. Um interpretador de comando só pode ser inicializado sem um comando se ambas as condições a seguir forem atendidas:

- A inicialização do interpretador da linha de comando é permitida.
- O comando a ser executado é permitido.

Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security só considerará as regras de permissão ao inicializar o interpretador da linha de comando. A inicialização será negada se nenhuma regra de permissão for aplicável ou se o processo executável não for considerado confiável pela KSN. Se uma regra de permissão for aplicável ou se o processo for considerado confiável pela KSN, um interpretador da linha de comando pode ser inicializado com ou sem um comando a ser executado.

O Kaspersky Embedded Systems Security reconhece os seguintes interpretadores da linha de comando:

- cmd.exe
- powershell.exe
- python.exe
- perl.exe

Esta caixa é desmarcada por padrão.

3. Na seção **Gerenciamento de regras**, defina as configurações para a aplicação de regras:
   a. Clique no botão **Lista de regras** para adicionar as regras de permissão para a tarefa de Controle de Inicialização de Aplicativos.

   O Kaspersky Embedded Systems Security não reconhece caminhos que contêm barras "/". Use a barra invertida "\" para inserir o caminho corretamente.

   b. Selecione o modo para a aplicação das regras:

   - **Substituir regras locais por regras de política**.

     O aplicativo aplica a lista de regras especificada na política para o Controle de Inicialização de Aplicativos centralizado em um grupo de computadores. As listas de regras locais não podem ser criadas, editas ou aplicadas.

   - **Adicionar regras de política às regras locais**.

     O aplicativo aplica a lista de regras especificada em uma política junto com as listas de regra locais. É possível editar as listas de regras locais usando a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos.

   Por padrão, o Kaspersky Embedded Systems Security aplica duas regras predefinidas que permitem uma lista de scripts, pacotes MSI e arquivos executáveis se esses objetos estiverem assinados com uma assinatura digital confiável.

4. Na seção **Escopo de uso das regras**, especifique as seguintes configurações:

   - **Aplicar regras a arquivos executáveis**.

     A caixa de seleção ativa ou desativa o controle de inicialização de arquivos executáveis.

     Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security permitirá ou bloqueará a inicialização de arquivos executáveis usando as regras especificas cujas definições especificam **Arquivos executáveis** como escopo.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não controlará a inicialização de arquivos executáveis usando as regras especificas. A

inicialização de arquivos executáveis será permitida.

A caixa de seleção é selecionada por padrão.

- **Monitorar o carregamento de módulos DLL**.

  A caixa de seleção ativa ou desativa o controle de carregamento de módulos DLL.

  Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security permitirá ou bloqueará o carregamento de módulos DLL usando as regras especificas cujas definições especificam **Arquivos executáveis** como escopo.

  Se essa caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não controlará o carregamento de módulos DLL usando as regras especificas. O carregamento de módulos DLL será permitido.

  A caixa de seleção estará ativa se a caixa se seleção **Aplicar regras a arquivos executáveis** estiver selecionada.

  Esta caixa é desmarcada por padrão.

O controle do carregamento de módulos DLL pode afetar o desempenho do sistema operacional.

- **Aplicar regras a scripts e pacotes MSI**.

  A caixa de seleção ativa ou desativa a inicialização de scripts e pacotes MSI.

  Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security permitirá ou bloqueará a inicialização de scripts e pacotes MSI usando as regras especificas cujas definições especificam scripts e pacotes MSI como escopo.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não controlará a inicialização de scripts e pacotes MSI usando regras especificas. A inicialização de scripts e pacotes MSI é permitida.

  A caixa de seleção é selecionada por padrão.

5. No grupo **Uso da KSN**, defina as seguintes configurações de inicialização de aplicativos:

   - **Proibir aplicativos não confiáveis pela KSN**.

     A caixa de seleção ativa ou desativa o Controle de Inicialização de Aplicativos de acordo com a reputação do aplicativo na KSN.

     Se essa caixa estiver selecionada, o Kaspersky Embedded Systems Security bloqueará a execução de qualquer aplicativo que não for considerado confiável pela KSN. As regras de permissão de Controle de Inicialização de Aplicativos que se aplicam a aplicativos não confiáveis pela KSN não serão acionadas. A seleção da caixa fornece proteção adicional contra malware.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não considerará a reputação de aplicativos não confiáveis na KSN e permitirá ou bloqueará a inicialização de acordo com as regras que se aplicam a esses programas.

     Esta caixa é desmarcada por padrão.

   - **Permitir aplicativos confiáveis pela KSN**.

     A caixa de seleção ativa ou desativa o Controle de Inicialização de Aplicativos de acordo com a reputação do aplicativo na KSN.

     Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security permitirá a

execução de aplicativos considerados confiáveis pela KSN. Regras de negação de Controle de Inicialização de Aplicativos aplicáveis aos aplicativos considerados como confiáveis pela KSN têm prioridade mais alta: se um aplicativo for considerado confiável pelos serviços da KSN, a inicialização desse aplicativo será negada.

Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não considerará a reputação de aplicativos considerados confiáveis pela KSN e permitirá ou negará a inicialização conforme as regras que se aplicam a esses aplicativos.

Esta caixa é desmarcada por padrão.

- Os usuários e/ou grupos de usuário permitiram a inicialização de aplicativos confiáveis na KSN.

6. Na guia **Controle de distribuição de software**, defina as configurações do controle de distribuição de software (consulte a seção "Configuração do Controle de Distribuição de Software" na página 303).
7. Na guia **Gerenciamento da tarefa**, defina as configurações de início da tarefa programada (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 130).
8. Clique em **OK** na janela **Configurações de tarefa**.

O Kaspersky Embedded Systems Security aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

Configuração do controle de distribuição de software

► *Para adicionar um pacote de distribuição confiável:*

1. Abra a janela **Controle de Inicialização de Aplicativos** (consulte a seção "Abertura das configurações de política para a tarefa de Controle de Inicialização de Aplicativos" na página 298).
2. Na guia **Controle de distribuição de software**, selecione a caixa **Permitir distribuição automática de software para aplicativos e pacotes listados**.

   A caixa de seleção ativa e desativa a criação automática de exclusões para todos os arquivos iniciados usando os pacotes de distribuição especificados na lista.

   Se a caixa de seleção for marcada, o aplicativo permite automaticamente que os arquivos nos pacotes de distribuição confiáveis sejam inicializados. A lista de aplicativos e pacotes de distribuição com inicialização permitida pode ser editada.

   Se a caixa de seleção for desmarcada, o aplicativo não aplicará as exclusões específicas na lista.

   Esta caixa é desmarcada por padrão.

   É possível selecionar **Permitir distribuição automática de software para aplicativos e pacotes listados** se a caixa de seleção **Aplicar regras a arquivos executáveis** na guia **Geral** estiver marcada nas configurações da tarefa de **Controle de Inicialização de Aplicativos**.

3. Desmarque a caixa de seleção **Sempre permitir distribuição de software via Windows Installer**, se necessário.

   A caixa de seleção ativa e desativa a criação automática de exclusões para todos os arquivos executados por meio do Windows Installer.

   Se a caixa de seleção estiver marcada, arquivos instalados por meio do Windows Installer

sempre terão permissão para inicializar.

Se a caixa de seleção estiver desmarcada, os arquivos não terão permissão incondicional para inicializar, mesmo que tenham sido instalados por meio do Windows Installer.

A caixa de seleção é selecionada por padrão.

A caixa de seleção não é editável se a caixa **Permitir distribuição automática de software para aplicativos e pacotes listados** não estiver marcada.

Desmarcar a caixa de seleção **Sempre permitir distribuição de software via Windows Installer** só é recomendado se for absolutamente necessário. Desativar essa função pode causar problemas na atualização de arquivos do sistema operacional e também impedir a inicialização de arquivos extraídos de um pacote de distribuição.

4. Se necessário, marque a caixa de seleção **Sempre permitir distribuição de software via SCCM usando o Background Intelligent Transfer Service**.

   A caixa de seleção ativa e desativa a distribuição automática de software usando o System Center Configuration Manager.

   Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security automaticamente permitirá a implantação do Microsoft Windows usando o Gerenciador de configuração do centro do sistema. O aplicativo permite a distribuição de software apenas através do Serviço de transferência inteligente em segundo plano.

   O aplicativo controla a inicialização dos objetos com as seguintes extensões:

   - .exe
   - .msi

   Esta caixa é desmarcada por padrão.

O aplicativo controla o ciclo de distribuição de software no computador, da entrega do pacote à instalação ou atualização. O aplicativo não controla processos se algum dos estágios da distribuição tiver sido executado antes da instalação do aplicativo no computador.

5. Para editar a lista de pacotes de distribuição confiáveis, clique em **Alterar lista de pacotes** e selecione um dos seguintes métodos na janela exibida:

   - **Adicionar um pacote de distribuição**.

     a. Clique no botão **Procurar** e selecione um arquivo executável ou pacote de distribuição.

        A seção **Critérios de confiança** é automaticamente preenchida com os dados sobre o arquivo selecionado.

     b. Desmarque ou selecione a caixa **Permitir a inicialização para todos os arquivos desta cadeia de extração do pacote de distribuição**.

     c. Selecione uma das duas opções disponíveis para os critérios a serem usados para determinar se um arquivo ou pacote de distribuição é confiável:

        - **Usar certificado digital**
        - **Usar hash SHA256**

   - **Adicionar diversos pacotes de distribuição por hash**.

É possível selecionar um número ilimitado de arquivos executáveis e pacotes de distribuição e adicioná-los à lista ao mesmo tempo. O Kaspersky Embedded Systems Security examina o hash e permite que o sistema operacional inicie os arquivos especificados.

- **Alterar pacote selecionado**.

  Use esta opção para selecionar um arquivo executável ou pacote de distribuição diferente, ou para alterar os critérios de confiança.

- **Importar lista de pacotes de distribuição do arquivo**.

  É possível importar a lista de pacotes de distribuição confiáveis de um arquivo de configuração. Para que seja reconhecido pelo Kaspersky Embedded Systems Security, o arquivo deve satisfazer os seguintes parâmetros:

  - A extensão do arquivo é TXT.
  - O arquivo contém informações estruturadas como uma lista de linhas, onde cada linha inclui dados para um dos arquivos confiáveis.
  - O arquivo deve conter uma lista em um dos seguintes formatos:
    - <nome do arquivo>:<hash SHA256>.
    - <hash SHA256>*<nome do arquivo>.

  Na janela **Abrir**, especifique o arquivo de configuração que contém uma lista de pacotes de distribuição confiáveis.

6. Se quiser remover um aplicativo ou pacote de distribuição previamente adicionado da lista de confiáveis, clique no botão **Excluir pacotes de distribuição**. Arquivos extraídos não poderão ser executados.

   Para evitar que arquivos extraídos sejam iniciados, desinstale o aplicativo no computador protegido ou crie uma regra de negação nas configurações da tarefa de Controle de Inicialização de Aplicativos.

7. Clique em **OK**.

As configurações recém-definidas foram salvas.

Configuração da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos

► *Para configurar a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos, faça o seguinte:*

1. Abra a janela **Propriedades: Gerador de Regras de Controle de Inicialização de Aplicativos** (consulte a seção "**Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos**" na página 299).
2. Na seção **Notificações**, defina as configurações de notificação do evento da tarefa.

   Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.

3. Na seção **Configurações**, é possível definir as seguintes configurações:

- Adicione um prefixo para nomes de regra.
- Configure o escopo de uso das regras de permissão:
  - Criar regras de permissão com base nos aplicativos em execução;
  - Criar regras de permissão para aplicativos das pastas específicas.

4. Na seção **Opções**, é possível especificar ações para execução ao criar regras de permissão para o controle de inicialização de aplicativos:

- **Usar certificado digital**

Se essa opção estiver selecionada, a presença de um certificado digital será especificada como critério para acionamento de regras nas configurações das regras de permissão geradas recentemente para o Controle de Inicialização de Aplicativos. O aplicativo permitirá agora a inicialização de programas iniciados usando arquivos com um certificado digital. Recomendamos essa opção se você quiser permitir a inicialização de qualquer aplicativo que seja confiável no sistema operacional.

Esta opção é selecionada por padrão.

- **Usar o assunto e a miniatura de certificado digital**

  A caixa de seleção ativa ou desativa o uso do requerente e da impressão digital do certificado digital do arquivo como critério para acionamento de regras de permissão no Controle de inicialização de aplicativos. A seleção desta caixa permite a especificação de condições de verificação mais rigorosas para o certificado digital.

  Se essa caixa estiver selecionada, os valores de requerente e impressão digital do certificado digital dos arquivos para os quais as regras serão geradas serão estabelecidos como um critério para acionamento das regras de permissão no Controle de inicialização de aplicativos. O Kaspersky Embedded Systems Security permitirá que os aplicativos que sejam iniciados usando arquivos com uma impressão digital e um certificado digital especificados.

  A seleção dessa caixa restringe fortemente o acionamento de regras de permissão com base em um certificado digital, pois a impressão digital é um identificador único de um certificado digital e não pode ser forjada.

  Se esta caixa estiver desmarcada, a existência de qualquer certificado digital confiável no sistema operacional é estabelecida como um critério para acionamento de regras de permissão de Controle de inicialização de aplicativos.

  A caixa de seleção estará ativa se a opção **Usar certificado digital** estiver selecionada.

  A caixa de seleção é selecionada por padrão.

- **Se o certificado estiver ausente, use**

  Essa é uma lista suspensa que permite que você selecione o critério para acionamento de uma regra de permissão de Controle de inicialização de aplicativos se o arquivo usado para gerar a regra não tiver um certificado digital.

  - **Hash SHA256**. O valor da soma de verificação do arquivo usado para gerar a regra é estabelecido como o critério para acionamento da regra de permissão de Controle de inicialização de aplicativos. O aplicativo permitirá a inicialização de programas iniciados usando arquivos com a soma de verificação especificada.
  - **caminho do arquivo**. O caminho do arquivo usado para gerar a regra é estabelecido como o critério para acionamento da regra de permissão de Controle de inicialização de aplicativos. O aplicativo agora permitirá a inicialização de programas usando arquivos localizados nas pastas especificadas na tabela **Criar regras de permissão para aplicativos das pastas** na seção

Configurações.

- **Usar hash SHA256**

Se esta opção estiver selecionada, o valor da soma de verificação do arquivo usado para gerar a regra será especificado como um critério para acionamento de regras nas configurações das regras de permissão geradas recentemente para o Controle de inicialização de aplicativos. O aplicativo permitirá a inicialização de programas iniciados usando arquivos com a soma de verificação especificada.

Recomendamos essa opção para casos em que as regras geradas devem alcançar o nível de segurança mais alto: a soma de verificação do SHA256 pode ser usada como um ID único de arquivo. O uso da soma de verificação do SHA256 como critério para acionamento de regras restringe o escopo de uso das regras para um arquivo.

Esta opção é desmarcada por padrão.

- **Gerar regras para usuário ou grupo de usuários**.

  Esse é um campo que exibe um usuário ou grupo de usuários. O aplicativo controlará qualquer aplicativo executado pelo usuário ou grupo de usuários especificado.

  A seleção padrão é **Todos**.

Você pode definir as configurações para arquivos de configuração com listas de regras de permissão que o Kaspersky Embedded Systems Security cria após a conclusão da tarefa.

1. Configurar o agendamento de tarefa na seção **Programação** (você pode configurar um agendamento para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).
2. Na seção **Conta**, especifique a conta cujos direitos serão usados para a execução de tarefa.
3. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**.

   Para obter informações detalhadas sobre a definição das configurações nestas seções, consulte a *Ajuda do Kaspersky Security Center*.

4. Na janela **Propriedades: <Nome da tarefa>**, clique em **OK**.

   As configurações de tarefas de grupo definidas recentemente são salvas.

Configuração de regras de Controle de inicialização de aplicativos por meio do Kaspersky Security Center

Saiba como gerar uma lista de regras com base em vários critérios ou criar regras de permissão ou negação manualmente usando a tarefa de Controle de Inicialização de Aplicativos.

Nesta seção

Adição de uma regra de Controle de Inicialização de Aplicativos 308
Ativar o modo de permissão padrão 311
Criação de regras de permissão dos eventos do Kaspersky Security Center 311
Importação de regras a partir de um relatório do Kaspersky Security Center sobre aplicativos bloqueados 312
Importação de regras de Controle de inicialização de aplicativos de um arquivo XML 314
Verificação da inicialização de aplicativos 315

Adição de uma regra de Controle de Inicialização de Aplicativos

► *Para adicionar uma regra de Controle de inicialização de aplicativos:*

1. Abra a janela de **Regras de Controle de Inicialização de Aplicativos** (consulte a seção "Abertura da lista de regras de Controle de inicialização de aplicativos" na página 299).
2. Clique no botão **Adicionar**.
3. No menu de contexto do botão, selecione **Adicionar uma regra**.

   A janela **Configurações de regra** é exibida.
4. Defina as seguintes configurações:
   a. No campo **Nome**, digite o nome da regra.
   b. Na lista suspensa **Tipo**, selecione o tipo de regra:
      - **Permissão** se você quiser que a regra permita a inicialização de aplicativos de acordo com os critérios especificados nas configurações da regra.
      - **Proibição** se você quiser que a regra bloqueie a inicialização dos aplicativos de acordo com os critérios especificados nas configurações da regra.
   c. Na lista suspensa **Escopo**, selecione o tipo de arquivo cuja execução será controlada pela regra:
      - **Arquivos executáveis** se você quiser que a regra controle a inicialização de arquivos executáveis.
      - **Pacotes de scripts e MSI** se você quiser que a regra controle a inicialização de scripts e pacotes MSI.
   d. No campo **Usuário ou grupo de usuários**, especifique os usuários que terão permissão ou não para iniciar programas com base no tipo da regra. Para isso, execute as seguintes ações:
      i. Clique no botão **Procurar**.
      ii. A janela **Selecionar usuários ou grupos** padrão do Microsoft Windows é exibida.
      iii. Especifique a lista usuário e/ou grupos usuário.
      iv. Clique em **OK**.
   e. Se você deseja obter os valores dos critérios para acionamento de regras listados na seção **Critério para acionamento de regras** a partir de um arquivo específico:
      i. Clique no botão **Definir critério disponíveis de regra a partir das propriedades do arquivo**.

A janela **Abrir** padrão do Microsoft Windows é exibida.

ii. Selecione o arquivo.

iii. Clique no botão **Abrir**.

Os valores de critérios no arquivo serão exibidos nos campos da seção **Critério para acionamento de regras**. O critério para o qual os dados estão disponíveis nas propriedades de arquivo é selecionado por padrão.

f. Na seção **Critério para acionamento de regras**, selecione uma das seguintes opções:

- **Certificado digital** se você quiser que a regra controle a inicialização de programas que usam arquivos assinados com um certificado digital:
  - Marque a caixa de seleção **Usar assunto** se você quiser que regra controle a inicialização de arquivos assinados com um certificado digital somente com o cabeçalho especificado.
  - Marque a caixa de seleção **Usar miniatura** se você quiser que a regra controle a inicialização de arquivos assinados com um certificado digital somente com a impressão digital especificada.
- **Hash SHA256** se você quiser que a regra controle a inicialização de programas que usam arquivos cuja soma de verificação corresponde àquela especificada.
- **Caminho do arquivo** se você quiser que a regra controle a inicialização de programas que usam arquivos localizados no caminho especificado.

> O Kaspersky Embedded Systems Security não reconhece caminhos que contêm barras "/". Use a barra invertida "\" para inserir o caminho corretamente.

g. Se deseja adicionar exclusões de regra:

i. Na seção **Exclusões da regra**, clique no botão **Adicionar**.

A janela **Exclusão da regra** é exibida.

ii. No campo **Nome**, digite o nome da exclusão.

iii. Especifique as configurações para exclusão dos arquivos de aplicativos da regra de Controle de inicialização de aplicativos. Você pode preencher os campos de configurações a partir das propriedades do arquivo clicando no botão **Def. excl. com base nas prop. do arq.**

- **Certificado digital**

Se essa opção estiver selecionada, a presença de um certificado digital será especificada como critério para acionamento de regras nas configurações das regras de permissão geradas recentemente para o Controle de Inicialização de Aplicativos. O aplicativo permitirá agora a inicialização de programas iniciados usando arquivos com um certificado digital. Recomendamos essa opção se você quiser permitir a inicialização de qualquer aplicativo que seja confiável no sistema operacional.

Esta opção é selecionada por padrão.

- **Usar assunto**

  A caixa de seleção ativa ou desativa o uso do requerente do certificado digital como critério para acionamento de regras.

  Se a caixa estiver selecionada, o requerente especificado do certificado digital será usado como critério para acionamento de regras. A regra criada controlará a inicialização de aplicativos somente para o fornecedor especificado no requerente.

Se a caixa estiver desmarcada, o aplicativo não usará o requerente do certificado digital como critério para acionamento de regras. Se o critério do **Certificado digital** for selecionado, a regra criada controlará a inicialização de aplicativos assinados com um certificado digital que contenha qualquer requerente.

O requerente do certificado digital usado para assinar o arquivo pode ser especificado somente a partir das propriedades do arquivo selecionado usando o botão **Definir critério disponíveis de regra a partir das propriedades do arquivo** localizado acima da seção **Critério para acionamento de regras**.

Esta caixa é desmarcada por padrão.

- **Usar miniatura**

  A caixa de seleção ativa ou desativa o uso da impressão digital do certificado digital como critério para acionamento de regras.

  Se a caixa estiver selecionada, a impressão digital especificada do certificado digital será usada como critério para acionamento de regras. A regra criada controlará a inicialização de aplicativos assinados com um certificado digital com a impressão digital especificada.

  Se a caixa estiver desmarcada, o aplicativo não usará a impressão digital do certificado digital como critério para acionamento de regras. Se o critério do **Certificado digital** for selecionado, o aplicativo controlará a inicialização de aplicativos assinados com um certificado digital que contenha qualquer impressão digital.

  A impressão digital do certificado digital usada para assinar o arquivo pode ser especificada somente a partir das propriedades do arquivo selecionado usando o botão **Definir critério disponíveis de regra a partir das propriedades do arquivo** localizado acima da seção **Critério para acionamento de regras**.

  Esta caixa é desmarcada por padrão.

- **Hash SHA256**

Se esta opção estiver selecionada, o valor da soma de verificação do arquivo usado para gerar a regra será especificado como um critério para acionamento de regras nas configurações das regras de permissão geradas recentemente para o Controle de inicialização de aplicativos. O aplicativo permitirá a inicialização de programas iniciados usando arquivos com a soma de verificação especificada.

Recomendamos essa opção para casos em que as regras geradas devem alcançar o nível de segurança mais alto: a soma de verificação do SHA256 pode ser usada como um ID único de arquivo. O uso da soma de verificação do SHA256 como critério para acionamento de regras restringe o escopo de uso das regras para um arquivo.

Esta opção é desmarcada por padrão.

- **Caminho do arquivo**

  Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security usará o caminho completo do arquivo para determinar se o processo é confiável.

  Se a caixa de seleção estiver desmarcada, o caminho para o arquivo não é usado para determinar se o processo é confiável.

  Esta caixa é desmarcada por padrão.

i. Clique em **OK**.

ii. Se necessário, repita os itens (i)-(iv) para incluir exclusões adicionais.

1. Clique em **OK** na janela **Configurações de regra**.

A regra criada é exibida na lista na janela **Regras de Controle de Inicialização de Aplicativos**.

Ativar o modo de Permissão padrão

O modo de Permissão padrão permite que todos os aplicativos sejam inicializados se não estiverem bloqueados por regras ou pela conclusão da KSN de que não são confiáveis. O modo de Permissão padrão pode ser ativado adicionando regras de permissão específicas. Você pode ativar a Permissão padrão apenas para scripts ou para todos os arquivos executáveis.

► *Para adicionar uma regra de Permissão padrão:*

1. Abra a janela **Regras de Controle de Inicialização de Aplicativos** (consulte a seção "**Abertura da lista de regras de Controle de inicialização de aplicativos**" na página 299).
2. Clique no botão **Adicionar** e, no menu de contexto do botão, selecione a opção **Adicionar uma regra**.

   A janela **Configurações de regra** é exibida.
3. No campo **Nome**, digite o nome da regra.
4. Na lista suspensa **Tipo**, selecione o tipo de regra **Permissão**.
5. Na lista suspensa **Escopo**, selecione o tipo de arquivo cuja execução será controlada pela regra:
   - **Arquivos executáveis** se você quiser que a regra controle a inicialização de arquivos executáveis de aplicativos.
   - **Pacotes de scripts e MSI** se você quiser que a regra controle a inicialização de scripts e pacotes MSI.
6. Na seção **Critério para acionamento de regras**, selecione a opção **Caminho do arquivo**.
7. Insira a seguinte máscara: `?:\`
8. Clique em **OK** na janela **Configurações de regra**.

O Kaspersky Embedded Systems Security aplicará o modo de Permissão padrão.

Criação de regras de permissão dos eventos do Kaspersky Security Center

► *Para gerar as regras de permissão de aplicativos a partir de eventos do Kaspersky Security Center no Controle de Inicialização de Aplicativos:*

1. Abra a janela **Regras de Controle de Inicialização de Aplicativos** (consulte a seção "**Abertura da lista de regras de Controle de inicialização de aplicativos**" na página 299).
2. Clique no botão **Adicionar** e, no menu de contexto do botão, selecione **Criar regras de permissão para aplicativos de eventos do Kaspersky Security Center**.
3. Selecione o princípio para adicionar as regras à lista de regras de Controle de Inicialização de Aplicativos criadas anteriormente:
   - **Adicionar às regras existentes** se você quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.
   - **Substituir as regras existentes** se você quiser substituir as regras existentes pelas regras importadas.
   - **Mesclar com as regras existentes** se você quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo

menos um parâmetro de regra for único.

A janela **Gerar regras de controle de geração de aplicativos** é exibida.

4. Defina as seguintes configurações de solicitação:
   - **Endereço do Servidor de Administração**
   - **Porta**
   - **Usuário**
   - **Senha**
5. Selecione os tipos de eventos que você quer que a tarefa de geração utilize:
   - **Modo somente estatísticas: inicialização de aplicativos negada**.
   - **Inicialização do aplicativo negada**.
6. Selecionar o período de tempo na lista suspensa **Solicitação de eventos que foram gerados dentro do período**.
7. Clique no botão **Gerar regras**.
8. Clique no botão **Salvar** na janela **Regras de Controle de Inicialização de Aplicativos**.

   A lista de regras na tarefa de Controle de Inicialização de Aplicativos será preenchida com as novas regras geradas com base em dados do sistema do computador com o Console de Administração do Kaspersky Security Center instalado.

   Se a lista de regras de Controle de Inicialização de Aplicativos já tiver sido especificada na política, o Kaspersky Embedded Systems Security adicionará as regras selecionadas dos eventos de bloqueio às regras já especificadas. As regras com o mesmo hash não serão adicionadas, pois todas as regras em uma lista devem ser únicas.

Importação de regras a partir de um relatório do Kaspersky Security Center sobre aplicativos bloqueados

Você pode importar dados sobre inicializações bloqueadas de aplicativos a partir do relatório gerado no Kaspersky Security Center após a conclusão da tarefa no modo **Somente Estatísticas** e usar estes dados para gerar uma lista de regras de permissão de Controle de Inicialização de Aplicativos na política que está sendo configurada.

Ao gerar o relatório sobre eventos ocorridos durante a execução da tarefa de Controle de Inicialização de Aplicativos, você pode acompanhar os aplicativos cuja inicialização foi bloqueada.

Ao importar dados do relatório sobre aplicativos bloqueados para as definições da política, certifique-se de que a lista que está sendo usada contém somente aplicativos cuja inicialização você deseja permitir.

► *Para especificar regras de permissão de Controle de Inicialização de Aplicativos para um grupo de computadores com base no relatório de aplicativos bloqueados do Kaspersky Security Center:*

1. Abra a janela **Controle de Inicialização de Aplicativos** (consulte a seção "Abertura das configurações de política para a tarefa de Controle de Inicialização de Aplicativos" na página 298).
2. Na seção **Modo da tarefa**, selecione o modo **Somente Estatísticas**.

3. Nas propriedades da política, na seção **Notificação de evento**, certifique-se de que:

   - Para **Eventos críticos**, o período de retenção do log de tarefas para eventos de **Inicialização do aplicativo negada** excede o período planejado para execução da tarefa no modo **Somente Estatísticas** (o valor padrão é 30 dias).
   - Para eventos com um nível de importância de **Aviso**, o período de retenção do log de tarefas para eventos de **Modo somente estatísticas: inicialização de aplicativos negada** excede o período planejado para a execução da tarefa no modo **Somente Estatísticas** (o valor padrão é 30 dias).

   Quando o período de retenção para eventos é excedido, as informações sobre os eventos registrados são excluídas e não são refletidas no relatório. Antes de executar a tarefa de Controle de inicialização de aplicativos no modo **Somente Estatísticas**, certifique-se de que o tempo de execução da tarefa não exceda o tempo de configurado para os eventos especificados.

4. Quando a tarefa tiver sido concluída, exporte os eventos registrados para um arquivo TXT:

   a. Na área de trabalho do nó **Servidor de Administração** no Kaspersky Security Center, selecione a guia **Eventos**.

   b. Clique no botão **Criar uma seleção** para criar uma seleção de eventos com base no critério *Bloqueado* para visualizar os aplicativos cujo início será bloqueado pela tarefa de Controle de Inicialização de Aplicativos.

   c. No painel de detalhes da seleção, clique na lista **Exportar eventos** para arquivo para salvar o relatório de inicializações bloqueadas de aplicativos em um arquivo TXT.

   Antes de importar e aplicar o relatório gerado a uma política, certifique-se de que o relatório contém dados somente sobre aqueles aplicativos cuja inicialização você deseja permitir.

5. Importe os dados sobre inicializações de aplicativos bloqueadas na tarefa de Controle de Inicialização de Aplicativos. Para fazer isso, nas propriedades da política nas configurações de tarefa de Controle de inicialização de aplicativos:

   a. Na guia **Geral**, clique no botão **Lista de regras**.

      A janela **Regras de Controle de Inicialização de Aplicativos** é exibida.

   b. Clique no botão **Adicionar** e, no menu de contexto do botão, selecione **Importar dados de aplicativos bloqueados do relatório do Kaspersky Security Center**.

   c. Selecione o princípio para adição de regras da lista criada com base em um relatório do Kaspersky Security Center à lista de regras previamente configuradas de Controle de inicialização de aplicativos:

      - **Adicionar às regras existentes** se você quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.
      - **Substituir as regras existentes** se você quiser substituir as regras existentes pelas regras importadas.
      - **Mesclar com as regras existentes** se você quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.

   d. Na janela padrão do Microsoft Windows exibida, selecione o arquivo TXT para o qual os eventos do relatório de inicializações bloqueadas de aplicativos foram exportados.

   e. Clique em **OK** na janela Regras de controle de inicialização de aplicativos e na janela **Configurações**

de tarefa.

As regras criadas com base no relatório do Kaspersky Security Center sobre aplicativos bloqueados serão adicionadas à lista de regras de controle de inicialização de aplicativos.

Importação de regras de Controle de inicialização de aplicativos de um arquivo XML

Você pode importar relatórios gerados após a conclusão da tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos e aplicá-los como uma lista de regras de permissão na política que estiver configurando.

Quando a tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos for concluída, o aplicativo exportará as regras de permissão criadas para arquivos XML salvos na pasta compartilhada especificada. Cada arquivo com a lista de regras é criado com base na análise de arquivos executados e aplicativos iniciados em cada computador separado na rede corporativa. As listas contêm regras de permissão para arquivos e aplicativos cujo tipo corresponde ao tipo especificado na tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos.

► *Para especificar regras de permissão de Controle de Inicialização de Aplicativos para um grupo de computadores com base em uma lista de regras de permissão gerada automaticamente:*

1. Na guia **Tarefas** no painel de controle do grupo de computadores que você está configurando, crie uma tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos ou selecione uma tarefa existente (consulte a seção "Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos" na página 299).
2. Nas propriedades da tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos criada ou no assistente de tarefa, especifique as seguintes configurações:
   - Na seção **Notificação**, defina as configurações para salvar o relatório de execução da tarefa.

     Para obter instruções detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*

   - Na seção **Configurações**, especifique os tipos de aplicativos cuja inicialização será permitida pelas regras criadas. Você pode editar o conjunto de pastas que contêm aplicativos permitidos: exclua as pastas padrão do escopo da tarefa ou adicione novas pastas manualmente.
   - Na seção **Opções**, especifique as operações a serem executadas pela tarefa durante a sua execução e após a sua conclusão. Especifique o critério com base no qual as regras serão geradas e o nome do arquivo para o qual essas regras serão exportadas.
   - Na janela **Programação**, defina as configurações da programação de inicialização da tarefa.
   - Na seção **Conta**, especifique a conta de usuário sob a qual a tarefa será executada.
   - Na seção **Exclusões do escopo de tarefa**, especifique os grupos de computadores a serem excluídos do escopo da tarefa.

     O Kaspersky Embedded Systems Security não criará regras de permissão para aplicativos iniciados em computadores excluídos.

3. Na guia **Tarefas** no painel de controle do grupo de computadores sendo configurados, na lista de tarefas de grupo selecione a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos que você criou e clique no botão **Iniciar** para iniciar a tarefa.

Quando a tarefa for concluída, as listas de regras de permissão geradas automaticamente serão salvas em arquivos XML em uma pasta compartilhada.

> Antes de usar a tarefa de Controle de inicialização de aplicativos na rede, certifique-se de que todos os computadores protegidos tenham acesso a uma pasta compartilhada. Se a política da organização não prevê o uso de uma pasta compartilhada na rede, recomendamos que você inicie a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos em um computador em um grupo de computadores de teste ou em uma máquina de referência.

4. Para adicionar as listas de regras de permissão geradas à tarefa de Controle de Inicialização de Aplicativos:
   a. Abra a janela de **regras de Controle de inicialização de aplicativos** (consulte a seção "Abertura da lista de regras de Controle de inicialização de aplicativos" na página 299).
   b. Clique no botão **Adicionar** e na lista exibida selecione **Importar regras do arquivo XML**.
   c. Selecione o princípio para adicionar as regras de permissão geradas automaticamente à lista de regras de Controle de inicialização de aplicativos criadas anteriormente:
      - **Adicionar às regras existentes** se você quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.
      - **Substituir as regras existentes** se você quiser substituir as regras existentes pelas regras importadas.
      - **Mesclar com as regras existentes** se você quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.
   d. Na janela padrão do Microsoft Windows, selecione os arquivos XML criados após a conclusão da tarefa de grupo do Gerador de Regras de Controle de Inicialização de Aplicativos.
   e. Clique em **OK** na janela **Regras de controle de inicialização de aplicativos** e na janela **Configurações de tarefa**.
5. Se você quiser aplicar as regras criadas para controlar a inicialização de aplicativos, na política nas propriedades da tarefa de Controle de Inicialização de Aplicativos, selecione o modo **Ativa** para a tarefa.

Regras de permissão geradas automaticamente com base em execuções de tarefa em cada computador separado são aplicadas a todos os computadores de rede abrangidos pela política que está sendo configurada. Nesses computadores, o aplicativo permitirá a inicialização somente daqueles aplicativos para os quais foram criadas regras de permissão.

Verificação da inicialização de aplicativos

Antes de aplicar as regras de Controle de inicialização de aplicativos configuradas, você pode testar qualquer aplicativo para determinar quais regras de controle de inicialização de aplicativos são acionadas pelo aplicativo.

O Kaspersky Embedded Systems Security nega a inicialização de aplicativos cuja inicialização não é permitida por uma única regra. Para evitar a negação da inicialização de aplicativos importantes você deve criar regras de permissão para eles.

Se a inicialização do aplicativo for controlada por várias regras de tipos diferentes, as regras de negação têm prioridade: a inicialização do aplicativo será negada se cair em ao menos uma regra de negação.

► *Para testar as regras de Controle de Inicialização de Aplicativos:*

1. Abra a janela de **Regras de Controle de Inicialização de Aplicativos** (consulte a seção "Abertura da lista de regras de Controle de inicialização de aplicativos" na página 299).
2. Na janela exibida, clique no botão **Mostrar regras do arquivo**.

   A janela padrão do Microsoft Windows é exibida.
3. Selecione o arquivo cujo controle de inicialização você deseja testar.

O caminho do arquivo especificado é exibido no campo de pesquisa. A lista contém todas as regras que serão acionadas na inicialização do arquivo selecionado.

Criação de uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos

► *Para criar e configurar as definições da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:*

1. Abra a janela **Configurações** no Assistente de nova tarefa (consulte a seção "Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos" na página 299).
2. Defina as seguintes configurações:
   - Especifique um **Pref. p/ nomes reg**.

     Essa é a primeira parte de um nome de regra. A segunda parte do nome da regra é formada a partir do nome do objeto para o qual a inicialização é permitida.

     O prefixo padrão é o nome do computador no qual o Kaspersky Embedded Systems Security está instalado. Você pode modificar o prefixo dos nomes de regras de permissão.
   - Configuração do escopo de uso das regras de permissão (consulte a seção "Restrição do escopo de uso de tarefa" na página 335).
3. Clique em **Avançar**.
4. Especifique as ações que devem ser executadas pelo Kaspersky Embedded Systems Security:
   - Ao gerar regras de permissão (consulte a seção "Ações a serem executadas durante a geração automática de regras" na página 335).
   - Ao concluir uma tarefa (consulte a seção "Ações a serem executadas após a conclusão da geração automática de regras" na página 337).
5. Na janela **Agendar**, defina as configurações de programação de inicialização da tarefa.
6. Clique em **Avançar**.
7. Na janela **Seleção de uma conta para a executar a tarefa**, especifique a conta que você quer usar.
8. Clique em **Avançar**.
9. Defina um nome de tarefa.
10. Clique em **Avançar**.

O nome da tarefa não deve ter mais de 100 caracteres e não pode conter os seguintes símbolos:

```
" * < > & \ : |
```

A janela **Conclusão da criação da tarefa** será aberta.

11. Você também pode executar a tarefa após a finalização do Assistente marcando a caixa de seleção **Executar a tarefa após a finalização do Assistente**.
12. Clique em **Concluir** para concluir a criação da tarefa.

► *Para configurar uma regra existente no Kaspersky Security Center,*

abra a janela **Propriedades: Gerador de Regras de Controle de Inicialização de Aplicativos** e ajuste as configurações descritas acima.

As informações sobre data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

Nesta seção

Restrição do escopo de uso da tarefa 317
Ações a serem executadas durante a geração automática de regras 318
Ações a serem executadas após a conclusão da geração automática de regras 319

Restrição do escopo de uso da tarefa

► *Para restringir o escopo da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:*

1. Abra a janela **Propriedades: Gerador de Regras de Controle de Inicialização de Aplicativos** (consulte a seção "Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos" na página 299).
2. Defina as seguintes configurações da tarefa:
   - **Criar regras de permissão com base nos aplicativos em execução**.

     Essa caixa ativa ou desativa a geração de regras de Controle de Inicialização de Aplicativos para aplicativos que já estão em execução. Esta opção é recomendada se o computador tiver um conjunto de referência de aplicativos com base no qual você deseja criar regras de permissão.

     Se essa caixa estiver selecionada, as regras de permissão de Controle de inicialização de aplicativos serão geradas de acordo com os aplicativos em execução.

     Se essa caixa de seleção estiver desmarcada, os aplicativos em execução não serão considerados ao gerar regras de permissão.

     A caixa de seleção é selecionada por padrão.

     Esta caixa não pode ser desmarcada se nenhuma das pastas estiver selecionada na tabela **Criar regras de permissão para aplicativos das pastas**.
   - **Criar regras de permissão para aplicativos das pastas**.

Você pode usar a tabela para selecionar ou especificar pastas para a tarefa e os tipos de arquivos executáveis a serem considerados ao criar as regras de Controle de inicialização de aplicativos. A tarefa gerará regras de permissão para os arquivos dos tipos selecionados que estão localizados nas pastas especificadas.

3. Clique em **OK**.

As configurações especificadas são salvas.

Ações a serem executadas durante a geração automática de regras

► *Para configurar as ações que o Kaspersky Embedded Systems Security deverá executar enquanto a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos estiver sendo executada:*

1. Abra a janela **Propriedades: Gerador de Regras de Controle de Inicialização de Aplicativos** (consulte a seção "**Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos**" na página 299).
2. Abra a guia **Opções**.
3. Na seção **Ao gerar regras de permissão**, defina as seguintes configurações:
   - **Usar certificado digital**

Se essa opção estiver selecionada, a presença de um certificado digital será especificada como critério para acionamento de regras nas configurações das regras de permissão geradas recentemente para o Controle de Inicialização de Aplicativos. O aplicativo permitirá agora a inicialização de programas iniciados usando arquivos com um certificado digital. Recomendamos essa opção se você quiser permitir a inicialização de qualquer aplicativo que seja confiável no sistema operacional.

Esta opção é selecionada por padrão.

- **Usar o assunto e a miniatura de certificado digital**

  A caixa de seleção ativa ou desativa o uso do requerente e da impressão digital do certificado digital do arquivo como critério para acionamento de regras de permissão no Controle de inicialização de aplicativos. A seleção desta caixa permite a especificação de condições de verificação mais rigorosas para o certificado digital.

  Se essa caixa estiver selecionada, os valores de requerente e impressão digital do certificado digital dos arquivos para os quais as regras serão geradas serão estabelecidos como um critério para acionamento das regras de permissão no Controle de inicialização de aplicativos. O Kaspersky Embedded Systems Security permitirá que os aplicativos que sejam iniciados usando arquivos com uma impressão digital e um certificado digital especificados.

  A seleção dessa caixa restringe fortemente o acionamento de regras de permissão com base em um certificado digital, pois a impressão digital é um identificador único de um certificado digital e não pode ser forjada.

  Se esta caixa estiver desmarcada, a existência de qualquer certificado digital confiável no sistema operacional é estabelecida como um critério para acionamento de regras de permissão de Controle de inicialização de aplicativos.

  A caixa de seleção estará ativa se a opção **Usar certificado digital** estiver selecionada.

  A caixa de seleção é selecionada por padrão.

- **Se o certificado estiver ausente, use**

Essa é uma lista suspensa que permite que você selecione o critério para acionamento de uma regra de permissão de Controle de inicialização de aplicativos se o arquivo usado para gerar a regra não tiver um certificado digital.

- **Hash SHA256**. O valor da soma de verificação do arquivo usado para gerar a regra é estabelecido como o critério para acionamento da regra de permissão de Controle de inicialização de aplicativos. O aplicativo permitirá a inicialização de programas iniciados usando arquivos com a soma de verificação especificada.
- **caminho do arquivo**. O caminho do arquivo usado para gerar a regra é estabelecido como o critério para acionamento da regra de permissão de Controle de inicialização de aplicativos. O aplicativo agora permitirá a inicialização de programas usando arquivos localizados nas pastas especificadas na tabela **Criar regras de permissão para aplicativos das pastas** na seção **Configurações**.

- **Usar hash SHA256**

Se esta opção estiver selecionada, o valor da soma de verificação do arquivo usado para gerar a regra será especificado como um critério para acionamento de regras nas configurações das regras de permissão geradas recentemente para o Controle de inicialização de aplicativos. O aplicativo permitirá a inicialização de programas iniciados usando arquivos com a soma de verificação especificada.

Recomendamos essa opção para casos em que as regras geradas devem alcançar o nível de segurança mais alto: a soma de verificação do SHA256 pode ser usada como um ID único de arquivo. O uso da soma de verificação do SHA256 como critério para acionamento de regras restringe o escopo de uso das regras para um arquivo.

Esta opção é desmarcada por padrão.

- **Gerar regras para usuário ou grupo de usuários**.

  Esse é um campo que exibe um usuário ou grupo de usuários. O aplicativo controlará qualquer aplicativo executado pelo usuário ou grupo de usuários especificado.

  A seleção padrão é **Todos**.

1. Clique em **OK**.

As configurações especificadas são salvas.

Ações a serem executadas após a conclusão da geração automática de regras

► *Para configurar as ações a serem executadas pelo Kaspersky Embedded Systems Security após a execução da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:*

1. Abra a janela **Propriedades: Gerador de Regras de Controle de Inicialização de Aplicativos** (consulte a seção "Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos" na página 299).
2. Abra a guia **Opções**.
3. Na seção **Após a conclusão da tarefa**, configure as seguintes configurações:
   - **Adicionar regras de permissão à lista de regras de Controle de Inicialização de Aplicativos**.

     A caixa de seleção ativa ou desativa a adição de regras de permissão geradas recentemente à lista de regras de Controle Inicialização de Aplicativos. A lista de regras de Controle de inicialização de aplicativos é exibida quando você clica no link **Regras de Controle de Inicialização de Aplicativos** no painel de detalhes do nó Controle de inicialização de aplicativos.

Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security adicionará as regras que foram geradas pela tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos à lista de regras de Controle de inicialização de aplicativos com base no princípio selecionado para adição de regras.

Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não adicionará as regras de permissão geradas recentemente à lista de regras de Controle de inicialização de aplicativos. As regras geradas são exportadas somente para um arquivo.

A caixa de seleção é selecionada por padrão.

- **Princípio da adição**.

  Essa lista suspensa é usada para especificar o método utilizado para a adição de regras de permissão geradas recentemente à lista de regras de Controle de Inicialização de Aplicativos.

  - **Adicionar às regras existentes**. As regras são adicionadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.
  - **Substituir as regras existentes**. As regras substituem as regras existentes na lista.
  - **Mesclar com as regras existentes**. As regras são adicionadas à lista de regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.

  Por padrão, o método **Mesclar com as regras existentes** é selecionado.

- **Exportar regras de permissão para o arquivo**.
- **Adicionar informações do computador ao nome do arquivo**.

  A caixa de seleção ativa ou desativa a adição de informações sobre o computador protegido ao nome do arquivo para o qual as regras de permissão serão exportadas.

  Se esta caixa estiver selecionada, o aplicativo adicionará o nome de computador protegido e a data e hora de criação de arquivos ao nome do arquivo de exportação.

  Se a caixa estiver desmarcada, o aplicativo não adicionará informações sobre o computador protegido ao nome do arquivo de exportação.

  A caixa de seleção é selecionada por padrão.

4. Clique em **OK**.

As configurações especificadas são salvas.

Gerenciamento do Controle de Inicialização de Aplicativos por meio do Console do Aplicativo

Nesta seção, aprenda como navegar pela interface do Console do Aplicativo e definir configurações de tarefa em um computador local.

Nesta seção

Navegação 321
Definição de configurações da tarefa de Controle de Inicialização de Aplicativos 322
Configuração de regras de Controle de inicialização de aplicativos 329
Configuração de uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos 334

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface.

Nesta seção

Abertura das configurações da tarefa de Controle de Inicialização de Aplicativos 321
Abertura da janela de regras de Controle de Inicialização de Aplicativos 321
Abertura das definições da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos 322

Abertura das configurações da tarefa de Controle de Inicialização de Aplicativos

► *Para definir as configurações gerais da tarefa de Controle de inicialização de Aplicativos por meio do Console do Aplicativo:*

1. Na árvore do Console do Aplicativo, expanda o nó **Controle do computador**.
2. Selecione o nó filho **Controle de Inicialização de Aplicativos**.
3. No painel de detalhes do nó filho **Controle de Inicialização de Aplicativos**, clique no link **Propriedades**.

   A janela **Configurações de tarefa** é exibida.

Abertura da janela de regras de Controle de Inicialização de Aplicativos

► *Para abrir a lista de regras de Controle de Inicialização de Aplicativos por meio do Console do Aplicativo:*

1. Na árvore do Console do Aplicativo, expanda o nó **Controle do computador**.
2. Selecione o nó filho **Controle de Inicialização de Aplicativos**.
3. No painel de detalhes do nó **Controle de Inicialização de Aplicativos**, clique no link **Regras de Controle de Inicialização de Aplicativos**.

   A janela **Regras de Controle de Inicialização de Aplicativos** é exibida.
4. Configure a lista de regras conforme necessário.

Abertura das definições da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos

► *Para configurar a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:*

1. Na árvore do Console do Aplicativo, expanda o nó **Geradores de regra automáticos**.
2. Selecione o nó filho **Gerador de Regras de Controle de Inicialização de Aplicativos**.
3. No painel de detalhes do nó filho **Gerador de Regras de Controle de Inicialização de Aplicativos**, clique no link **Propriedades**.

   A janela **Configurações de tarefa** é exibida.
4. Configure a tarefa conforme necessário.

Definição de configurações da tarefa de Controle de Inicialização de Aplicativos

► *Para definir as configurações gerais da tarefa de Controle de Inicialização de Aplicativos:*

1. Abra a janela **Configurações de tarefa** (consulte a seção "Abertura das configurações da tarefa de Controle de Inicialização de Aplicativos" na página 321).
2. Defina as seguintes configurações da tarefa:
   - Na guia **Geral**:
     - Modo da tarefa de Controle de Inicialização de Aplicativos (consulte a seção "Seleção do modo da tarefa de Controle de Inicialização de Aplicativos" na página 323).
     - Escopo de uso das regras na tarefa (consulte a seção "Configuração do escopo da tarefa de Controle de Inicialização de Aplicativos" na página 324).
     - Uso da KSN (consulte a seção "Configuração do uso da KSN" na página 325).
   - Configurações de Controle de Distribuição de Software (consulte a seção "Controle de Distribuição de Software" na página 326) na guia **Controle de distribuição de software**.
   - Configurações de programação de inicialização da tarefa (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 151) nas guias **Agendar** e **Avançado**.
3. Clique em **OK** na janela **Configurações de tarefa**.

   As configurações modificadas são salvas.

O Kaspersky Embedded Systems Security aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

Nesta seção

Seleção do modo da tarefa de Controle de Inicialização de Aplicativos 323
Configuração do escopo da tarefa de Controle de Inicialização de Aplicativos 324
Configuração do uso da KSN 325
Controle de Distribuição de Software 326

Seleção do modo da tarefa de Controle de Inicialização de Aplicativos

► *Para configurar o modo da tarefa de Controle de inicialização de aplicativos:*

1. Abra a janela **Configurações de tarefa** (consulte a seção "**Abertura das configurações da tarefa de Controle de Inicialização de Aplicativos**" na página 321).
2. Na guia **Geral**, na lista suspensa **Modo da tarefa**, especifique o modo da tarefa.

   Nesta lista suspensa você pode selecionar um modo de tarefa de Controle de inicialização de aplicativos:

   - **Ativa**. O Kaspersky Embedded Systems Security usa as regras especificadas para controlar a inicialização de qualquer aplicativo.
   - **Somente Estatísticas**. O Kaspersky Embedded Systems Security não usa as regras especificadas para controlar a inicialização de aplicativos. Em vez disso, ele simplesmente registra informações sobre essas inicializações no log de tarefas. Todos os programas podem ser inicializados. Você pode usar esse modo para gerar uma lista de regras de Controle de Inicialização de Aplicativos com base nas informações de bloqueio registradas no log de tarefas.

   Por padrão, a tarefa de Controle de Inicialização de Aplicativos é executada no modo **Somente Estatísticas**.
3. Desmarque ou selecione a caixa de seleção **Repetir ação da primeira inicialização de arquivo em todas as inicializações subsequentes deste arquivo**.

   A caixa de seleção ativa ou desativa o controle de inicialização para a segunda tentativa e todas as tentativas subsequentes de inicialização de aplicativos com base nas informações de eventos armazenadas em cache.

   Se a caixa estiver selecionada, o Kaspersky Embedded Systems Security permitirá ou negará uma inicialização subsequente do aplicativo com base na conclusão da tarefa referente à primeira inicialização do aplicativo. Por exemplo, se a primeira inicialização de aplicativo foi permitida pelas regras, as informações sobre essa decisão serão armazenadas em cache e a segunda e todas as inicializações subsequentes também serão permitidas, sem qualquer verificação adicional.

   Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security analisará o aplicativo a cada tentativa de inicialização.

   A caixa de seleção é selecionada por padrão.

O Kaspersky Embedded Systems Security cria uma nova lista de eventos em cache sempre que as configurações da tarefa de Controle de Inicialização de Aplicativos forem modificadas. Isso significa que o Controle de Inicialização de Aplicativos é executado de acordo com as configurações de segurança atuais.

4. Desmarque ou selecione **Negar a inicialização de interpretadores da linha de comando sem o comando para executar**.

   Se a caixa estiver selecionada, o Kaspersky Embedded Systems Security negará a inicialização de interpretadores da linha de comando, mesmo que a inicialização de interpretadores seja permitida. Um interpretador de comando só pode ser inicializado sem um comando se ambas as condições a seguir forem atendidas:

   - A inicialização do interpretador da linha de comando é permitida.
   - O comando a ser executado é permitido.

   Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security só considerará as regras de permissão ao inicializar o interpretador da linha de comando. A inicialização será negada se nenhuma regra de permissão for aplicável ou se o processo executável não for considerado confiável pela KSN. Se uma regra de permissão for aplicável ou se o processo for considerado confiável pela KSN, um interpretador da linha de comando pode ser inicializado com ou sem um comando a ser executado.

   O Kaspersky Embedded Systems Security reconhece os seguintes interpretadores da linha de comando:

   - cmd.exe
   - powershell.exe
   - python.exe
   - perl.exe

   Esta caixa é desmarcada por padrão.

5. Clique em **OK**.

As configurações especificadas são salvas.

Todas as tentativas de iniciar aplicativos são registradas no log de tarefas.

Configuração do escopo da tarefa de Controle de Inicialização de Aplicativos

► *Para definir o escopo da tarefa de Controle de Inicialização de Aplicativos:*

1. Abra a janela **Configurações de tarefa** (consulte a seção "**Abertura das configurações da tarefa de Controle de Inicialização de Aplicativos**" na página 321).
2. Na guia **Geral**, na seção **Escopo de uso das regras**, especifique as seguintes configurações:
   - **Aplicar regras a arquivos executáveis**

     A caixa de seleção ativa ou desativa o controle de inicialização de arquivos executáveis.

     Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security permitirá ou bloqueará a inicialização de arquivos executáveis usando as regras especificas cujas

definições especificam **Arquivos executáveis** como escopo.

Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não controlará a inicialização de arquivos executáveis usando as regras especificas. A inicialização de arquivos executáveis será permitida.

A caixa de seleção é selecionada por padrão.

- **Monitorar o carregamento de módulos DLL**

  A caixa de seleção ativa ou desativa o controle de carregamento de módulos DLL.

  Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security permitirá ou bloqueará o carregamento de módulos DLL usando as regras especificas cujas definições especificam **Arquivos executáveis** como escopo.

  Se essa caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não controlará o carregamento de módulos DLL usando as regras especificas. O carregamento de módulos DLL será permitido.

  A caixa de seleção estará ativa se a caixa se seleção **Aplicar regras a arquivos executáveis** estiver selecionada.

  Esta caixa é desmarcada por padrão.

  O controle do carregamento de módulos DLL pode afetar o desempenho do sistema operacional.

- **Aplicar regras a scripts e pacotes MSI**

  A caixa de seleção ativa ou desativa a inicialização de scripts e pacotes MSI.

  Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security permitirá ou bloqueará a inicialização de scripts e pacotes MSI usando as regras especificas cujas definições especificam scripts e pacotes MSI como escopo.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não controlará a inicialização de scripts e pacotes MSI usando regras especificas. A inicialização de scripts e pacotes MSI é permitida.

  A caixa de seleção é selecionada por padrão.

3. Clique em **OK**.

As configurações especificadas são salvas.

Configuração do uso da KSN

► *Para configurar o uso dos serviços da KSN na tarefa de Controle de Inicialização de Aplicativos:*

1. Abra a janela **Configurações de tarefa** (consulte a seção "**Abertura das configurações da tarefa de Controle de Inicialização de Aplicativos**" na página 321).
2. Na guia **Geral**, na seção **Uso da KSN**, defina as configurações para uso dos serviços da KSN:
   - Se necessário, marque a caixa de seleção **Proibir aplicativos não confiáveis pela KSN**.

     A caixa de seleção ativa ou desativa o Controle de Inicialização de Aplicativos de acordo com a reputação do aplicativo na KSN.

     Se essa caixa estiver selecionada, o Kaspersky Embedded Systems Security bloqueará a execução de qualquer aplicativo que não for considerado confiável pela KSN. As regras

de permissão de Controle de Inicialização de Aplicativos que se aplicam a aplicativos não confiáveis pela KSN não serão acionadas. A seleção da caixa fornece proteção adicional contra malware.

Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não considerará a reputação de aplicativos não confiáveis na KSN e permitirá ou bloqueará a inicialização de acordo com as regras que se aplicam a esses programas.

Esta caixa é desmarcada por padrão.

- Se necessário, marque a caixa de seleção **Permitir aplicativos confiáveis pela KSN**.

  A caixa de seleção ativa ou desativa o Controle de Inicialização de Aplicativos de acordo com a reputação do aplicativo na KSN.

  Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security permitirá a execução de aplicativos considerados confiáveis pela KSN. Regras de negação de Controle de Inicialização de Aplicativos aplicáveis aos aplicativos considerados como confiáveis pela KSN têm prioridade mais alta: se um aplicativo for considerado confiável pelos serviços da KSN, a inicialização desse aplicativo será negada.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não considerará a reputação de aplicativos considerados confiáveis pela KSN e permitirá ou negará a inicialização conforme as regras que se aplicam a esses aplicativos.

  Esta caixa é desmarcada por padrão.

- Se a caixa de seleção **Permitir aplicativos confiáveis pela KSN** for marcada, indique os usuários e/ou grupos de usuários que podem iniciar aplicativos confiáveis na KSN. Para isso, execute as seguintes ações:

  a. Clique no botão **Editar**.

     A janela **Selecionar usuários ou grupos** padrão do Microsoft Windows é exibida.

  b. Especifique a lista usuário e/ou grupos usuário.

  c. Clique em **OK**.

3. Clique em **OK** na janela **Configurações de tarefa**.

As configurações especificadas são salvas.

Controle de Distribuição de Software

► *Para adicionar um pacote de distribuição confiável:*

1. Abra a janela **Configurações de tarefa** (consulte a seção "**Abertura das configurações da tarefa de Controle de Inicialização de Aplicativos**" na página 321).
2. Na guia **Controle de distribuição de software**, selecione a caixa **Permitir distribuição automática de software para aplicativos e pacotes listados**.

   A caixa de seleção ativa e desativa a criação automática de exclusões para todos os arquivos iniciados usando os pacotes de distribuição especificados na lista.

   Se a caixa de seleção for marcada, o aplicativo permite automaticamente que os arquivos nos pacotes de distribuição confiáveis sejam inicializados. A lista de aplicativos e pacotes de distribuição com inicialização permitida pode ser editada.

   Se a caixa de seleção for desmarcada, o aplicativo não aplicará as exclusões específicas

na lista.

Esta caixa é desmarcada por padrão.

É possível selecionar **Permitir distribuição automática de software para aplicativos e pacotes listados** se a caixa de seleção **Aplicar regras a arquivos executáveis** na guia **Geral** estiver marcada nas configurações da tarefa de **Controle de Inicialização de Aplicativos**.

3. Desmarque a caixa de seleção **Sempre permitir distribuição de software via Windows Installer**, se necessário.

   A caixa de seleção ativa e desativa a criação automática de exclusões para todos os arquivos executados por meio do Windows Installer.

   Se a caixa de seleção estiver marcada, arquivos instalados por meio do Windows Installer sempre terão permissão para inicializar.

   Se a caixa de seleção estiver desmarcada, os arquivos não terão permissão incondicional para inicializar, mesmo que tenham sido instalados por meio do Windows Installer.

   A caixa de seleção é selecionada por padrão.

   A caixa de seleção não é editável se a caixa **Permitir distribuição automática de software para aplicativos e pacotes listados** não estiver marcada.

Desmarcar a caixa de seleção **Sempre permitir distribuição de software via Windows Installer** só é recomendado se for absolutamente necessário. Desativar essa função pode causar problemas na atualização de arquivos do sistema operacional e também impedir a inicialização de arquivos extraídos de um pacote de distribuição.

4. Se necessário, marque a caixa de seleção **Sempre permitir distribuição de software via SCCM usando o Background Intelligent Transfer Service**.

   A caixa de seleção ativa e desativa a distribuição automática de software usando o System Center Configuration Manager.

   Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security automaticamente permitirá a implantação do Microsoft Windows usando o Gerenciador de configuração do centro do sistema. O aplicativo permite a distribuição de software apenas através do Serviço de transferência inteligente em segundo plano.

   O aplicativo controla a inicialização dos objetos com as seguintes extensões:

   - .exe
   - .msi

   Esta caixa é desmarcada por padrão.

O aplicativo controla o ciclo de distribuição de software no computador, da entrega do pacote à instalação ou atualização. O aplicativo não controla processos se algum dos estágios da distribuição tiver sido executado antes da instalação do aplicativo no computador.

5. Para editar a lista de pacotes de distribuição confiáveis, clique em **Alterar lista de pacotes** e selecione um dos seguintes métodos na janela exibida:

   - **Adicionar um pacote de distribuição**.

a. Clique no botão **Procurar** e selecione um arquivo executável ou pacote de distribuição.

   A seção **Critérios de confiança** é automaticamente preenchida com os dados sobre o arquivo selecionado.

b. Desmarque ou selecione a caixa **Permitir a inicialização para todos os arquivos desta cadeia de extração do pacote de distribuição**.

c. Selecione uma das duas opções disponíveis para os critérios a serem usados para determinar se um arquivo ou pacote de distribuição é confiável:

   - **Usar certificado digital**
   - **Usar hash SHA256**

- **Adicionar diversos pacotes de distribuição por hash**.

  É possível selecionar um número ilimitado de arquivos executáveis e pacotes de distribuição e adicioná-los à lista ao mesmo tempo. O Kaspersky Embedded Systems Security examina o hash e permite que o sistema operacional inicie os arquivos especificados.

- **Alterar pacote selecionado**.

  Use esta opção para selecionar um arquivo executável ou pacote de distribuição diferente, ou para alterar os critérios de confiança.

- **Importar lista de pacotes de distribuição do arquivo**.

  É possível importar a lista de pacotes de distribuição confiáveis de um arquivo de configuração. Para que seja reconhecido pelo Kaspersky Embedded Systems Security, o arquivo deve satisfazer os seguintes parâmetros:

  - A extensão do arquivo é TXT.
  - O arquivo contém informações estruturadas como uma lista de linhas, onde cada linha inclui dados para um dos arquivos confiáveis.
  - O arquivo deve conter uma lista em um dos seguintes formatos:
    - <nome do arquivo>:<hash SHA256>.
    - <hash SHA256>*<nome do arquivo>.

  Na janela **Abrir**, especifique o arquivo de configuração que contém uma lista de pacotes de distribuição confiáveis.

6. Se quiser remover um aplicativo ou pacote de distribuição previamente adicionado da lista de confiáveis, clique no botão **Excluir pacotes de distribuição**. Arquivos extraídos não poderão ser executados.

   Para evitar que arquivos extraídos sejam iniciados, desinstale o aplicativo no computador protegido ou crie uma regra de negação nas configurações da tarefa de Controle de Inicialização de Aplicativos.

7. Clique em **OK**.

As configurações recém-definidas foram salvas.

Configuração de regras de Controle de Inicialização de Aplicativos

Aprenda como gerar, importar e exportar uma lista de regras ou criar manualmente regras de permissão ou de negação permitindo usando a tarefa de Controle de Inicialização de Aplicativos.

Nesta seção

Adição de uma regra de Controle de Inicialização de Aplicativos....329
Ativar o modo de permissão padrão....332
Criação de regras de permissão a partir de eventos da tarefa de Controle de Inicialização de Aplicativos....332
Exportando regras de Controle de inicialização de aplicativos....333
Importação de regras de Controle de inicialização de aplicativos de um arquivo XML....333
Removendo regras de Controle de inicialização de aplicativos....334

Adição de uma regra de Controle de Inicialização de Aplicativos

► *Para adicionar uma regra de Controle de inicialização de aplicativos, siga as etapas a seguir:*

1. Abertura da janela de **Regras de Controle de Inicialização de Aplicativos**.
2. Clique no botão **Adicionar**.
3. No menu de contexto do botão, selecione **Adicionar uma regra**.

   A janela **Configurações de regra** é exibida.
4. Defina as seguintes configurações:
   a. No campo **Nome**, digite o nome da regra.
   b. Na lista suspensa **Tipo**, selecione o tipo de regra:
      - **Permissão** se você quiser que a regra permita a inicialização de aplicativos de acordo com os critérios especificados nas configurações da regra.
      - **Proibição** se você quiser que a regra bloqueie a inicialização dos aplicativos de acordo com os critérios especificados nas configurações da regra.
   c. Na lista suspensa **Escopo**, selecione o tipo de arquivo cuja execução será controlada pela regra:
      - **Arquivos executáveis** se você quiser que a regra controle a inicialização de arquivos executáveis.
      - **Pacotes de scripts e MSI** se você quiser que a regra controle a inicialização de scripts e pacotes MSI.
   d. No campo **Usuário ou grupo de usuários**, especifique os usuários que terão permissão ou não para iniciar programas com base no tipo da regra. Para isso, execute as seguintes ações:
      i. Clique no botão **Procurar**.
      ii. A janela **Selecionar usuários ou grupos** padrão do Microsoft Windows é exibida.
      iii. Especifique a lista usuário e/ou grupos usuário.
      iv. Clique em **OK**.
   e. Se você deseja obter os valores dos critérios para acionamento de regras listados na seção **Critério**

para acionamento de regras a partir de um arquivo específico:

i. Clique no botão **Definir critério disponíveis de regra a partir das propriedades do arquivo**.

A janela **Abrir** padrão do Microsoft Windows é exibida.

ii. Selecione o arquivo.

iii. Clique no botão **Abrir**.

Os valores de critérios no arquivo serão exibidos nos campos da seção **Critério para acionamento de regras**. O critério para o qual os dados estão disponíveis nas propriedades de arquivo é selecionado por padrão.

f. Na seção **Critério para acionamento de regras**, selecione uma das seguintes opções:

- **Certificado digital** se você quiser que a regra controle a inicialização de programas que usam arquivos assinados com um certificado digital:
  - Marque a caixa de seleção **Usar assunto** se você quiser que regra controle a inicialização de arquivos assinados com um certificado digital somente com o cabeçalho especificado.
  - Marque a caixa de seleção **Usar miniatura** se você quiser que a regra controle a inicialização de arquivos assinados com um certificado digital somente com a impressão digital especificada.
- **Hash SHA256** se você quiser que a regra controle a inicialização de programas que usam arquivos cuja soma de verificação corresponde àquela especificada.
- **Caminho do arquivo** se você quiser que a regra controle a inicialização de programas que usam arquivos localizados no caminho especificado.

> O Kaspersky Embedded Systems Security não reconhece caminhos que contêm barras "/". Use a barra invertida "\" para inserir o caminho corretamente.

g. Se deseja adicionar exclusões de regra:

i. Na seção **Exclusões da regra**, clique no botão **Adicionar**.

A janela **Exclusão da regra** é exibida.

ii. No campo **Nome**, digite o nome da exclusão.

iii. Especifique as configurações para exclusão dos arquivos de aplicativos da regra de Controle de inicialização de aplicativos. Você pode preencher os campos de configurações a partir das propriedades do arquivo clicando no botão **Def. excl. com base nas prop. do arq.**

- **Certificado digital**

Se essa opção estiver selecionada, a presença de um certificado digital será especificada como critério para acionamento de regras nas configurações das regras de permissão geradas recentemente para o Controle de Inicialização de Aplicativos. O aplicativo permitirá agora a inicialização de programas iniciados usando arquivos com um certificado digital. Recomendamos essa opção se você quiser permitir a inicialização de qualquer aplicativo que seja confiável no sistema operacional.

Esta opção é selecionada por padrão.

- **Usar assunto**

  A caixa de seleção ativa ou desativa o uso do requerente do certificado digital como critério para acionamento de regras.

Se a caixa estiver selecionada, o requerente especificado do certificado digital será usado como critério para acionamento de regras. A regra criada controlará a inicialização de aplicativos somente para o fornecedor especificado no requerente.

Se a caixa estiver desmarcada, o aplicativo não usará o requerente do certificado digital como critério para acionamento de regras. Se o critério do **Certificado digital** for selecionado, a regra criada controlará a inicialização de aplicativos assinados com um certificado digital que contenha qualquer requerente.

O requerente do certificado digital usado para assinar o arquivo pode ser especificado somente a partir das propriedades do arquivo selecionado usando o botão **Definir critério disponíveis de regra a partir das propriedades do arquivo** localizado acima da seção **Critério para acionamento de regras**.

Esta caixa é desmarcada por padrão.

- **Usar miniatura**

  A caixa de seleção ativa ou desativa o uso da impressão digital do certificado digital como critério para acionamento de regras.

  Se a caixa estiver selecionada, a impressão digital especificada do certificado digital será usada como critério para acionamento de regras. A regra criada controlará a inicialização de aplicativos assinados com um certificado digital com a impressão digital especificada.

  Se a caixa estiver desmarcada, o aplicativo não usará a impressão digital do certificado digital como critério para acionamento de regras. Se o critério do **Certificado digital** for selecionado, o aplicativo controlará a inicialização de aplicativos assinados com um certificado digital que contenha qualquer impressão digital.

  A impressão digital do certificado digital usada para assinar o arquivo pode ser especificada somente a partir das propriedades do arquivo selecionado usando o botão **Definir critério disponíveis de regra a partir das propriedades do arquivo** localizado acima da seção **Critério para acionamento de regras**.

  Esta caixa é desmarcada por padrão.

- **Hash SHA256**

Se esta opção estiver selecionada, o valor da soma de verificação do arquivo usado para gerar a regra será especificado como um critério para acionamento de regras nas configurações das regras de permissão geradas recentemente para o Controle de inicialização de aplicativos. O aplicativo permitirá a inicialização de programas iniciados usando arquivos com a soma de verificação especificada.

Recomendamos essa opção para casos em que as regras geradas devem alcançar o nível de segurança mais alto: a soma de verificação do SHA256 pode ser usada como um ID único de arquivo. O uso da soma de verificação do SHA256 como critério para acionamento de regras restringe o escopo de uso das regras para um arquivo.

Esta opção é desmarcada por padrão.

- **Caminho do arquivo**

  Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security usará o caminho completo do arquivo para determinar se o processo é confiável.

  Se a caixa de seleção estiver desmarcada, o caminho para o arquivo não é usado para determinar se o processo é confiável.

  Esta caixa é desmarcada por padrão.

i. Clique em **OK**.

ii. Se necessário, repita os itens (i)-(iv) para incluir exclusões adicionais.

1. Clique em **OK** na janela **Configurações de regra**.

A regra criada é exibida na lista na janela **Regras de Controle de Inicialização de Aplicativos**.

Ativar o modo de Permissão padrão

O modo de Permissão padrão permite que todos os aplicativos sejam inicializados se não estiverem bloqueados por regras ou pela conclusão da KSN de que não são confiáveis. O modo de Permissão padrão pode ser ativado adicionando regras de permissão específicas. Você pode ativar a Permissão padrão apenas para scripts ou para todos os arquivos executáveis.

► *Para adicionar uma regra de Permissão padrão:*

1. Abertura da janela de **Regras de Controle de Inicialização de Aplicativos**.
2. Clique no botão **Adicionar**.
3. No menu de contexto do botão, selecione **Adicionar uma regra**.

   A janela **Configurações de regra** é exibida.
4. No campo **Nome**, digite o nome da regra.
5. Na lista suspensa **Tipo**, selecione o tipo de regra **Permissão**.
6. Na lista suspensa **Escopo**, selecione o tipo de arquivo cuja execução será controlada pela regra:
   - **Arquivos executáveis** se você quiser que a regra controle a inicialização de arquivos executáveis de aplicativos.
   - **Pacotes de scripts e MSI** se você quiser que a regra controle a inicialização de scripts e pacotes MSI.
7. Na seção **Critério para acionamento de regras**, selecione a opção **Caminho do arquivo**.
8. Insira a seguinte máscara: `?:\`
9. Clique em **OK** na janela **Configurações de regra**.

O Kaspersky Embedded Systems Security aplicará o modo de Permissão padrão.

Criação de regras de permissão a partir de eventos da tarefa de Controle de Inicialização de Aplicativos

► *Para criar um arquivo de configuração contendo regras de permissão geradas a partir de eventos da tarefa de Controle de Inicialização de Aplicativos:*

1. Inicie a tarefa de Controle de Inicialização de Aplicativos no modo **Somente Estatísticas** (consulte a seção "Seleção do modo da tarefa de Controle de Inicialização de Aplicativos" na página 323) para registrar informações sobre todas as inicializações de aplicativos em um computador protegido no log de tarefas.
2. Após a conclusão da tarefa no modo **Somente Estatísticas**, abra o log de tarefas clicando no botão **Abrir log da tarefa** na seção **Gerenciamento** do painel de detalhes do nó **Controle de Inicialização de Aplicativos**.
3. Na janela **Logs**, clique em **Gerar regras com base em eventos**.

O Kaspersky Embedded Systems Security gerará um arquivo de configuração XML contendo a lista de regras com base em eventos da tarefa de Controle de Inicialização de Aplicativos no modo **Somente Estatísticas**.

Você pode aplicar esta lista de regras (consulte a seção "Importação de regras de Controle de inicialização de aplicativos de um arquivo XML" na página 333) na tarefa de Controle de Inicialização de Aplicativos.

Antes de aplicar a lista de regras gerada a partir dos eventos registrados d tarefa, recomendamos que você analise e processe a lista manualmente para certificar-se de que a inicialização de arquivos críticos (por exemplo, arquivos de sistema) seja permitida pelas regras especificadas.

Todos os eventos de tarefa são registrados no log de tarefas independentemente do modo da tarefa. Você pode gerar um arquivo de configuração com uma lista de regras baseada no log criado enquanto a tarefa está sendo executada no modo **Ativa**. Este cenário não é recomendado, exceto em casos urgentes, porque uma lista final de regras deve ser gerada antes que a tarefa seja executada no modo **Ativa** para que seja eficiente.

Exportando regras de Controle de inicialização de aplicativos

► *Importando regras de Controle de inicialização de aplicativos para um arquivo de configuração:*

1. Abertura da janela de **Regras de Controle de Inicialização de Aplicativos**.
2. Clique no botão **Exportar para um arquivo**.

   A janela padrão do Microsoft Windows é exibida.
3. Na janela exibida, especifique o arquivo ao qual deseja exportar as regras. Se nenhum arquivo existir, ele será criado. Se um arquivo com o nome especificado já existir, o seu conteúdo será sobrescrito após a exportação das regras.
4. Clique no botão **Salvar**.

As configurações de regra serão exportadas para o arquivo especificado.

Importação de regras de Controle de inicialização de aplicativos de um arquivo XML

► *Para importar as regras de Controle de Inicialização de Aplicativos:*

1. Abertura da janela de **Regras de Controle de Inicialização de Aplicativos**.
2. Clique no botão **Adicionar**.
3. No menu de contexto do botão, selecione **Importar regras do arquivo XML**.
4. Especifique o método para adicionar as regras importadas. Para fazer isso, selecione uma das opções do menu de contexto do botão **Importar regras do arquivo XML**:
   - **Adicionar às regras existentes** se você quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.
   - **Substituir as regras existentes** se você quiser substituir as regras existentes pelas regras importadas.
   - **Mesclar com as regras existentes** se você quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.

   A janela **Abrir** padrão do Microsoft Windows é exibida.
5. Na janela **Abrir**, selecione o arquivo XML que contém as regras de Controle de Inicialização de Aplicativos.

6. Clique no botão **Abrir**.

As regras importadas serão exibidas na lista da janela **Regras de Controle de Inicialização de Aplicativos**.

Removendo regras de Controle de inicialização de aplicativos

► *Para remover as regras de Controle de inicialização de aplicativos:*

1. Abertura da janela de **Regras de Controle de Inicialização de Aplicativos**.
2. Na lista, selecione uma ou mais regras que você deseja excluir.
3. Clique no botão **Remover selecionado**.
4. Clique no botão **Salvar**.

As regras de Controle de inicialização de aplicativos selecionados são excluídas.

Configuração de uma tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos

► *Para definir as configurações da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:*

1. Abra a janela **Configurações de tarefa** (consulte a seção "**Abertura das definições da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos**" na página 322) da tarefa do **Gerador de Regras de Controle de Inicialização de Aplicativos**.
2. Defina as seguintes configurações:
   - Na guia **Geral**:
     - Especifique um **Pref. p/ nomes reg**.

       Essa é a primeira parte de um nome de regra. A segunda parte do nome da regra é formada a partir do nome do objeto para o qual a inicialização é permitida.

       O prefixo padrão é o nome do computador no qual o Kaspersky Embedded Systems Security está instalado. Você pode modificar o prefixo dos nomes de regras de permissão.
     - Configuração do escopo de uso das regras de permissão (consulte a seção "Restrição do escopo de uso de tarefa" na página 335).
   - Na guia **Ação**, especifique as ações que devem ser executadas pelo Kaspersky Embedded Systems Security:
     - Ao gerar regras de permissão (consulte a seção "Ações a serem executadas durante a geração automática de regras" na página 335).
     - Ao concluir uma tarefa (consulte a seção "Ações a serem executadas após a conclusão da geração automática de regras" na página 337).
   - Nas guias **Programação** e **Avançado**, defina as configurações de início da tarefa agendada (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 151).
   - Na guia **Executar como**, defina as configurações de inicialização da tarefa com permissões de conta (consulte a seção "Especificação de uma conta de usuário para iniciar uma tarefa" na página 153).

3. Clique em **OK**.

O Kaspersky Embedded Systems Security aplica imediatamente as novas configurações à tarefa em execução. Informações sobre data e hora quando as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação.

Nesta seção

Restrição do escopo de uso da tarefa 335

Ações a serem executadas durante a geração automática de regras 335

Ações a serem executadas após a conclusão da geração automática de regras 337

Restrição do escopo de uso da tarefa

► *Para restringir o escopo da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:*

1. Abra a janela **Configurações de tarefa** (consulte a seção "**Abertura das definições da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos**" na página 322) da tarefa do **Gerador de Regras de Controle de Inicialização de Aplicativos**.
2. Defina as seguintes configurações da tarefa:
   - **Criar regras de permissão com base nos aplicativos em execução**.

     Essa caixa ativa ou desativa a geração de regras de Controle de Inicialização de Aplicativos para aplicativos que já estão em execução. Esta opção é recomendada se o computador tiver um conjunto de referência de aplicativos com base no qual você deseja criar regras de permissão.

     Se essa caixa estiver selecionada, as regras de permissão de Controle de inicialização de aplicativos serão geradas de acordo com os aplicativos em execução.

     Se essa caixa de seleção estiver desmarcada, os aplicativos em execução não serão considerados ao gerar regras de permissão.

     A caixa de seleção é selecionada por padrão.

     Esta caixa não pode ser desmarcada se nenhuma das pastas estiver selecionada na tabela **Criar regras de permissão para aplicativos das pastas**.
   - **Criar regras de permissão para aplicativos das pastas**.

     Você pode usar a tabela para selecionar ou especificar pastas para a tarefa e os tipos de arquivos executáveis a serem considerados ao criar as regras de Controle de inicialização de aplicativos. A tarefa gerará regras de permissão para os arquivos dos tipos selecionados que estão localizados nas pastas especificadas.
3. Clique em **OK**.

As configurações especificadas são salvas.

Ações a serem executadas durante a geração automática de regras

► *Para configurar as ações que o Kaspersky Embedded Systems Security deverá executar enquanto a*

tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos estiver sendo executada:

1. Abra a janela **Configurações de tarefa** (consulte a seção "**Abertura das definições da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos**" na página 322) da tarefa do **Gerador de Regras de Controle de Inicialização de Aplicativos**.
2. Abra a guia **Opções**.
3. Na seção **Ao gerar regras de permissão**, defina as seguintes configurações:
   - **Usar certificado digital**

Se essa opção estiver selecionada, a presença de um certificado digital será especificada como critério para acionamento de regras nas configurações das regras de permissão geradas recentemente para o Controle de Inicialização de Aplicativos. O aplicativo permitirá agora a inicialização de programas iniciados usando arquivos com um certificado digital. Recomendamos essa opção se você quiser permitir a inicialização de qualquer aplicativo que seja confiável no sistema operacional.

Esta opção é selecionada por padrão.

- **Usar o assunto e a miniatura de certificado digital**

  A caixa de seleção ativa ou desativa o uso do requerente e da impressão digital do certificado digital do arquivo como critério para acionamento de regras de permissão no Controle de inicialização de aplicativos. A seleção desta caixa permite a especificação de condições de verificação mais rigorosas para o certificado digital.

  Se essa caixa estiver selecionada, os valores de requerente e impressão digital do certificado digital dos arquivos para os quais as regras serão geradas serão estabelecidos como um critério para acionamento das regras de permissão no Controle de inicialização de aplicativos. O Kaspersky Embedded Systems Security permitirá que os aplicativos que sejam iniciados usando arquivos com uma impressão digital e um certificado digital especificados.

  A seleção dessa caixa restringe fortemente o acionamento de regras de permissão com base em um certificado digital, pois a impressão digital é um identificador único de um certificado digital e não pode ser forjada.

  Se esta caixa estiver desmarcada, a existência de qualquer certificado digital confiável no sistema operacional é estabelecida como um critério para acionamento de regras de permissão de Controle de inicialização de aplicativos.

  A caixa de seleção estará ativa se a opção **Usar certificado digital** estiver selecionada.

  A caixa de seleção é selecionada por padrão.

- **Se o certificado estiver ausente, use**

  Essa é uma lista suspensa que permite que você selecione o critério para acionamento de uma regra de permissão de Controle de inicialização de aplicativos se o arquivo usado para gerar a regra não tiver um certificado digital.

  - **Hash SHA256**. O valor da soma de verificação do arquivo usado para gerar a regra é estabelecido como o critério para acionamento da regra de permissão de Controle de inicialização de aplicativos. O aplicativo permitirá a inicialização de programas iniciados usando arquivos com a soma de verificação especificada.
  - **caminho do arquivo**. O caminho do arquivo usado para gerar a regra é estabelecido como o critério para acionamento da regra de permissão de Controle de inicialização de aplicativos. O aplicativo agora permitirá a inicialização de programas usando arquivos localizados nas pastas especificadas na tabela **Criar regras de permissão para aplicativos das pastas** na seção

Configurações.

- **Usar hash SHA256**

Se esta opção estiver selecionada, o valor da soma de verificação do arquivo usado para gerar a regra será especificado como um critério para acionamento de regras nas configurações das regras de permissão geradas recentemente para o Controle de inicialização de aplicativos. O aplicativo permitirá a inicialização de programas iniciados usando arquivos com a soma de verificação especificada.

Recomendamos essa opção para casos em que as regras geradas devem alcançar o nível de segurança mais alto: a soma de verificação do SHA256 pode ser usada como um ID único de arquivo. O uso da soma de verificação do SHA256 como critério para acionamento de regras restringe o escopo de uso das regras para um arquivo.

Esta opção é desmarcada por padrão.

- **Gerar regras para usuário ou grupo de usuários**.

  Esse é um campo que exibe um usuário ou grupo de usuários. O aplicativo controlará qualquer aplicativo executado pelo usuário ou grupo de usuários especificado.

  A seleção padrão é **Todos**.

1. Clique em **OK**.

As configurações especificadas são salvas.

Ações a serem executadas após a conclusão da geração automática de regras

► *Para configurar as ações a serem executadas pelo Kaspersky Embedded Systems Security após a execução da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos:*

1. Abra a janela **Configurações de tarefa** (consulte a seção "**Abertura das definições da tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos**" na página 322) da tarefa do **Gerador de Regras de Controle de Inicialização de Aplicativos**.
2. Abra a guia **Opções**.
3. Na seção **Após a conclusão da tarefa**, configure as seguintes configurações:
   - **Adicionar regras de permissão à lista de regras de Controle de Inicialização de Aplicativos**.

     A caixa de seleção ativa ou desativa a adição de regras de permissão geradas recentemente à lista de regras de Controle Inicialização de Aplicativos. A lista de regras de Controle de inicialização de aplicativos é exibida quando você clica no link **Regras de Controle de Inicialização de Aplicativos** no painel de detalhes do nó Controle de inicialização de aplicativos.

     Se esta caixa estiver selecionada, o Kaspersky Embedded Systems Security adicionará as regras que foram geradas pela tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos à lista de regras de Controle de inicialização de aplicativos com base no princípio selecionado para adição de regras.

     Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não adicionará as regras de permissão geradas recentemente à lista de regras de Controle de inicialização de aplicativos. As regras geradas são exportadas somente para um arquivo.

     A caixa de seleção é selecionada por padrão.

   - **Princípio da adição**.

Essa lista suspensa é usada para especificar o método utilizado para a adição de regras de permissão geradas recentemente à lista de regras de Controle de Inicialização de Aplicativos.

- **Adicionar às regras existentes**. As regras são adicionadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.
- **Substituir as regras existentes**. As regras substituem as regras existentes na lista.
- **Mesclar com as regras existentes**. As regras são adicionadas à lista de regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.

Por padrão, o método **Mesclar com as regras existentes** é selecionado.

- **Exportar regras de permissão para o arquivo**.
- **Adicionar informações do computador ao nome do arquivo**.

  A caixa de seleção ativa ou desativa a adição de informações sobre o computador protegido ao nome do arquivo para o qual as regras de permissão serão exportadas.

  Se esta caixa estiver selecionada, o aplicativo adicionará o nome de computador protegido e a data e hora de criação de arquivos ao nome do arquivo de exportação.

  Se a caixa estiver desmarcada, o aplicativo não adicionará informações sobre o computador protegido ao nome do arquivo de exportação.

  A caixa de seleção é selecionada por padrão.

4. Clique em **OK**.

As configurações especificadas são salvas.

Controle de Dispositivos

Esta seção contém informações sobre a tarefa Controle de dispositivos, bem como instruções para definir as configurações de tarefa.

Neste capítulo

Sobre a tarefa Controle de Dispositivos 339
Sobre as regras de Controle de dispositivos 340
Sobre o preenchimento da lista de regras de Controle de dispositivos 342
Sobre a tarefa do Gerador de Regras de Controle de Dispositivos 344
Cenários de geração de regras de Controle de Dispositivos 344
Configurações padrão de tarefa Controle de dispositivos 345
Gerenciamento do Controle de Dispositivos por meio do Plug-in de Administração 346
Gerenciamento do Controle de Dispositivos por meio do Console do Aplicativo 357

Sobre a tarefa Controle de Dispositivos

O Kaspersky Embedded Systems Security controla o registro e uso de dispositivos de armazenamento em massa e unidades de CD/DVD para proteger o computador contra ameaças de segurança, que podem ocorrer no processo da troca de arquivos com pendrives ou outros tipos de dispositivo externo conectado via USB. O dispositivo de armazenamento em massa é um dispositivo externo que pode ser conectado a um computador para copiar ou armazenar arquivos.

O Kaspersky Embedded Systems Security controla as seguintes conexões de dispositivos externos USB:

- Pendrives conectados por USB
- Unidades de CD/DVD-ROM
- Unidades de disquete conectadas por USB
- Dispositivos móveis MTP conectados por USB

O Kaspersky Embedded Systems Security informará sobre todos os dispositivos conectados via USB com o evento correspondente nos logs de tarefa e de evento. Os detalhes do evento incluem o tipo de dispositivo e o caminho de conexão. Quando a tarefa Controle de Dispositivos for iniciada, o Kaspersky Embedded Systems Security verificará e listará todos os dispositivos conectados via USB. Você pode configurar as notificações na seção de configurações de notificação do Kaspersky Security Center.

A tarefa Controle de Dispositivos monitora todas as tentativas de conexão de dispositivos externos a um computador protegido via USB e bloqueia a conexão se não houver regras de permissão para tais dispositivos. Após a conexão ser bloqueada, o dispositivo não fica disponível.

O aplicativo atribui um dos seguintes status a cada dispositivo de armazenamento em massa conectado:

- *Confiável*. O dispositivo para o qual você deseja permitir a troca de arquivos. Após a geração da lista de regras, o valor do *Caminho da instância do dispositivo* será incluído no escopo de uso de pelo menos uma regra.
- *Não confiável*. Dispositivo para o qual você deseja restringir a troca de arquivos. O caminho da instância do dispositivo não está incluído em nenhum escopo de uso das regras de permissão.

Você pode criar regras de permissão para dispositivos externos para permitir a troca de dados usando a tarefa do Gerador de Regras de Controle de Dispositivos. Você também pode expandir o escopo de uso das regras já especificadas. Você não pode criar regras de permissão manualmente.

O Kaspersky Embedded Systems Security identifica os dispositivos de armazenamento em massa registrados pelo sistema usando o valor de Caminho da instância do dispositivo. O Caminho da instância do dispositivo é um recurso padrão especificado unicamente para cada dispositivo externo. O valor do Caminho da instância do dispositivo é especificado para cada dispositivo externo nas suas propriedades Windows e é automaticamente determinado pelo Kaspersky Embedded Systems Security durante a geração de regras.

A tarefa Controle de Dispositivos pode operar em dois modos:

- **Ativa**. O Kaspersky Embedded Systems Security aplica regras para controlar a conexão de pendrives e outros dispositivos externos e permite ou bloqueia o uso de todos os dispositivos de acordo com o princípio de Negação Padrão e as regras de permissão especificadas. O uso de dispositivos externos confiáveis é permitido. Por padrão, o uso de dispositivos externos não confiáveis é bloqueado.

  Se um dispositivo externo que você considera não confiável for conectado a um computador protegido antes que a tarefa Controle de Dispositivos seja executada no modo **Ativa**, o dispositivo não será bloqueado pelo aplicativo. Recomendamos que desconecte o dispositivo não confiável manualmente ou reinicie o computador. Caso contrário, o princípio de Negação Padrão não será aplicado ao dispositivo.

- **Somente Estatísticas**. O Kaspersky Embedded Systems Security não controla a conexão de pendrives e outros dispositivos externos, só registra em log as informações sobre a conexão e o registro de dispositivos externos em um computador protegido e sobre as regras de permissão de Controle de Dispositivos acionadas pelos dispositivos conectados. O uso de todos os dispositivos externos é permitido. Este modo está definido por padrão.

  Você pode aplicar este modo da geração de regras com base nas informações de bloqueio registradas em log durante a execução da tarefa (consulte a seção "Preenchimento da lista de regras com base em eventos da tarefa Controle de dispositivos" na página 360).

Sobre as regras de Controle de dispositivos

As regras são geradas exclusivamente para cada dispositivo que está conectado atualmente ou foi alguma vez conectado a um computador protegido se as informações sobre este dispositivo estiverem armazenadas no Registro do sistema.

Para gerar regras de permissão para o controle de dispositivos, você pode fazer o seguinte:

- Aplicar a tarefa do Gerador de Regras de Controle de Dispositivos (consulte a seção "Sobre a tarefa do Gerador de Regras de Controle de Dispositivos" na página 344).
- Executar a tarefa Controle de Dispositivos no modo Somente estatísticas (consulte a seção

"Preenchimento da lista de regras com base em eventos de tarefa Controle de Dispositivos" na página 360).

- Aplicar informações de sistema sobre dispositivos previamente conectados (consulte a seção "Adição de uma regra de permissão para um ou mais dispositivos externos" na página 361).
- Expandir o escopo de uso das regras já especificadas (consulte a seção "Expandindo o escopo de uso das regras de Controle de dispositivos" na página 363).

O número máximo de regras de Controle de Dispositivos suportado pelo Kaspersky Embedded Systems Security é 3072.

As regras de Controle de dispositivos estão descritas abaixo.

Tipo de regra

O tipo de regra é sempre *permissão*. Por padrão, a tarefa Controle de Dispositivos bloqueia todos os pendrives e outras conexões de dispositivos externos se esses dispositivos não estiverem incluídos em algum escopo de uso da regra de permissão.

Critério para acionamento e escopo de uso da regra

As regras de Controle de Dispositivos identificam pendrives e outros dispositivos externos com base no *Caminho da instância do dispositivo*. O caminho da instância do dispositivo é um critério único atribuído a um dispositivo pelo sistema quando o dispositivo for conectado e registrado como um Dispositivo de armazenamento em massa ou uma unidade de CD/DVD (por exemplo, IDE ou SCSI).

O Kaspersky Embedded Systems Security controla a conexão das unidades de CD/DVD independentemente do barramento utilizado para a conexão. Ao conectar esse dispositivo via USB, o sistema operacional registra dois valores de caminho para a instância do dispositivo: para o dispositivo de armazenamento em massa e para a unidade de CD/DVD (por exemplo, IDE ou SCSI). Para conectar esses dispositivos corretamente, as regras de permissão para cada valor de caminho para instância devem ser definidas.

O Kaspersky Embedded Systems Security define automaticamente o caminho da instância do dispositivo e analisa o valor obtido nos seguintes elementos:

- Fabricante do dispositivo (VID)
- Tipo de controlador do dispositivo (PID)
- Número de série do dispositivo

Você não pode definir manualmente o caminho da instância do dispositivo. Os critérios para acionamento da regra de permissão definem o escopo de uso da regra. Por padrão, o escopo de uso das regras criadas recentemente inclui um dispositivo inicial, com base nas propriedades que o Kaspersky Embedded Systems Security utilizou para gerar a regra. Você pode configurar os valores nas configurações da regra criada usando uma máscara para expandir o escopo de uso da regra (consulte a seção "Expansão do escopo de uso das regras de Controle de dispositivos" na página 363).

Valores iniciais de dispositivo

Propriedades de dispositivo que o Kaspersky Embedded Systems Security usou para permitir a geração de regras e que são exibidas no Gerente de Dispositivos do Windows para cada dispositivo conectado.

Os valores de dispositivo iniciais contêm as seguintes informações:

- **Caminho da instância do dispositivo**. Com base nessa propriedade, o Kaspersky Embedded Systems Security define os critérios para acionamento de regras e preenche os seguintes campos: **Fabricante (VID)**, **Tipo de controlador (PID)**, **Número de série** na seção **Escopo de uso da regra** da janela **Propriedades da regra**.
- **Nome amigável**. O nome claro de dispositivo que é estabelecido nas propriedades de dispositivo por seu fabricante.

O Kaspersky Embedded Systems Security define automaticamente valores de dispositivo iniciais quando a regra é gerada. Mais tarde você pode usar estes valores para reconhecer o dispositivo que foi usado como base para a geração de regra. Os valores de dispositivo iniciais não estão disponíveis para edição.

Descrição

Você pode adicionar informações adicionais para cada regra de Controle de dispositivos criada no campo **Descrição**, por exemplo, você pode anotar o nome do pendrive conectado ou definir seu proprietário. A descrição é exibida em um gráfico correspondente na janela **Regras de Controle de Dispositivos**.

A descrição e os valores iniciais de dispositivo não são permitidos para o acionamento de regra e são prescritos somente para simplificar uma identificação de dispositivo pelo usuário.

Sobre o preenchimento da lista de regras de Controle de dispositivos

Você pode importar regras de permissão de controle de dispositivos dos arquivos XML que foram automaticamente gerados durante a execução das tarefas de Controle de dispositivos ou Gerador de Regras de Controle de Dispositivos.

Por padrão, o Kaspersky Embedded Systems Security restringe conexões de qualquer pendrive e outros dispositivos externos se eles não estiverem incluídos no escopo de uso das regras de controle de dispositivos especificadas.

Tabela 49. Destinos e cenários para a geração de lista de regras de controle de dispositivos

Cenário de geração de regra	Destino
A tarefa do Gerador de Regras de Controle de Dispositivos	• Adiciona regras de permissão para dispositivos confiáveis conectados antes da primeira inicialização da tarefa Controle de dispositivos. • Gera a lista de regras para dispositivos confiáveis na rede de computadores protegida.
Geração de regras baseada em dados do sistema	Adiciona regras de permissão para um ou vários dispositivos conectados recentemente.
A tarefa Controle de Dispositivos no modo **Somente Estatísticas**	Gerar regras de permissão para um grande número de dispositivos confiáveis.

O uso da tarefa do Gerador de Regras de Controle de Dispositivos

O arquivo XML, gerado após a conclusão da tarefa do Gerador de Regras de Controle de Dispositivos, contém

regras de permissão para aqueles pendrives e outros dispositivos externos cujos dados foram armazenados em um registro do sistema.

Durante a execução da tarefa, o Kaspersky Embedded Systems Security recebe dados do sistema sobre todos os dispositivos de armazenamento em massa que já foram conectados ou estão atualmente conectados a um computador protegido e gera a lista de regras de permissão com base nos dados do sistema para os dispositivos detectados. Após a conclusão da tarefa o aplicativo cria o arquivo XML na pasta que está situada pelo caminho especificado nas configurações de tarefa. Você pode configurar a importação automática das regras geradas na lista de regras para a tarefa Controle de dispositivos.

Este cenário é recomendado para gerar a lista de regras de permissão antes do primeiro início da tarefa Controle de dispositivos, para que as regras de permissão geradas abranjam todos os dispositivos externos confiáveis que são usados em um computador protegido.

Uso de dados do sistema sobre todos os dispositivos conectados

Durante a execução da tarefa, o Kaspersky Embedded Systems Security recebe dados do sistema sobre todos os dispositivos externos que foram alguma vez conectados ou que estão atualmente conectados a um computador protegido e exibe os dispositivos detectados na lista da janela **Gerar regras com base nas informações do sistema**.

Para cada dispositivo detectado o Kaspersky Embedded Systems Security analisa os valores do fabricante (VID), tipo de controlador (PID), nome amigável, número de série e caminho da instância do dispositivo. Você pode gerar regras de permissão para qualquer dispositivo de armazenamento em massa cujos dados foram armazenados no sistema e adicionar diretamente regras criadas recentemente à lista das regras de controle de dispositivos.

Este cenário é recomendado para renovar uma lista de regras já especificada quando é necessário confiar em uma pequena quantidade de novos dispositivos de armazenamento em massa.

O Kaspersky Embedded Systems Security não adquire o acesso a dados do sistema sobre dispositivos móveis conectados via MTP. Você não pode gerar regras de permissão para dispositivos móveis conectados por MTP.

Uso da tarefa Controle de Dispositivos no modo Somente estatísticas

O arquivo XML recebido após a conclusão da tarefa Controle de Dispositivos no modo **Somente Estatísticas** é gerado com base no log de tarefas.

Durante a execução da tarefa, o Kaspersky Embedded Systems Security registra em log informações sobre todas as conexões de pendrives e outros dispositivos de armazenamento em massa em um computador protegido. Você pode gerar regras de permissão baseadas em eventos de tarefa e exportá-las a um arquivo XML. Antes de iniciar a tarefa no modo **Somente Estatísticas**, recomenda-se configurar o período de execução da tarefa para que durante este tempo especificado sejam realizadas todas as conexões possíveis de dispositivos externos a um computador protegido.

Este cenário é recomendado para renovar uma lista de regras já gerada se isso for necessário para permitir uma quantidade grande de novos dispositivos externos.

Se a geração de lista de regra segundo este cenário for executada em uma máquina modelo, você pode aplicar uma lista de regras de permissão gerada ao configurar a tarefa Controle de dispositivos através do Kaspersky Security Center. Dessa maneira será possível permitir o uso de dispositivos externos que estejam conectados a uma máquina modelo em todos os computadores incluídos em uma rede protegida.

Sobre a tarefa do Gerador de Regras de Controle de Dispositivos

A tarefa do Gerador de Regras de Controle de Dispositivos pode criar automaticamente uma lista de regras de permissão para pendrives e outros dispositivos de armazenamento em massa conectados com base em dados do sistema sobre todos os dispositivos externos que já foram alguma vez conectados a um computador protegido.

O Kaspersky Embedded Systems Security não adquire o acesso a dados do sistema sobre dispositivos móveis conectados via MTP. Você não pode gerar regras de permissão para dispositivos móveis conectados por MTP.

Depois da conclusão da tarefa, o Kaspersky Embedded Systems Security cria um arquivo de configuração XML que contém a lista de regras de permissão para todos os dispositivos externos detectados ou adiciona diretamente regras geradas na tarefa Controle de dispositivos dependendo das configurações do Gerador de Regras de Controle de Dispositivos. O aplicativo permitirá posteriormente dispositivos para os quais as regras de permissão foram geradas automaticamente.

As regras geradas e adicionadas nas regras da tarefa são exibidas na janela **Regras de Controle de Dispositivos**.

Cenários de geração de regras de Controle de Dispositivos

Você pode gerar regras (consulte a seção "Geração de regras de Controle de dispositivos para todos os computadores por meio do Kaspersky Security Center" na página 349) com base em dados do Windows sobre todos os dispositivos de armazenamento em massa que já foram conectados alguma vez ou que estão conectados atualmente por três cenários:

- Usando a tarefa de grupo do Gerador de Regras de Controle de Dispositivos. Use este cenário durante o processo de geração de regras para considerar todos os dispositivos de armazenamento em massa que já foram conectados alguma vez e que estão registrados pelos sistemas em todos os computadores de rede.
- Uso da opção **Gerar regras com base nos dados do sistema**. Use este cenário durante o processo de geração de regras para considerar todos os dispositivos de armazenamento em massa que já foram conectados alguma vez e que estão registrados pelo sistema do computador com o Console de Administração do Kaspersky Security Center instalado.
- Usando **Gerar regras com base nos dispositivos conectados** na janela de **Regras de Controle de Dispositivos** e configurações da tarefa do Gerador de Regras de Controle de Dispositivos. Use este método se quiser considerar apenas os dados sobre dispositivos atualmente conectados ao computador protegido ao gerar as regras de permissão.

O Kaspersky Embedded Systems Security não adquire o acesso a dados do sistema sobre dispositivos móveis conectados via MTP. Você não pode gerar regras de permissão para dispositivos móveis confiáveis conectados via MTP usando cenários para o preenchimento da lista de regras na base de dados do sistema sobre todos os dispositivos conectados.

Configurações padrão de tarefa Controle de dispositivos

Por padrão, a tarefa Controle de dispositivos possui as configurações descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Tabela 50. Configurações padrão da tarefa Controle de dispositivos

Configuração	Valor padrão	Descrição
Modo da tarefa	**Somente Estatísticas**	A tarefa registra informações sobre os dispositivos externos que foram bloqueados ou permitidos de acordo com as regras especificadas. Os dispositivos externos não estão realmente bloqueados. Você pode selecionar o modo **Ativa** para a proteção do computador para de fato bloquear o uso de dispositivos externos.
Permitir o uso de todos os dispositivos de armazenamento em massa quando a tarefa Controle de dispositivos não estiver em execução	Não aplicado	O Kaspersky Embedded Systems Security bloqueia o uso de dispositivos externos, independente do estado da tarefa Controle de dispositivos. Isso fornece um nível máximo de proteção contra o surgimento de ameaças à segurança do computador quando arquivos são trocados com dispositivos externos. Você pode ajustar a configuração para que o Kaspersky Embedded Systems Security permita o uso de todos os dispositivos externos quando a tarefa Controle de dispositivos não for executada.
Programação de inicialização da tarefa	A primeira execução não está programada.	A tarefa Controle de dispositivos não inicia automaticamente no momento da inicialização do Kaspersky Embedded Systems Security. Você pode configurar a programação de inicialização da tarefa.

Tabela 51. Configurações padrão da tarefa do Gerador de Regras de Controle de Dispositivos

Configuração	Valor padrão	Descrição
Modo da tarefa	**Considere os dados do sistema a respeito de todos os armazenamentos em massa que foram conectados**	Modo operacional da tarefa. Você pode selecionar o modo da tarefa **Considere somente os armazenamentos em massa conectados atualmente**.
Ações após a conclusão da tarefa	As regras de permissão são adicionadas à lista das regras de Controle de dispositivos; as novas regras são agregadas às existentes; as regras duplicadas são removidas.	Você pode adicionar regras às regras existentes sem agregá-las e sem apagar as regras duplicadas, ou substituir as regras existentes por regras novas de permissão ou configurar a exportação de regras de permissão para um arquivo.

Configuração	Valor padrão	Descrição
Programação de inicialização da tarefa	A primeira execução não está programada.	A tarefa do Gerador de Regras de Controle de Dispositivos não inicia automaticamente no momento da inicialização do Kaspersky Embedded Systems Security. É possível iniciar a tarefa manualmente ou configurar um início programado.

Gerenciamento do Controle de Dispositivos por meio do Plug-in de Administração

Nesta seção, aprenda como navegar pela interface do Plug-in de Administração e gerenciar conexões de qualquer dispositivo de armazenamento em massa para todos os computadores na rede gerando listas de regras por meio do Kaspersky Security Center para os grupos de computadores.

Nesta seção

Navegação 346
Configuração da tarefa Controle de Dispositivos 348
Geração de regras de Controle de dispositivos para todos os computadores por meio do Kaspersky Security Center 349
Configurando a tarefa do Gerador de Regras de Controle de Dispositivos 351
Configuração de regras de Controle de Dispositivos por meio do Kaspersky Security Center 351

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface.

Nesta seção

Abertura das configurações de política para a tarefa Controle de Dispositivos 346
Abertura da lista de regras de Controle de Dispositivos 347
Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Dispositivos 347

Abertura das configurações de política para a tarefa Controle de Dispositivos

► *Para abrir a configuração da tarefa Controle de Dispositivos por meio da política do Kaspersky Security Center:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security

Center.

2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Controle de atividade local**.
6. Clique no botão **Configurações**, na subseção **Controle de dispositivos**.

   A janela **Controle de Dispositivos** será aberta.
7. Configure a política conforme necessário.

Abertura da lista de regras de Controle de Dispositivos

► *Para abrir a lista de regras de Controle de Dispositivos por meio do Kaspersky Security Center:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Controle de atividade local**.
6. Clique no botão **Configurações**, na subseção **Controle de dispositivos**.

   A janela **Controle de Dispositivos** será aberta.
7. Na guia **Geral**, clique no botão **Lista de regras**.

   A janela **Regras de Controle de dispositivos** é exibida.
8. Configure a política conforme necessário.

Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Dispositivos

► *Para inicializar a criação da tarefa do Gerador de Regras de Controle de Dispositivos:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Tarefas**.
4. Clique no botão **Criar uma tarefa**.

   A janela **Assistente de Nova Tarefa** será aberta.
5. Selecione a tarefa **Gerador de Regras de Controle de Dispositivos**.
6. Clique em **Avançar**.

A janela **Configurações** é exibida.

► *Para configurar a tarefa do Gerador de Regras de Controle de Dispositivos existente:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Tarefas**.
4. Clique duas vezes no nome da tarefa na lista de tarefas no Kaspersky Security Center.

   A janela **Propriedades: Gerador de Regras de Controle de Dispositivos** será aberta.

Consulte a seção Configuração da tarefa do Gerador de Regras de Controle de Dispositivos para detalhes sobre a configuração da tarefa.

Configuração da tarefa Controle de Dispositivos

► *Para definir as configurações da tarefa Controle de dispositivos:*

1. Abra a janela de **Controle de Dispositivos** (consulte a seção "Abertura das configurações de política para a tarefa Controle de Dispositivos" na página 346).
2. Na guia **Geral**, defina as seguintes configurações de tarefa:
   - Na seção **Modo da tarefa**, selecione um dos modos de tarefa:
     - **Ativa**.

       O Kaspersky Embedded Systems Security aplica regras para controlar a conexão de pendrives e outros dispositivos externos e permite ou bloqueia o uso de todos os dispositivos de acordo com o princípio de Negação Padrão e as regras de permissão especificadas. O uso de dispositivos externos confiáveis é permitido. Por padrão, o uso de dispositivos externos não confiáveis é bloqueado.

       Se um dispositivo externo que você considera não confiável for conectado a um computador protegido antes que a tarefa Controle de Dispositivos seja executada no modo Ativa, o dispositivo não será bloqueado pelo aplicativo. Recomendamos que desconecte o dispositivo não confiável manualmente ou reinicie o computador. Caso contrário, o princípio de Negação Padrão não será aplicado ao dispositivo.

     - **Somente Estatísticas**.

       O Kaspersky Embedded Systems Security não controla a conexão de pendrives e outros dispositivos externos, só registra em log as informações sobre a conexão e o registro de dispositivos externos em um computador protegido e sobre as regras de permissão de Controle de Dispositivos acionadas pelos dispositivos conectados. O uso de todos os dispositivos externos é permitido. Este modo está definido por padrão.

   - Selecione ou desmarque a caixa **Permitir o uso de todos os dispositivos de armazenamento em massa quando a tarefa Controle de Dispositivos não estiver em execução**.

     A caixa de seleção permite ou bloqueia o uso de dispositivos de armazenamento em massa quando a tarefa Controle de Dispositivos não estiver sendo executada.

Se a caixa de seleção for marcada e a tarefa Controle de Dispositivos não estiver sendo executada, o Kaspersky Embedded Systems Security permitirá o uso de qualquer dispositivo de armazenamento em massa em um computador protegido.

Se a caixa de seleção estiver desmarcada, o aplicativo bloqueará o uso de dispositivos de armazenamento em massa não confiáveis em um computador protegido nos seguintes casos: quando a tarefa Controle de Dispositivos não estiver sendo executada ou se o Kaspersky Security Service tiver sido desativado. Esta opção é recomendada para maximizar o nível da proteção contra ameaças de segurança do computador que surgem após a troca de arquivos com dispositivos externos.

Esta caixa é desmarcada por padrão.

3. Clique no botão **Lista de regras** para editar a lista de regras de Controle de Dispositivos (consulte a seção "Configuração de regras de Controle de Dispositivos por meio do Kaspersky Security Center" na página 351).
4. Se necessário, configure a programação de inicialização da tarefa na guia **Gerenciamento da tarefa**.
5. Clique em **OK**.

O Kaspersky Embedded Systems Security aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora quando as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no Log de tarefas.

Geração de regras de Controle de dispositivos para todos os computadores por meio do Kaspersky Security Center

Você pode criar listas de regras de Controle de dispositivos usando tarefas do Kaspersky Security Center para todos os computadores e os grupos de computadores na rede corporativa ao mesmo tempo.

Você pode criar listas de regras de Controle de dispositivos no lado do Kaspersky Security Center das seguintes maneiras:

- Usando a tarefa de grupo do Gerador de Regras de Controle de Dispositivos.

  Segundo este cenário, a tarefa de grupo gera listas de regras com base nos dados de sistema de cada computador sobre todos os dispositivos de armazenamento em massa que já foram conectados a computadores protegidos. A tarefa também permite todos os dispositivos de armazenamento em massa conectados no momento da execução da tarefa. Após a conclusão de tarefa de grupo o Kaspersky Embedded Systems Security gera listas de regras de permissão para todos os dispositivos de armazenamento em massa registrados na rede e salva estas listas em um arquivo XML em uma pasta especificada. Em seguida, você pode importar manualmente regras geradas nas configurações da tarefa Controle de dispositivos. Diferentemente de uma tarefa em um computador local, a política não permite configurar a adição automática das regras criadas à lista de regras de Controle de Dispositivos quando a tarefa de grupo do Gerador de Regras de Controle de Dispositivos é concluída.

  Este cenário é recomendado para gerar listas de regras de permissão antes do primeiro início da tarefa Controle de dispositivos no modo da aplicação **Ativa** de regras.

Antes de usar a política de Controle de Dispositivos na rede, certifique-se de que todos os computadores protegidos tenham acesso a uma pasta de rede compartilhada. Se a política da organização não permitir o uso de uma pasta compartilhada na rede, recomenda-se iniciar a tarefa de Gerador de Regras de Controle de Dispositivos para regras de controle do computador no grupo de computadores de teste ou em uma máquina modelo.

- Com base em um relatório sobre eventos de tarefa gerado no Kaspersky Security Center para a tarefa Controle de dispositivos no modo **Somente Estatísticas**.

  Segundo este cenário, o Kaspersky Embedded Systems Security não restringe conexões de dispositivos de armazenamento em massa, mas registra informações sobre todas as conexões de dispositivos e registros de dispositivos de armazenamento em massa em todos os computadores da rede durante a execução da tarefa Controle de dispositivos no modo **Somente Estatísticas**. As informações registradas em log podem ser encontradas na guia **Eventos** da área de trabalho do nó **Servidor de Administração** do Kaspersky Security Center. O Kaspersky Security Center gerará uma lista unificada de eventos de restrição e permissão de dispositivos de armazenamento em massa com base no log de tarefas.

  Você deve configurar o período de execução da tarefa de forma que todas as conexões de dispositivos de armazenamento em massa sejam realizadas durante o período estabelecido. Em seguida, conforme as regras são adicionadas à tarefa Controle de dispositivos, você pode importar dados sobre as conexões de dispositivos do arquivo de relatório de evento salvo do Kaspersky Security Center (no formato TXT) e gerar regras de permissão de Controle de dispositivos para tais dispositivos com base nestes dados. O tipo dos eventos, no qual um log importado é baseado, não influencia no tipo de regras gerado; somente regras de permissão são geradas.

  Este cenário é recomendado para adicionar regras de permissão para um grande número de novos dispositivos de armazenamento em massa, bem como gerar regras para dispositivos móveis confiáveis conectados por MTP.

- Com base nos dados do sistema sobre dispositivos de armazenamento em massa conectados (usando a opção **Gerar regras com base nos dados do sistema** nas configurações da tarefa Controle de Dispositivos).

  De acordo com este cenário, o Kaspersky Embedded Systems Security gerará regras de permissão para dispositivos de armazenamento em massa que já foram conectados alguma vez ou estão atualmente conectados a um computador com o Kaspersky Security Center instalado.

  Este cenário é recomendado para gerar regras para um pequeno número de novos dispositivos de armazenamento em massa no qual você deseja confiar em todos os computadores na rede.

- Com base nos dados sobre os dispositivos atualmente conectados (usando **Gerar regras com base nos dispositivos conectados**).

  Neste cenário, o Kaspersky Embedded Systems Security gera regras de permissão apenas para dispositivos conectados. É possível selecionar um ou mais dispositivos para os quais você deseja gerar regras de permissão.

  O Kaspersky Embedded Systems Security não adquire o acesso a dados do sistema sobre dispositivos móveis conectados via MTP. Você não pode gerar regras de permissão para dispositivos móveis confiáveis conectados via MTP usando cenários para o preenchimento da lista de regras na base de dados do sistema sobre todos os dispositivos conectados.

Configurando a tarefa do Gerador de Regras de Controle de Dispositivos

► *Para configurar a tarefa do Gerador de Regras de Controle de Dispositivos, faça o seguinte:*

1. Abra a janela **Propriedades: Gerador de Regras de Controle de Dispositivos** (consulte a seção "**Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Dispositivos**" na página 347).
2. Na seção **Notificações**, defina as configurações de notificação do evento da tarefa.

   Para obter informações detalhadas sobre a definição das configurações nesta seção, consulte a *Ajuda do Kaspersky Security Center*.

3. Na seção **Configurações**, é possível definir as seguintes configurações:
   - Selecione o modo de operação: considere dados de sistema sobre todos os armazenamentos em massa que já estiveram conectados alguma vez ou considere somente os armazenamentos em massa conectados atualmente.
   - Defina as configurações para arquivos de configuração com listas de regras de permissão que o Kaspersky Embedded Systems Security cria após a conclusão da tarefa.
4. Configurar o agendamento de tarefa na seção **Programação** (você pode configurar um agendamento para todos os tipos de tarefa, exceto Reversão da Atualização do Banco de Dados).
5. Na seção **Conta**, especifique a conta cujos direitos serão usados para a execução de tarefa.
6. Se necessário, especifique os objetos a serem excluídos do escopo da tarefa na seção **Exclusões do escopo da tarefa**.

   Para obter informações detalhadas sobre a definição das configurações nestas seções, consulte a *Ajuda do Kaspersky Security Center*.

7. Na janela **Propriedades: <Nome da tarefa>**, clique em **OK**.

   As configurações de tarefas de grupo definidas recentemente são salvas.

Configuração de regras de Controle de Dispositivos por meio do Kaspersky Security Center

Aprenda como gerar uma lista de regras com base em vários critérios ou crie regras de permissão ou negação manualmente usando a tarefa Controle de Dispositivos.

Nesta seção

Criação de regras de permissão com base nos dados de sistema em uma política do Kaspersky Security Center 352

Geração de regras para dispositivos conectados 352

Importação de regras a partir do relatório do Kaspersky Security Center sobre dispositivos bloqueados 353

Criação de regras usando a tarefa do Gerador de Regras de Controle de Dispositivos 354

Adicionar as regras geradas à lista de regras de Controle de Dispositivos 356

Criação de regras de permissão com base nos dados de sistema em uma política do Kaspersky Security Center

► *Para especificar regras de permissão usando a opção **Gerar regras com base nos dados do sistema** na tarefa Controle de dispositivos:*

1. Se necessário, conecte um novo dispositivo de armazenamento em massa que você deseja definir como confiável a um computador com o Console de Administração do Kaspersky Security Center instalado.
2. Abra a janela de **Regras de Controle de dispositivos** (consulte a seção "Abertura da lista de regras de Controle de Dispositivos" na página 347).
3. Clique no botão **Adicionar** e, no menu de contexto exibido, selecione a opção **Gerar regras com base nos dados do sistema**.
4. Selecione o princípio para adicionar as regras de permissão à lista de regras de Controle de dispositivos criadas anteriormente:
   - Na lista de dispositivos na janela **Gerar regras com base nas informações do sistema**, selecione um dispositivos.
   - Clique em **Adicionar regras para os disp. selec**.
5. Clique no botão **Salvar**, na janela **Regras de Controle de dispositivos**.

A lista de regras na tarefa Controle de dispositivos será preenchida com novas regras geradas com base em dados do sistema do computador com o Console de Administração do Kaspersky Security Center instalado.

Geração de regras para dispositivos conectados

► *Para especificar regras de permissão usando a opção **Gerar regras com base nos dispositivos conectados** na tarefa Controle de dispositivos:*

1. Abra a janela de **Regras de Controle de dispositivos** (consulte a seção "**Abertura da lista de regras de Controle de Dispositivos**" na página 347).
2. Clique no botão **Adicionar** e, no menu de contexto, selecione **Gerar regras com base nos dispositivos conectados**.

   A janela **Gerar regras com base nas informações do sistema** é exibida.
3. Na lista de dispositivos detectados conectados ao computador protegido, selecione os dispositivos para os quais você deseja gerar as regras de permissão.

4. Clique no botão **Adicionar regras para os disp. selec**.
5. Clique no botão **Salvar**, na janela **Regras de Controle de dispositivos**.

A lista de regras na tarefa Controle de dispositivos será preenchida com novas regras geradas com base em dados do sistema do computador com o Console de Administração do Kaspersky Security Center instalado.

Importação de regras a partir do relatório do Kaspersky Security Center sobre dispositivos bloqueados

Você pode importar dados sobre conexões de dispositivos bloqueados a partir do relatório gerado no Kaspersky Security Center após a conclusão da tarefa Controle de dispositivos no modo **Somente Estatísticas** (consulte a seção "Configuração da tarefa Controle de Dispositivos" na página 348) e usar esses dados para gerar uma lista de regras de permissão de Controle de dispositivos na política que está sendo configurada.

Ao gerar o relatório sobre eventos que ocorrem durante a tarefa Controle de dispositivos, você poderá acompanhar os dispositivos cuja conexão é restringida.

► *Para especificar regras de permissão para a conexão de dispositivos para um grupo de computadores com base no relatório do Kaspersky Security Center sobre dispositivos bloqueados:*

1. Nas propriedades da política, na seção **Notificação de evento**, certifique-se de que:
   - Para o nível de importância **Eventos críticos**, o período para armazenamento do log de tarefas para o evento *Armazenamento em massa restrito* excede o tempo planejado de operação no modo **Somente Estatísticas** (o valor padrão é 30 dias).
   - Para o nível de importância **Aviso**, o período para armazenamento do log de tarefas para o evento *Somente estatísticas: armazenamento em massa não confiável detectado* excede o tempo planejado de operação da tarefa no modo **Somente Estatísticas** (o valor padrão é 30 dias).

   Quando o período especificado para armazenamento dos eventos for excedido, as informações sobre eventos registrados serão excluídas e não serão refletidas no relatório. Antes de executar a tarefa Controle de dispositivos no modo **Somente Estatísticas**, certifique-se de que o tempo de execução da tarefa não exceda o tempo de armazenamento configurado para os eventos especificados.

2. Inicie a tarefa Controle de Dispositivos no modo **Somente Estatísticas**. Na área de trabalho do nó **Servidor de Administração** no Kaspersky Security Center**,** selecione a guia **Eventos**. Clique no botão **Criar uma seleção** e crie uma seleção de eventos com base no critério *armazenamento em massa não confiável detectado* para visualizar os dispositivos cujas conexões serão restringidas pela tarefa Controle de Dispositivos. No painel de detalhes da seleção, clique no link **Exportar eventos para arquivo** para salvar o relatório de conexões restritas em um arquivo TXT.

   Antes de importar e aplicar o relatório gerado em uma política, certifique-se de que o relatório contenha somente dados sobre os dispositivos cuja conexão você deseja permitir.

3. Importar dados sobre conexões de dispositivos restritos na tarefa Controle de dispositivos:
   a. Abra a janela de **Regras de Controle de dispositivos** (consulte a seção "Abertura da lista de regras de Controle de Dispositivos" na página 347).
   b. Clique no botão **Adicionar** e, no menu de contexto do botão, selecione **Importar dados de**

dispositivos bloqueados do relatório do Kaspersky Security Center.

c. Selecione o princípio para adicionar regras da lista criada com base no relatório do Kaspersky Security Center à lista de regras de Controle de dispositivos previamente configuradas:

- **Adicionar às regras existentes** se você quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.
- **Substituir as regras existentes** se você quiser substituir as regras existentes pelas regras importadas.
- **Mesclar com as regras existentes** se você quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.

d. Na janela padrão do Microsoft Windows exibida, selecione o arquivo TXT ao qual os eventos do relatório sobre dispositivos restringidos foram exportados.

e. Clique no botão **Salvar**, na janela **Regras de Controle de dispositivos**.

4. Clique em **OK** na janela **Controle de Dispositivos**.

As regras criadas com base no relatório do Kaspersky Security Center sobre dispositivos restringidos são adicionadas à lista de regras de Controle de dispositivos.

Criação de regras usando a tarefa do Gerador de Regras de Controle de Dispositivos

► *Para especificar regras de permissão de controle de dispositivos para um grupo de computadores usando a tarefa do Gerador de Regras de Controle de Dispositivos:*

1. Abra a janela **Configurações** no **Assistente de nova tarefa**(consulte a seção "**Abertura do assistente e das propriedades da tarefa do Gerador de Regras de Controle de Dispositivos**" na página 347).
2. Defina as seguintes configurações:
   - Na seção **Modo**:
     - **Considere os dados do sistema a respeito de todos os armazenamentos em massa que foram conectados**.
     - **Considere somente os armazenamentos em massa conectados atualmente**.
   - Na seção **Após a conclusão da tarefa**:
     - **Adicionar regras de permissão à lista de regras de Controle de dispositivos**.

       A caixa de seleção ativa ou desativa a adição de regras de permissão geradas recentemente à lista de regras de Controle de dispositivos. A lista de regras de Controle de dispositivos é exibida ao clicar no link **Regras de Controle de Dispositivos** no painel de detalhes do nó **Controle de Dispositivos**.

       Se a caixa estiver selecionada, o Kaspersky Embedded Systems Security adicionará as regras que foram geradas pela tarefa do Gerador de regras de Controle de dispositivos à lista de regras de controle de dispositivos com base no princípio selecionado para adição de regras.

       Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não adicionará as regras de permissão geradas recentemente à lista de regras de Controle de dispositivos. As regras geradas são exportadas somente para um arquivo.

       A caixa de seleção é selecionada por padrão.

A caixa não pode ser selecionada se a caixa **Exportar regras de permissão para o arquivo** não tiver sido selecionada.

- **Princípio da adição**.

  Essa lista suspensa é usada para especificar o método utilizado para a adição de regras de permissão geradas recentemente à lista de regras de Controle de Inicialização de Aplicativos.

  - **Adicionar às regras existentes**. As regras são adicionadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.
  - **Substituir as regras existentes**. As regras substituem as regras existentes na lista.
  - **Mesclar com as regras existentes**. As regras são adicionadas à lista de regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.

  Por padrão, o método **Mesclar com as regras existentes** é selecionado.

- **Exportar regras de permissão para o arquivo**.

  A caixa ativa ou desativa a exportação de regras de permissão de Controle de Dispositivos a um arquivo.

  Se a caixa estiver selecionada, o Kaspersky Embedded Systems Security exportará as regras de permissão para o arquivo especificado no campo abaixo quando a tarefa do Gerador de Regras de Controle de Dispositivos for concluída.

  Se essa caixa estiver desmarcada, o aplicativo não exportará as regras de permissão geradas para um arquivo quando a tarefa do Gerador de Regras de Controle de Dispositivos for concluída. Em vez disso, elas serão apenas adicionadas à lista de regras de Controle de Dispositivos.

  Esta caixa é desmarcada por padrão.

  A caixa não pode ser selecionada se a caixa **Adicionar regras de permissão à lista de regras de Controle de Dispositivos** não tiver sido selecionada.

- **Adicionar informações do computador ao nome do arquivo**.

  A caixa de seleção ativa ou desativa a adição de informações sobre o computador protegido ao nome do arquivo para o qual as regras de permissão serão exportadas.

  Se esta caixa estiver selecionada, o aplicativo adicionará o nome de computador protegido e a data e hora de criação de arquivos ao nome do arquivo de exportação.

  Se a caixa estiver desmarcada, o aplicativo não adicionará informações sobre o computador protegido ao nome do arquivo de exportação.

  A caixa de seleção é selecionada por padrão.

3. Clique em **Avançar**.
4. Na janela **Agendar**, defina as configurações de programação de inicialização da tarefa.
5. Clique em **Avançar**.
6. Na janela **Seleção de uma conta para a executar a tarefa**, especifique a conta que você quer usar.
7. Clique em **Avançar**.
8. Defina um nome de tarefa.
9. Clique em **Avançar**.

> O nome da tarefa não deve ter mais de 100 caracteres e não pode conter os seguintes símbolos: " * < > & \ : |

A janela **Conclusão da criação da tarefa** será aberta.

10. Você também pode executar a tarefa após a finalização do Assistente marcando a caixa de seleção **Executar a tarefa após a finalização do Assistente**.
11. Clique em **Concluir** para concluir a criação da tarefa.
12. Na guia **Tarefas** na área de trabalho do grupo de computadores sendo configurados, na lista de tarefas de grupo, selecione o Gerador de Regras de Controle de Dispositivos que você criou.
13. Clique no botão **Iniciar** para inicializar a tarefa.

    Quando a tarefa for concluída, as listas de regras de permissão geradas automaticamente serão salvas em arquivos XML em uma pasta compartilhada.

> Antes de usar a política de Controle de Dispositivos na rede, certifique-se de que todos os computadores protegidos tenham acesso a uma pasta de rede compartilhada. Se a política da organização não permitir o uso de uma pasta compartilhada na rede, recomenda-se iniciar a tarefa de Gerador de Regras de Controle de Dispositivos para regras de controle do computador no grupo de computadores de teste ou em uma máquina modelo.

Adicionar as regras geradas à lista de regras de Controle de dispositivos

► *Para adicionar as listas geradas de regras de permissão à tarefa Controle de dispositivos:*

1. Abra a janela de **Regras de Controle de dispositivos** (consulte a seção "Abertura da lista de regras de Controle de Dispositivos" na página 347).
2. Clique no botão **Adicionar**.
3. No menu de contexto do botão **Adicionar**, selecione a opção **Importar regras do arquivo XML**.
4. Selecione o princípio para adicionar as regras de permissão geradas automaticamente à lista de regras de Controle de dispositivos criadas anteriormente:
   - **Adicionar às regras existentes** se você quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.
   - **Substituir as regras existentes** se você quiser substituir as regras existentes pelas regras importadas.
   - **Mesclar com as regras existentes** se você quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.
5. Na janela padrão do Microsoft Windows exibida, selecione arquivos XML criados após a conclusão da tarefa de grupo Gerador de Regras de Controle de Dispositivos.
6. Clique em **Abrir**.

   Todas as regras geradas do arquivo XML serão adicionadas à lista de acordo com o princípio selecionado.
7. Clique no botão **Salvar**, na janela **Regras de Controle de dispositivos**.
8. Se você deseja aplicar as regras de controle de dispositivos geradas, selecione o modo de tarefa **Ativa** nas

configurações de política de **Controle de Dispositivos**.

Regras de permissão geradas automaticamente com base em dados do sistema em cada computador separado são aplicadas a todos os computadores de rede abrangidos pela política sendo configurada. Nestes computadores, o aplicativo permitirá a conexão somente daqueles dispositivos para os quais as regras de permissão foram criadas.

Gerenciamento do Controle de Dispositivos por meio do Console do Aplicativo

Nesta seção, aprenda como navegar pela interface do Console do Aplicativo e definir configurações de tarefa em um computador local.

Nesta seção

Navegação 357
Definição das configurações de tarefa Controle de Dispositivos 358
Configuração de regras de Controle de dispositivos 359
Configurando a tarefa do Gerador de Regras de Controle de Dispositivos 364

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface.

Nesta seção

Abertura das configurações da tarefa Controle de Dispositivos 357
Abertura da janela de regras de Controle de Dispositivos 358
Abertura das configurações da tarefa do Gerador de Regras de Controle de Dispositivos 358

Abertura das configurações da tarefa Controle de Dispositivos

► *Para abrir as configurações da tarefa do Controle de Dispositivos por meio do Console do Aplicativo:*

1. Na árvore do Console do Aplicativo, expanda o nó **Controle do computador**.
2. Selecione o nó filho **Controle de Dispositivos**.
3. No painel de detalhes do nó filho **Controle de Dispositivos**, clique no link **Propriedades**.

   A janela **Configurações de tarefa** é exibida.
4. Configure a tarefa conforme necessário.

Abertura da janela de regras de Controle de dispositivos

► *Para abrir a lista de regras de Controle de Dispositivos por meio do Console do Aplicativo:*

1. Na árvore do Console do Aplicativo, expanda o nó **Controle do computador**.
2. Selecione o nó filho **Controle de Dispositivos**.
3. No painel de detalhes do nó **Controle de Dispositivos**, clique no link **Regras de Controle de Dispositivos**.

   A janela **Regras de Controle de Dispositivos** é exibida.
4. Configure a lista de regras conforme necessário.

Abertura das configurações da tarefa do Gerador de Regras de Controle de Dispositivos

► *Para configurar a tarefa do Gerador de Regras de Controle de Dispositivos:*

1. Na árvore do Console do Aplicativo, expanda o nó **Geradores de regra automáticos**.
2. Selecione o nó filho **Gerador de Regras de Controle de Dispositivos**.
3. No painel de detalhes do nó filho **Gerador de Regras de Controle de Dispositivos**, clique no link **Propriedades**.

   A janela **Configurações de tarefa** é exibida.
4. Configure a tarefa conforme necessário.

Definição das configurações de tarefa Controle de Dispositivos

► *Para definir as configurações da tarefa Controle de dispositivos:*

1. Abra a janela **Configurações de tarefa** (consulte a seção “Abertura das configurações da tarefa Controle de Dispositivos” na página 357).
2. Na guia **Geral**, defina as seguintes configurações de tarefa:
   - Na seção **Modo da tarefa**, selecione um dos modos de tarefa:
     - **Ativa**.

       O Kaspersky Embedded Systems Security aplica regras para controlar a conexão de pendrives e outros dispositivos externos e permite ou bloqueia o uso de todos os dispositivos de acordo com o princípio de Negação Padrão e as regras de permissão especificadas. O uso de dispositivos externos confiáveis é permitido. Por padrão, o uso de dispositivos externos não confiáveis é bloqueado.

Se um dispositivo externo que você considera não confiável for conectado a um computador protegido antes que a tarefa Controle de Dispositivos seja executada no modo Ativa, o dispositivo não será bloqueado pelo aplicativo. Recomendamos que desconecte o dispositivo não confiável manualmente ou reinicie o computador. Caso contrário, o princípio de Negação Padrão não será aplicado ao dispositivo.

- **Somente Estatísticas**.

  O Kaspersky Embedded Systems Security não controla a conexão de pendrives e outros dispositivos externos, só registra em log as informações sobre a conexão e o registro de dispositivos externos em um computador protegido e sobre as regras de permissão de Controle de Dispositivos acionadas pelos dispositivos conectados. O uso de todos os dispositivos externos é permitido. Este modo está definido por padrão.

- Selecione ou desmarque a caixa **Permitir o uso de todos os dispositivos de armazenamento em massa quando a tarefa Controle de dispositivos não estiver em execução**.

  A caixa de seleção permite ou bloqueia o uso de dispositivos de armazenamento em massa quando a tarefa Controle de Dispositivos não estiver sendo executada.

  Se a caixa de seleção for marcada e a tarefa Controle de Dispositivos não estiver sendo executada, o Kaspersky Embedded Systems Security permitirá o uso de qualquer dispositivo de armazenamento em massa em um computador protegido.

  Se a caixa de seleção estiver desmarcada, o aplicativo bloqueará o uso de dispositivos de armazenamento em massa não confiáveis em um computador protegido nos seguintes casos: quando a tarefa Controle de Dispositivos não estiver sendo executada ou se o Kaspersky Security Service tiver sido desativado. Esta opção é recomendada para maximizar o nível da proteção contra ameaças de segurança do computador que surgem após a troca de arquivos com dispositivos externos.

  Esta caixa é desmarcada por padrão.

3. Se necessário, nas guias **Agendar** e **Avançado**, defina as configurações de inicialização de tarefa programada (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 151).
4. Para editar a lista de regras de controle de dispositivos (consulte a seção "Sobre o preenchimento da lista de regras de Controle de dispositivos" na página 342), clique no link **Regras de Controle de Dispositivos** na parte inferior do painel de detalhes do nó **Controle de Dispositivos**.

O Kaspersky Embedded Systems Security aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

Configuração de regras de Controle de dispositivos

Aprenda como gerar, importar e exportar uma lista de regras, ou criar manualmente regras de permissão ou de negação utilizando a tarefa Controle de Dispositivos.

Nesta seção

Importação das regras de Controle de Dispositivos do arquivo XML 360
Preenchendo a lista de regras com base em eventos de tarefa Controle de Dispositivos 360
Adicionar uma regra de permissão para um ou vários dispositivos externos 361
Removendo regras de Controle de Dispositivos 362
Exportando regras de Controle de Dispositivos 362
Ativando e desativando regras de Controle de Dispositivos 362
Expandindo o escopo de uso das regras de Controle de Dispositivos 363

Importação das regras de Controle de dispositivos do arquivo XML

► *Para importar as regras de Controle de dispositivos, siga as etapas a seguir:*

1. Abra a janela de **Regras de Controle de Dispositivos** (consulte a seção "**Abertura da janela de regras de Controle de Dispositivos**" na página 358).
2. Clique no botão **Adicionar**.
3. No menu de contexto do botão, selecione **Importar regras do arquivo XML**.
4. Especifique o método para adicionar as regras importadas. Para fazer isso, selecione uma das opções do menu de contexto do botão **Importar regras do arquivo XML**:
   - **Adicionar às regras existentes** se quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas são duplicadas.
   - **Substituir as regras existentes** se quiser substituir as regras existentes pelas importadas.
   - **Mesclar com as regras existentes** se quiser adicionar as regras importadas à lista das regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.

   A janela **Abrir** padrão do Microsoft Windows é exibida.
5. Na janela **Abrir**, selecione o arquivo XML que contém as configurações das regras de Controle de dispositivos.
6. Clique no botão **Abrir**.

As regras importadas serão exibidas na lista da janela **Regras de Controle de Dispositivos**.

Preenchendo a lista de regras com base em eventos de tarefa Controle de dispositivos

► *Para criar um arquivo de configuração que contenha regras de controle de dispositivos com base nos eventos da tarefa Controle de dispositivos:*

1. Inicie a tarefa Controle de Dispositivos no modo **Somente Estatísticas** (consulte a seção "**Definição das configurações da tarefa Controle de Dispositivos**" na página 358), para registrar em log todos os eventos de pendrives e outras conexões de dispositivos externos a um computador protegido.
2. Após concluir a tarefa no modo **Somente Estatísticas**, abra o log de tarefas clicando no botão **Abrir log da**

tarefa na seção **Gerenciamento** do nó **Controle de Dispositivos** no painel de detalhes.

3. Na janela **Logs**, clique em **Gerar regras com base em eventos**.

O Kaspersky Embedded Systems Security criará um arquivo de configuração XML que contém a lista de regras gerada com base em eventos de tarefa Controle de dispositivos no modo **Somente Estatísticas**. Você pode aplicar essa lista à tarefa Controle de Dispositivos (consulte a seção "Importação das regras de Controle de dispositivos do arquivo XML" na página 360).

Antes de aplicar uma lista de regras gerada com base nos eventos de tarefa, recomenda-se analisar e, em seguida, processar manualmente a lista de regras para se certificar de que não haja dispositivos não confiáveis permitidos pelas regras especificadas.

Durante a conversão de um arquivo XML com os eventos de tarefa a uma lista de regras, o aplicativo gera regras de permissão para todos os eventos registrados, incluindo as restrições de dispositivos.

Todos os eventos de tarefa são registrados no log de tarefas independente do modo de tarefa. Você pode criar um arquivo de configuração com uma lista de regras com base nos eventos da tarefa no modo **Ativa**. Este cenário não é recomendado, exceto em casos urgentes, desde que a eficiência da tarefa necessite gerar uma versão de lista de regras final antes que a tarefa seja executada no modo ativo.

Adicionar uma regra de permissão para um ou vários dispositivos externos

A função do manual que adiciona regras uma por vez não é suportada na tarefa Controle de dispositivos. No entanto, em casos onde é necessário adicionar regras de um ou vários dispositivos externos novos, é possível usar a opção **Gerar regras com base nos dados do sistema**. Se este cenário for aplicado, o aplicativo utilizará dados do Windows sobre todos os dispositivos externos já conectados e também permite que dispositivos atualmente conectados preencham uma lista de regras de permissão.

O Kaspersky Embedded Systems Security não adquire o acesso a dados do sistema sobre dispositivos móveis conectados via MTP. Você não pode gerar regras de permissão para dispositivos móveis conectados por MTP.

► *Para adicionar uma regra de permissão para um ou mais dispositivos externos que estão conectados atualmente:*

1. Abra a janela de **Regras de Controle de Dispositivos** (consulte a seção "Abertura da janela de regras de Controle de dispositivos" na página 358).
2. Clique no botão **Adicionar**.
3. No menu de contexto exibido selecione a opção **Gerar regras com base nos dados do sistema**.
4. Na janela exibida, reveja a lista de dispositivos detectados e selecione um dispositivo único ou vários dispositivos nos quais deseja confiar em um computador protegido.
5. Clique no botão **Adicionar regras para os disp. selec**.

As novas regras serão geradas e adicionadas à lista de regras de controle de dispositivos.

Removendo regras de Controle de dispositivos

► *Para remover regras de Controle de dispositivos:*

1. Abra a janela de **Regras de Controle de Dispositivos** (consulte a seção "**Abertura da janela de regras de Controle de Dispositivos**" na página 358).
2. Na lista, selecione uma ou várias regras que deseja excluir.
3. Clique no botão **Remover selecionado**.
4. Clique no botão **Salvar**.

As regras de Controle de dispositivos selecionadas serão removidas.

Exportando regras de Controle de dispositivos

► *Para exportar as regras de Controle de dispositivos para um arquivo de configuração:*

1. Abra a janela de **Regras de Controle de Dispositivos** (consulte a seção "**Abertura da janela de regras de Controle de Dispositivos**" na página 358).
2. Clique no botão **Exportar para um arquivo**.

   A janela padrão do Microsoft Windows é exibida.
3. Na janela exibida, especifique o arquivo ao qual deseja exportar as regras. Se nenhum arquivo existir, ele será criado. Se um arquivo com o nome especificado já existir, os seus conteúdos serão reescritos após as regras terem sido exportadas.
4. Clique no botão **Salvar**.

As regras e as suas configurações serão exportadas no arquivo especificado.

Ativando e desativando regras de Controle de dispositivos

Você pode ativar e desativar as regras de controle de dispositivos criadas sem removê-las.

► *Para ativar ou desativar uma regra de controle de dispositivos criada, siga as etapas a seguir:*

1. Abra a janela de **Regras de Controle de Dispositivos** (consulte a seção "**Abertura da janela de regras de Controle de Dispositivos**" na página 358).
2. Na lista de regras especificadas, abra a janela **Propriedades da regra** clicando duas vezes na regra cujas propriedades você deseja configurar.
3. Na janela exibida, selecione ou desmarque a caixa **Aplicar regra**.

   A caixa ativa ou desativa uma regra de controle de dispositivos.

   Se a caixa estiver selecionada para uma regra, a regra será ativada. É permitida a conexão para dispositivos externos que estão incluídos no escopo de uso da regra.

   Se a caixa estiver desmarcada nas propriedades da regra, a regra ficará inativa. É bloqueada a conexão para dispositivos externos que estão incluídos no escopo de uso da regra.

Por padrão, a caixa de seleção fica marcada nas configurações para cada regra criada.

4. Clique em **OK**.

O Status de aplicação da regra será salvo e exibido para a regra especificada.

Expandindo o escopo de uso das regras de Controle de dispositivos

Cada regra de controle de dispositivos gerada automaticamente abrange somente um dispositivo externo. Você pode expandir manualmente um escopo de uso da regra estabelecendo a máscara do caminho da instância do dispositivo em propriedades de qualquer regra especificada.

O aplicativo do caminho da instância do dispositivo reduz o número total de regras especificadas e simplifica o processamento de regras. Mas a expansão de um escopo de uso da regra pode levar à redução da eficiência de controle de dispositivos de armazenamento em massa.

► *Para aplicar uma máscara de caminho da instância do dispositivo em propriedades da regra de controle de dispositivos:*

1. Abra a janela de **Regras de Controle de Dispositivos** (consulte a seção "**Abertura da janela de regras de Controle de Dispositivos**" na página 358).
2. Na janela que se abre, selecione uma regra para usar suas propriedades para o aplicativo de máscara.
3. Abra a janela **Propriedades da regra** clicando duas vezes em uma regra de Controle de dispositivos selecionada.
4. Na janela exibida, execute as seguintes operações:
   - Selecione a caixa **Usar máscara** ao lado do campo **Tipo de controlador (PID)** se desejar que uma regra selecionada permita conexões para todos os dispositivos de armazenamento em massa que corresponderem às informações especificadas sobre o fabricante e número de série do dispositivo.
   - Selecione a caixa **Usar máscara** ao lado do campo **Número de série** se desejar que uma regra selecionada permita conexões para todos os dispositivos de armazenamento em massa que corresponderem às informações especificadas sobre o fabricante do dispositivo e o tipo de controlador.
   - Selecione as caixas **Usar máscara** ao lado do campo **Tipo de controlador (PID)** e do campo **Número de série** se desejar que uma regra selecionada permita conexões para todos os dispositivos de armazenamento em massa que corresponderem às informações especificadas sobre o fabricante do dispositivo.

   Se a caixa de seleção **Usar máscara** for marcada em pelo menos um dos campos, os dados dos campos com a caixa selecionada serão substituídos por um * e não serão considerados quando a regra for aplicada.
5. Se necessário, especifique as informações adicionais sobre a regra no campo **Descrição**. Por exemplo, especifique os dispositivos afetados pela regra.
6. Clique em **OK**.

As propriedades da regra definidas recentemente serão salvas. O escopo de uso da regra será expandido de acordo com uma máscara de caminho da instância do dispositivo especificada.

Configurando a tarefa do Gerador de Regras de Controle de Dispositivos

► *Para configurar a tarefa do Gerador de Regras de Controle de Dispositivos:*

1. Na árvore do Console do Aplicativo, expanda o nó **Geradores de regra automáticos**.
2. Selecione o nó filho **Gerador de Regras de Controle de Dispositivos**.
3. Clique no link **Propriedades** no painel de detalhes do nó **Gerador de Regras de Controle de Dispositivos**.

   A janela **Configurações de tarefa** é exibida.
4. Na guia **Geral**, selecione o modo de operação da tarefa na seção **Modo da tarefa**:
   - **Considere os dados do sistema a respeito de todos os armazenamentos em massa que foram conectados**.
   - **Considere somente os armazenamentos em massa conectados atualmente**.
5. Na seção **Após a conclusão da tarefa**, especifique as ações que devem ser executadas pelo Kaspersky Embedded Systems Security após a conclusão da tarefa:
   - **Adicionar regras de permissão à lista de regras de Controle de dispositivos**.

     A caixa de seleção ativa ou desativa a adição de regras de permissão geradas recentemente à lista de regras de Controle de dispositivos. A lista de regras de Controle de dispositivos é exibida ao clicar no link **Regras de Controle de Dispositivos** no painel de detalhes do nó **Controle de Dispositivos**.

     Se a caixa estiver selecionada, o Kaspersky Embedded Systems Security adicionará as regras que foram geradas pela tarefa do Gerador de regras de Controle de dispositivos à lista de regras de controle de dispositivos com base no princípio selecionado para adição de regras.

     Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security não adicionará as regras de permissão geradas recentemente à lista de regras de Controle de dispositivos. As regras geradas são exportadas somente para um arquivo.

     A caixa de seleção é selecionada por padrão.

     A caixa não pode ser selecionada se a caixa **Exportar regras de permissão para o arquivo** não tiver sido selecionada.
   - **Princípio da adição**.

     Essa lista suspensa é usada para especificar o método utilizado para a adição de regras de permissão geradas recentemente à lista de regras de Controle de Inicialização de Aplicativos.

     - **Adicionar às regras existentes**. As regras são adicionadas à lista de regras existentes. As regras com configurações idênticas são duplicadas.
     - **Substituir as regras existentes**. As regras substituem as regras existentes na lista.
     - **Mesclar com as regras existentes**. As regras são adicionadas à lista de regras existentes. As regras com configurações idênticas não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único.

     Por padrão, o método **Mesclar com as regras existentes** é selecionado.
   - **Exportar regras de permissão para o arquivo**.

A caixa ativa ou desativa a exportação de regras de permissão de Controle de Dispositivos a um arquivo.

Se a caixa estiver selecionada, o Kaspersky Embedded Systems Security exportará as regras de permissão para o arquivo especificado no campo abaixo quando a tarefa do Gerador de Regras de Controle de Dispositivos for concluída.

Se essa caixa estiver desmarcada, o aplicativo não exportará as regras de permissão geradas para um arquivo quando a tarefa do Gerador de Regras de Controle de Dispositivos for concluída. Em vez disso, elas serão apenas adicionadas à lista de regras de Controle de Dispositivos.

Esta caixa é desmarcada por padrão.

A caixa não pode ser selecionada se a caixa **Adicionar regras de permissão à lista de regras de Controle de Dispositivos** não tiver sido selecionada.

- **Adicionar informações do computador ao nome do arquivo**.

  A caixa de seleção ativa ou desativa a adição de informações sobre o computador protegido ao nome do arquivo para o qual as regras de permissão serão exportadas.

  Se esta caixa estiver selecionada, o aplicativo adicionará o nome de computador protegido e a data e hora de criação de arquivos ao nome do arquivo de exportação.

  Se a caixa estiver desmarcada, o aplicativo não adicionará informações sobre o computador protegido ao nome do arquivo de exportação.

  A caixa de seleção é selecionada por padrão.

6. Nas guias **Agendar** e **Avançado**, defina as configurações de início da tarefa agendada (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 151).
7. Clique em **OK**.

O Kaspersky Embedded Systems Security aplica imediatamente as novas configurações à tarefa em execução. As informações sobre data e hora em que as configurações foram modificadas e os valores de configurações de tarefa antes e após a modificação são salvos no log de auditoria do sistema.

Gerenciamento de Firewall

Esta seção contém informações sobre a tarefa Gerenciamento de Firewall e como configurá-la.

Neste capítulo

Sobre a tarefa de Gerenciamento de Firewall 366
Sobre as regras de Firewall 367
Configurações padrão da tarefa de Gerenciamento de Firewall 369
Gerenciamento das regras de Firewall por meio do Plug-in de Administração 369
Gerenciamento das regras de Firewall por meio do Console do Aplicativo 373

Sobre a tarefa de Gerenciamento de Firewall

O Kaspersky Embedded Systems Security fornece uma solução confiável e ergonômica para proteger conexões de rede usando a tarefa de Gerenciamento de Firewall.

A tarefa de Gerenciamento de Firewall não executa a filtragem de tráfego de rede independente, mas permite que você gerencie o Firewall do Windows através da interface gráfica do Kaspersky Embedded Systems Security. Durante a tarefa de Gerenciamento de Firewall, o Kaspersky Embedded Systems Security assume o gerenciamento das configurações e políticas do firewall do sistema operacional e bloqueia qualquer possibilidade de configuração externa do firewall.

Durante a instalação do aplicativo, o componente de Gerenciamento de Firewall lê e copia o status do Firewall do Windows e todas as regras especificadas. Depois disso, o conjunto de regras e os parâmetros da regra podem apenas ser alterados, e o firewall pode apenas ser ativado ou desativado no Kaspersky Embedded Systems Security.

Se o Firewall do Windows for desativado durante a instalação do Kaspersky Embedded Systems Security, a tarefa de Gerenciamento de Firewall não será executada após a conclusão da instalação. Se o Firewall do Windows for ativado durante a instalação do aplicativo, a tarefa de Gerenciamento de Firewall será executada após a instalação ser concluída, bloqueando todas as conexões de rede que não são permitidas pelas regras especificadas.

O componente de Gerenciamento de Firewall não é instalado por padrão, já que não está incluído no conjunto de componentes para a Instalação recomendada.

A tarefa de Gerenciamento de Firewall impõe o bloqueio de todas as conexões de entrada e de saída não permitidas pelas regras especificadas da tarefa.

A tarefa pesquisa o Firewall do Windows regularmente e monitora o seu status. Por padrão, o intervalo de pesquisa é definido como 1 minuto e não pode ser alterado. Se durante a pesquisa, o Kaspersky Embedded Systems

Security detectar uma não correspondência entre as configurações do Firewall do Windows e as da tarefa de Gerenciamento de Firewall, o aplicativo aplicará de maneira forçada as configurações da tarefa no firewall do sistema operacional.

Com a pesquisa minuto a minuto do Firewall do Windows, o Kaspersky Embedded Systems Security monitorará o seguinte:

- Status de operação do Firewall do Windows.
- O status de regras adicionadas após a instalação do Kaspersky Embedded Systems Security por outros aplicativos ou ferramentas (por exemplo, a adição de uma nova regra de aplicativo para uma porta/aplicativo usando o wf.msc).

Ao aplicar as novas regras ao Firewall do Windows, o Kaspersky Embedded Systems Security cria um conjunto de regra do Kaspersky Security Group no snap-in do **Firewall do Windows**. Esse conjunto de regras une todas as regras criadas pelo Kaspersky Embedded Systems Security usando a tarefa de Gerenciamento de Firewall. As regras no Kaspersky Security Group não são monitoradas pelo aplicativo durante a pesquisa a cada minuto e não são automaticamente sincronizadas com a lista de regras especificadas nas configurações da tarefa de Gerenciamento de Firewall.

► *Para atualizar manualmente as regras do Kaspersky Security Group,*

reinicie a tarefa de Gerenciamento de Firewall do Kaspersky Embedded Systems Security.

Também é possível editar as regras do Kaspersky Security Group manualmente usando o snap-in do **Firewall do Windows**.

Se o Firewall do Windows for gerenciado pela política de grupo do Kaspersky Security Center, a tarefa de Gerenciamento de Firewall não poderá ser iniciada.

Sobre as Regras de Firewall

A tarefa de Gerenciamento de Firewall controla a filtragem do tráfego de entrada e de saída da rede usando regras de permissão aplicadas de maneira forçada no Firewall do Windows durante a execução da tarefa.

Na primeira vez que a tarefa é iniciada, o Kaspersky Embedded Systems Security lê e copia todas as regras de tráfego de rede recebido especificadas nas configurações do Firewall do Windows nas configurações da tarefa de Gerenciamento de Firewall. Em seguida, o aplicativo funciona de acordo com as seguintes regras:

- Se uma nova regra for criada nas configurações do Firewall do Windows (manual ou automaticamente durante uma nova instalação do aplicativo), o Kaspersky Embedded Systems Security excluirá a regra.
- Se uma regra existente for excluída das configurações do Firewall do Windows, o Kaspersky Embedded Systems Security restaurará a regra quando a tarefa for reinicializada.
- Se os parâmetros de uma regra existente forem alterados nas configurações do Firewall do Windows, o Kaspersky Embedded Systems Security reverterá as alterações.
- Se uma nova regra for criada nas configurações da Gerenciamento de Firewall, o Kaspersky Embedded Systems Security aplicará de maneira forçada essa regra ao Firewall do Windows.
- Se uma regra existente for excluída das configurações de Gerenciamento de Firewall, o Kaspersky Embedded Systems Security será forçado a excluir a regra das configurações do Firewall do Windows.

O Kaspersky Embedded Systems Security não funciona com regras de bloqueio ou regras de controle do tráfego de rede de saída. Após o início da tarefa de Gerenciamento de Firewall, o Kaspersky Embedded Systems Security excluirá todas essas regras das configurações do Firewall do Windows.

É possível definir, excluir e editar as regras de filtragem para o tráfego de rede de entrada.

Não é possível especificar uma nova regra para controlar o tráfego de rede de saída nas configurações da tarefa de Gerenciamento de Firewall. Todas as regras do Firewall especificadas no Kaspersky Embedded Systems Security controlam apenas o tráfego de rede de entrada.

É possível gerenciar os seguintes tipos de regras de Firewall:

- Regras do aplicativo.
- Regras da porta.

Regras do aplicativo

Este tipo de regra permite conexões direcionadas de rede para aplicativos especificados. O critério para acionamento dessas regras baseia-se em um caminho para um arquivo executável.

É possível gerenciar regras do aplicativo:

- Adicionar novas regras.
- Remover regras existentes.
- Ativar ou desativar regras especificadas.
- Editar os parâmetros das regras especificadas: especifique o nome da regra, caminho até o arquivo executável e escopo de uso da regra.

Regras da porta

Este tipo de regra permite conexões de rede para portas e protocolos (TCP/UDP) especificados. Os critérios para acionamento destas regras baseiam-se no número da porta e tipo de protocolo.

É possível gerenciar regras de portas:

- Adicionar novas regras.
- Remover regras existentes.
- Ativar ou desativar regras especificadas.
- Editar os parâmetros das regras especificadas: defina o nome da regra, número da porta, tipo de protocolo e escopo para o aplicativo da regra.

As regras de porta implicam um escopo mais amplo do que as de aplicativo. Ao permitir conexões com base nas regras de porta, você reduz o nível de segurança do computador protegido.

Configurações padrão da tarefa de Gerenciamento de Firewall

A tarefa de Gerenciamento de Firewall usa as configurações padrão descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Tabela 52. Configurações padrão da tarefa de Gerenciamento de Firewall

Configuração	Valor padrão	Descrição
Regras de Firewall para o aplicativo	Duas regras padrão para o aplicativo ativadas	Você pode desativar as regras padrão ou adicionar novas regras.
Regras de Firewall para portas	Seis regras padrão para portas ativadas	Você pode desativar as regras padrão ou adicionar novas regras.
Programação de inicialização da tarefa	A primeira execução não está programada.	A tarefa de Gerenciamento de Firewall não inicia automaticamente no momento da inicialização do Kaspersky Embedded Systems Security. Você pode configurar a programação de inicialização da tarefa.

Gerenciamento das regras de Firewall por meio do Plug-in de Administração

Nesta seção, aprenda como gerenciar as regras de Firewall por meio da interface do Console do Aplicativo.

Nesta seção

Como ativar e desativar as regras de Firewall 369
Adição de regras de Firewall manualmente 370
Exclusão de regras de Firewall..... 372

Como ativar e desativar as regras de Firewall

► *Para ativar ou desativar uma regra existente para a filtragem do tráfego de entrada de rede, execute as seguintes ações:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na

página 115).

- Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

  Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

4. Na seção **Controle de atividade de rede**, clique no botão **Configurações** na subseção **Gerenciamento de Firewall**.
5. Clique no botão **Lista de regras** na janela que se abre.

   A janela **Regras de firewall** é aberta.
6. Dependendo do tipo da regra cujo status você deseja modificar, selecione **Aplicativos** ou **Portas**.
7. Na lista de regras, selecione a regra cujo status você deseja modificar e execute uma das seguintes ações:
   - Se você quiser ativar uma regra desativada, marque a caixa de seleção à esquerda do nome da regra.

     A regra selecionada será ativada.
   - Se você quiser desativar uma regra ativada, desmarque a caixa de seleção à esquerda do nome da regra.

     A regra selecionada será desativada.
8. Clique em **OK** na janela **Regras de Firewall**.
9. Clique em **OK** na janela **Gerenciamento de Firewall**.
10. Clique em **OK** na janela **Propriedades: <Nome da política>**.

As configurações da tarefa especificadas serão salvas. Os novos parâmetros de regra serão enviados ao Firewall do Windows.

Adição de regras de Firewall manualmente

Só é possível adicionar e editar regras para aplicativos e portas. Não é possível adicionar novas regras de grupo ou editar regras de grupo existentes.

► *Para adicionar ou editar uma regra existente para a filtragem de tráfego de entrada de rede, faça o seguinte:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na

página 115).

- Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

  Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

4. Na seção **Controle de atividade de rede**, clique no botão **Configurações** na subseção **Gerenciamento de Firewall**.
5. Clique no botão **Lista de regras** na janela que se abre.

   A janela **Regras de firewall** é aberta.
6. Dependendo do tipo de regra que você deseja adicionar, selecione a guia **Aplicativos** ou **Portas** e execute uma das seguintes ações:
   - Para editar uma regra existente, selecione a regra que deseja editar na lista de regras e clique em **Editar**.
   - Para adicionar uma nova regra, clique em **Adicionar**.

     Dependendo do tipo de regra que estiver sendo configurada, a janela **Regra da porta** ou **Regra de aplicativo** é exibida.
7. Na janela exibida, execute as seguintes operações:
   - Se você estiver trabalhando com uma regra de aplicativo, faça o seguinte:
     a. Digite o **Nome da regra** editada.
     b. Especifique o **Caminho do aplicativo** para o arquivo executável do aplicativo para o qual você está permitindo uma conexão modificando esta regra.

        É possível configurar o caminho manualmente ou usando o botão **Procurar**.
     c. No campo **Escopo de aplicação da regra**, especifique os endereços de rede aos quais a regra modificada será aplicada.

     Você pode usar apenas endereços IP IPv4.

   - Se você estiver trabalhando com uma regra de porta, faça o seguinte:
     a. Digite o **Nome da regra** editada.
     b. Especifique o **Número da porta** para o qual o aplicativo permitirá conexões.
     c. Selecione o tipo de protocolo (TCP/UDP) para o qual o aplicativo permitirá conexões.
     d. No campo **Escopo de aplicação da regra**, especifique os endereços de rede aos quais a regra modificada será aplicada.

     Você pode usar apenas endereços IP IPv4.
8. Clique em **OK** na janela **Regra de aplicativo** ou **Regra da porta**.

9. Clique em **OK** na janela **Gerenciamento de Firewall**.
10. Clique em **OK** na janela **Propriedades: <Nome da política>**.

As configurações da tarefa especificadas serão salvas. Os novos parâmetros de regra serão enviados ao Firewall do Windows.

Exclusão de regras de Firewall

Só é possível excluir regras de aplicativos e de porta. Não é possível excluir regras de grupo existentes.

► *Para excluir uma regra existente para a filtragem do tráfego de entrada de rede, execute as seguintes ações:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
4. Na seção **Controle de atividade de rede**, clique no botão **Configurações** na subseção **Gerenciamento de Firewall.**
5. Clique no botão **Lista de regras** na janela que se abre.

   A janela **Regras de firewall** é aberta.
6. Dependendo do tipo da regra cujo status você deseja modificar, selecione a guia **Aplicativos** ou **Portas**.
7. Na lista de regras, selecione a regra que você deseja excluir.
8. Clique no botão **Remover**.

   A regra selecionada é excluída.
9. Clique em **OK** na janela **Regras de Firewall**.
10. Clique em **OK** na janela **Gerenciamento de Firewall**.
11. Clique em **OK** na janela **Propriedades: <Nome da política>**.

As configurações da tarefa de Gerenciamento de Firewall especificadas são salvas. Os novos parâmetros de regra serão enviados ao Firewall do Windows.

Gerenciamento das regras de Firewall por meio do Console do Aplicativo

Nesta seção, aprenda como gerenciar as regras de Firewall por meio da interface do Console do Aplicativo.

Nesta seção

Como ativar e desativar as regras de Firewall 373

Adição de regras de Firewall manualmente 373

Exclusão de regras de Firewall 374

Como ativar e desativar as regras de Firewall

► *Para ativar ou desativar uma regra existente para a filtragem do tráfego de entrada de rede, execute as seguintes ações:*

1. Na árvore do Console do Aplicativo, expanda o nó **Controle do computador**.
2. Selecionar o nó filho **Gerenciamento de Firewall**.
3. Clique no link **Regras de Firewall** no painel de detalhes do nó **Gerenciamento de Firewall**.

   A janela **Regras de firewall** é aberta.
4. Dependendo do tipo da regra cujo status você deseja modificar, selecione **Aplicativos** ou **Portas**.
5. Na lista de regras, selecione a regra cujo status você deseja modificar e execute uma das seguintes ações:
   - Se você quiser ativar uma regra desativada, marque a caixa de seleção à esquerda do nome da regra.

     A regra selecionada será ativada.
   - Se você quiser desativar uma regra ativada, desmarque a caixa de seleção à esquerda do nome da regra.

     A regra selecionada será desativada.
6. Clique em **Salvar** na janela **Regras de Firewall**.

As configurações da tarefa especificadas serão salvas. Os novos parâmetros de regra serão enviados ao Firewall do Windows.

Adição de regras de Firewall manualmente

► *Para adicionar ou editar uma regra existente para a filtragem de tráfego de entrada de rede, faça o seguinte:*

1. Na árvore do Console do Aplicativo, expanda o nó **Controle do computador**.
2. Selecionar o nó filho **Gerenciamento de Firewall**.
3. Clique no link **Regras de Firewall** no painel de detalhes do nó **Gerenciamento de Firewall**.

A janela **Regras de firewall** é aberta.

4. Dependendo do tipo de regra que você deseja adicionar, selecione a guia **Aplicativos** ou **Portas** e execute uma das seguintes ações:
   - Para editar uma regra existente, selecione a regra que deseja editar na lista de regras e clique em **Editar**.
   - Para adicionar uma nova regra, clique em **Adicionar**.

     Dependendo do tipo de regra que estiver sendo configurada, a janela **Regra da porta** ou **Regra de aplicativo** é exibida.
5. Na janela exibida, execute as seguintes operações:
   - Se você estiver trabalhando com uma regra de aplicativo, faça o seguinte:
     a. Digite o **Nome da regra** editada.
     b. Especifique o **Caminho do aplicativo** para o arquivo executável do aplicativo para o qual você está permitindo uma conexão modificando esta regra.

        É possível configurar o caminho manualmente ou usando o botão **Procurar**.
     c. No campo **Escopo de aplicação da regra**, especifique os endereços de rede aos quais a regra modificada será aplicada.

     > Você pode usar apenas endereços IP IPv4.

   - Se você estiver trabalhando com uma regra de porta, faça o seguinte:
     a. Digite o **Nome da regra** editada.
     b. Especifique o **Número da porta** para o qual o aplicativo permitirá conexões.
     c. Selecione o tipo de protocolo (TCP/UDP) para o qual o aplicativo permitirá conexões.
     d. No campo **Escopo de aplicação da regra**, especifique os endereços de rede aos quais a regra modificada será aplicada.

     > Você pode usar apenas endereços IP IPv4.
6. Clique em **OK** na janela **Regra de aplicativo** ou **Regra da porta**.
7. Clique em **Salvar** na janela **Regras de Firewall**.

As configurações da tarefa especificadas serão salvas. Os novos parâmetros de regra serão enviados ao Firewall do Windows.

Exclusão de regras de Firewall

> Só é possível excluir regras de aplicativos e de porta. Não é possível excluir regras de grupo existentes.

► *Para excluir uma regra existente para a filtragem do tráfego de entrada de rede, execute as seguintes*

ações:

1. Na árvore do Console do Aplicativo, expanda o nó **Controle do computador**.
2. Selecionar o nó filho **Gerenciamento de Firewall**.
3. Clique no link **Regras de Firewall** no painel de detalhes do nó **Gerenciamento de Firewall**.

   A janela **Regras de firewall** é aberta.
4. Dependendo do tipo da regra cujo status você deseja modificar, selecione a guia **Aplicativos** ou **Portas**.
5. Na lista de regras, selecione a regra que você deseja excluir.
6. Clique no botão **Remover**.

   A regra selecionada é excluída.
7. Clique em **Salvar** na janela **Regras de Firewall**.

As configurações da tarefa especificadas serão salvas. Os novos parâmetros de regra serão enviados ao Firewall do Windows.

Monitor de Integridade de Arquivos

Esta seção contém informações sobre a inicialização e a configuração da tarefa de Monitor de Integridade de Arquivos.

Neste capítulo

Sobre a tarefa Monitor de Integridade de Arquivos 376
Sobre regras de monitoramento de operações de arquivos 377
Configurações padrão da tarefa de Monitor de Integridade de Arquivos 379
Gerenciamento do Monitor de Integridade de Arquivos por meio do Plug-in de Administração 380
Gerenciamento do Monitor de Integridade de Arquivos por meio do Console do Aplicativo 385

Sobre a tarefa Monitor de Integridade de Arquivos

A tarefa Monitor de Integridade de Arquivos foi projetada para rastrear ações realizadas com os arquivos e as pastas especificados nos escopos de monitoramento definidos nas configurações da tarefa. É possível usar a tarefa para detectar alterações no arquivo que possam indicar uma violação de segurança no computador protegido. Também é possível configurar que as alterações no arquivo sejam rastreadas durante períodos em que o monitoramento é interrompido.

Uma *interrupção do monitoramento* ocorre quando o escopo de monitoramento fica temporariamente fora do escopo da tarefa, por exemplo, se a tarefa for interrompida ou se um dispositivo de armazenamento em massa não estiver fisicamente presente em um computador protegido. O Kaspersky Embedded Systems Security informa sobre operações de arquivos detectadas no escopo de monitoramento assim que um dispositivo de armazenamento em massa é reconectado.

Se as tarefas deixarem de ser executadas no escopo de monitoramento especificado devido a uma reinstalação do componente do Monitor de Integridade de Arquivos, isso não constituirá uma interrupção do monitoramento. Neste caso, a tarefa de Monitor de Integridade de Arquivos não é executada.

Requisitos no ambiente

Para iniciar a tarefa Monitor de Integridade de Arquivos, as seguintes condições devem ser satisfeitas:

- Um dispositivo de armazenamento em massa compatível com os sistemas ReFS e NTFS deve ser instalado no computador protegido.
- O USN Journal do Windows deve estar ativo. O componente solicita ao Journal para receber informações sobre as operações do arquivo.

  Se você ativar o USN Journal após uma regra ter sido criada para um volume e a tarefa de Monitor de Integridade de Arquivos tiver sido iniciada, a tarefa deverá ser reiniciada. Senão, a regra não será aplicada durante o monitoramento.

Escopos de monitoramento excluídos

É possível criar escopos de monitoramento excluídos (consulte a seção "Configuração de regras de monitoramento" na página 382). As exclusões são especificadas para cada regra separada e funcionam apenas para o escopo de monitoramento indicado. É possível especificar um número ilimitado de exclusões para cada regra.

As exclusões têm uma prioridade mais alta do que o escopo de monitoramento e não são monitoradas pela tarefa, mesmo se uma pasta ou arquivo indicado estiver no escopo. Se as configurações para uma das regras especificarem um escopo de monitoramento em um nível inferior do que a pasta especificada nas exclusões, este não será considerado quando a tarefa for executada.

Para especificar exclusões, você pode usar as mesmas máscaras que as utilizadas para especificar escopos de monitoramento.

Sobre regras de monitoramento de operações de arquivos

O Monitor de Integridade de Arquivos é executado com base nas regras de monitoramento de operações de arquivos. É possível usar os critérios para acionamento de regras para configurar as condições que acionam a tarefa e ajustar o nível de importância dos eventos para operações de arquivos detectadas e registradas no log de tarefas.

Uma regra de monitoramento de operações de arquivos é especificada para cada escopo de monitoramento.

É possível configurar os seguintes critérios para acionamento de regras:

- Usuários confiáveis.
- Marcadores de operação do arquivo.

Usuários confiáveis

Por padrão, o aplicativo trata todas as ações de usuário como potenciais violações de segurança. A lista de usuários confiáveis está vazia. É possível configurar o nível de importância de evento criando uma lista de usuários confiáveis nas configurações da regra de monitoramento de operações de arquivos.

Usuário não confiável - qualquer usuário não indicado na lista de usuário confiável nas configurações da regra de escopo de monitoramento. Se o Kaspersky Embedded Systems Security detectar uma operações de arquivos realizada por um usuário não confiável, a tarefa Monitor de Integridade de Arquivos registrará um Evento crítico no Log de tarefas.

Usuário confiável - um usuário ou grupo de usuários autorizados a realizar operações de arquivos no escopo de monitoramento especificado. Se o Kaspersky Embedded Systems Security detectar operações de arquivos realizadas por um usuário confiável, a tarefa Monitor de Integridade de Arquivos registrará um Evento informativo no Log de tarefas.

O Kaspersky Embedded Systems Security não é capaz de determinar os usuários que iniciam operações durante os períodos de interrupção de monitoramento. Neste caso, o status do usuário é determinado como desconhecido.

Usuário desconhecido - este status é atribuído a um usuário se o Kaspersky Embedded Systems Security não puder receber informações sobre um usuário devido a uma interrupção da tarefa ou uma falha no driver de sincronização de dados ou USN Journal. Se o Kaspersky Embedded Systems Security detectar uma operações de arquivos realizada por um usuário desconhecido, a tarefa Monitor de Integridade de Arquivos registrará um evento

de *Aviso* no Log de tarefas.

Marcadores de operação do arquivo

Quando a tarefa Monitor de Integridade de Arquivos for executada, o Kaspersky Embedded Systems Security usará os marcadores de operação do arquivo para determinar que uma ação foi realizada em um arquivo.

Um marcador de operações de arquivos é um descritor único que pode caracterizar uma operações de arquivos.

Cada operações de arquivos pode ser uma ação única ou uma cadeia de ações com arquivos. Cada ação dessa espécie é comparada a um marcador de operações de arquivos. Se o marcador especificado como um critério para acionamento de regras for detectado em uma cadeia de operações de arquivos, o aplicativo registrará um evento indicando que a determinada operações de arquivos foi realizada.

O nível de importância dos eventos registrados em log não depende dos marcadores de operação do arquivo selecionados ou do número de eventos.

Por padrão, o Kaspersky Embedded Systems Security considera todos os marcadores de operação do arquivo disponíveis. É possível selecionar marcadores de operação do arquivo manualmente nas configurações de regra da tarefa.

Tabela 53. Marcadores de operação do arquivo

ID de operações de arquivos	Marcador de operações de arquivos	Sistemas de arquivos compatíveis
BASIC_INFO_CHANGE	Os atributos ou marcadores de tempo de um arquivo ou pasta foram alterados	NTFS, ReFS
COMPRESSION_CHANGE	A compactação de um arquivo ou pasta foi alterada	NTFS, ReFS
DATA_EXTEND	O tamanho de um arquivo ou pasta foi aumentado	NTFS, ReFS
DATA_OVERWRITE	Os dados em um arquivo ou pasta foram substituídos	NTFS, ReFS
DATA_TRUNCATION	Arquivo ou pasta truncados	NTFS, ReFS
EA_CHANGE	Os atributos do arquivo ou pasta estendidos foram alterados	Somente NTFS
ENCRYPTION_CHANGE	O status de criptografia de um arquivo ou pasta foi alterado	NTFS, ReFS
FILE_CREATE	Arquivo ou pasta criados pela primeira vez	NTFS, ReFS
FILE_DELETE	O arquivo ou a pasta foi permanentemente excluído usando a combinação SHIFT+DEL	NTFS, ReFS
HARD_LINK_CHANGE	Conexão física criada ou excluída para o arquivo ou pasta	Somente NTFS

ID de operações de arquivos	Marcador de operações de arquivos	Sistemas de arquivos compatíveis
INDEXABLE_CHANGE	O status de indexação de um arquivo ou pasta foi alterado	NTFS, ReFS
INTEGRITY_CHANGE	O atributo de integridade foi alterado para um fluxo de arquivo nomeado	Somente ReFS
NAMED_DATA_EXTEND	O tamanho de um fluxo de arquivo nomeado foi aumentado	NTFS, ReFS
NAMED_DATA_OVERWRITE	Fluxo do arquivo nomeado substituído	NTFS, ReFS
NAMED_DATA_TRUNCATION	Fluxo do arquivo nomeado truncado	NTFS, ReFS
OBJECT_ID_CHANGE	Identificador de arquivo ou pasta alterado	NTFS, ReFS
RENAME_NEW_NAME	Novo nome atribuído ao arquivo ou à pasta	NTFS, ReFS
REPARSE_POINT_CHANGE	O novo ponto de reanálise criado ou existente alterado para um arquivo ou pasta	NTFS, ReFS
SECURITY_CHANGE	Direitos de acesso de arquivo ou pasta alterados	NTFS, ReFS
STREAM_CHANGE	Nova fluxo de arquivo nomeado criado ou existente alterado	NTFS, ReFS
TRANSACTED_CHANGE	Fluxo de arquivo nomeado alterado pela transação TxF	Somente ReFS

Configurações padrão da tarefa de Monitor de Integridade de Arquivos

Por padrão, a tarefa de Monitor de integridade de arquivos possui as configurações descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Tabela 54. Configurações padrão da tarefa de Monitor de Integridade de Arquivos

Configuração	Valor padrão	Descrição
Escopo de monitoramento	Não configurado	É possível especificar as pastas e os arquivos para os quais as ações serão monitoradas. Os eventos de monitoramento serão gerados para as pastas e os arquivos no escopo de monitoramento especificado.

Configuração	Valor padrão	Descrição
Lista de usuários confiáveis	Não configurado	É possível especificar usuários e/ou grupos de usuários cujas ações nas pastas especificadas serão tratadas como seguras pelo componente.
Monitorar operações de arquivos quando a tarefa não for executada	Usada	É possível ativar ou desativar o registro de operações de arquivos em log executadas nos escopos de monitoramento indicados durante os períodos em que a tarefa não está sendo executada.
Excluir as seguintes pastas do controle	Não aplicado	É possível verificar o uso de exclusões das pastas onde as operações de arquivos não precisam ser monitoradas. Quando a tarefa Monitor de Integridade de Arquivos for executada, o Kaspersky Embedded Systems Security ignorará os escopos de monitoramento especificados como exclusões.
Cálculo da soma de verificação	Não aplicado	É possível configurar o cálculo da soma de verificação de arquivo depois que as alterações no arquivo forem feitas.
Considerar marcadores de operação do arquivo	Todos os marcadores de operação do arquivo disponíveis serão considerados	É possível especificar o conjunto de marcadores de operação do arquivo. Se uma operações de arquivos executada em um escopo de monitoramento for caracterizada por um ou mais marcadores especificados, ao Kaspersky Embedded Systems Security gerará um evento de auditoria.
Programação de inicialização da tarefa	A primeira execução não está programada	Você pode definir as configurações de inicialização programada da tarefa.

Gerenciamento do Monitor de Integridade de Arquivos por meio do Plug-in de Administração

Nesta seção, aprenda como configurar a tarefa de Monitor de Integridade de Arquivos por meio do Plug-in de Administração.

Nesta seção

Definição de configurações da tarefa Monitor de Integridade de Arquivos 381

Configuração de regras de monitoramento 382

Definição de configurações da tarefa Monitor de Integridade de Arquivos

Para definir as configurações gerais da tarefa Monitor de Integridade de Arquivos, implemente as seguintes etapas:

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
4. Na seção **Inspeção do sistema** no bloco **Monitor de Integridade de Arquivos**, clique no botão **Configurações**.

   A janela do **Monitor de Integridade de Arquivos** é aberta.
5. Na guia **Configurações de monitoramento de operações de arquivos**, na janela que se abre, defina as configurações do escopo de monitoramento:
   a. Desmarque ou marque a caixa de seleção **informações de log sobre operações de arquivos que aparecem durante o período de interrupção do monitoramento**.

      A caixa de seleção ativa ou desativa o monitoramento das operações de arquivos especificadas nas configurações da tarefa Monitor de Integridade de Arquivos quando a tarefa não estiver sendo executada por alguma razão (remoção de um disco rígido, tarefa interrompida pelo usuário, erro de software).

      Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security registrará eventos em todos os escopos de monitoramento quando a tarefa Monitor de Integridade de Arquivos não estiver sendo executada.

      Se a caixa de seleção for desmarcada, o aplicativo não registrará em log operações de arquivos em escopos de monitoramento quando a tarefa não estiver sendo executada.

      A caixa de seleção é selecionada por padrão.

   b. Adicione os escopos de monitoramento (consulte a seção "Configuração de regras de monitoramento" na página 382) a ser controlados pela tarefa.
6. Na guia **Gerenciamento da tarefa**, configure os parâmetros de inicialização da tarefa com base em uma programação (consulte a seção "Gerenciamento de programações de tarefas" na página 130).
7. Clique em **OK** para salvar as alterações.

Configuração de regras de monitoramento

É possível alterar as configurações padrão da tarefa de Monitor de Integridade de Arquivos (consulte a tabela abaixo).

Tabela 55. Configurações padrão da tarefa de Monitor de Integridade de Arquivos

Configuração	Valor padrão	Descrição
Escopo de monitoramento	Não configurado	É possível especificar as pastas e os arquivos para os quais as ações serão monitoradas. Os eventos de monitoramento serão gerados para as pastas e os arquivos no escopo de monitoramento especificado.
Lista de usuários confiáveis	Não configurado	É possível especificar usuários e/ou grupos de usuários cujas ações nas pastas especificadas serão tratadas como seguras pelo componente.
Monitorar operações de arquivos quando a tarefa não for executada	Usada	É possível ativar ou desativar o registro de operações de arquivos em log executadas nos escopos de monitoramento indicados durante os períodos em que a tarefa não está sendo executada.
Excluir as seguintes pastas do controle	Não aplicado	É possível verificar o uso de exclusões das pastas onde as operações de arquivos não precisam ser monitoradas. Quando a tarefa Monitor de Integridade de Arquivos for executada, o Kaspersky Embedded Systems Security ignorará os escopos de monitoramento especificados como exclusões.
Cálculo da soma de verificação	Não aplicado	É possível configurar o cálculo da soma de verificação de arquivo depois que as alterações no arquivo forem feitas.
Considerar marcadores de operação do arquivo	Todos os marcadores de operação do arquivo disponíveis serão considerados	É possível especificar o conjunto de marcadores de operação do arquivo. Se uma operações de arquivos executada em um escopo de monitoramento for caracterizada por um ou mais marcadores especificados, ao Kaspersky Embedded Systems Security gerará um evento de auditoria.
Programação de inicialização da tarefa	A primeira execução não está programada	Você pode definir as configurações de inicialização programada da tarefa.

► *Para adicionar um escopo de monitoramento, execute estas etapas:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas**

e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).

- Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

> Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

4. Na seção **Inspeção do sistema** no bloco **Monitor de Integridade de Arquivos**, clique no botão **Configurações**.

   A janela **Propriedades: Monitor de Integridade de Arquivos** é aberta.

5. Na seção **Escopo de monitoramento**, clique no botão **Adicionar**.

   A janela **escopo de monitoramento** é aberta.

6. Adicione um escopo de monitoramento de uma das seguintes formas:

   - Se quiser selecionar pastas através da caixa de diálogo padrão do Microsoft Windows:

     a. Clique no botão **Procurar**.

        A janela padrão Procurar Pasta do Microsoft Windows é aberta.

     b. Na janela exibida, selecione a pasta para a qual deseja monitorar operações e clique no botão **OK**.

   - Se quiser especificar um escopo de monitoramento manualmente, adicione um caminho usando uma máscara com suporte:

     - <*.ext> - todos os arquivos com a extensão <ext>, independentemente da sua localização;
     - <*\nome.ext> - todos os arquivos com o nome <nome> e a extensão <ext>, independentemente da sua localização;
     - <\dir*> - todos os arquivos na pasta <\dir>;
     - <\dir*\nome.ext> - todos os arquivos com o nome <nome> e a extensão <ext> na pasta <\dir> e todas as subpastas.

> Ao especificar um escopo de monitoramento manualmente, certifique-se de que o caminho esteja no seguinte formato: <letra do volume>: \<máscara>. Se a letra do volume estiver faltando, o Kaspersky Embedded Systems Security não adicionará o escopo de monitoramento especificado.

7. Na guia **Usuários confiáveis**, clique no botão **Adicionar**.

   A janela **Selecionar usuários ou grupos** padrão do Microsoft Windows é exibida.

8. Selecione os usuários ou grupos de usuários para os quais as operações de arquivos são permitidas no escopo de monitoramento selecionado e clique em **OK**.

> Por padrão, o Kaspersky Embedded Systems Security trata todos os usuários que não estejam na lista de usuários confiáveis como não confiáveis (consulte a seção "Sobre regras de monitoramento de operações de arquivos" na página 377), e gera eventos críticos para eles.

9. Selecione a guia **Marcadores de operação do arquivo**.
10. Se necessário, realize as ações a seguir para selecionar um número de marcadores:
    a. Selecione a opção **Detectar operações de arquivos com base nos seguintes marcadores**.
    b. Na lista de operações de arquivos disponíveis (consulte a seção "Sobre regras de monitoramento de operações de arquivos" na página 377), selecione as caixas ao lado das operações que deseja monitorar.

    Por padrão, o Kaspersky Embedded Systems Security detecta todos os marcadores de operação do arquivo, a opção **Detectar operações de arquivos com base em todos os marcadores reconhecíveis** está marcada.

11. Se quiser que o Kaspersky Embedded Systems Security calcule a soma de verificação de arquivos após a operação ser realizada, faça o seguinte:
    a. Selecione **Calcular a soma de verificação do arquivo, se possível. A soma de verificação estará disponível para visualização na** caixa de seleção **do relatório de tarefa**.

        Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security calculará a soma de verificação do arquivo modificado, onde a operações de arquivos com pelo menos um marcador selecionado tenha sido detectado.

        Se a operações de arquivos for detectada por um número de marcadores, apenas a soma de verificação do arquivo final após todas as modificações será calculada.

        Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security não calculará a soma de verificação para os arquivos modificados.

        Nenhum cálculo da soma de verificação será realizado nos casos a seguir:

        - Se o arquivo ficar indisponível (por exemplo, devido à modificação de permissões de acesso).
        - Se a operações de arquivos for detectada no arquivo que foi removido posteriormente.

        Esta caixa é desmarcada por padrão.

    b. Na lista suspensa **Calcule a soma de verificação usando o algoritmo**, selecione uma das opções:
        - **Hash MD5**
        - **Hash SHA256**

12. Se não quiser monitorar todas as operações de arquivos na lista de operações de arquivos disponíveis (consulte a seção "Sobre regras de monitoramento de operações de arquivos" na página 377), marque as caixas de seleção ao lado das operações que deseja monitorar.
13. Se necessário, adicione escopos de monitoramento realizando as seguintes etapas:
    a. Selecione a guia **Exclusões**.
    b. Marque a caixa de seleção **Excluir as seguintes pastas do controle**.

        A caixa de seleção desativa o uso de exclusões para pastas em que as operações de arquivos não precisam ser monitoradas.

        Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security ignorará os escopos de monitoramento especificados na lista de exclusões quando a tarefa Monitor de Integridade de Arquivos não for executada.

Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security registrará eventos para todos os escopos de monitoramento especificados.

Por padrão, a caixa de seleção está desmarcada e a lista de exclusão, vazia.

c. Clique no botão **Adicionar**.

A janela **Selecionar pasta para adicionar** é aberta.

d. Na janela exibida, especifique a pasta que deseja excluir do escopo de monitoramento.

e. Clique em **OK**.

A pasta especificada é adicionada à lista de escopos excluídos.

14. Clique em **OK** na janela **Regras de monitoramento de operações de arquivos**.

As configurações da regra especificada serão aplicadas ao escopo de monitoramento selecionado da tarefa de Monitor de Integridade de Arquivos.

Gerenciamento do Monitor de Integridade de Arquivos por meio do Console do Aplicativo

Nesta seção, aprenda como configurar a tarefa de Monitor de Integridade de Arquivos por meio do Console do Aplicativo.

Nesta seção

Definição de configurações da tarefa Monitor de Integridade de Arquivos 385

Configuração de regras de monitoramento 386

Definição de configurações da tarefa Monitor de Integridade de Arquivos

► *Para definir as configurações gerais da tarefa Monitor de Integridade de Arquivos, implemente as seguintes etapas:*

1. Na árvore do Console do Aplicativo, expanda o nó **Inspeção do sistema**.
2. Selecione o nó filho **Monitor de Integridade de Arquivos**.
3. Clique no link **Propriedades** no painel de detalhes do nó **Monitor de Integridade de Arquivos**.

A janela **Configurações de tarefa** é exibida.

4. Na janela aberta, na guia **Geral**, desmarque ou selecione a caixa de seleção **Informações de log sobre operações de arquivos que aparecem durante o período de interrupção do monitoramento**.

A caixa de seleção ativa ou desativa o monitoramento das operações de arquivos especificadas nas configurações da tarefa Monitor de Integridade de Arquivos quando a tarefa não estiver sendo executada por alguma razão (remoção de um disco rígido, tarefa interrompida pelo usuário, erro de software).

Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security registrará

eventos em todos os escopos de monitoramento quando a tarefa Monitor de Integridade de Arquivos não estiver sendo executada.

Se a caixa de seleção for desmarcada, o aplicativo não registrará em log operações de arquivos em escopos de monitoramento quando a tarefa não estiver sendo executada.

A caixa de seleção é selecionada por padrão.

5. Nas guias **Programação** e **Avançado**, configure a programação de início da tarefa (consulte a seção "Gerenciando programações de tarefas" na página 130).
6. Clique em **OK** para salvar as alterações.

Configuração de regras de monitoramento

É possível alterar as configurações padrão da tarefa de Monitor de Integridade de Arquivos (consulte a tabela abaixo).

Tabela 56. Configurações padrão da tarefa de Monitor de Integridade de Arquivos

Configuração	Valor padrão	Descrição
Escopo de monitoramento	Não configurado	É possível especificar as pastas e os arquivos para os quais as ações serão monitoradas. Os eventos de monitoramento serão gerados para as pastas e os arquivos no escopo de monitoramento especificado.
Lista de usuários confiáveis	Não configurado	É possível especificar usuários e/ou grupos de usuários cujas ações nas pastas especificadas serão tratadas como seguras pelo componente.
Monitorar operações de arquivos quando a tarefa não for executada	Usada	É possível ativar ou desativar o registro de operações de arquivos em log executadas nos escopos de monitoramento indicados durante os períodos em que a tarefa não está sendo executada.
Excluir as seguintes pastas do controle	Não aplicado	É possível verificar o uso de exclusões das pastas onde as operações de arquivos não precisam ser monitoradas. Quando a tarefa Monitor de Integridade de Arquivos for executada, o Kaspersky Embedded Systems Security ignorará os escopos de monitoramento especificados como exclusões.
Cálculo da soma de verificação	Não aplicado	É possível configurar o cálculo da soma de verificação de arquivo depois que as alterações no arquivo forem feitas.
Considerar marcadores de operação do arquivo	Todos os marcadores de operação do arquivo disponíveis serão considerados	É possível especificar o conjunto de marcadores de operação do arquivo. Se uma operações de arquivos executada em um escopo de monitoramento for caracterizada por um ou mais marcadores especificados, ao Kaspersky Embedded Systems Security gerará um evento de auditoria.

Configuração	Valor padrão	Descrição
Programação de inicialização da tarefa	A primeira execução não está programada	Você pode definir as configurações de inicialização programada da tarefa.

► *Para adicionar um escopo de monitoramento, execute estas etapas:*

1. Na árvore do Console do Aplicativo, expanda o nó **Inspeção do sistema**.
2. Selecione o nó filho **Monitor de Integridade de Arquivos**.
3. Clique no link **Regras de monitoramento de operações de arquivos** no painel de detalhes do nó **Monitor de Integridade de Arquivos**.

   A janela **Monitoramento das operações do arquivo** é aberta.
4. Adicione um escopo de monitoramento de uma das seguintes formas:
   - Se quiser selecionar pastas através da caixa de diálogo padrão do Microsoft Windows:
     a. No lado esquerdo da janela, clique no botão **Procurar**.

        A janela padrão **Procurar Pasta** do Microsoft Windows é aberta.
     b. Na janela exibida, selecione a pasta para a qual deseja monitorar operações e clique no botão **OK**.
     c. Clique o botão **Adicionar** para que o Kaspersky Embedded Systems Security comece a monitorar as operações de arquivos no escopo de monitoramento indicado.
   - Se quiser especificar um escopo de monitoramento manualmente, adicione um caminho usando uma máscara com suporte:
     - <*.ext> - todos os arquivos com a extensão <ext>, independentemente da sua localização;
     - <*\nome.ext> - todos os arquivos com o nome <nome> e a extensão <ext>, independentemente da sua localização;
     - <\dir*> - todos os arquivos na pasta <\dir>;
     - <\dir*\nome.ext> - todos os arquivos com o nome <nome> e a extensão <ext> na pasta <\dir> e todas as subpastas.

   Ao especificar um escopo de monitoramento manualmente, certifique-se de que o caminho esteja no seguinte formato: <letra do volume>: \<máscara>. Se a letra do volume estiver faltando, o Kaspersky Embedded Systems Security não adicionará o escopo de monitoramento especificado.

   No lado direito da janela, a guia **Descrição da regra** exibe os usuários confiáveis e marcadores de operação do arquivo selecionados para este escopo de monitoramento.
5. Na lista de escopos de monitoramento adicionados, selecione as configurações cujo escopo você deseja definir.
6. Selecione a guia **Usuários confiáveis**.
7. Clique no botão **Adicionar**.

   A janela **Selecionar usuários ou grupos** padrão do Microsoft Windows é exibida.
8. Selecione os usuários ou grupos que o Kaspersky Embedded Systems Security considerará confiável para o escopo de monitoramento selecionado.

9. Clique em **OK**.

> Por padrão, o Kaspersky Embedded Systems Security trata todos os usuários que não estejam na lista de usuários confiáveis como não confiáveis (consulte a seção "Sobre regras de monitoramento de operações de arquivos" na página 377), e gera eventos críticos para eles.

10. Selecione a guia **Definir marcadores de operação do arquivo**.
11. Se necessário, realize as ações a seguir para selecionar um número de marcadores:
    a. Selecione a opção **Detectar operações de arquivos com base nos seguintes marcadores**.
    b. Na lista de operações de arquivos disponíveis (consulte a seção "Sobre regras de monitoramento de operações de arquivos" na página 377), selecione as caixas ao lado das operações que deseja monitorar.

> Por padrão, o Kaspersky Embedded Systems Security detecta todos os marcadores de operação do arquivo, a opção **Detectar operações de arquivos com base em todos os marcadores reconhecíveis** está marcada.

12. Se quiser que o Kaspersky Embedded Systems Security calcule a soma de verificação de arquivos após a operação ser realizada, faça o seguinte:
    a. Na seção **Cálculo da soma de verificação**, marque a caixa de seleção **Calcular a soma de verificação para uma versão final de arquivo, após o arquivo ter sido alterado, se possível**.

       Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security calculará a soma de verificação do arquivo modificado, onde a operações de arquivos com pelo menos um marcador selecionado tenha sido detectado.

       Se a operações de arquivos for detectada por um número de marcadores, apenas a soma de verificação do arquivo final após todas as modificações será calculada.

       Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security não calculará a soma de verificação para os arquivos modificados.

       Nenhum cálculo da soma de verificação será realizado nos casos a seguir:

       - Se o arquivo ficar indisponível (por exemplo, devido à modificação de permissões de acesso).
       - Se a operações de arquivos for detectada no arquivo que foi removido posteriormente.

       Esta caixa é desmarcada por padrão.

    b. Na lista suspensa **Calcule a soma de verificação usando o algoritmo**, selecione uma das opções:
       - **Hash MD5**.
       - **Hash SHA256**.
13. Se necessário, adicione escopos de monitoramento realizando as seguintes etapas:
    a. Selecione a guia **Definir exclusões**.
    b. Marque a caixa de seleção **Considere o escopo de monitoramento excluído**.

       A caixa de seleção desativa o uso de exclusões para pastas em que as operações de arquivos não precisam ser monitoradas.

Se a caixa de seleção for marcada, o Kaspersky Embedded Systems Security ignorará os escopos de monitoramento especificados na lista de exclusões quando a tarefa Monitor de Integridade de Arquivos não for executada.

Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security registrará eventos para todos os escopos de monitoramento especificados.

Por padrão, a caixa de seleção está desmarcada e a lista de exclusão, vazia.

c. Clique no botão **Procurar**.

A janela padrão **Procurar Pasta** do Microsoft Windows é aberta.

d. Na janela exibida, especifique a pasta que deseja excluir do escopo de monitoramento.

e. Clique em **OK**.

f. Clique no botão **Adicionar**.

A pasta especificada é adicionada à lista de escopos excluídos.

> Também é possível adicionar escopos de monitoramento excluídos manualmente usando as mesmas máscaras utilizadas para especificar os escopos de monitoramento.

14. Clique no botão **Salvar** para aplicar a nova configuração de regra.

Inspeção de Log

Esta seção contém informações sobre a tarefa de Inspeção de Log e definição de configurações de tarefa.

Neste capítulo

Sobre a tarefa de Inspeção de Log 390
Configurações padrão da tarefa de Inspeção de Log 391
Gerenciamento das regras de inspeção de log por meio do Plug-in de Administração 392
Gerenciamento das regras de inspeção de log por meio do Console do Aplicativo 395

Sobre a tarefa de Inspeção de Log

Quando a tarefa de Inspeção de Log é executada, o Kaspersky Embedded Systems Security, monitora a integridade do ambiente protegido com base nos resultados de uma inspeção dos Logs de Eventos do Windows. O aplicativo notifica o administrador quando detecta um comportamento anormal no sistema, que pode ser uma indicação de tentativas de ataques cibernéticos.

O Kaspersky Embedded Systems Security considera os logs de eventos do Windows e identifica violações com base nas regras especificadas por um usuário ou pelas configurações do analisador heurístico, que é utilizado pela tarefa para inspecionar logs.

Regras predefinidas e análise heurística

É possível utilizar a tarefa de Inspeção de Log para monitorar o estado do sistema protegido com base na heurística existente. O analisador heurístico identifica atividade anormal no computador protegido, o que pode ser uma evidência de tentativa de ataque. Modelos para identificar comportamento anormal estão incluídos nas regras disponíveis nas configurações de regras predefinidas.

Sete regras estão incluídas na lista de regras da tarefa de Inspeção de Log. Você pode ativar ou desativar o uso de qualquer uma dessas regras. Não é possível eliminar as regras existentes ou criar novas regras.

É possível configurar critérios para acionamento de regras que monitoram eventos para as seguintes operações:

- Detecção de ataque de força bruta de senha
- Detecção de login na rede

Também é possível configurar exclusões nas configurações da tarefa. O analisador heurístico não é ativado quando um login é realizado por um usuário confiável ou a partir de um endereço IP confiável.

O Kaspersky Embedded Systems Security não usa a heurística para inspecionar os logs do Windows se o analisador heurístico não for usado pela tarefa. Por padrão, o analisador heurístico fica ativo.

Quando as regras são aplicadas, o aplicativo registra um *Evento crítico* no log de tarefas de Inspeção de Log.

Regras personalizadas para a tarefa de Inspeção de Log

Você pode usar as configurações de regra de tarefa para especificar e alterar os critérios para as regras de acionamento após a detecção de eventos selecionados no log especificado do Windows. Por padrão, a lista das regras da tarefa de Inspeção de Log contém quatro regras. Você pode ativar e desativar o uso dessas regras, removê-las e editar suas configurações.

Você pode configurar os seguintes critérios para acionamento de regras para cada uma delas:

- Lista de identificadores no Log de Eventos do Windows.

  A regra é acionada quando um novo registro é criado no Log de Eventos do Windows, se as propriedades de eventos incluírem um identificador de evento especificado para a regra. Também é possível adicionar e remover identificadores para cada regra especificada.

- Fonte de evento.

  Para cada regra, é possível definir um sublog do Log de Eventos do Windows. O aplicativo procurará registros com os identificadores de evento especificados apenas nesse sublog. Você pode selecionar um dos sublogs padrão (Aplicativo, Segurança ou Sistema), ou especificar um sublog personalizado digitando o nome no campo de seleção de fonte.

  O aplicativo não verifica se o sublog especificado realmente existe no Log de Eventos do Windows.

Quando a regra é acionada, o Kaspersky Embedded Systems Security registra um Evento crítico no log de tarefas de Inspeção de Log.

Por padrão, a tarefa de Inspeção de Log aplica regras personalizadas.

Antes de iniciar a tarefa de Inspeção de Log certifique-se de que a política de auditoria do sistema esteja configurada corretamente. Consulte o artigo da Microsoft https://technet.microsoft.com/en-us/library/cc952128.aspx para detalhes.

Configurações padrão da tarefa de Inspeção de Log

Por padrão, a tarefa de Inspeção de Log possui as configurações descritas na tabela abaixo. Você pode alterar os valores destas configurações.

Tabela 57. Configurações padrão da tarefa de Monitor de Integridade de Arquivos

Configuração	Valor padrão	Descrição
Aplicar regras personalizadas para a Inspeção de Log	Aplicada.	Você pode ativar, desativar, adicionar ou alterar as regras personalizadas.
Aplicar regras predefinidas para a Inspeção de Log	Aplicada.	Você pode ativar ou desativar o analisador heurístico, que detecta atividades anormais no servidor protegido.

Configuração	Valor padrão	Descrição
Detecção de ataque de força bruta	10 falhas de login por 300 segundos.	É possível definir o número de tentativas e um período quando essas tentativas ocorreram, que serão considerados como acionadores para o analisador heurístico.
Login da rede	0:00:00.	É possível indicar o início e o fim do intervalo de tempo durante o qual o Kaspersky Embedded Systems Security encara tentativas de conexão como atividades anormais.
Exclusões	Não aplicado.	Você pode especificar usuários e endereços IP que não acionarão o analisador heurístico.
Programação de inicialização da tarefa	A primeira execução não está programada.	Você pode definir as configurações de inicialização programada da tarefa.

Gerenciamento das regras de inspeção de log por meio do Plug-in de Administração

Nesta seção, aprenda como adicionar e configurar regras de inspeção de log por meio do Plug-in de Administração.

Nesta seção

Gerenciamento de regras de tarefa predefinidas por meio do Plug-in de Administração 392

Adicionando regras de inspeção de log por meio do Plug-in de Administração 394

Gerenciamento de regras de tarefa predefinidas por meio do Plug-in de Administração

► *Realize as seguintes ações para configurar regras predefinidas para a tarefa de Inspeção de Log:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.

4. Na seção **Inspeção do sistema**, clique no botão **Configurações** no bloco **Inspeção de Log**.

   A janela **Inspeção de Log** é exibida.

5. Selecione a guia **Regras predefinidas**.
6. Marque ou desmarque a caixa de seleção **Aplicar regras personalizadas para Inspeção de log**.

   Se esta caixa de seleção for marcada, o Kaspersky Embedded Systems Security aplicará o analisador heurístico para detectar atividade anormal no computador protegido.

   Se esta caixa de seleção for desmarcada, o analisador heurístico será executado e o Kaspersky Embedded Systems Security aplicará as regras predefinidas ou personalizadas para detectar uma atividade anormal.

   A caixa de seleção é selecionada por padrão.

Para que a tarefa seja executada, pelo menos uma regra de inspeção de log deve ser selecionada.

7. Selecione as regras que deseja aplicar, na lista de regras predefinidas:
   - Existem padrões de um possível ataque de força bruta no sistema.
   - Existem padrões de uma possível violação no Log de Eventos do Windows.
   - Ações atípicas detectadas em nome de um novo serviço instalado.
   - Detectado login atípico que usa credenciais explícitas.
   - Existem padrões de um possível ataque PAC se passando por Kerberos (MS14-068) no sistema.
   - Ações atípicas detectadas, direcionadas a Administradores do grupo integrado privilegiado.
   - Foi detectada uma atividade atípica durante uma sessão de login na rede.
8. Para configurar as regras selecionadas, clique no botão **Configurações avançadas**.

   A janela **Inspeção de Log** é exibida.

9. Na seção **Detecção de ataque de força bruta**, defina o número de tentativas e um período quando essas tentativas ocorreram, que serão considerados como acionadores para o analisador heurístico.
10. Na seção **Detecção de login de rede**, indique a início e o fim do intervalo de tempo durante o qual o Kaspersky Embedded Systems Security encara tentativas de conexão como atividades anormais.
11. Selecione a guia **Exclusões**.
12. Execute as seguintes ações para adicionar usuários confiáveis:
    a. Clique no botão **Procurar**.
    b. Selecione um usuário.
    c. Clique em **OK**.

       Um usuário selecionado é adicionado à lista de usuários confiáveis.
13. Execute as seguintes ações para adicionar endereços IP confiáveis:

a. Insira o endereço IP.

b. Clique no botão **Adicionar**.

14. Um endereço IP inserido é adicionado à lista de endereços IP confiáveis.
15. Na guia **Gerenciamento da tarefa** configure a programação de inicialização da tarefa (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 130).
16. Clique em **OK**.

A configuração da tarefa de Inspeção de Log é salva.

Adicionando regras de inspeção de log por meio do Plug-in de Administração

► *Execute as seguintes ações para adicionar e configurar uma nova regra personalizada de Inspeção de log:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar as configurações do aplicativo.
3. Execute uma das seguintes ações no painel de detalhes do grupo de administração selecionado:
   - Para definir as configurações do aplicativo para um grupo de computadores, selecione a guia **Políticas** e abra a janela **Propriedades: <Nome da política>** (consulte a seção "Configuração de políticas" na página 115).
   - Para configurar o aplicativo para um único computador, selecione a guia **Dispositivos** e abra a janela **Configurações do aplicativo** (consulte a seção "Definição de tarefas locais na janela Configurações do aplicativo do Kaspersky Security Center" na página 119).

     Se uma política ativa do Kaspersky Security Center for aplicada a um dispositivo e esta política bloquear alterações às configurações do aplicativo, então estas configurações não poderão ser editadas na janela **Configurações do aplicativo**.
4. Na seção **Inspeção do sistema**, clique no botão **Configurações** no bloco **Inspeção de Log**.

   A janela **Inspeção de Log** é exibida.
5. Na guia **Regras personalizadas**, marque ou desmarque a caixa de seleção **Aplicar regras personalizadas para inspeção de log**.

   Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security aplicará regras personalizadas à Inspeção de Log segundo as configurações de cada regra. É possível adicionar, remover ou configurar regras de Inspeção de Log.

   Se a caixa de seleção for desmarcada, você não poderá adicionar ou modificar as regras personalizadas. O Kaspersky Embedded Systems Security aplica as configurações de regras padrão.

   A caixa de seleção é selecionada por padrão. Apenas a regra de Detecção de pop-up do aplicativo está ativa.

É possível controlar se as regras predefinidas serão aplicadas à Inspeção de Log. Marque as caixas de seleção correspondentes às regras que deseja aplicar à Inspeção de Log.

6. Para adicionar uma nova regra personalizada, clique no botão **Adicionar**.

   A janela **Regras de inspeção de log** é exibida.

7. Na seção **Geral**, insira as seguintes informações sobre a nova regra:

   - **Nome da regra**
   - **Origem**

     Selecione um log de origem para usar eventos registrados para a análise. Os seguintes tipos de log de eventos do Windows estão disponíveis:

     - Aplicativo
     - Segurança
     - Sistema

     Você pode adicionar um novo log personalizado inserindo o nome do log no campo **Origem**.

8. Na seção **ID de eventos acionados**, especifique os IDs do item que acionará a regra na detecção:

   a. Insira um valor numérico para os IDs.

   b. Clique no botão **Adicionar**.

      Um ID de regra selecionado é adicionado à lista. É possível adicionar um número ilimitado de identificadores para cada regra.

   c. Clique em **OK**.

   A regra de Inspeção de Log é adicionada à lista de regras.

Gerenciamento das regras de inspeção de log por meio do Console do Aplicativo

Nesta seção, aprenda como adicionar e configurar regras de inspeção de log por meio do Console do Aplicativo.

Nesta seção

Gerenciamento de regras de tarefa predefinidas por meio do Console do Aplicativo 396

Configuração de regras de Inspeção de Log 397

Gerenciamento de regras de tarefa predefinidas por meio do Console do Aplicativo

► *Realize as seguintes ações para configurar o analisador heurístico para a tarefa de Inspeção de Log:*

1. Na árvore do Console do Aplicativo, expanda o nó **Inspeção do sistema**.
2. Selecione o nó filho **Inspeção de Log**.
3. Clique no link **Propriedades** no painel de detalhes do nó **Inspeção de Log**.

   A janela **Configurações de tarefa** é exibida.
4. Selecione a guia **Regras predefinidas**.
5. Marque ou desmarque a caixa de seleção **Aplicar regras personalizadas para Inspeção de log**.

   Se esta caixa de seleção for marcada, o Kaspersky Embedded Systems Security aplicará o analisador heurístico para detectar atividade anormal no computador protegido.

   Se esta caixa de seleção for desmarcada, o analisador heurístico será executado e o Kaspersky Embedded Systems Security aplicará as regras predefinidas ou personalizadas para detectar uma atividade anormal.

   A caixa de seleção é selecionada por padrão.

   Para que a tarefa seja executada, pelo menos uma regra de inspeção de log deve ser selecionada.
6. Selecione as regras que deseja aplicar, na lista de regras predefinidas:
   - Existem padrões de um possível ataque de força bruta no sistema.
   - Existem padrões de uma possível violação no Log de Eventos do Windows.
   - Ações atípicas detectadas em nome de um novo serviço instalado.
   - Detectado login atípico que usa credenciais explícitas.
   - Existem padrões de um possível ataque PAC se passando por Kerberos (MS14-068) no sistema.
   - Ações atípicas detectadas, direcionadas a Administradores do grupo integrado privilegiado.
   - Foi detectada uma atividade atípica durante uma sessão de login na rede.
7. Para configurar as regras selecionadas, vá até a guia **Estendido**.
8. Na **Detecção de ataque de força bruta**, defina o número de tentativas e um período quando essas tentativas ocorreram, que serão considerados como acionadores para a análise heurística.
9. Na seção **Login da rede**, indique o início e o fim do intervalo de tempo durante o qual o Kaspersky Embedded Systems Security encara tentativas de conexão como atividades anormais.
10. Selecione a guia **Exclusões**.
11. Execute as seguintes ações para adicionar usuários confiáveis:
    a. Clique no botão **Procurar**.
    b. Selecione um usuário.
    c. Clique em **OK**.

       Um usuário selecionado é adicionado à lista de usuários confiáveis.

12. Execute as seguintes ações para adicionar endereços IP confiáveis:
    a. Insira o endereço IP.
    b. Clique no botão **Adicionar**.

       Um endereço IP inserido é adicionado à lista de endereços IP confiáveis.
13. Selecione as guias **Programação** e **Avançado** para configurar a programação de inicialização da tarefa.
14. Clique em **OK**.

    A configuração da tarefa de Inspeção de Log é salva.

Configuração de regras de Inspeção de Log

Execute as seguintes ações para adicionar e configurar uma nova regra personalizada de Inspeção de Log:

1. Na árvore do Console do Aplicativo, expanda o nó **Inspeção do sistema**.
2. Selecione o nó filho **Inspeção de Log**.
3. No painel de detalhes do nó **Inspeção de Log**, clique no link **Regras de Inspeção de Log**.

   A janela **Regras de inspeção de log** é exibida.
4. Marque ou desmarque a caixa de seleção **Aplicar regras personalizadas para a Inspeção de Log**.

   Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security aplicará regras personalizadas à Inspeção de Log segundo as configurações de cada regra. É possível adicionar, remover ou configurar regras de Inspeção de Log.

   Se a caixa de seleção for desmarcada, você não poderá adicionar ou modificar as regras personalizadas. O Kaspersky Embedded Systems Security aplica as configurações de regras padrão.

   A caixa de seleção é selecionada por padrão. Apenas a regra de Detecção de pop-up do aplicativo está ativa.

   É possível controlar se as regras predefinidas serão aplicadas à tarefa de Inspeção de Log. Marque as caixas de seleção correspondentes às regras que deseja aplicar à Inspeção de Log.
5. Para criar uma nova regra personalizada, faça o seguinte:
   a. Digite o nome da nova regra.
   b. Clique no botão **Adicionar**.

      A regra criada é adicionada à lista de regra geral.
6. Para configurar uma regra, siga as etapas a seguir:
   a. Clique com o botão esquerdo para selecionar uma regra na lista.

      Na área direita da janela, a guia **Descrição** exibe as informações gerais sobre a regra.

      A descrição da nova regra está em branco.
   b. Selecione a guia **Descrição da regra**.

c. Na seção **Geral**, edite o nome de regra, se necessário.

d. Selecionar a **Fonte**.

7. Na seção **Identificadores de eventos**, especifique os IDs do item que acionarão a regra na detecção:

a. Insira um valor numérico para os IDs.

b. Clique no botão **Adicionar**.

Um ID de regra selecionado é adicionado à lista. É possível adicionar um número ilimitado de identificadores para cada regra.

c. Clique no botão **Salvar**.

As regras de inspeção de log configuradas serão aplicadas.

Verificação por Demanda

Esta seção fornece informações sobre as tarefas de Verificação por Demanda e instruções sobre a definição de configurações da tarefa de Verificação por Demanda e configurações de segurança no computador protegido.

Neste capítulo

Sobre tarefas de Verificação por Demanda 399
Sobre o escopo da verificação 400
Escopos de verificação predefinidos 401
Verificação de arquivos no armazenamento na nuvem 402
Configurações de segurança do nó selecionado nas tarefas de Verificação por Demanda 404
Sobre os níveis de segurança predefinidos para tarefas de Verificação por Demanda 404
Sobre a Verificação de Unidades Removíveis 406
Configurações padrão das tarefas de Verificação por Demanda 407
Gerenciamento da Verificação por demanda por meio do Plug-in de Administração 409
Gerenciamento da Verificação por demanda por meio do Console do Aplicativo 426

Sobre tarefas de Verificação por Demanda

O Kaspersky Embedded Systems Security verifica a área especificada quanto à existência de vírus e outras ameaças à segurança do computador. O Kaspersky Embedded Systems Security verifica arquivos de computador e a RAM, bem como objetos de execução automática.

O Kaspersky Embedded Systems Security fornece as seguintes tarefas de Verificação por Demanda do sistema:

- A tarefa Verificação na Inicialização do Sistema Operacional é executada sempre que o Kaspersky Embedded Systems Security é iniciado. O Kaspersky Embedded Systems Security verifica setores de inicialização e MBRs dos discos rígidos e removíveis, da memória do sistema e da memória de processos. Cada vez que o Kaspersky Embedded Systems Security executa a tarefa, ele cria uma cópia dos setores de inicialização não infectados. Se, ao executar a tarefa novamente, ele detectar uma ameaça nesses setores, eles serão substituídos pela cópia de backup.
- Por padrão, a tarefa de Verificação de Áreas Críticas é executada semanalmente de acordo com a programação. O Kaspersky Embedded Systems Security verifica objetos em áreas críticas do sistema operacional: objetos de execução automática, setores de inicialização e MBRs dos discos rígidos e removíveis, a memória do sistema e a memória de processos. O aplicativo verifica arquivos nas pastas do sistema, por exemplo, %windir%\system32. O Kaspersky Embedded Systems Security aplica valores de configurações de segurança correspondentes ao nível Recomendado (consulte a seção "Sobre os níveis de segurança predefinidos para tarefas de Verificação por Demanda" na página 404). Você pode modificar as configurações da tarefa de Verificação de Áreas Críticas.
- A tarefa de Verificação da Quarentena é executada por padrão de acordo com a programação após cada atualização dos bancos de dados. O escopo da tarefa de Verificação da Quarentena não podem ser modificadas.

- A tarefa de Controle de Integridade de Aplicativos é executada diariamente. Ela fornece a opção de verificar módulos do Kaspersky Embedded Systems Security quanto à presença de danos ou de modificações. A pasta de instalação do aplicativo é marcada. As estatísticas de execução de tarefa contêm informações sobre o número de módulos verificados e corrompidos. Os valores das configurações de tarefa são definidos por padrão e não podem ser editados. As configurações da programação de inicialização da tarefa podem ser editadas.

Adicionalmente. você pode criar tarefas de Verificação por Demanda personalizadas, por exemplo, uma tarefa para verificar pastas compartilhadas no computador.

O Kaspersky Embedded Systems Security pode executar várias tarefas de Verificação por Demanda simultaneamente.

Sobre o escopo da verificação

Você pode configurar o escopo da verificação para as tarefas de Verificação na Inicialização do Sistema Operacional, de Verificação de Áreas Críticas e de Verificação por Demanda.

Por padrão, as tarefas de Verificação por Demanda verificam todos os objetos do sistema de arquivos do computador. Se não houver requisito de segurança para verificar todos os objetos do sistema de arquivos, você pode limitar a verificação ao escopo da verificação.

No Console do Aplicativo, o escopo da verificação é exibido como uma árvore ou como uma lista dos recursos de arquivos do computador que o Kaspersky Embedded Systems Security pode controlar. Por padrão, os recursos de arquivos de rede do computador protegido são exibidos em um modo de visualização em lista.

► *Para exibir recursos de arquivos de rede no modo de visualização em árvore,*

abra a lista suspensa no setor superior esquerdo da janela de **Configurações do escopo da verificação** e selecione **Visualização em árvore**.

Os nós são exibidos em um modo de visualização em lista ou em árvore dos recursos de arquivo de Computador como se segue:

☑ O nó é incluído no escopo da verificação.

☐ O nó é excluído do escopo da verificação.

☑ Pelo menos um dos nós filhos desse nó é excluído do escopo da verificação ou as configurações de segurança do(s) nó filho(s) são diferentes das desse nó (somente para o modo de visualização em árvore).

O ícone ☑ é exibido se todos os nós filhos forem selecionados, mas se o nó pai não for selecionado. Neste caso, as modificações na composição dos arquivos e das pastas do nó pai são desconsideradas automaticamente quando o escopo da verificação do nó filho selecionado estiver sendo modificado.

Os nomes dos nós virtuais no escopo da verificação são exibidos em azul.

Escopos de verificação predefinidos

A árvore ou a lista de recursos de arquivo de computador para a tarefa de Verificação por Demanda selecionada é exibida na guia **Configurações do escopo da verificação**.

A árvore ou a lista de recursos de arquivos exibem os nós aos quais você tem o acesso à leitura com base nas configurações de segurança definidas do Microsoft Windows.

O Kaspersky Embedded Systems Security contém os escopos de verificação predefinidos a seguir:

- **Meu Computador**. O Kaspersky Embedded Systems Security verifica o computador inteiro.
- **Discos rígidos locais**. O Kaspersky Embedded Systems Security verifica os objetos em um disco rígido de computador. É possível incluir ou excluir do escopo da verificação todos os discos rígidos, discos, pastas ou arquivos individuais.
- **Unidades removíveis**. O Kaspersky Embedded Systems Security verifica arquivos em dispositivos externos, como unidades USB ou em CDs. É possível incluir ou excluir do escopo da verificação todos os discos removíveis, discos, pastas ou arquivos individuais.
- **Rede**. Pastas ou arquivos de rede podem ser adicionados ao escopo da verificação especificando seu caminho no formato UNC (Universal Naming Convention). A conta usada para executar a tarefa deve ter permissões de acesso às pastas e aos arquivos de rede adicionados. Por padrão, as tarefas de Verificação por Demanda são executadas com a conta do sistema.

  As unidades de rede conectadas também não serão exibidas na árvore de recursos de arquivos do computador. Para incluir objetos das unidades de rede no escopo da verificação, especifique o caminho da pasta que corresponde a essa unidade de rede no formato UNC.

- **Memória do sistema**. O Kaspersky Embedded Systems Security verifica os arquivos executáveis e módulos dos processos em execução no sistema operacional quando a verificação é iniciada.
- **Objetos de inicialização**. O Kaspersky Embedded Systems Security verifica objetos aos quais as chaves do registro e os arquivos de configuração se referem, por exemplo, WIN.INI ou SYSTEM.INI, bem como os módulos do aplicativo iniciados automaticamente na inicialização do computador.
- **Pastas compartilhadas**. Você pode incluir pastas compartilhadas no computador protegido no escopo da verificação.
- **Unidades virtuais**. Pastas e arquivos dinâmicos e unidades que são temporariamente conectadas ao computador podem ser incluídas no escopo da verificação, por exemplo, unidades de cluster comuns.

  As unidades virtuais criadas usando o comando SUBST não são exibidas na árvore de recursos de arquivos do computador no Console do Aplicativo. Para verificar objetos em uma unidade virtual, inclua a pasta do computador com a qual essa unidade virtual está associada no escopo da verificação.

Por padrão, você pode visualizar e configurar escopos da verificação predefinidos na árvore de recursos de arquivos de rede; você também pode adicionar escopos predefinidos à lista de recursos de arquivos de rede durante sua formação nas configurações do escopo da verificação.

Por padrão, as tarefas de Verificação por Demanda são executadas nos seguintes escopos:

- Tarefa de Verificação na Inicialização do Sistema operacional:
  - **Discos rígidos locais**
  - **Unidades removíveis**
  - **Memória do sistema**
- Verificação de áreas críticas:
  - **Discos rígidos locais** (excluindo pastas Windows)
  - **Unidades removíveis**
  - **Memória do sistema**
  - **Objetos de inicialização**
- Outras tarefas:
  - **Discos rígidos locais** (excluindo pastas Windows)
  - **Unidades removíveis**
  - **Memória do sistema**
  - **Objetos de inicialização**
  - **Pastas compartilhadas**

Verificação de arquivos no armazenamento na nuvem

Sobre arquivos na nuvem

O Kaspersky Embedded Systems Security pode interagir com arquivos na nuvem do Microsoft OneDrive. O aplicativo é compatível com o novo recurso de Arquivos por Demanda do OneDrive.

O Kaspersky Embedded Systems Security não é compatível com outros armazenamentos na nuvem.

O recurso Arquivos por Demanda do OneDrive ajuda você a acessar todos os seus arquivos no OneDrive sem precisar baixar de todos eles e usar espaço de armazenamento no seu dispositivo. Você pode baixar arquivos no seu disco rígido quando precisar.

Quando o recurso de Arquivos por Demanda do OneDrive estiver ativo, você verá ícones de status ao lado de cada arquivo na coluna **Status** no Explorador de Arquivos. Cada arquivo tem um dos seguintes status:

Este ícone de status indica que o arquivo *está disponível apenas online*. Os arquivos disponíveis apenas online não estão fisicamente armazenados em seu disco rígido. Você não pode abrir arquivos apenas online quando o seu dispositivo não estiver conectado à Internet.

Este ícone de status indica que um arquivo está *disponível localmente*. Isso acontece quando você abre um arquivo disponível apenas online e o baixa para o seu dispositivo. Você pode abrir um arquivo disponível localmente a qualquer momento, mesmo sem acesso à internet. Para limpar espaço, você pode alterar o arquivo novamente para disponível apenas online.

Este ícone de status indica que um arquivo está *armazenado em seu disco rígido e sempre está disponível*.

Verificação de arquivo na nuvem

O Kaspersky Embedded Systems Security só pode verificar arquivos na nuvem armazenados localmente em um computador protegido. Tais arquivos de OneDrive têm o status e . Os arquivos são ignorados durante a verificação, já que não estão fisicamente localizados no computador protegido.

O Kaspersky Embedded Systems Security não baixa automaticamente arquivos da nuvem durante a verificação, mesmo se eles estiverem incluídos no escopo da verificação.

Os arquivos na nuvem são processados por várias tarefas do Kaspersky Embedded Systems Security em vários cenários, dependendo do tipo de tarefa:

- Verificação de arquivos na nuvem em tempo real: você pode adicionar pastas que contêm arquivos na nuvem ao escopo da proteção de tarefa de Proteção de Arquivos em Tempo Real. O arquivo é verificado quando for acessado pelo usuário. Se um arquivo for acessado pelo usuário, ele é baixado, fica localmente disponível e seu status é alterado para . Isso permite que o arquivo seja processado pela tarefa de Proteção de Arquivos em Tempo Real.
- Verificação de arquivos por demanda: você pode adicionar pastas que contêm arquivos na nuvem ao escopo da verificação da tarefa de Verificação por Demanda. A tarefa verifica arquivos com o status e . Se algum arquivo for encontrado no escopo, eles serão ignorados durante a verificação e um evento informativo será registrado no log de tarefas indicando que o arquivo verificado é apenas um marcador de posição para um arquivo na nuvem, e que não existe em uma unidade local.
- Geração e uso de regra de controle do aplicativo: você pode criar regras de permissão e negação para arquivos e usando a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos. A tarefa de Controle de Inicialização de Aplicativos aplica o princípio de Negação padrão e cria regras para processar e bloquear arquivos na nuvem.

  A tarefa de Controle de Inicialização de Aplicativos bloqueia o início de todos os arquivos na nuvem, independentemente do status. Os arquivos não são incluídos no escopo da geração de regra pelo aplicativo, já que não estão fisicamente armazenados em um disco rígido. Já que nenhuma regra de permissão não pode ser criada para tais arquivos, eles ficam sujeitos ao princípio de Negação padrão.

Quando uma ameaça for detectada em um arquivo na nuvem do OneDrive, o aplicativo aplicará a ação especificada nas configurações da tarefa que executa a verificação. Assim, o arquivo pode ser removido, desinfectado, movido para a Quarentena ou gravado em Backup.

As alterações em arquivos locais são sincronizadas com as cópias armazenadas no OneDrive conforme os princípios indicados na documentação relevante do Microsoft OneDrive.

Configurações de segurança do nó selecionado nas tarefas de Verificação por Demanda

Na tarefa de Verificação por Demanda selecionada, os valores padrão das configurações de segurança podem ser modificados definindo-os como configurações comuns para todo o escopo da proteção ou da verificação, ou como configurações diferentes para nós ou itens diferentes na árvore ou lista de recursos de arquivos do computador.

As configurações de segurança definidas para o nó pai selecionado são automaticamente aplicadas a todos os nós filhos. As configurações de segurança do nó pai não são aplicadas a nós filhos configurados separadamente.

As configurações de um escopo de verificação ou escopo da proteção selecionado podem ser definidas usando um dos seguintes métodos:

- Selecione um de três níveis de segurança predefinidos (**Desempenho máximo**, **Recomendado** ou **Proteção máxima**).
- Modifique manualmente as configurações de segurança para os nós ou itens selecionados na árvore ou na lista dos recursos de arquivos do computador (o nível de segurança é alterado para **Personalizado**).

O conjunto de configurações de um nó pode ser salvo em um modelo para ser aplicado posteriormente a outros nós.

Sobre os níveis de segurança predefinidos para tarefas de Verificação por Demanda

As configurações de segurança **Usar a tecnologia iChecker**, **Usar a tecnologia iSwift**, **Usar o analisador heurístico** e **Verificar assinatura da Microsoft nos arquivos** não são incluídas nos níveis de segurança predefinidos. Se o status de configurações como **Usar a tecnologia iChecker**, **Usar a tecnologia iSwift**, **Usar o analisador heurístico** e **Verificar assinatura da Microsoft nos arquivos** for alterado, o nível de segurança predefinido selecionado não será alterado.

Um dos três níveis de segurança predefinidos para o nó selecionado na árvore de recursos de arquivos do computador pode ser aplicado: **Desempenho máximo**, **Recomendado** e **Proteção máxima**. Cada um desses níveis contém seu próprio conjunto de configurações de segurança predefinido (veja a tabela abaixo).

Desempenho máximo

O nível de segurança **Desempenho máximo** é recomendado se, além de usar o Kaspersky Embedded Systems Security nos computadores, existirem medidas de segurança adicionais nos computadores da rede como, por exemplo, firewalls e políticas de segurança existentes.

Recomendado

O nível de segurança **Recomendado** assegura uma combinação ideal de impacto de proteção e desempenho nos computadores protegidos. Esse nível é recomendado pelos especialistas da Kaspersky Lab como suficiente para proteger computadores na maioria das redes corporativas. O nível de segurança **Recomendado** é configurado por padrão.

Proteção máxima

O nível de segurança de **Proteção máxima** é recomendado se a rede da sua organização tiver requisitos elevados

de segurança para seus computadores.

Tabela 58. Níveis de segurança predefinidos e valores de configurações de segurança correspondentes

Opções	Nível de segurança		
	Desempenho máximo	Recomendado	Proteção máxima
Verificar objetos	Por formato	Todos os objetos	Todos os objetos
Verificar apenas arquivos novos e modificados	Ativado	Desativado	Desativado
Ação a ser executada em objetos infectados e outros	Desinfectar. Remover se a desinfecção falhar	Executar ação recomendada (desinfectar. Remover se a desinfecção falhar)	Desinfectar. Remover se a desinfecção falhar
Ação a ser executada em objetos possivelmente infectados	Quarentena	Executar ação recomendada (Quarentena)	Quarentena
Excluir arquivos	Não	Não	Não
Não detectar	Não	Não	Não
Parar a verificação se demorar mais que (s)	60 seg.	Não	Não
Não verificar obj. compostos com mais de (MB)	8 MB	Não	Não
Verificar fluxos NTFS alternativos	Sim	Sim	Sim
Verificar setores de inicialização do disco e MBR	Sim	Sim	Sim

Opções	Nível de segurança		
Verificação de objetos compostos	• Arquivos compactados SFX* • Objetos compactados* • Objetos OLE incorporados* * Somente objetos novos e modificados	• Arquivos compactados* • Arquivos compactados SFX* • Objetos compactados* • Objetos OLE incorporados* * Todos os objetos	• Arquivos compactados* • Arquivos compactados SFX* • Bancos de dados de e-mail* • E-mails sem formatação* • Objetos compactados* • Objetos OLE incorporados* * Todos os objetos

Sobre a Verificação de Unidades Removíveis

É possível configurar a verificação de unidades removíveis conectadas ao computador protegido por meio da porta USB.

O Kaspersky Embedded Systems Security verifica uma unidade removível usando a tarefa de Verificação por Demanda. O aplicativo cria uma nova tarefa de Verificação por Demanda automaticamente quando a unidade removível é conectada e a exclui após a verificação ser concluída. A tarefa criada é executada com o nível de segurança predefinido para a verificação de unidades removíveis. Não é possível definir as configurações da tarefa temporária de Verificação por Demanda.

Se você instalou o Kaspersky Embedded Systems Security sem os bancos de dados de antivírus, a verificação de unidades removíveis ficará indisponível.

O Kaspersky Embedded Systems Security verifica uma unidade removível usando a tarefa de Verificação por Demanda. O aplicativo cria uma nova tarefa de Verificação por Demanda automaticamente quando a unidade removível é conectada e a exclui após a verificação ser concluída. A tarefa criada é executada com o nível de segurança predefinido para a verificação de unidades removíveis. Não é possível definir as configurações da tarefa temporária de Verificação por Demanda.

O Kaspersky Embedded Systems Security verifica as unidades USB removíveis conectadas quando elas são registradas como dispositivos de armazenamento USB em massa no sistema operacional. O aplicativo não verifica uma unidade removível se a conexão for bloqueada pela tarefa Controle de Dispositivos. O aplicativo não verifica os dispositivos móveis conectados por MTP.

O Kaspersky Embedded Systems Security permite o acesso a unidades removíveis durante a verificação.

Os resultados para cada unidade removível estão disponíveis no log para a tarefa de Verificação por Demanda criada após a conexão da unidade removível.

É possível alterar as configurações do componente de Verificação de unidades removíveis (consulte a tabela abaixo).

Tabela 59. Configurações de verificação de unidades removíveis

Configuração	Valor padrão	Descrição
Verificar unidades removíveis na conexão via USB	A caixa de seleção é desmarcada	É possível ligar e desligar a verificação de unidades removíveis após a conexão via USB com o computador protegido.
Verificar unidades removíveis se o volume de dados armazenados não exceder (MB)	1024 MB	É possível reduzir o escopo do componente configurando o volume máximo de dados na unidade verificada. O Kaspersky Embedded Systems Security não realiza a verificação de unidades removíveis se o volume de dados armazenados exceder o valor especificado.
Verificação com nível de segurança	Proteção máxima	É possível configurar as tarefas criadas de Verificação por Demanda selecionando um dos três níveis de segurança: • **Proteção máxima** • **Recomendado** • **Desempenho máximo** O algoritmo utilizado quando objetos infectados, possivelmente infectados e outros são detectados, bem como as outras configurações de verificação para cada nível de segurança, correspondem àqueles predefinidos nas tarefas de Verificação por Demanda.

Configurações padrão das tarefas de Verificação por Demanda

Por padrão, as tarefas de Verificação por Demanda possuem as configurações descritas na tabela abaixo. Você pode configurar tarefas de Verificação por Demanda de sistema e de usuário.

Tabela 60. Configurações padrão das tarefas de Verificação por Demanda

Configuração	Valor	Descrição
Escopo da verificação	Aplicado no sistema e em tarefas personalizadas: • **Verificação na Inicialização do Sistema Operacional**: o servidor inteiro, excluindo pastas compartilhadas e objetos de execução automática. • **Verificação de Áreas Críticas**: o servidor inteiro, excluindo pastas compartilhadas e certos arquivos de sistema operacional. • Tarefas personalizadas de **Verificação por demanda**: o servidor inteiro.	Você pode alterar o escopo da verificação. O escopo da verificação não pode ser configurado para as tarefas do sistema **Verificação da Quarentena** e de **Controle de Integridade de Aplicativos**.
Configurações de segurança	As configurações comuns de todo o escopo da verificação correspondem ao nível de segurança **Recomendado**.	Para os nós selecionados na lista ou na árvore de recursos de arquivos de computador, você pode: • Selecionar um nível de segurança predefinido diferente • Alterar manualmente as configurações de segurança Você pode salvar um conjunto de configurações de segurança para um nó selecionado como um modelo para ser usado posteriormente para outro nó.
Usar o analisador heurístico	É usado com o nível de análise **Médio** para Verificação de Áreas Críticas, Verificação na Inicialização do Sistema Operacional e tarefas personalizadas. É usado com o nível de análise **Profundo** para a tarefa de Verificação da Quarentena.	É possível ativar ou desativar o analisador heurístico, e configurar o nível de análise. O nível de análise da tarefa de Verificação da quarentena não pode ser configurado. O analisador heurístico não é usado na tarefa de Controle de Integridade de Aplicativos.
Aplicar à Zona Confiável	Aplicado (Não aplicado a tarefa de Verificação da Quarentena)	Lista geral de exclusões que podem ser usadas em tarefas selecionadas.
Usar a KSN para verificação	Aplicada	Você pode melhorar a proteção do seu servidor usando a infraestrutura dos serviços na nuvem da Kaspersky Security Network.
Configurações de inicialização de tarefa com permissões	A tarefa é iniciada em uma conta do sistema.	Você pode editar configurações de inicialização com permissões de conta para todas as tarefas de Verificação por Demanda do sistema e de usuário, exceto tarefas de Verificação da Quarentena e de Controle de Integridade de Aplicativos.

Configuração	Valor	Descrição
Executar tarefa em segundo plano (baixa prioridade)	Não aplicado	Você pode configurar o nível de prioridade das tarefas de Verificação por Demanda.
Programação de inicialização da tarefa	Aplicado em tarefas do sistema: • Verificação na Inicialização do Sistema operacional - **Ao iniciar o aplicativo** • Verificação de Áreas Críticas - **Semanalmente** • Verificação da Quarentena - **Após a atualização do banco de dados do aplicativo** • Controle de Integridade de Aplicativos - **Diariamente** Não usado em tarefas personalizadas criadas recentemente.	Você pode definir as configurações de inicialização programada da tarefa.
Registro da execução da verificação e atualização do status de proteção do servidor	O status de proteção do servidor é atualizado semanalmente após a Verificação de áreas críticas ser executada.	Você pode definir configurações para registrar a execução da Verificação de áreas críticas das seguintes maneiras: • Editar as configurações da programação de inicialização da tarefa de Verificação de áreas críticas. • Editar o escopo da verificação da tarefa de Verificação de áreas críticas. • Criar uma tarefa de Verificação por Demanda de usuário.

Gerenciamento da Verificação por demanda por meio do Plug-in de Administração

Nesta seção, aprenda como navegar pela interface do Plug-in de Administração e definir configurações de tarefa para um ou todos os computadores na rede.

Nesta seção

Navegação 410
Criando uma tarefa de Verificação por Demanda 411
Configuração do escopo da verificação da tarefa 416
Seleção de níveis de segurança predefinidos para tarefas de Verificação por Demanda 417
Definição manual de configurações de segurança 418
Configuração da Verificação de Unidades Removíveis 425

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface.

Nesta seção

Abertura do assistente da tarefa de Verificação por Demanda 410
Abertura das propriedades da tarefa de Verificação por Demanda 411

Abertura do assistente da tarefa de Verificação por Demanda

► *Para começar a criar uma nova tarefa de Verificação por Demanda personalizada:*

1. Para criar uma tarefa local:
   a. Expanda o nó **Dispositivos gerenciados** no Console de Administração do Kaspersky Security Center.
   b. Selecione o grupo de administração ao qual o computador pertence.
   c. No painel de detalhes, na guia **Dispositivos**, abra o menu de contexto do servidor protegido.
   d. Selecione a opção de menu **Propriedades**.
   e. Na janela exibida, clique no botão **Adicionar** na seção **Tarefas**.

   A janela **Assistente de Nova Tarefa** será aberta.
2. Para criar uma tarefa de grupo:
   a. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
   b. Selecione o grupo de administração para o qual você deseja criar uma tarefa.
   c. Abra a guia **Tarefas**.
   d. Clique no botão **Criar uma tarefa**.

   A janela **Assistente de Nova Tarefa** será aberta.
3. Para criar uma tarefa para um conjunto personalizado de computadores:
   a. No nó **Seleções de dispositivos** na árvore do Console de Administração do Kaspersky Security

Center, clique no botão **Executar seleção** para executar uma seleção de dispositivo.

b. Abra a guia **Resultados da seleção "nome da seleção"**.

c. Na lista suspensa **Executar seleção**, selecione a opção **Criar uma tarefa para um resultado de seleção**.

A janela **Assistente de Nova Tarefa** será aberta.

4. Selecione a tarefa **Verificação por demanda** na lista de tarefas disponíveis para o Kaspersky Embedded Systems Security.
5. Clique em **Avançar**.

   A janela **Configurações** é exibida.

Defina as configurações da tarefa conforme necessário.

► *Para configurar uma tarefa de Verificação por Demanda existente,*

Clique duas vezes no nome da tarefa na lista de tarefas no Kaspersky Security Center.

A janela **Propriedades: Verificação por Demanda** é exibida.

Abertura das propriedades da tarefa de Verificação por Demanda

► *Para abrir as propriedades do aplicativo para a tarefa de Verificação por Demanda para um único computador:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração ao qual o computador protegido pertence.
3. Selecione a guia **Dispositivos**.
4. Clique duas vezes no nome do computador para o qual deseja configurar o escopo da verificação.

   A janela **Propriedades: <nome do computador>** é exibida.
5. Selecione a seção **Tarefas**.
6. Na lista de tarefas criadas para o dispositivo, selecione a tarefa de Verificação por Demanda que você criou.
7. Clique no botão **Propriedades**.

   A janela **Propriedades: Verificação por Demanda** é exibida.

Defina as configurações da tarefa conforme necessário.

Criando uma tarefa de Verificação por Demanda

► *Para criar uma tarefa de Verificação por Demanda personalizada:*

1. Abra as **Configurações** (consulte a seção "**Abertura do assistente da tarefa de Verificação por Demanda**" na página 410) no **Assistente de nova tarefa**.

2. Selecione o **Método de criação da tarefa** necessário.
3. Clique em **Avançar**.
4. Crie um escopo de verificação na janela **Escopo da verificação**:

> Por padrão, o escopo da verificação inclui áreas críticas do computador. Os escopos da verificação são marcados na tabela com o ícone ☑. Os escopos da verificação excluídos são marcados com o ícone ☐ na tabela.
> Você pode alterar o escopo da verificação: adicione escopos, discos, pastas, objetos de rede e arquivos e atribua configurações de segurança específicas para cada escopo adicionado.

- Para excluir todas as áreas críticas da verificação, abra o menu de contexto de cada linha e selecione a opção **Remover escopo**.
- Para incluir um escopo de verificação predefinido, um disco, uma pasta, um objeto de rede ou um arquivo no escopo da verificação:
  a. Clique com o botão direito na tabela **Escopo da verificação** e selecione **Adicionar escopo** ou clique no botão **Adicionar**.
  b. Na janela **Adicionar objetos ao escopo da verificação**, selecione o escopo predefinido na lista **Escopo predefinido**, especifique a unidade do computador, pasta, objeto de rede ou arquivo no computador ou em outro computador da rede e clique no botão **OK**.
- Para excluir subpastas ou arquivos da verificação, selecione a pasta adicionada (disco) na janela **Escopo da verificação** do assistente:
  a. Abra o menu de contexto e selecione opção **Configurar**.
  b. Clique no botão **Configurações** na janela **Nível de segurança**.
  c. Na guia **Geral** da janela **Configurações da verificação por demanda** desmarque as caixas de seleção **Subpastas** e **Subarquivos**.
- Para alterar as configurações de segurança do escopo da verificação:
  a. Abra o menu de contexto do escopo cujas configurações você deseja definir e selecione **Configurar**.
  b. Na janela **Configurações da verificação por demanda**, selecione um dos níveis de segurança predefinidos ou clique no botão **Configurações** para definir as configurações de segurança manualmente.

> As configurações de segurança são definidas do mesmo modo para a tarefa Proteção de Arquivos em Tempo Real (consulte a seção "Definição manual de configurações de segurança" na página 249).

- Para ignorar objetos incorporados no escopo da verificação adicionado:
  a. Abra o menu de contexto na tabela **Escopo da verificação** e selecione **Adicionar exclusão**.
  b. Especifique os objetos a serem excluídos: selecione o escopo predefinido na lista **Escopo predefinido**, especifique o disco de computador, a pasta, o objeto de rede ou o arquivo do computador ou em outro computador de rede.
  c. Clique no botão **OK**.

5. Na janela **Opções**, configure o analisador heurístico e a integração com outros componentes:

- Configure o uso do analisador heurístico (consulte a seção "Configuração do Analisador Heurístico e integração com outros componentes do aplicativo" na página 245).
- Selecione a caixa **Aplicar Zona Confiável** se desejar excluir os objetos adicionados à lista da Zona Confiável do escopo da verificação da tarefa.

  Esta caixa de seleção ativa/desativa o uso da zona confiável em uma tarefa.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security adiciona operações de arquivos de processos confiáveis às exclusões da verificação definidas nas configurações de tarefa.

  Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security desconsiderará as operações de arquivos de processos confiáveis ao formar o escopo da proteção para a tarefa.

  A caixa de seleção é selecionada por padrão.
- Selecione a caixa **Usar a KSN para verificação** se quiser usar os serviços na nuvem da Kaspersky Security Network para a tarefa.

  Esta caixa ativa/desativa o uso de serviços na nuvem da Kaspersky Security Network (KSN) na tarefa.

  Se a caixa é selecionada, o aplicativo usa os dados de recebidos dos serviços da KSN para garantir um tempo de resposta mais rápido pelo aplicativo para novas ameaças e reduzir a probabilidade de falsos positivos.

  Se a caixa estiver desmarcada, a tarefa de Verificação por Demanda não usará os serviços da KSN.

  A caixa de seleção é selecionada por padrão.
- Para atribuir a prioridade *Baixa* ao processo de trabalho onde a tarefa será executada, selecione a caixa de seleção **Executar tarefa em segundo plano** na janela **Opções**.

  A caixa modifica a prioridade da tarefa.

  Se a caixa de seleção estiver selecionada, a prioridade da tarefa no sistema operacional será reduzida. O sistema operacional oferece recursos para a execução da tarefa dependendo da carga da CPU e do sistema de arquivos do computador a partir de outras tarefas e outros aplicativos do Kaspersky Embedded Systems Security. Como resultado, o desempenho da tarefa será reduzido durante cargas maiores e acelerado durante cargas menores.

  Se a caixa de seleção estiver desmarcada, a tarefa será iniciada e executada com a mesma prioridade de outras tarefas do Kaspersky Embedded Systems Security e de outros aplicativos. Nesse caso, a velocidade de execução da tarefa será aumentada.

  Esta caixa é desmarcada por padrão.

  Por padrão, os processos de trabalho em que as tarefas do Kaspersky Embedded Systems Security são executadas têm a prioridade *Médio* (Normal).
- Para usar a tarefa criada como uma tarefa de Verificação de Áreas Críticas, selecione a caixa **Considerar tarefa como verificação de áreas críticas** na janela **Opções**.

  A caixa de seleção altera a prioridade da tarefa: ativa ou desativa o registro em log do evento de *Verificação de Áreas Críticas* e a atualização do status de proteção do computador. O Kaspersky Security Center avalia a classificação de segurança do

computador (computadores) pelos resultados de desempenho de tarefas com o status de *Verificação de Áreas Críticas*. A caixa não está disponível nas propriedades do sistema local e nas tarefas personalizadas do Kaspersky Embedded Systems Security. Você pode editar esta definição apenas do lado do Kaspersky Security Center.

Se esta caixa estiver selecionada, o Servidor de Administração registrará a conclusão da Verificação de áreas críticas e atualizará o status da proteção do computador com base nos resultados da execução da tarefa. A tarefa de verificação tem prioridade alta.

Se a caixa estiver desmarcada, a tarefa será executada com uma prioridade baixa.

Esta caixa é desmarcada por padrão para tarefas por demanda personalizadas.

6. Clique em **Avançar**.
7. Na janela **Agendar**, defina as configurações de programação de inicialização da tarefa.
8. Clique em **Avançar**.
9. Na janela **Seleção de uma conta para a executar a tarefa**, especifique a conta que você quer usar.
10. Clique em **Avançar**.
11. Defina um nome de tarefa.
12. Clique em **Avançar**.

> O nome da tarefa não deve ter mais de 100 caracteres e não pode conter os seguintes símbolos: " * < > & \ : |

A janela **Conclusão da criação da tarefa** será aberta.

13. Você também pode executar a tarefa após a finalização do Assistente marcando a caixa de seleção **Executar a tarefa após a finalização do Assistente**.
14. Clique em **Concluir** para concluir a criação da tarefa.

A nova tarefa de Verificação por Demanda será criada para um computador ou um grupo de computadores selecionado.

Nesta seção

Atribuindo o status de tarefa de Verificação de Áreas Críticas a uma tarefa de Verificação por Demanda.....414
Executando uma tarefa de Verificação por Demanda em segundo plano.....415
Registrando a execução de Verificação de Áreas Críticas.....416

Atribuindo o status de tarefa de Verificação de Áreas Críticas a uma tarefa de Verificação por Demanda

Por padrão, o Kaspersky Security Center atribui o status *Aviso* ao computador se a tarefa Verificação de Áreas Críticas for executada com menos frequência do que o especificado na configuração de limite de geração de eventos *A verificação das áreas críticas não é realizada há muito tempo* do Kaspersky Embedded Systems Security.

► *Para configurar a verificação de todos os computadores em um único grupo de administração, siga as*

etapas a seguir:

1. Crie uma tarefa de Verificação por Demanda de grupo (consulte a seção "Criar uma tarefa de Verificação por Demanda" na página 411).
2. Na janela **Opções** do assistente de tarefas, selecione a caixa **Considerar tarefa como verificação de áreas críticas**. As configurações da tarefa especificadas (o escopo da verificação e as configurações de segurança) serão aplicadas a todos os computadores do grupo. Configure a programação da tarefa.

   É possível marcar a caixa de seleção **Considerar tarefa como verificação de áreas críticas** ao criar a tarefa de Verificação por Demanda para um grupo de computadores ou, mais tarde, na janela **Propriedades: <Nome da tarefa>** (consulte da seção "Abertura das propriedades da tarefa de Verificação por Demanda" na página 411).

3. Usando uma política nova ou existente, desative o início programado de tarefas de verificação por demanda do sistema (consulte a seção "Configuração da inicialização programada de tarefas locais do sistema" na página 97) nos computadores de grupo.

O Servidor de Administração do Kaspersky Security Center avaliará então o status de segurança do computador protegido e notificará você sobre ele com base nos resultados da última execução da tarefa com o status *Verificação de Áreas Críticas*, em vez de o fazer com base nos resultados da tarefa do sistema Verificação de Áreas Críticas.

Você pode atribuir o status da tarefa *Verificação de Áreas Críticas* às tarefas de grupo de Verificação por Demanda e a tarefas de conjuntos de computadores.

O Console do Aplicativo pode ser usado para visualizar se a tarefa de Verificação por Demanda é uma tarefa de Verificação de Áreas Críticas.

No Console do Aplicativo, a caixa de seleção **Considerar tarefa como verificação de áreas críticas** é exibida nas propriedades da tarefa, mas não pode ser editada.

Executando uma tarefa de Verificação por Demanda em segundo plano

Por padrão, é atribuída a prioridade *Médio* (Normal) aos processos nos quais as tarefas do Kaspersky Embedded Systems Security são executadas.

O processo que executará a tarefa de Verificação por Demanda pode receber uma prioridade *Baixa*. Ao reduzir a prioridade do processo, aumenta o tempo necessário para executar a tarefa, mas isso pode ter um efeito positivo sobre a velocidade de execução dos processos de outros programas ativos.

É possível executar várias tarefas em segundo plano em um único processo de trabalho com prioridade baixa. Você pode especificar o número máximo de processos para tarefas de Verificação por Demanda em segundo plano.

► *Para alterar a prioridade de uma tarefa de Verificação por Demanda existente:*

1. Abra a janela **Propriedades: Verificação por Demanda** (consulte a seção "Abertura do assistente da tarefa de Verificação por Demanda" na página 410).
2. Selecione ou desmarque a caixa **Executar tarefa em segundo plano**.

A caixa modifica a prioridade da tarefa.

Se a caixa de seleção estiver selecionada, a prioridade da tarefa no sistema operacional será reduzida. O sistema operacional oferece recursos para a execução da tarefa dependendo da carga da CPU e do sistema de arquivos do computador a partir de outras tarefas e outros aplicativos do Kaspersky Embedded Systems Security. Como resultado, o desempenho da tarefa será reduzido durante cargas maiores e acelerado durante cargas menores.

Se a caixa de seleção estiver desmarcada, a tarefa será iniciada e executada com a mesma prioridade de outras tarefas do Kaspersky Embedded Systems Security e de outros aplicativos. Nesse caso, a velocidade de execução da tarefa será aumentada.

Esta caixa é desmarcada por padrão.

3. Clique em **OK**.

As configurações de tarefa definidas serão salvadas e aplicadas imediatamente à tarefa sendo executada. Se a tarefa não estiver sendo executada, as configurações modificadas serão aplicadas na próxima execução.

Registrando a execução de Verificação de áreas críticas

Por padrão, o status de proteção do computador é exibido no painel de detalhes do nó **Kaspersky Embedded Systems Security** e é atualizado semanalmente após a execução da tarefa de Verificação de áreas críticas.

O tempo da atualização de status de proteção do computador está vinculado à programação da tarefa de Verificação por Demanda em cujas configurações a caixa **Considerar tarefa como verificação de áreas críticas** está selecionada. Por padrão, a caixa é selecionada somente para a tarefa de Verificação de áreas críticas e não pode ser modificada para esta tarefa.

Você pode selecionar a tarefa de Verificação por Demanda vinculada ao status de proteção do computador apenas no Kaspersky Security Center.

Configuração do escopo da verificação da tarefa

Se você modificar o escopo da verificação nas tarefas de Verificação na Inicialização do Sistema Operacional e Verificação de Áreas Críticas, poderá restaurar o escopo da verificação padrão nessas tarefas restaurando o próprio Kaspersky Embedded Systems Security (**Iniciar** > **Programas** > **Kaspersky Embedded Systems Security** > **Modificar ou remover o Kaspersky Embedded Systems Security**). No assistente de instalação, selecione **Reparar componentes instalados**, clique em **Avançar** e, em seguida, selecione a caixa **Restaurar configurações recomendadas do aplicativo**.

► *Para configurar o escopo da verificação de uma tarefa de Verificação por Demanda existente:*

1. Abra a janela **Propriedades: Verificação por Demanda** (consulte a seção "Abertura das propriedades da tarefa de Verificação por Demanda" na página 411).
2. Selecione a guia **Escopo da verificação**.
3. Para incluir itens no escopo da verificação:
   a. Abra o menu de contexto no espaço vazio da lista do escopo da verificação.

b. Selecione a opção **Adicionar escopo** no menu de contexto.

c. Na janela aberta **Adicionar objetos ao escopo da verificação**, selecione um tipo de objeto que deseja adicionar:

- **Escopo predefinido** para adicionar um dos escopos predefinidos em um servidor protegido. Em seguida, na lista suspensa, selecione um escopo de verificação necessário.
- **Disco, pasta ou local de rede** para incluir um objeto individual de unidade, pasta ou rede em um escopo de verificação. Em seguida, selecione um escopo necessário clicando no botão **Procurar**.
- **Arquivo** para incluir um arquivo individual no escopo da verificação. Em seguida, selecione um escopo necessário clicando no botão **Procurar**.

Você não pode adicionar um objeto em um escopo de verificação se ele já foi adicionado como uma exclusão fora de um escopo de verificação.

4. Para excluir nós individuais do escopo da verificação, desmarque as caixas ao lado dos nomes destes nós ou siga as etapas a seguir:

a. Abra o menu de contexto no escopo da verificação clicando com o botão direito nele.

b. No menu de contexto selecione a opção **Adicionar exclusão**.

c. Na janela **Adicionar exclusão**, selecione um tipo de objeto que deseja adicionar como uma exclusão fora do escopo da verificação seguindo a lógica de adicionar o objeto a um procedimento de escopo da verificação.

5. Para modificar o escopo da verificação ou uma exclusão adicionada, selecione a opção **Editar escopo** no menu de contexto do escopo necessário.

6. Para ocultar o escopo da verificação adicionado anteriormente ou uma exclusão na lista de recursos de arquivos de rede, selecione a opção **Remover escopo** no menu de contexto do escopo necessário.

O escopo da verificação é excluído do escopo da tarefa de Verificação por Demanda na sua remoção da lista de recursos de arquivos de rede.

7. Clique no botão **OK**.

A janela Configurações do escopo da verificação será fechada. As configurações recém-definidas foram salvas.

Seleção de níveis de segurança predefinidos para tarefas de Verificação por Demanda

Um dos três níveis de segurança predefinidos para um item selecionado na lista de recursos de arquivos de rede do computador pode ser aplicado: **Desempenho máximo**, **Recomendado** e **Proteção máxima**.

► *Para selecionar um dos níveis de segurança predefinidos:*

1. Abra a janela **Propriedades: Verificação por Demanda** (consulte a seção "**Abertura das propriedades da tarefa de Verificação por Demanda**" na página 411).
2. Selecione a guia **Escopo da verificação**.
3. Na lista do computador, selecione um item incluído no escopo da verificação para estabelecer o nível de

segurança predefinido.

4. Clique no botão **Configurar**.

   A janela **Configurações da verificação por demanda** é exibida.

5. Na guia **Nível de segurança**, selecione o nível de segurança a ser aplicado.

   A janela exibe a lista de configurações de segurança correspondentes ao nível de segurança selecionado.

6. Clique no botão **OK**.

7. Clique no botão **OK** na janela **Propriedades: Verificação por Demanda**.

   As configurações de tarefa definidas serão salvadas e aplicadas imediatamente à tarefa sendo executada. Se a tarefa não estiver sendo executada, as configurações modificadas serão aplicadas na próxima execução.

Definição manual de configurações de segurança

Por padrão as tarefas de Verificação por Demanda usam configurações de segurança comuns para o escopo da verificação inteiro. Estas configurações correspondem ao nível de segurança predefinido **Recomendado** (consulte a seção "Níveis de segurança predefinidos" na página 238).

Os valores padrão das configurações de segurança podem ser modificados, definindo-os como configurações em comum para todo o escopo da proteção ou como configurações distintas para diferentes itens na lista de recursos de arquivos de computador ou nós da árvore.

► *Para definir as configurações de segurança manualmente:*

1. Abra a janela **Propriedades: Verificação por Demanda** (consulte a seção "Abertura das propriedades da tarefa de Verificação por Demanda" na página 411).
2. Selecione a guia **Escopo da verificação**.
3. Selecione os itens na lista do escopo da verificação para os quais deseja definir configurações de segurança.

   Um modelo predefinido contendo configurações de segurança (consulte a seção "Sobre modelos de configurações de segurança" na página 157) pode ser aplicado a um nó ou item selecionado no escopo da verificação.

4. Clique no botão **Configurar**.

   A janela **Configurações da verificação por demanda** é exibida.

5. Defina as configurações de segurança necessárias para o nó ou item selecionado de acordo com seus requisitos:
   - As configurações **Geral** (consulte a seção "Definir configurações gerais de tarefas" na página 419)
   - **Ações** (consulte a seção "**Configurar ações**" na página 422)
   - **Desempenho** (consulte a seção "**Configurar o desempenho**" na página 423)
6. Clique em **OK** na janela **Configurações da verificação por demanda**.
7. Clique em **OK** na janela **Escopo da verificação**.

As novas configurações de escopo da verificação são salvas.

Nesta seção

Definir configurações gerais de tarefas 419
Configurar ações 422
Configurar o desempenho 423

Definir configurações gerais de tarefas

► *Para definir as configurações gerais da tarefa de Verificação por Demanda:*

1. Abra a janela **Propriedades: Verificação por Demanda** (consulte a seção "**Abertura das propriedades da tarefa de Verificação por Demanda**" na página 411).
2. Selecione a guia **Escopo da verificação**.
3. Clique no botão **Configurar**.

   A janela **Configurações da verificação por demanda** é exibida.
4. Clique no botão **Configurações**.
5. Na guia **Geral** da seção **Verificar objetos**, especifique os tipos de objetos que deseja incluir no escopo da verificação:
   - **Objetos a serem verificados**
     - **Todos os objetos**

       O Kaspersky Embedded Systems Security verifica todos os objetos.
     - **Objetos verificados por formato**

       O Kaspersky Embedded Systems Security verificará somente objetos infectáveis com base no formato do arquivo.

       A lista de formatos é compilada pela Kaspersky Lab. Ela está incluída nos bancos de dados do Kaspersky Embedded Systems Security.
     - **Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus**

       O Kaspersky Embedded Systems Security verificará somente objetos infectáveis com base na extensão do arquivo.

       A lista de extensões é compilada pela Kaspersky Lab. Ela está incluída nos bancos de dados do Kaspersky Embedded Systems Security.
     - **Objetos verificados pela lista de extensões especificada**

       O Kaspersky Embedded Systems Security verificará os arquivos baseados em suas extensões. A lista de extensões de arquivo pode ser personalizada manualmente na janela **Lista de extensões**, que pode ser aberta clicando no botão **Editar**.
   - **Subpastas**

- **Subarquivos**
- **Verificar setores de inicialização do disco e MBR**

  Ativa a proteção dos setores de inicialização e dos registros mestres de inicialização.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os setores de inicialização e os registros mestres de inicialização nos discos rígidos e unidades removíveis do computador.

  A caixa de seleção é selecionada por padrão.

- **Verificar fluxos NTFS alternativos**

  Verificação de fluxos alternativos de arquivos e pastas nas unidades do sistema de arquivos NTFS.

  Se a caixa estiver selecionada, o aplicativo verifica um objeto possivelmente infectado e todos os fluxos NTFS associados àquele objeto.

  Se a caixa estiver desmarcada, o aplicativo verifica apenas o objeto detectado e considerado possivelmente infectado.

  A caixa de seleção é selecionada por padrão.

6. Na seção **Desempenho**, selecione ou desmarque a caixa **Verificar apenas arquivos novos e modificados**.

   Esta caixa de seleção ativa/desativa a verificação e a proteção de arquivos que foram reconhecidos pelo Kaspersky Embedded Systems Security como novos ou modificados desde a última verificação.

   Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará e protegerá apenas os arquivos reconhecidos como novos ou modificados desde a última verificação.

   Se a caixa estiver desmarcada, você poderá selecioná-la se quiser verificar e proteger apenas arquivos novos ou todos os arquivos, desconsiderando o status de modificação.

   Por padrão, a caixa de seleção está selecionada para o nível de segurança **Desempenho máximo**. Se os níveis de segurança **Proteção máxima** ou **Recomendado** estiverem definidos, a caixa estará desmarcada.

   Para alternar entre as opções disponíveis quando a caixa estiver desmarcada, clique no link **Todos** / **Apenas novos** para cada um dos tipos de objetos compostos.

7. Na seção **Verificação de objetos compostos**, especifique os objetos compostos que deseja incluir no escopo da verificação:

   - **Todos / Apenas novos arquivos compactados**

     Verificação dos arquivos compactados ZIP, CAB, RAR, ARJ e de outros formatos.

     Se essa a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos compactados.

     Se essa caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos compactados durante a verificação.

     O valor padrão depende do nível de proteção selecionado.

   - **Todos / Apenas novos arquivos compactados SFX**

Verificação de arquivos compactados autoextraíveis.

Se essa caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos compactados durante a verificação.

Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos compactados SFX durante a verificação.

O valor padrão depende do nível de proteção selecionado.

Essa opção fica ativa quando a caixa de seleção **Arquivos compactados** é desmarcada.

- **Todos / Apenas novos bancos de dados de e-mail**

  Verificação de arquivos de banco de dados de correio do Microsoft Outlook e Microsoft Outlook Express.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos de bancos de dados de e-mail.

  Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos de bancos de dados de e-mail durante a verificação.

  O valor padrão depende do nível de segurança selecionado.

- **Todos / Apenas novos objetos compactados**

  Verificação de arquivos executáveis compactados por compactadores de código binário, como UPX ou ASPack.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos executáveis compactados por compactadores de código binário.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos executáveis compactados por compactadores de código binário durante a verificação.

  O valor padrão depende do nível de proteção selecionado.

- **Todos / Apenas novos e-mails sem formatação**

  Verificação de arquivos de formato de e-mail, como mensagens do Microsoft Outlook e Microsoft Outlook Express.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos de formato de e-mail.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos de formato de e-mail durante a verificação.

  O valor padrão depende do nível de segurança selecionado.

- **Todos / Apenas novos objetos OLE incorporados**

  Verificação de objetos incorporados em arquivos (como macros do Microsoft Word ou anexos de e-mail).

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os objetos inseridos em arquivos.

  Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os objetos inseridos em arquivos durante a verificação.

  O valor padrão depende do nível de proteção selecionado.

8. Clique em **OK**.

A nova configuração de tarefa será salva.

Configurar ações

► *Para configurar ações em objetos infectados e outros objetos detectados durante a execução da tarefa de Verificação por Demanda:*

1. Abra a janela **Propriedades: Verificação por Demanda** (consulte a seção "**Abertura das propriedades da tarefa de Verificação por Demanda**" na página 411).
2. Selecione a guia **Escopo da verificação**.
3. Clique no botão **Configurar**.

   A janela **Configurações da verificação por demanda** é exibida.
4. Clique no botão **Configurações**.
5. Selecione a guia **Ações**.
6. Selecione a ação a ser executada em objetos infectados e outros objetos detectados.
   - **Notificar somente**.

     Quando esse modo estiver selecionado, o Kaspersky Embedded Systems Security não bloqueará o acesso a objetos infectados ou outros objetos detectados, nem executará qualquer ação sobre eles. O seguinte evento é registrado no log de tarefas: *Objeto não desinfectado. Motivo: nenhuma ação foi executada para neutralizar o objeto detectado devido a configurações definidas pelos usuários.* O evento especifica todas as informações disponíveis sobre o objeto detectado.

     O modo **Notificar somente** deve ser configurado separadamente para cada área de verificação. Este modo não é usado por padrão para qualquer um dos níveis de segurança. Se você selecionar esse modo, o Kaspersky Embedded Systems Security alterará automaticamente o nível de segurança para **Personalizado**.
   - **Desinfectar**.
   - **Desinfectar. Desinfectar. Remover se a desinfecção falhar**.
   - **Remover**.
   - **Executar ação recomendada**.
7. Selecione a ação a ser executada em objetos possivelmente infectados:
   - **Notificar somente**.

     Quando esse modo estiver selecionado, o Kaspersky Embedded Systems Security não bloqueará o acesso a objetos infectados ou outros objetos detectados, nem executará qualquer ação sobre eles. O seguinte evento é registrado no log de tarefas: *Objeto não desinfectado. Motivo: nenhuma ação foi executada para neutralizar o objeto detectado devido a configurações definidas pelos usuários.* O evento especifica todas as informações disponíveis sobre o objeto detectado.

     O modo **Notificar somente** deve ser configurado separadamente para cada área de verificação. Este modo não é usado por padrão para qualquer um dos níveis de segurança. Se você selecionar esse modo, o Kaspersky Embedded Systems Security alterará automaticamente o nível de segurança para **Personalizado**.

- **Quarentena**.
- **Remover**.
- **Executar ação recomendada**.

8. Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:
   a. Desmarque ou selecione a caixa **Executar ações dependendo do tipo de objeto detectado**.

      Se a caixa for selecionada, você pode definir a ação primária e secundária independentemente para cada tipo de objeto detectado clicando no botão **Configurações** ao lado da caixa. Nesse caso, o Kaspersky Embedded Systems Security não permitirá que um objeto infectado seja aberto ou executado independentemente da sua escolha.

      Se a caixa de seleção for desmarcada, o Kaspersky Embedded Systems Security executará as ações selecionadas nas seções **Ação a ser executada em objetos infectados e outros** e **Ação a ser executada em objetos possivelmente infectados** para os tipos de objetos indicados, respectivamente.

      Esta caixa é desmarcada por padrão.

   b. Clique no botão **Configurações**.
   c. Na janela que se abre, selecione a ação primária e secundária (se a primeira ação falhar) para cada tipo de objeto detectado.
   d. Clique em **OK**.
9. Selecione a ação a ser executada em objetos compostos incuráveis: selecione ou desmarque a caixa **Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte objeto incorporado**.

   Esta caixa ativa ou desativa a remoção forçada do arquivo composto pai quando um objeto malicioso, possivelmente infectado ou outro objeto filho incorporado for detectado.

   Se a caixa estiver selecionada e a tarefa for configurada para remover objetos infectados e possivelmente infectados, o Kaspersky Embedded Systems Security forçosamente removerá todo o objeto composto pai quando um objeto incorporado malicioso ou outro objeto for detectado. A remoção forçada de um arquivo pai juntamente com todo o seu conteúdo ocorrerá se o aplicativo não puder remover apenas o objeto filho detectado (por exemplo, se o objeto pai não puder ser modificado).

   Se esta caixa estiver desmarcada e a tarefa for configurada para remover objetos infectados e possivelmente infectados, o Kaspersky Embedded Systems Security não executará a ação selecionada se o objeto pai não puder ser modificado.
10. Clique em **OK**.

A nova configuração de tarefa será salva.

Configurar o desempenho

► *Para configurar o desempenho da tarefa de Verificação por Demanda:*

1. Abra a janela **Propriedades: Verificação por Demanda (consulte a seção "Abertura das propriedades da tarefa de Verificação por Demanda" na página** 411**)**.
2. Selecione a guia **Escopo da verificação**.
3. Clique no botão **Configurar**.

A janela **Configurações da verificação por demanda** é exibida.

4. Clique no botão **Configurações**.
5. Selecione a guia **Desempenho**.
6. Na seção **Exclusões**:
   - Desmarque ou selecione a caixa **Excluir arquivos**.

     Excluindo arquivos da verificação pelo nome de arquivo ou pela máscara de nome de arquivo.

     Se esta caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará os objetos especificados durante a verificação.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará todos os objetos.

     Esta caixa é desmarcada por padrão.

   - Desmarque ou selecione a caixa **Não detectar**.

     Os objetos são excluídos da verificação pelo nome ou pela máscara de nome do objeto detectável. A lista de nomes de objetos detectáveis está disponível no site da Enciclopédia de Vírus https://encyclopedia.kaspersky.com/knowledge/classification/.

     Se esta caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará os objetos detectáveis especificados durante a verificação.

     Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security detectará todos os objetos especificados no aplicativo por padrão.

     Esta caixa é desmarcada por padrão.

   - Clique no botão **Editar** de cada configuração para adicionar exclusões.
7. Na seção **Configurações avançadas**:
   - **Parar a verificação se demorar mais que (s)**

     Limita a duração da verificação do objeto. O valor padrão é 60 segundos.

     Se a caixa de seleção estiver selecionada, a duração da verificação será limitada ao valor especificado.

     Se a caixa de seleção estiver desmarcada, a duração da verificação será ilimitada.

     Por padrão, a caixa de seleção está selecionada para o nível de segurança **Desempenho máximo**.

   - **Não verificar obj. compostos com mais de (MB)**

     Exclui objetos maiores do que o tamanho especificado na verificação.

     Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará objetos compostos cujo tamanho exceda o limite especificado durante a verificação de vírus.

     Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará os objetos compostos de qualquer tamanho.

     Por padrão, a caixa de seleção está selecionada para o nível de segurança **Desempenho máximo**.

   - **Usar a tecnologia iSwift**

A tecnologia iSwift compara o identificador NTFS do arquivo armazenado em um banco de dados com um identificador atual. A verificação é executada apenas para arquivos cujos identificadores foram alterados (novos arquivos e arquivos modificados desde a última verificação dos objetos do sistema NTFS).

Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará apenas os novos arquivos ou aqueles modificados desde a última verificação dos objetos do sistema NTFS.

Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará objetos do sistema de arquivos NTFS sem considerar a data de criação ou modificação do arquivo, exceto em arquivos das pastas de rede.

A caixa de seleção é selecionada por padrão.

- **Usar a tecnologia iChecker**

  A tecnologia iChecker calcula e lembra de somas de verificação de arquivos verificados. Se um objeto for modificado a soma de verificação é alterada. O aplicativo compara todas as somas de verificação durante a tarefa de verificação e verifica apenas objetos novos e modificados desde a última verificação de arquivos.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará apenas arquivos novos e modificados.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará os arquivos sem considerar a data de criação ou modificação do arquivo.

  A caixa de seleção é selecionada por padrão.

8. Clique em **OK**.

A nova configuração de tarefa será salva.

Configuração da Verificação de Unidades Removíveis

► *Para configurar a verificação das unidades removíveis após a conexão ao computador protegido:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Políticas**.
4. Clique duas vezes no nome da política que você quer configurar.

   Na janela **Propriedades: <Nome da política>**, selecione a seção **Suplementar**.
5. Clique no botão **Configurações** na subseção **Verificações de unidades removíveis**.

   A janela **Verificações de unidades removíveis** é exibida.
6. Na seção **Verificação na conexão**, faça o seguinte:

   - Marque a caixa de seleção **Verificar unidades removíveis na conexão via USB**, se desejar que o Kaspersky Embedded Systems Security verifique automaticamente as unidades removíveis quando elas forem conectadas.
   - Se necessário, selecione **Verificar unidades removíveis se o volume de dados armazenados não**

exceder (MB) e especifique o valor máximo no campo à direita.

- Na lista suspensa **Verificação com nível de segurança**, especifique o nível de segurança com as configurações exigidas para a verificação de unidades removíveis.

7. Clique em **OK**.

As configurações específicas são salvas e aplicadas.

Gerenciamento da Verificação por demanda por meio do Console do Aplicativo

Nesta seção, aprenda como navegar pela interface do Console do Aplicativo e definir configurações de tarefa em um computador local.

Nesta seção

Navegação 426
Criação e configuração de uma tarefa de Verificação por Demanda 427
Escopo da verificação em tarefas de Verificação por Demanda 429
Seleção de níveis de segurança predefinidos para tarefas de Verificação por Demanda 433
Definição manual de configurações de segurança 433
Verificação de unidades removíveis 440
Estatísticas da tarefa de Verificação por Demanda 441

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface.

Nesta seção

Abertura das configurações da tarefa de Verificação por Demanda 426

Abertura das configurações da tarefa de Verificação por Demanda

► *Para abrir as configurações gerais da tarefa de Verificação por Demanda por meio do Console do Aplicativo:*

1. Expanda o nó **Verificação por Demanda** na árvore do Console do Aplicativo.
2. Selecione o nó filho que corresponde à tarefa que deseja configurar.
3. No painel de detalhes do nó filho, clique no link **Propriedades**.

   A janela **Configurações de tarefa** é exibida.

► *Para abrir a janela de configurações do escopo da verificação por meio do Console do Aplicativo:*

1. Expanda o nó **Verificação por Demanda** na árvore do Console do Aplicativo.
2. Selecione o nó filho que corresponde a uma tarefa de Verificação por Demanda que deseja configurar.
3. No painel de detalhes do nó selecionado clique no link **Configurar o escopo da verificação**.

   A janela **Configurações do escopo da verificação** é exibida.

Criação e configuração de uma tarefa de Verificação por Demanda

É possível criar tarefas personalizadas para um único computador no nó **Verificação por Demanda**. Nos outros componentes funcionais do Kaspersky Embedded Systems Security, não é possível criar tarefas personalizadas.

► *Para criar e configurar uma nova tarefas de Verificação por Demanda:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Verificação por Demanda**.
2. Selecione **Adicionar tarefa**.

   A janela **Adicionar tarefa** é exibida.
3. Defina as seguintes configurações da tarefa:
   - **Nome** – nome da tarefa com no máximo 100 caracteres, pode conter quaisquer símbolos, exceto **" * < > & \ : |**.

     Você não pode salvar uma tarefa ou configurar uma nova tarefa nas guias **Agendar**, **Avançado** e **Executar como** se o nome da tarefa não for especificado.
   - **Descrição** - quaisquer informações adicionais sobre a tarefa, com no máximo 2000 caracteres. Essas informações serão exibidas na janela de propriedades de tarefa.
   - **Usar o analisador heurístico**.

     Esta caixa ativa/desativa o analisador heurístico durante a verificação do objeto.

     Se a caixa de seleção estiver selecionada, o Analisador Heurístico será ativado.

     Se a caixa de seleção estiver desmarcada, o Analisador Heurístico será desativado.

     A caixa de seleção é selecionada por padrão.
   - **Executar tarefa em segundo plano**.

     A caixa modifica a prioridade da tarefa.

     Se a caixa de seleção estiver selecionada, a prioridade da tarefa no sistema operacional será reduzida. O sistema operacional oferece recursos para a execução da tarefa dependendo da carga da CPU e do sistema de arquivos do computador a partir de outras tarefas e outros aplicativos do Kaspersky Embedded Systems Security. Como resultado, o desempenho da tarefa será reduzido durante cargas maiores e acelerado durante cargas menores.

     Se a caixa de seleção estiver desmarcada, a tarefa será iniciada e executada com a mesma prioridade de outras tarefas do Kaspersky Embedded Systems Security e de outros aplicativos. Nesse caso, a velocidade de execução da tarefa será aumentada.

Esta caixa é desmarcada por padrão.

- **Aplicar à Zona Confiável**.

  Esta caixa de seleção ativa/desativa o uso da zona confiável em uma tarefa.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security adiciona operações de arquivos de processos confiáveis às exclusões da verificação definidas nas configurações de tarefa.

  Se a caixa estiver desmarcada, o Kaspersky Embedded Systems Security desconsiderará as operações de arquivos de processos confiáveis ao formar o escopo da proteção para a tarefa.

  A caixa de seleção é selecionada por padrão.

- **Considerar tarefa como verificação de áreas críticas**.

  A caixa de seleção altera a prioridade da tarefa: ativa ou desativa o registro em log do evento de *Verificação de Áreas Críticas* e a atualização do status de proteção do computador. O Kaspersky Security Center avalia a classificação de segurança do computador (computadores) pelos resultados de desempenho de tarefas com o status de *Verificação de Áreas Críticas*. A caixa não está disponível nas propriedades do sistema local e nas tarefas personalizadas do Kaspersky Embedded Systems Security. Você pode editar esta definição apenas do lado do Kaspersky Security Center.

  Se esta caixa estiver selecionada, o Servidor de Administração registrará a conclusão da Verificação de áreas críticas e atualizará o status da proteção do computador com base nos resultados da execução da tarefa. A tarefa de verificação tem prioridade alta.

  Se a caixa estiver desmarcada, a tarefa será executada com uma prioridade baixa.

  Esta caixa é desmarcada por padrão para tarefas por demanda personalizadas.

- **Usar a KSN para verificação**.

  Esta caixa ativa/desativa o uso de serviços na nuvem da Kaspersky Security Network (KSN) na tarefa.

  Se a caixa é selecionada, o aplicativo usa os dados de recebidos dos serviços da KSN para garantir um tempo de resposta mais rápido pelo aplicativo para novas ameaças e reduzir a probabilidade de falsos positivos.

  Se a caixa estiver desmarcada, a tarefa de Verificação por Demanda não usará os serviços da KSN.

  A caixa de seleção é selecionada por padrão.

4. Defina as configurações de programação de inicialização da tarefa (consulte a seção "Definição das configurações da programação de inicialização da tarefa" na página 151) nas guias **Agendar** e **Avançado**.
5. Na guia **Executar como**, defina as configurações de inicialização da tarefa com permissões de conta (consulte a seção "Especificação de uma conta de usuário para iniciar uma tarefa" na página 153).
6. Clique em **OK** na janela **Adicionar tarefa**.

   É criada uma nova tarefa de Verificação por Demanda. Um nó com o nome da nova tarefa é exibido na árvore do Console do Aplicativo. A operação é registrada no log de auditoria do sistema (na página 202).
7. Se necessário, no painel de detalhes do nó selecionado, selecione **Configurar o escopo da verificação**.

   A janela **Configurações do escopo da verificação** é exibida.
8. Na árvore ou lista de recursos de arquivos de computador, selecione os nós ou itens que deseja incluir no

escopo da verificação.

9. Selecione um dos níveis de segurança predefinidos (consulte a seção "Sobre os níveis de segurança predefinidos para tarefas de Verificação por Demanda" na página 404) ou defina as configurações de verificação manualmente (consulte a seção "Definição manual de configurações de segurança" na página 433).
10. Clique em **Salvar** na janela **Configurações do escopo da verificação**.

As configurações definidas são aplicadas na próxima inicialização da tarefa.

Escopo da verificação em tarefas de Verificação por Demanda

Esta seção contém informações sobre a criação e utilização de um escopo de verificação nas tarefas de Verificação por Demanda.

Nesta seção

Configurando o modo de visualização de recursos de arquivos de rede 429
Criando um escopo de verificação 429
Incluindo objetos de rede no escopo da verificação 431
Criando um escopo de verificação virtual 432

Configurando o modo de visualização de recursos de arquivos de rede

► *Para selecionar o modo da visualização para os recursos de arquivos de rede durante a definição das configurações do escopo da verificação:*

1. Abra a janela **Configurações do escopo da verificação** (na página 427).
2. Abra a lista suspensa na seção esquerda superior da janela. Execute uma das seguintes etapas:
   - Selecione a opção **Visualização em árvore** para exibir os recursos de arquivos de rede em um modo de visualização em árvore.
   - Selecione a opção **Visualização em lista** para exibir os recursos de arquivos de rede em um modo de visualização de lista.

   Por padrão, os recursos de arquivos de rede do computador protegido são exibidos em um modo de visualização em lista.
3. Clique no botão **Salvar**.

A janela Configurações do escopo da verificação será fechada. As configurações recém-definidas serão aplicadas.

Criando um escopo de verificação

Se estiver gerenciando o Kaspersky Embedded Systems Security remotamente no computador protegido usando o Console do Aplicativo instalado na estação de trabalho do administrador, você deverá ser membro do grupo de

administradores no computador protegido para poder exibir suas pastas.

Os nomes de configurações podem variar em diferentes sistemas operacionais Windows.

Se você modificar o escopo da verificação nas tarefas de Verificação na Inicialização do Sistema Operacional e Verificação de Áreas Críticas, poderá restaurar o escopo da verificação padrão nessas tarefas restaurando o próprio Kaspersky Embedded Systems Security (**Iniciar** > **Programas** > **Kaspersky Embedded Systems Security** > **Modificar ou remover o Kaspersky Embedded Systems Security**). No assistente de instalação, selecione **Reparar componentes instalados**, clique em **Avançar** e, em seguida, selecione a caixa **Restaurar configurações recomendadas do aplicativo**.

O procedimento para criar um escopo de tarefa de Verificação por Demanda depende do modo de visualização de recursos de arquivos de rede (consulte a seção "Configurando o modo de visualização de recursos de arquivos de rede" na página 429). Você pode configurar o modo de visualização de recursos de arquivos de rede como uma árvore ou como uma lista (definir como padrão).

► *Para criar um escopo de verificação trabalhando com uma árvore de recursos de arquivos de rede:*

1. Abra a janela **Configurações do escopo da verificação** (na página 427).
2. Na seção esquerda da janela, abra a árvore de recursos de arquivos de rede para exibir todos os nós e os nós filhos.
3. Faça o seguinte:
   - Para excluir nós individuais do escopo da verificação, desmarque as caixas ao lado dos nomes destes nós.
   - Para incluir nós individuais no escopo da verificação, desmarque a caixa de seleção **Meu Computador** e faça o seguinte:
     - Se todas as unidades de um tipo devem ser incluídas no escopo da verificação, selecione a caixa ao lado do nome do tipo de unidade requerida (por exemplo, para adicionar todas as unidades removíveis no computador, selecione a caixa **Unidades removíveis**).
     - Para incluir uma unidade individual de um determinado tipo no escopo da verificação, expanda o nó que contém a lista de unidades desse tipo e marque a caixa ao lado do nome da unidade desejada. Por exemplo, para selecionar a unidade removível **F:**, expanda o nó **Unidades removíveis** e selecione a caixa da unidade **F:**.
     - Se deseja incluir somente uma única pasta ou arquivo na unidade, selecione a caixa ao lado do nome daquela pasta ou arquivo.
4. Clique no botão **Salvar**.

A janela Configurações do escopo da verificação será fechada. As configurações recém-definidas serão salvas.

► *Para criar um escopo da verificação usando a lista de recursos de arquivos de rede:*

1. Abra a janela **Configurações do escopo da verificação** (na página 427).
2. Para incluir nós individuais no escopo da verificação, desmarque a caixa de seleção **Meu Computador** e faça o seguinte:
   a. Abra o menu de contexto no escopo da verificação clicando com o botão direito nele.
   b. No menu de contexto do botão, selecione **Adicionar escopo de verificação**.

c. Na janela aberta **Adicionar escopo de verificação**, selecione um tipo de objeto que deseja adicionar:

- **Escopo predefinido** para adicionar um dos escopos predefinidos em um computador protegido. Em seguida, na lista suspensa, selecione um escopo de verificação necessário.
- **Disco, pasta ou local de rede** para incluir um objeto individual de unidade, pasta ou rede em um escopo de verificação. Em seguida, selecione um escopo necessário clicando no botão **Procurar**.
- **Arquivo** para incluir um arquivo individual no escopo da verificação. Em seguida, selecione um escopo necessário clicando no botão **Procurar**.

Você não pode adicionar um objeto em um escopo de verificação se ele já foi adicionado como uma exclusão fora de um escopo de verificação.

3. Para excluir nós individuais do escopo da verificação, desmarque as caixas ao lado dos nomes destes nós ou siga as etapas a seguir:
   a. Abra o menu de contexto no escopo da verificação clicando com o botão direito nele.
   b. No menu de contexto selecione a opção **Adicionar exclusão**.
   c. Na janela **Adicionar exclusão**, selecione um tipo de objeto que deseja adicionar como uma exclusão fora do escopo da verificação seguindo a lógica de adicionar o objeto a um procedimento de escopo da verificação.
4. Para modificar o escopo da verificação ou uma exclusão adicionada, selecione a opção **Editar escopo** no menu de contexto do escopo necessário.
5. Para ocultar o escopo da verificação adicionado anteriormente ou uma exclusão na lista de recursos de arquivos de rede, selecione a opção **Remover da lista** no menu de contexto do escopo necessário.

   O escopo da verificação é excluído do escopo da tarefa de Verificação por Demanda na sua remoção da lista de recursos de arquivos de rede.

6. Clique no botão **Salvar**.

A janela Configurações do escopo da verificação será fechada. As configurações recém-definidas serão salvas.

Incluindo objetos de rede no escopo da verificação

Unidades, pastas ou arquivos de rede podem ser adicionados ao escopo da verificação especificando seu caminho no formato UNC (Universal Naming Convention).

Você pode verificar pastas de rede na conta do sistema.

► *Para adicionar um local de rede ao escopo da verificação:*

1. Abra a janela **Configurações do escopo da verificação** (na página 427).
2. Abra a lista suspensa no setor esquerdo superior da janela e selecione **Visualização em árvore**.
3. No menu de contexto do nó **Rede**:
   - Selecione **Adicionar pasta de rede**, se deseja adicionar uma pasta de rede ao escopo da verificação.

- Selecione **Adicionar arquivo de rede**, se deseja adicionar um arquivo de rede ao escopo da verificação.

4. Insira o caminho para a pasta ou arquivo de rede em formato UNC e pressione a tecla **ENTER**.
5. Selecione a caixa ao lado do objeto de rede adicionado recentemente para incluí-lo no escopo da verificação.
6. Se necessário, altere as configurações de segurança do objeto de rede adicionado.
7. Clique no botão **Salvar**.

As configurações de tarefa modificadas são salvas.

Criando um escopo de verificação virtual

As unidades, pastas e arquivos dinâmicos podem ser incluídos no escopo da verificação para criar um escopo de verificação virtual.

Você pode expandir o escopo da proteção/verificação adicionando unidades virtuais individuais, pastas ou arquivos somente se o escopo da proteção/verificação for apresentado como uma árvore de recursos de arquivos (consulte a seção "Configurando o modo de visualização de recursos de arquivos de rede" na página 429).

► *Para adicionar uma unidade virtual ao escopo da verificação:*

1. Abra a janela **Configurações do escopo da verificação** (na página 427).
2. Abra a lista suspensa no setor esquerdo superior da janela e selecione **Visualização em árvore**.
3. Na árvore de recursos de arquivos de computador, abra o menu de contexto no nó **Unidades virtuais**, clique em **Adicionar unidade virtual** e selecione o nome da unidade virtual da lista de nomes disponíveis.
4. Selecione a caixa ao lado da unidade adicionada para incluir a unidade no escopo da verificação.
5. Clique no botão **Salvar**.

As configurações de tarefa modificadas são salvas.

► *Para adicionar uma pasta ou um arquivo virtual ao escopo da verificação:*

1. Abra a janela **Configurações do escopo da verificação** (na página 427).
2. Abra a lista suspensa no setor esquerdo superior da janela e selecione **Visualização em árvore**.
3. Na árvore de recursos de arquivos de computador abra o menu de contexto do nó para adicionar uma pasta ou arquivo e selecione uma das seguintes opções:
   - **Adicionar pasta virtual** se você deseja adicionar uma pasta virtual ao escopo da verificação.
   - **Adicionar arquivo virtual** se você deseja adicionar um arquivo virtual ao escopo da verificação.
4. No campo de entrada, especifique o nome da pasta ou arquivo.
5. Na linha com o nome da pasta ou arquivo criado selecione a caixa de seleção para incluir essa pasta ou arquivo no escopo da verificação.
6. Clique no botão **Salvar**.

As configurações de tarefa modificadas são salvas.

Seleção de níveis de segurança predefinidos para tarefas de Verificação por Demanda

Um dos três níveis de segurança predefinidos para um nó ou item selecionado na árvore ou lista de recursos de arquivos de rede do computador pode ser aplicado: **Desempenho máximo**, **Recomendado** e **Proteção máxima**.

► *Para selecionar um dos níveis de segurança predefinidos:*

1. Abra a janela **Configurações do escopo da verificação** (na página 427).
2. Na árvore ou na lista dos recursos de arquivos de rede de computador selecione um nó ou item para estabelecer o nível de segurança predefinido.
3. Certifique-se de que o nó ou item selecionado seja incluído no escopo da verificação.
4. No setor direito da janela, na guia **Nível de segurança** selecione o nível de segurança a ser aplicado.

   A janela exibe a lista de configurações de segurança correspondentes ao nível de segurança selecionado.
5. Clique no botão **Salvar**.

   As configurações de tarefa definidas serão salvadas e aplicadas imediatamente à tarefa sendo executada. Se a tarefa não estiver sendo executada, as configurações modificadas serão aplicadas na próxima execução.

Definição manual de configurações de segurança

Por padrão as tarefas de Verificação por Demanda usam configurações de segurança comuns para o escopo da verificação inteiro. Estas configurações correspondem ao nível de segurança predefinido **Recomendado** (consulte a seção "Níveis de segurança predefinidos" na página 238).

Os valores padrão das configurações de segurança podem ser modificados, definindo-os como configurações em comum para todo o escopo da proteção ou como configurações distintas para diferentes itens na lista de recursos de arquivos de computador ou nós da árvore.

Ao trabalhar com a árvore de recursos de arquivos de rede, as configurações de segurança definidas para o nó pai selecionado são automaticamente aplicadas a todos os nós filhos. As configurações de segurança do nó pai não são aplicadas a nós filhos configurados separadamente.

► *Para definir as configurações de segurança manualmente:*

1. Abra a janela **Configurações do escopo da verificação** (na página 427).
2. Na seção esquerda da janela, selecione o nó ou item para definir as configurações de segurança.

   Um modelo predefinido contendo configurações de segurança (consulte a seção "Sobre modelos de configurações de segurança" na página 157) pode ser aplicado a um nó ou item selecionado no escopo da verificação.
3. Defina as configurações de segurança necessárias para o nó ou item selecionado de acordo com seus requisitos nas seguintes guias:
   - As configurações gerais (consulte a seção "Definir configurações gerais de tarefas" na página 434)

- Ações (consulte a seção "Configurar ações" na página 437)
- Desempenho (consulte a seção "Configurar o desempenho" na página 438)
- Armazenamento hierárquico

4. Clique em **Salvar** na janela **Configurações do escopo da verificação**.

As novas configurações de escopo da verificação são salvas.

Nesta seção

Definir configurações gerais de tarefas 434
Configurar ações 437
Configurar o desempenho 438
Configuração de armazenamento hierárquico 440

Definir configurações gerais de tarefas

► *Para definir as configurações de segurança gerais da tarefa de Verificação por Demanda:*

1. Abra a janela **Configurações do escopo da verificação** (na página 427).
2. Selecione a guia **Geral**.
3. Na seção **Verificar objetos**, especifique os tipos objeto que deseja incluir no escopo da verificação:
   - **Objetos a serem verificados**
     - **Todos os objetos**

       O Kaspersky Embedded Systems Security verifica todos os objetos.
     - **Objetos verificados por formato**

       O Kaspersky Embedded Systems Security verificará somente objetos infectáveis com base no formato do arquivo.

       A lista de formatos é compilada pela Kaspersky Lab. Ela está incluída nos bancos de dados do Kaspersky Embedded Systems Security.
     - **Objetos verificados de acordo com a lista de extensões especificada no banco de dados do antivírus**

       O Kaspersky Embedded Systems Security verificará somente objetos infectáveis com base na extensão do arquivo.

       A lista de extensões é compilada pela Kaspersky Lab. Ela está incluída nos bancos de dados do Kaspersky Embedded Systems Security.
     - **Objetos verificados pela lista de extensões especificada**

       O Kaspersky Embedded Systems Security verificará os arquivos baseados em suas extensões. A lista de extensões de arquivo pode ser personalizada manualmente na janela **Lista de extensões**, que pode ser aberta clicando no botão **Editar**.
   - **Verificar setores de inicialização do disco e MBR**

Ativa a proteção dos setores de inicialização e dos registros mestres de inicialização.

Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os setores de inicialização e os registros mestres de inicialização nos discos rígidos e unidades removíveis do computador.

A caixa de seleção é selecionada por padrão.

- **Verificar fluxos NTFS alternativos**

  Verificação de fluxos alternativos de arquivos e pastas nas unidades do sistema de arquivos NTFS.

  Se a caixa estiver selecionada, o aplicativo verifica um objeto possivelmente infectado e todos os fluxos NTFS associados àquele objeto.

  Se a caixa estiver desmarcada, o aplicativo verifica apenas o objeto detectado e considerado possivelmente infectado.

  A caixa de seleção é selecionada por padrão.

4. Na seção **Desempenho**, selecione ou desmarque a caixa **Verificar apenas arquivos novos e modificados**.

   Esta caixa de seleção ativa/desativa a verificação e a proteção de arquivos que foram reconhecidos pelo Kaspersky Embedded Systems Security como novos ou modificados desde a última verificação.

   Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará e protegerá apenas os arquivos reconhecidos como novos ou modificados desde a última verificação.

   Se a caixa estiver desmarcada, você poderá selecioná-la se quiser verificar e proteger apenas arquivos novos ou todos os arquivos, desconsiderando o status de modificação.

   Por padrão, a caixa de seleção está selecionada para o nível de segurança **Desempenho máximo**. Se os níveis de segurança **Proteção máxima** ou **Recomendado** estiverem definidos, a caixa estará desmarcada.

   Para alternar entre as opções disponíveis quando a caixa estiver desmarcada, clique no link **Todos** / **Apenas novos** para cada um dos tipos de objetos compostos.

5. Na seção **Verificação de objetos compostos**, especifique os objetos compostos que deseja incluir no escopo da verificação:

   - **Todos / Apenas novos arquivos compactados**

     Verificação dos arquivos compactados ZIP, CAB, RAR, ARJ e de outros formatos.

     Se essa a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos compactados.

     Se essa caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos compactados durante a verificação.

     O valor padrão depende do nível de proteção selecionado.

   - **Todos / Apenas novos arquivos compactados SFX**

     Verificação de arquivos compactados autoextraíveis.

     Se essa caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security

ignorará os arquivos compactados durante a verificação.

Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos compactados SFX durante a verificação.

O valor padrão depende do nível de proteção selecionado.

Essa opção fica ativa quando a caixa de seleção **Arquivos compactados** é desmarcada.

- **Todos / Apenas novos bancos de dados de e-mail**

  Verificação de arquivos de banco de dados de correio do Microsoft Outlook e Microsoft Outlook Express.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos de bancos de dados de e-mail.

  Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos de bancos de dados de e-mail durante a verificação.

  O valor padrão depende do nível de segurança selecionado.

- **Todos / Apenas novos objetos compactados**

  Verificação de arquivos executáveis compactados por compactadores de código binário, como UPX ou ASPack.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos executáveis compactados por compactadores de código binário.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos executáveis compactados por compactadores de código binário durante a verificação.

  O valor padrão depende do nível de proteção selecionado.

- **Todos / Apenas novos e-mails sem formatação**

  Verificação de arquivos de formato de e-mail, como mensagens do Microsoft Outlook e Microsoft Outlook Express.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os arquivos de formato de e-mail.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os arquivos de formato de e-mail durante a verificação.

  O valor padrão depende do nível de segurança selecionado.

- **Todos / Apenas novos objetos OLE incorporados**

  Verificação de objetos incorporados em arquivos (como macros do Microsoft Word ou anexos de e-mail).

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará os objetos inseridos em arquivos.

  Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security ignorará os objetos inseridos em arquivos durante a verificação.

  O valor padrão depende do nível de proteção selecionado.

6. Clique em **Salvar**.

A nova configuração de tarefa será salva.

Configurar ações

► *Para configurar as ações em objetos infectados e outros objetos detectados da tarefa Verificação por Demanda:*

1. Abra a janela **Configurações do escopo da verificação** (na página 427).
2. Selecione a guia **Ações**.
3. Selecione a ação a ser executada em objetos infectados e outros objetos detectados.
   - **Notificar somente**.

     Quando esse modo estiver selecionado, o Kaspersky Embedded Systems Security não bloqueará o acesso a objetos infectados ou outros objetos detectados, nem executará qualquer ação sobre eles. O seguinte evento é registrado no log de tarefas: *Objeto não desinfectado. Motivo: nenhuma ação foi executada para neutralizar o objeto detectado devido a configurações definidas pelos usuários.* O evento especifica todas as informações disponíveis sobre o objeto detectado.

     O modo **Notificar somente** deve ser configurado separadamente para cada área de verificação. Este modo não é usado por padrão para qualquer um dos níveis de segurança. Se você selecionar esse modo, o Kaspersky Embedded Systems Security alterará automaticamente o nível de segurança para **Personalizado**.
   - **Desinfectar**.
   - **Desinfectar. Desinfectar. Remover se a desinfecção falhar**.
   - **Remover**.
   - **Executar ação recomendada**.
4. Selecione a ação a ser executada em objetos possivelmente infectados:
   - **Notificar somente**.

     Quando esse modo estiver selecionado, o Kaspersky Embedded Systems Security não bloqueará o acesso a objetos infectados ou outros objetos detectados, nem executará qualquer ação sobre eles. O seguinte evento é registrado no log de tarefas: *Objeto não desinfectado. Motivo: nenhuma ação foi executada para neutralizar o objeto detectado devido a configurações definidas pelos usuários.* O evento especifica todas as informações disponíveis sobre o objeto detectado.

     O modo **Notificar somente** deve ser configurado separadamente para cada área de verificação. Este modo não é usado por padrão para qualquer um dos níveis de segurança. Se você selecionar esse modo, o Kaspersky Embedded Systems Security alterará automaticamente o nível de segurança para **Personalizado**.
   - **Quarentena**.
   - **Remover**.
   - **Executar ação recomendada**.
5. Configure ações a serem executadas em objetos dependendo do tipo de objeto detectado:
   a. Desmarque ou selecione a caixa **Executar ações dependendo do tipo de objeto detectado**.

      Se a caixa for selecionada, você pode definir a ação primária e secundária independentemente para cada tipo de objeto detectado clicando no botão **Configurações** ao lado da caixa. Nesse caso, o Kaspersky Embedded Systems Security não permitirá

que um objeto infectado seja aberto ou executado independentemente da sua escolha.

Se a caixa de seleção for desmarcada, o Kaspersky Embedded Systems Security executará as ações selecionadas nas seções **Ação a ser executada em objetos infectados e outros** e **Ação a ser executada em objetos possivelmente infectados** para os tipos de objetos indicados, respectivamente.

Esta caixa é desmarcada por padrão.

b. Clique no botão **Configurações**.

c. Na janela que se abre, selecione a ação primária e secundária (se a primeira ação falhar) para cada tipo de objeto detectado.

d. Clique em **OK**.

6. Selecione a ação a ser executada em objetos compostos incuráveis: selecione ou desmarque a caixa **Remover completamente o arquivo composto que não pode ser modificado pelo aplicativo caso detecte objeto incorporado**.

Esta caixa ativa ou desativa a remoção forçada do arquivo composto pai quando um objeto malicioso, possivelmente infectado ou outro objeto filho incorporado for detectado.

Se a caixa estiver selecionada e a tarefa for configurada para remover objetos infectados e possivelmente infectados, o Kaspersky Embedded Systems Security forçosamente removerá todo o objeto composto pai quando um objeto incorporado malicioso ou outro objeto for detectado. A remoção forçada de um arquivo pai juntamente com todo o seu conteúdo ocorrerá se o aplicativo não puder remover apenas o objeto filho detectado (por exemplo, se o objeto pai não puder ser modificado).

Se esta caixa estiver desmarcada e a tarefa for configurada para remover objetos infectados e possivelmente infectados, o Kaspersky Embedded Systems Security não executará a ação selecionada se o objeto pai não puder ser modificado.

7. Clique em **Salvar**.

A nova configuração de tarefa será salva.

Configurar o desempenho

► *Para configurar o desempenho da tarefa de Verificação por Demanda:*

1. Abra a janela **Configurações do escopo da verificação** (na página 427).
2. Selecione a guia **Desempenho**.
3. Na seção **Exclusões**:

- Desmarque ou selecione a caixa **Excluir arquivos**.

Excluindo arquivos da verificação pelo nome de arquivo ou pela máscara de nome de arquivo.

Se esta caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará os objetos especificados durante a verificação.

Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará todos os objetos.

Esta caixa é desmarcada por padrão.

- Desmarque ou selecione a caixa **Não detectar**.

Os objetos são excluídos da verificação pelo nome ou pela máscara de nome do objeto detectável. A lista de nomes de objetos detectáveis está disponível no site da Enciclopédia de Vírus https://encyclopedia.kaspersky.com/knowledge/classification/.

Se esta caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará os objetos detectáveis especificados durante a verificação.

Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security detectará todos os objetos especificados no aplicativo por padrão.

Esta caixa é desmarcada por padrão.

- Clique no botão **Editar** de cada configuração para adicionar exclusões.

4. Na seção **Configurações avançadas**:

- **Parar a verificação se demorar mais que (s)**

  Limita a duração da verificação do objeto. O valor padrão é 60 segundos.

  Se a caixa de seleção estiver selecionada, a duração da verificação será limitada ao valor especificado.

  Se a caixa de seleção estiver desmarcada, a duração da verificação será ilimitada.

  Por padrão, a caixa de seleção está selecionada para o nível de segurança **Desempenho máximo**.

- **Não verificar obj. compostos com mais de (MB)**

  Exclui objetos maiores do que o tamanho especificado na verificação.

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará objetos compostos cujo tamanho exceda o limite especificado durante a verificação de vírus.

  Se esta caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará os objetos compostos de qualquer tamanho.

  Por padrão, a caixa de seleção está selecionada para o nível de segurança **Desempenho máximo**.

- **Usar a tecnologia iSwift**

  A tecnologia iSwift compara o identificador NTFS do arquivo armazenado em um banco de dados com um identificador atual. A verificação é executada apenas para arquivos cujos identificadores foram alterados (novos arquivos e arquivos modificados desde a última verificação dos objetos do sistema NTFS).

  Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará apenas os novos arquivos ou aqueles modificados desde a última verificação dos objetos do sistema NTFS.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará objetos do sistema de arquivos NTFS sem considerar a data de criação ou modificação do arquivo, exceto em arquivos das pastas de rede.

  A caixa de seleção é selecionada por padrão.

- **Usar a tecnologia iChecker**

  A tecnologia iChecker calcula e lembra de somas de verificação de arquivos verificados. Se um objeto for modificado a soma de verificação é alterada. O aplicativo compara todas

as somas de verificação durante a tarefa de verificação e verifica apenas objetos novos e modificados desde a última verificação de arquivos.

Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security verificará apenas arquivos novos e modificados.

Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará os arquivos sem considerar a data de criação ou modificação do arquivo.

A caixa de seleção é selecionada por padrão.

5. Clique em **Salvar**.

A nova configuração de tarefa será salva.

Configuração de armazenamento hierárquico

► *Para configurar as ações em objetos infectados e outros objetos detectados da tarefa Verificação por Demanda:*

1. Abra a janela **Configurações do escopo da verificação** (na página 427).
2. Selecione a guia **Armazenamento hierárquico**.
3. Selecione a ação a ser executada nos arquivos offline:
   - **Não verificar**.
   - **Verificar apenas a parte residente do arquivo**.
   - **Verificar o arquivo inteiro**.

     Se esta ação for selecionada, você poderá especificar as seguintes opções:

     - Selecione ou desmarque a caixa **Somente se o arquivo foi acessado no período especificado (dias)** e especifique o número de dias.
     - Selecione ou desmarque a caixa **Não copiar o arquivo para o disco rígido local, se possível**.
4. Clique em **Salvar**.

A nova configuração de tarefa será salva.

Verificação de unidades removíveis

► *Para configurar a verificação de unidades removíveis após a conexão ao computador protegido no Console do Aplicativo:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Kaspersky Embedded Systems Security** e selecione a opção **Configurar verificação de unidades removíveis**.

   A janela **Verificações de unidades removíveis** é exibida.
2. Na seção **Verificação na conexão**, faça o seguinte:
   - Marque a caixa de seleção **Verificar unidades removíveis na conexão via USB**, se desejar que o Kaspersky Embedded Systems Security verifique automaticamente as unidades removíveis quando elas forem conectadas.
   - Se necessário, selecione **Verificar unidades removíveis se o volume de dados armazenados não**

exceder (MB) e especifique o valor máximo no campo à direita.

- Na lista suspensa **Verificação com nível de segurança**, especifique o nível de segurança com as configurações exigidas para a verificação de unidades removíveis.

3. Clique em **OK**.

As configurações específicas são salvas e aplicadas.

Estatísticas da tarefa de Verificação por Demanda

Enquanto uma tarefa de Verificação por Demanda está sendo executada, é possível exibir informações sobre o número de objetos processados pelo Kaspersky Embedded Systems Security desde que ele foi iniciado até o momento atual.

Essas informações permanecem disponíveis mesmo que a tarefa seja pausada. Você pode exibir estatísticas da tarefa no log de tarefas (consulte a seção "Visualizando estatísticas e informações sobre uma tarefa do Kaspersky Embedded Systems Security em logs de tarefas" na página 206).

► *Para exibir as estatísticas de uma tarefa de Verificação por Demanda, siga as etapas a seguir:*

1. Expanda o nó **Verificação por Demanda** na árvore do Console do Aplicativo.
2. Selecione a tarefa de Verificação por Demanda cujas estatísticas você deseja exibir.

As estatísticas de tarefa são exibidas na seção **Estatísticas** do painel de detalhes do nó selecionado.

É possível exibir as seguintes informações sobre os objetos processados pelo Kaspersky Embedded Systems Security desde que foi iniciado até o momento atual (veja a tabela abaixo).

Tabela 61. Estatísticas da tarefa de Verificação por Demanda

Campo	Descrição
Detectado	Número total de objetos detectados pelo Kaspersky Embedded Systems Security. Por exemplo, se o Kaspersky Embedded Systems Security detectar um malware em cinco arquivos, o valor desse campo aumentará em um.
Objetos infectados e outros detectados	O número de objetos que o Kaspersky Embedded Systems Security encontrou e classificou como infectados ou o número de arquivos de software legítimos encontrados, que não foram excluídos do escopo das tarefas de proteção em tempo real e por demanda e foram classificados como softwares legítimos que podem ser usados por intrusos para danificar seu computador ou seus dados pessoais.
Objetos detectados possivelmente suspeitos	Número de objetos encontrados pelo Kaspersky Embedded Systems Security que estão possivelmente infectados.
Objetos não desinfectados	Número de objetos que o Kaspersky Embedded Systems Security não desinfetou pelos seguintes motivos: • O tipo de objeto detectado não pode ser desinfectado. • Ocorreu um erro durante a desinfecção.
Objetos não movidos para a Quarentena	Número de objetos que o Kaspersky Embedded Systems Security tentou colocar na Quarentena mas que não conseguiu, devido a espaço insuficiente no disco.

Campo	Descrição
Objetos não removidos	Número de objetos que o Kaspersky Embedded Systems Security tentou excluir mas não conseguiu, devido, por exemplo, a um bloqueio no acesso ao objeto por parte de outro aplicativo.
Objetos não verificados	Número de objetos no escopo de proteção que o Kaspersky Embedded Systems Security não verificou devido, por exemplo, ao acesso ao objeto estar bloqueado por outro aplicativo.
Objetos sem backup	Número de objetos cujas cópias o Kaspersky Embedded Systems Security tentou salvar no Backup mas não conseguiu, por exemplo, devido a espaço de disco insuficiente.
Erros de processamento	Número de objetos cujo processamento resultou em um erro.
Objetos desinfectados	Número de objetos desinfectados pelo Kaspersky Embedded Systems Security.
Movidos para a Quarentena	Número de objetos colocados na Quarentena pelo Kaspersky Embedded Systems Security.
Movidos para o backup	Número de cópias de objetos salvas pelo Kaspersky Embedded Systems Security no Backup.
Objetos removidos	Número de objetos removidos pelo Kaspersky Embedded Systems Security.
Objetos protegidos por senha	Número de objetos (arquivos compactados, por exemplo) que o Kaspersky Embedded Systems Security ignorou porque estavam protegidos por senha.
Objetos corrompidos	Número de objetos ignorados pelo Kaspersky Embedded Systems Security devido a corrupção do formato.
Objetos processados	Número total de objetos processados pelo Kaspersky Embedded Systems Security.

Você também pode visualizar as estatísticas da tarefa de Verificação por Demanda no log de tarefas selecionado clicando no link **Abrir log da tarefa** na seção **Gerenciamento** do painel de detalhes.

Recomenda-se processar manualmente os eventos registrados no log de tarefas na guia **Eventos** após a conclusão da tarefa.

Zona Confiável

Essa seção fornece informações sobre a Zona Confiável do Kaspersky Embedded Systems Security, bem como instruções sobre como adicionar objetos à Zona Confiável ao executar tarefas.

Neste capítulo

Sobre a Zona Confiável 443
Gerenciamento da Zona Confiável por meio do Plug-in de Administração 444
Gerenciamento da Zona Confiável por meio do Console do Aplicativo 450

Sobre a Zona Confiável

A Zona Confiável é uma lista de exclusões da proteção ou escopo da verificação que você pode gerar e aplicar às tarefas de Verificação por Demanda e às de Proteção de Arquivos em Tempo Real.

Se você marcou as caixas de seleção **Adicionar arquivos recomendados pela Microsoft à lista de exclusões** e **Adicionar arquivos recomendados pela Kaspersky Lab à lista de exclusões** ao instalar o Kaspersky Embedded Systems Security, o Kaspersky Embedded Systems Security adicionará à Zona Confiável os arquivos recomendados pela Microsoft e pela Kaspersky Lab para as tarefas de Proteção do Computador em Tempo Real.

Você pode criar um Zona Confiável no Kaspersky Embedded Systems Security de acordo com as seguintes regras:

- Processos confiáveis. Objetos acessados por processos do aplicativo sensíveis a intercepções de arquivo são colocados na Zona Confiável.
- Operações de Backup. Objetos acessados por sistemas para fazer backup de discos rígidos em dispositivos externos são colocados na Zona Confiável.
- Exclusões. Objetos especificados por localização e/ou um objeto detectado dentro deles são colocados na Zona Confiável.

Você pode aplicar a Zona Confiável a tarefas de Proteção de Arquivos em Tempo Real, a tarefas personalizadas de Verificação por Demanda recém-criadas e em todas as tarefas de Verificação por Demanda do sistema, exceto a tarefa de Verificação da Quarentena.

A Zona Confiável é aplicada às tarefas de Proteção de Arquivos em Tempo Real e de Verificação por Demanda por padrão.

A lista de regras para gerar a Zona Confiável pode ser exportada a um arquivo de configuração no formato XML para que ele seja importado no Kaspersky Embedded Systems Security sendo executado em outro computador.

Processos confiáveis

Aplica-se às tarefas de Proteção de Arquivos em Tempo Real e de Segurança de Tráfego.

Alguns aplicativos no computador podem ser instáveis se os arquivos que acessam forem interceptados pelo Kaspersky Embedded Systems Security. Esses aplicativos incluem, por exemplo, controladores de domínio do sistema.

Para não afetar a operação desses aplicativos, você pode desativar a proteção de arquivos acessados pelos processos de execução desses aplicativos (dessa forma criando uma lista de processos confiáveis na Zona

Confiável).

A Microsoft Corporation recomenda excluir alguns arquivos do sistema operacional Microsoft Windows e arquivos de aplicativo da Microsoft da Proteção de Arquivos em Tempo Real como programas que não podem ser infectados. Os nomes de alguns deles estão listados no site da Microsoft https://www.microsoft.com/en-us/ (código do artigo: KB822158).

Você pode ativar ou desativar o uso de processos confiáveis na Zona Confiável.

Se o processo executável for modificado, por exemplo, se for atualizado, o Kaspersky Embedded Systems Security vai excluí-lo da lista de processos confiáveis.

O aplicativo não aplica o caminho ao valor do arquivo em um computador protegido para confiar no processo. O caminho para o arquivo no computador protegido é usado somente para procurar o arquivo, calcular uma soma de verificação e fornecer ao usuário informações sobre a origem do arquivo executável.

Operações de backup

Aplica-se a tarefas de Proteção do Computador em Tempo Real.

Enquanto os dados armazenados nos discos rígidos passam por backup em dispositivos externos, você pode desativar a proteção de objetos que são acessados durante as operações de backup. O Kaspersky Embedded Systems Security verificará os objetos que o aplicativo de cópia de backup abre para leitura com o atributo FILE_FLAG_BACKUP_SEMANTICS.

Exclusões

Aplica-se às tarefas de Proteção de Arquivos em Tempo Real e de Verificação por Demanda.

Você pode selecionar tarefas para as quais deseja usar todas as exclusões adicionadas à Zona Confiável. Além disso, você pode excluir objetos de verificações nas configurações do nível de segurança de todas as tarefas do Kaspersky Embedded Systems Security.

Você pode adicionar objetos à Zona Confiável de acordo com a localização no computador, por nome ou pela máscara de nomes do objeto detectado nesses objetos, ou usando ambos os critérios.

Com base na exclusão, o Kaspersky Embedded Systems Security pode ignorar objetos enquanto executa as tarefas especificadas de acordo com as configurações que se seguem:

- Objetos especificados detectáveis por nome ou máscara de nome nas áreas especificadas do computador.
- Todos os objetos detectáveis nas áreas especificadas do computador.
- Objetos detectáveis especificados por nome ou máscara de nome em todo o escopo da proteção ou da verificação.

Gerenciamento da Zona Confiável por meio do Plug-in de Administração

Nesta seção, aprenda como navegar pela interface do Plug-in de Administração e configurar a Zona Confiável para um ou para todos os computadores da rede.

Nesta seção

Navegação 445
Configuração da Zona Confiável por meio do Plug-in de Administração 446

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface.

Nesta seção

Gerenciamento do Aplicativo por meio do Kaspersky Security Center 445
Abertura da janela de propriedades da Zona Confiável 445

Gerenciamento do aplicativo por meio do Kaspersky Security Center

► *Para abrir a Zona Confiável por meio da política do Kaspersky Security Center:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Suplementar**.
6. Clique no botão **Configurações** na subseção **Zona Confiável**.

   A janela **Zona Confiável** é aberta.

Configure a política conforme necessário.

Se um computador estiver sendo gerenciado por uma política ativa do Kaspersky Security Center e esta política bloquear as alterações nas configurações do aplicativo, essas configurações não poderão ser editadas por meio do Console do Aplicativo.

Abertura da janela de propriedades da Zona Confiável

► *Para configurar a Zona Confiável na janela de propriedades do Aplicativo:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.

3. Selecione a guia **Dispositivos**.
4. Abra a janela **Propriedades: <Nome do computador>** de uma das seguintes maneiras:
   - Clique duas vezes no nome do computador protegido.
   - Selecione o item **Propriedades** no menu de contexto do computador protegido.

   A janela **Propriedades: <Nome do computador>** é exibida.
5. Na seção **Aplicativos**, selecione **Kaspersky Embedded Systems Security**.
6. Clique no botão **Propriedades**.

   A janela de **configurações do Kaspersky Embedded Systems Security** é exibida.
7. Selecione a seção **Suplementar**.
8. Clique no botão **Configurações** na subseção **Zona Confiável**.

   A janela **Zona Confiável** é aberta.

Configure a Zona Confiável conforme necessário.

Configuração da Zona Confiável por meio do Plug-in de Administração

Por padrão, a Zona Confiável é aplicada a todas as políticas e tarefas recém-criadas.

Para definir as configurações da Zona Confiável, faça o seguinte:

1. Especifique os objetos a serem ignorados (consulte a seção "Adicionar uma exclusão" na página 446) pelo Kaspersky Embedded Systems Security durante a execução da tarefa na guia **Exclusões**.
2. Especifique os processos a serem ignorados (consulte a seção "Adicionar processos confiáveis" na página 448) pela Kaspersky Embedded Systems Security durante a execução da tarefa na guia **Processos confiáveis**.
3. Aplique a máscara de não vírus (consulte a seção "Aplicação da máscara de não vírus" na página 450).

Nesta seção

Adição de uma exclusão....446
Adicionar processos confiáveis....448
Aplicar a máscara de não vírus....450

Adição de uma exclusão

► *Para adicionar uma exclusão à Zona Confiável por meio da política do Kaspersky Security Center:*

1. Abra a janela **Zona Confiável (consulte a seção "Gerenciamento do aplicativo por meio do Kaspersky Security Center" na página 445)**.
2. Na guia **Exclusões**, especifique os objetos a serem ignorados pelo Kaspersky Embedded Systems Security durante a verificação:
   - Para criar exclusões recomendadas, clique no botão **Adicionar exclusões recomendadas**.

     Clicar neste botão permite a extensão da lista de exclusões ao adicionar exclusões

recomendadas pela Microsoft, exclusões recomendadas pela Kaspersky Lab.

- Para importar exclusões, clique no botão **Importar** e, na janela exibida, selecione os arquivos que o Kaspersky Embedded Systems Security considerará confiável.
- Para especificar manualmente as condições sob as quais um arquivo será considerado confiável, clique no botão **Adicionar**.

  A janela **Exclusão** é aberta.

3. Na seção **O objeto não será verificado se as seguintes condições forem preenchidas**, especifique os objetos que deseja excluir do escopo da proteção/verificação e os objetos que deseja excluir dos objetos detectáveis:
   - Se você desejar excluir um objeto do escopo da proteção ou verificação:
     a. Marque a caixa de seleção **Objeto a ser verificado**.

        Adiciona um arquivo, pasta, disco rígido, ou arquivo de script a uma exclusão.

        Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security ignorará o escopo, arquivo, pasta, disco ou arquivo de script predefinido enquanto executa a verificação com o uso do componente do Kaspersky Embedded Systems Security selecionado na seção **Escopo de uso da regra**.

        Esta caixa é desmarcada por padrão.

     b. Clique no botão **Editar**.

        A janela **Selecionar objeto** será aberta.

     c. Especifique o objeto que você quer excluir do escopo da verificação.

        > Você pode usar símbolos especiais, como "?" e "*", ao especificar objetos.

     d. Clique em **OK**.

     e. Selecione a caixa **Aplicar também às subpastas** se você quiser excluir todos os arquivos e pastas filhos do objeto especificado do escopo de proteção ou verificação.
   - Se deseja especificar o nome de um objeto detectável:
     a. Marque a caixa de seleção **Objetos a ser detectados**.

        Os objetos são excluídos da verificação pelo nome ou pela máscara de nome do objeto detectável. A lista de nomes de objetos detectáveis está disponível no site da Enciclopédia de Vírus.

        Se esta caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará os objetos detectáveis especificados durante a verificação.

        Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security detectará todos os objetos especificados no aplicativo por padrão.

        Esta caixa é desmarcada por padrão.

     b. Clique no botão **Editar**.

        A janela **Lista de objetos a ser detectados** é exibida.

     c. Especifique o nome ou a máscara do nome do objeto detectável de acordo com a classificação da Enciclopédia de Vírus.

d. Clique no botão **Adicionar**.

e. Clique em **OK**.

4. Na seção **Escopo de uso da regra**, selecione as caixas junto aos nomes das tarefas às quais você deseja aplicar a exclusão.

   Nome da tarefa do Kaspersky Embedded Systems Security na qual a regra é usada.

5. Clique em **OK**.

A exclusão é exibida na lista na guia **Exclusões** da janela **Zona Confiável**.

Adicionar processos confiáveis

► *Para adicionar um ou um número de processos à lista de processos confiáveis:*

1. Abra a janela **Zona Confiável** (consulte a seção "Gerenciamento do aplicativo por meio do Kaspersky Security Center" na página 445).
2. Selecione a guia **Processos confiáveis**.
3. Selecione a caixa **Não verificar operações de backup de arquivos** para ignorar a verificação de operações de leitura de arquivos.

   A caixa de seleção ativa ou desativa a verificação de operações de leitura de arquivos se tais operações forem executadas pelas ferramentas de backup instaladas no computador.

   Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará as operações de leitura de arquivos executadas pelas ferramentas de Backup instaladas no computador.

   Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará as operações de leitura de arquivos executadas pelas ferramentas de Backup instaladas no computador.

   A caixa de seleção é selecionada por padrão.

4. Selecione a caixa **Não verificar a atividade dos arquivos dos processos especificados** para ignorar a verificação de operações em arquivos de processos confiáveis.

   A caixa de seleção ativa ou desativa a verificação da atividade dos arquivos dos processos confiáveis.

   Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará as operações dos processos confiáveis durante a verificação.

   Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará as operações de arquivos dos processos confiáveis.

   Esta caixa é desmarcada por padrão.

5. Clique no botão **Adicionar**.
6. A partir do menu de contexto do botão, selecione uma das seguintes opções:

   - **Múltiplos processos**.

     Na janela **Adicionando processos confiáveis** que se abre, configure o seguinte:

     a. **Use o caminho inteiro do processo no disco para saber se é confiável**

        Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security usará o

caminho completo do arquivo para determinar se o processo é confiável.

Se a caixa de seleção estiver desmarcada, o caminho para o arquivo não é usado para determinar se o processo é confiável.

Esta caixa é desmarcada por padrão.

b. **Use o hash de arquivo do processo para saber se é confiável**.

Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security usará o hash do arquivo selecionado para determinar o status de confiança do processo.

Se a caixa de seleção for desmarcada, o hash do arquivo não será usado para determinar o status de confiança do processo.

A caixa de seleção é selecionada por padrão.

c. Clique no **Procurar** para adicionar dados baseados em processos executáveis.

d. Selecione um outro arquivo executável na janela que se abre.

> É possível adicionar apenas um arquivo executável por vez. Repita as etapas c-d para adicionar outros arquivos executáveis.

e. Clique no botão **Processos** para adicionar dados baseados em processos em execução.

f. Selecione processos na janela que se abre. Para selecionar múltiplos processos, pressione e segure o botão **CTRL** ao selecionar.

g. Clique em **OK**.

> É requerido que a conta em que a tarefa Proteção de Arquivos em Tempo Real é executada tenha direitos de administrador no computador com o Kaspersky Embedded Systems Security instalado para que seja possível visualizar a lista de processos ativos. Você pode ordenar processos na lista de processos ativos por nome de arquivo, identificador do processo (PID) ou caminho para o arquivo executável do processo no computador local. Note que é possível selecionar processos em execução clicando no botão **Processos** usando apenas o Console do Aplicativo em um computador local, ou nas configurações do host especificado por meio do Kaspersky Security Center.

- **Um processo baseado no nome e no caminho do arquivo.**

  Na janela **Adicionando um processo**, faça o seguinte:

  a. Insira um caminho para o arquivo executável (inclusive o nome do arquivo).

  b. Clique em **OK**.

- **Um processo baseado nas propriedades do objeto.**

  Na janela **Adicionando um processo confiável**, configure o seguinte:

  a. Clique no botão **Procurar** e selecione um processo.

  b. **Use o caminho inteiro do processo no disco para saber se é confiável**

  Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security usará o caminho completo do arquivo para determinar se o processo é confiável.

  Se a caixa de seleção estiver desmarcada, o caminho para o arquivo não é usado para

determinar se o processo é confiável.

Esta caixa é desmarcada por padrão.

c. **Use o hash de arquivo do processo para saber se é confiável**.

Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security usará o hash do arquivo selecionado para determinar o status de confiança do processo.

Se a caixa de seleção for desmarcada, o hash do arquivo não será usado para determinar o status de confiança do processo.

A caixa de seleção é selecionada por padrão.

d. Clique em **OK**.

Para adicionar o processo selecionado à lista de processos confiáveis, pelo menos um critério de confiança deve ser selecionado.

7. Na janela **Adicionar processos confiáveis**, clique no botão **OK**.

O arquivo ou processo selecionado será adicionado à lista de processos confiáveis na janela **Zona Confiável**.

Aplicar a máscara de não vírus

A máscara de não vírus permite ignorar arquivos de software e recursos da web legítimos, que podem ser considerados perigosos, durante a verificação. A máscara afeta as seguintes tarefas:

- Proteção de Arquivos em Tempo Real.
- Verificação por Demanda.

Se a máscara não for adicionada à lista de exclusões, o Kaspersky Embedded Systems Security aplicará as ações especificadas nas configurações da tarefa para os recursos de software nesta categoria.

► *Para aplicar a máscara de não vírus:*

1. Abra a janela **Zona Confiável** (consulte a seção "Gerenciamento do aplicativo por meio do Kaspersky Security Center" na página 445).
2. Na guia **Exclusões** , na coluna **Objetos a ser detectados**, role a lista e selecione a linha com o valor **não vírus:***, se a caixa de seleção estiver desmarcada.
3. Clique em **OK**.

A nova configuração é aplicada.

Gerenciamento da Zona Confiável por meio do Console do Aplicativo

Nesta seção, aprenda como navegar pela interface do Console do Aplicativo e configurar a Zona Confiável em um computador local.

Nesta seção

Aplicar Zona Confiável para tarefas no Console do Aplicativo 451
Configuração da Zona Confiável no Console do Aplicativo 451

Aplicar Zona Confiável para tarefas no Console do Aplicativo

Por padrão, a Zona Confiável é aplicada à tarefa de Proteção de Arquivos em Tempo Real, tarefas de Verificação por Demanda personalizadas recém-criadas e em todas as tarefas de Verificação por Demanda do sistema, exceto a tarefa de Verificação da Quarentena.

Após a Zona Confiável ser ativada ou desativada, as exclusões especificadas serão aplicadas imediatamente ou deixarão de ser aplicadas a tarefas em execução.

► *Para ativar ou desativar o uso da Zona Confiável em tarefas do Kaspersky Embedded Systems Security:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto da tarefa para a qual deseja configurar o uso da Zona Confiável.
2. Selecione **Propriedades**.

   A janela **Configurações de tarefa** é exibida.
3. Na janela aberta, selecione a guia **Geral** e execute uma das seguintes ações:
   - Para aplicar a zona confiável à tarefa, selecione a caixa **Aplicar Zona Confiável**.
   - Para desativar a Zona Confiável na tarefa, desmarque a caixa de seleção **Aplicar Zona Confiável**.
4. Se você deseja configurar a Zona Confiável, clique no link sobre o nome da caixa de seleção **Aplicar Zona Confiável** .

   A janela **Zona Confiável** é aberta.
5. Clique em **OK** na janela **Configurações da tarefa** para salvar as alterações.

Configuração da Zona Confiável no Console do Aplicativo

Para definir as configurações da Zona Confiável, faça o seguinte:

1. Especifique os objetos a serem ignorados (consulte a seção "Adicionar uma exclusão à Zona Confiável" na página 452) pelo Kaspersky Embedded Systems Security durante a execução da tarefa na guia **Exclusões**.
2. Especifique os processos a serem ignorados (consulte a seção "Processos confiáveis" na página 453) pelo Kaspersky Embedded Systems Security durante a execução da tarefa na guia **Processos confiáveis**.
3. Aplicar a Zona Confiável para as tarefas do aplicativo (consulte a seção "Aplicação da Zona Confiável a tarefas no Console do Aplicativo" na página 451).
4. Aplique a máscara de não vírus (consulte a seção "Aplicação da máscara de não vírus" na página 455).

Nesta seção

Adição de uma exclusão à Zona Confiável 452
Processos confiáveis 453
Aplicar a máscara de não vírus 455

Adição de uma exclusão à Zona Confiável

► *Para adicionar uma exclusão manualmente à Zona Confiável por meio do Console do Aplicativo:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Kaspersky Embedded Systems Security**.
2. Selecione a opção de menu **Configurar a Zona Confiável**.

   A janela **Zona Confiável** é aberta.
3. Selecione a guia **Exclusões**.
4. Clique no botão **Adicionar**.

   A janela **Exclusão** é aberta.
5. Na seção **O objeto não será verificado se as seguintes condições forem preenchidas**, especifique os objetos que deseja excluir do escopo da proteção/verificação e os objetos que deseja excluir dos objetos detectáveis:
   - Se você desejar excluir um objeto do escopo da proteção ou verificação:
     a. Marque a caixa de seleção **Objeto a ser verificado**.

        Adiciona um arquivo, pasta, disco rígido, ou arquivo de script a uma exclusão.

        Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security ignorará o escopo, arquivo, pasta, disco ou arquivo de script predefinido enquanto executa a verificação com o uso do componente do Kaspersky Embedded Systems Security selecionado na seção **Escopo de uso da regra**.

        Esta caixa é desmarcada por padrão.

     b. Clique no botão **Editar**.

        A janela **Selecionar objeto** será aberta.

     c. Especifique o objeto que você quer excluir do escopo da verificação.

        > Você pode usar símbolos especiais, como "?" e "*", ao especificar objetos.

     d. Clique em **OK**.

     e. Selecione a caixa **Aplicar também às subpastas** se você quiser excluir todos os arquivos e pastas filhos do objeto especificado do escopo de proteção ou verificação.
   - Se deseja especificar o nome de um objeto detectável:
     a. Marque a caixa de seleção **Objetos a ser detectados**.

        Os objetos são excluídos da verificação pelo nome ou pela máscara de nome do objeto

detectável. A lista de nomes de objetos detectáveis está disponível no site da Enciclopédia de Vírus.

Se esta caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará os objetos detectáveis especificados durante a verificação.

Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security detectará todos os objetos especificados no aplicativo por padrão.

Esta caixa é desmarcada por padrão.

b. Clique no botão **Editar**.

A janela **Lista de objetos a ser detectados** é exibida.

c. Especifique o nome ou a máscara do nome do objeto detectável de acordo com a classificação da Enciclopédia de Vírus.

d. Clique no botão **Adicionar**.

e. Clique em **OK**.

6. Na seção **Escopo de uso da regra**, selecione as caixas junto aos nomes das tarefas às quais você deseja aplicar a exclusão.

Nome da tarefa do Kaspersky Embedded Systems Security na qual a regra é usada.

7. Clique em **OK**.

A exclusão é exibida na lista na guia **Exclusões** da janela **Zona Confiável**.

Processos confiáveis

Você pode adicionar um processo à lista de processos confiáveis usando um dos seguintes métodos:

- Selecione o processo na lista de processos em execução no computador protegido.
- Selecione o arquivo executável de um processo, independentemente de o processo estar ou não em execução no momento.

Se o arquivo executável de um processo tiver sido modificado, o Kaspersky Embedded Systems Security excluirá esse processo da lista de processos confiáveis.

► *Para adicionar um ou um número de processos à lista de processos confiáveis:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Kaspersky Embedded Systems Security**.
2. Selecione a opção de menu **Configurar a Zona Confiável**.

A janela **Zona Confiável** é aberta.

3. Selecione a guia **Processos confiáveis**.
4. Selecione a caixa **Não verificar operações de backup de arquivos** para ignorar a verificação de operações de leitura de arquivos.

A caixa de seleção ativa ou desativa a verificação de operações de leitura de arquivos se tais operações forem executadas pelas ferramentas de backup instaladas no computador.

Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security

ignorará as operações de leitura de arquivos executadas pelas ferramentas de Backup instaladas no computador.

Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará as operações de leitura de arquivos executadas pelas ferramentas de Backup instaladas no computador.

A caixa de seleção é selecionada por padrão.

5. Selecione a caixa **Não verificar a atividade dos arquivos dos processos especificados** para ignorar a verificação de operações em arquivos de processos confiáveis.

   A caixa de seleção ativa ou desativa a verificação da atividade dos arquivos dos processos confiáveis.

   Se a caixa de seleção estiver selecionada, o Kaspersky Embedded Systems Security ignorará as operações dos processos confiáveis durante a verificação.

   Se a caixa de seleção estiver desmarcada, o Kaspersky Embedded Systems Security verificará as operações de arquivos dos processos confiáveis.

   Esta caixa é desmarcada por padrão.

6. Clique no botão **Adicionar**.
7. A partir do menu de contexto do botão, selecione uma das seguintes opções:

   - **Múltiplos processos**.

     Na janela **Adicionando processos confiáveis** que se abre, configure o seguinte:

     a. **Use o caminho inteiro do processo no disco para saber se é confiável**

        Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security usará o caminho completo do arquivo para determinar se o processo é confiável.

        Se a caixa de seleção estiver desmarcada, o caminho para o arquivo não é usado para determinar se o processo é confiável.

        Esta caixa é desmarcada por padrão.

     b. **Use o hash de arquivo do processo para saber se é confiável**.

        Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security usará o hash do arquivo selecionado para determinar o status de confiança do processo.

        Se a caixa de seleção for desmarcada, o hash do arquivo não será usado para determinar o status de confiança do processo.

        A caixa de seleção é selecionada por padrão.

     c. Clique no **Procurar** para adicionar dados baseados em processos executáveis.

     d. Selecione um outro arquivo executável na janela que se abre.

        É possível adicionar apenas um arquivo executável por vez. Repita as etapas c-d para adicionar outros arquivos executáveis.

     e. Clique no botão **Processos** para adicionar dados baseados em processos em execução.

     f. Selecione processos na janela que se abre. Para selecionar múltiplos processos, pressione e segure o botão **CTRL** ao selecionar.

     g. Clique em **OK**.

É requerido que a conta em que a tarefa Proteção de Arquivos em Tempo Real é executada tenha direitos de administrador no computador com o Kaspersky Embedded Systems Security instalado para que seja possível visualizar a lista de processos ativos. Você pode ordenar processos na lista de processos ativos por nome de arquivo, identificador do processo (PID) ou caminho para o arquivo executável do processo no computador local. Note que é possível selecionar processos em execução clicando no botão **Processos** usando apenas o Console do Aplicativo em um computador local, ou nas configurações do host especificado por meio do Kaspersky Security Center.

- **Um processo baseado no nome e no caminho do arquivo.**

  Na janela **Adicionando um processo**, faça o seguinte:

  a. Insira um caminho para o arquivo executável (inclusive o nome do arquivo).

  b. Clique em **OK**.

- **Um processo baseado nas propriedades do objeto.**

  Na janela **Adicionando um processo confiável**, configure o seguinte:

  a. Clique no botão **Procurar** e selecione um processo.

  b. **Use o caminho inteiro do processo no disco para saber se é confiável**

     Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security usará o caminho completo do arquivo para determinar se o processo é confiável.

     Se a caixa de seleção estiver desmarcada, o caminho para o arquivo não é usado para determinar se o processo é confiável.

     Esta caixa é desmarcada por padrão.

  c. **Use o hash de arquivo do processo para saber se é confiável**.

     Se a caixa de seleção estiver marcada, o Kaspersky Embedded Systems Security usará o hash do arquivo selecionado para determinar o status de confiança do processo.

     Se a caixa de seleção for desmarcada, o hash do arquivo não será usado para determinar o status de confiança do processo.

     A caixa de seleção é selecionada por padrão.

  d. Clique em **OK**.

  Para adicionar o processo selecionado à lista de processos confiáveis, pelo menos um critério de confiança deve ser selecionado.

8. Na janela **Adicionar processos confiáveis**, clique no botão **OK**.

O arquivo ou processo selecionado será adicionado à lista de processos confiáveis na janela **Zona Confiável**.

Aplicar a máscara de não vírus

A máscara de não vírus permite ignorar arquivos de software e recursos da web legítimos, que podem ser considerados perigosos, durante a verificação. A máscara afeta as seguintes tarefas:

- Proteção de Arquivos em Tempo Real.
- Verificação por Demanda.

Se a máscara não for adicionada à lista de exclusões, o Kaspersky Embedded Systems Security aplicará as ações especificadas nas configurações da tarefa para os recursos de software ou da web nesta categoria.

► *Para aplicar a máscara de não vírus:*

1. Na árvore do Console do Aplicativo, abra o menu de contexto do nó **Kaspersky Embedded Systems Security**.
2. Selecione a opção de menu **Configurar a Zona Confiável**.

   A janela **Zona Confiável** é aberta.
3. Selecione a guia **Exclusões**.
4. Role pela lista e selecione a linha com o valor **não vírus:*** se a caixa de seleção estiver desmarcada.
5. Clique em **OK**.

A nova configuração é aplicada.

Prevenção de Exploits

Esta seção contém instruções sobre como definir configurações de proteção da memória do processo.

Neste capítulo

Sobre a Prevenção de Exploits 457

Gerenciamento da Prevenção de Exploits por meio do Plug-in de Administração 458

Gerenciamento da Prevenção de Exploits por meio do Console do Aplicativo 462

Técnicas de prevenção de exploits 466

Sobre a Prevenção de Exploits

O Kaspersky Embedded Systems Security oferece a capacidade de proteger a memória do processo contra exploits. Este recurso é implementado no componente de Prevenção de Exploits. Você pode alterar o status da atividade do componente e definir configurações de proteção da memória do processo.

O componente protege a memória do processo contra exploits inserindo um Agente de Proteção de Processo ("Agente") externo no processo protegido.

Um Agente de Proteção de Processo é um módulo do Kaspersky Embedded Systems Security dinamicamente carregado que é inserido em processos protegidos para monitorar a sua integridade e reduzir o risco de eles serem explorados.

A operação do Agente dentro do processo protegido exige a inicialização e a interrupção do processo: o carregamento inicial do Agente em um processo acrescentado à lista de processos protegidos só é possível se o processo for reiniciado. Além disso, depois que um processo foi removido da lista de processos protegidos, o Agente poderá ser descarregado somente depois que o processo foi reiniciado.

O Agente deve ser interrompido para descarregá-lo dos processos protegidos: se o componente de Prevenção de Exploits for desinstalado, o aplicativo congelará o ambiente e forçará o Agente a ser descarregado dos processos protegidos. Se durante a desinstalação do componente o Agente for introduzido em algum dos processos protegidos, você deverá encerrar o processo afetado. Pode ser necessário reiniciar o computador (por exemplo, se o processo do sistema estiver sendo protegido).

Se for detectada evidência de um ataque de exploit em um processo protegido, o Kaspersky Embedded Systems Security executará uma das seguintes ações:

- Encerrará o processo se uma tentativa de exploit for feita.
- Informará que o processo foi comprometido.

É possível interromper a proteção do processo usando um dos seguintes métodos:

- Desinstalação do componente.
- Remoção do processo da lista de processos protegidos e a sua reinicialização.

Serviço de Kaspersky Security Exploit Prevention

O Serviço de Kaspersky Security Exploit Prevention é necessário no computador protegido para que o componente de Prevenção de Exploits seja eficaz. Este serviço e o componente de Prevenção de Exploits fazem parte da instalação recomendada. Durante a instalação do serviço no computador protegido, o processo kavfswh é criado e iniciado. Ele comunica as informações sobre processos protegidos do componente para o Agente de Segurança.

Depois que o Serviço de Kaspersky Security Exploit Prevention for interrompido, o Kaspersky Embedded Systems Security continua a proteger os processos adicionados à lista de processos protegidos. Ele também será carregado nos processos recém-adicionados e aplicará todas as técnicas disponíveis de prevenção de exploits para proteger a memória do processo.

Se o seu computador executa o sistema operacional Windows 10 ou posterior, o aplicativo não continuará protegendo processos e memórias do processo depois que o Kaspersky Security Exploit Prevention for interrompido.

Se o Serviço de Kaspersky Security Exploit Prevention for interrompido, o aplicativo não receberá informações sobre os eventos que ocorrem com os processos protegidos (inclusive informações sobre ataques de exploits e o encerramento de processos). Além disso, o Agente não será capaz de receber informações sobre novas configurações de proteção e a adição de novos processos à lista de processos protegidos.

Modo de Prevenção de Exploits

É possível selecionar um dos seguintes modos para configurar ações para reduzir os riscos de que vulnerabilidades sejam exploradas em processos protegidos:

- **Encerrar no exploit**: aplique este modo para encerrar um processo quando uma tentativa de exploit for feita.

  Após detecção de uma tentativa de exploração de uma vulnerabilidade em um processo crítico do sistema operacional protegido, o Kaspersky Embedded Systems Security encerrará o processo, independentemente do modo indicado nas configurações do componente de Prevenção de Exploits.

- **Somente notificações**: aplique este modo para receber informações sobre exemplos de exploits em processos protegidos usando eventos no Log de segurança.

  Se este modo for selecionado, o Kaspersky Embedded Systems Security registra em log todas as tentativas de explorar vulnerabilidades durante a criação de eventos.

Gerenciamento da Prevenção de Exploits por meio do Plug-in de Administração

Nesta seção, aprenda como navegar pela interface do Plug-in de Administração e definir as configurações do componente para um ou todos os computadores na rede.

Nesta seção

Navegação 459
Definição das configurações de proteção da memória do processo 460
Adição de um processo para proteção 461

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface.

Nesta seção

Abertura das configurações de política para a Prevenção de Exploits 459
Abertura da janela de propriedades de Prevenção de Exploits 459

Abertura das configurações de política para a Prevenção de Exploits

► *Para abrir as configurações de Prevenção de Exploits por meio da política do Kaspersky Security Center:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Políticas**.
4. Clique duas vezes no nome da política que você quer configurar.
5. Na janela **Propriedades: <Nome da política>**, selecione a seção **Proteção do computador em tempo real**.
6. Clique no botão **Configurações**, na subseção **Prevenção de Exploits**.

   A janela **Prevenção de Exploits** é exibida.

Configure a Prevenção de Exploits conforme necessário.

Abertura da janela de propriedades de Prevenção de Exploits

► *Para abrir a janela **Propriedades: <Nome do servidor>** para a Prevenção de Exploits:*

1. Expanda o nó **Dispositivos gerenciados** na árvore do Console de Administração do Kaspersky Security Center.
2. Selecione o grupo de administração para o qual você deseja configurar a tarefa.
3. Selecione a guia **Dispositivos**.

4. Abra a janela **Propriedades: <Nome do computador>** de uma das seguintes maneiras:
   - Clique duas vezes no nome do computador protegido.
   - Selecione o item **Propriedades** no menu de contexto do computador protegido.

   A janela **Propriedades: <Nome do computador>** é exibida.
5. Na seção **Aplicativos**, selecione **Kaspersky Embedded Systems Security**.
6. Clique no botão **Propriedades**.

   A janela de **configurações do Kaspersky Embedded Systems Security** é exibida.
7. Selecione a seção **Proteção do computador em Tempo Real**.
8. Clique no botão **Configurações**, na subseção **Prevenção de Exploits**.

   A janela **Prevenção de Exploits** é exibida.

Configure a Prevenção de Exploits conforme necessário.

Definição das configurações de proteção da memória do processo

► *Para definir configurações para proteger a memória de processos adicionados à lista de processos protegidos, realize as seguintes ações:*

1. Abra a janela **Prevenção de Exploits** (consulte a seção "**Abertura das configurações de política para a Prevenção de Exploits**" na página 459).
2. No bloco **Modo de Prevenção de Exploits**, defina as seguintes configurações:
   - **Prevenir exploits de processos vulneráveis**.

     Se esta caixa de seleção for marcada, o Kaspersky Embedded Systems Security reduzirá os riscos de exploração das vulnerabilidades dos processos da lista de processos protegidos.

     Se esta caixa de seleção for desmarcada, o Kaspersky Embedded Systems Security não protegerá os processos do computador contra exploits.

     Esta caixa é desmarcada por padrão.
   - **Encerrar no exploit**.

     Se este modo for selecionado, o Kaspersky Embedded Systems Security encerrará um processo protegido após a detecção de uma tentativa de exploit se uma técnica de redução de impacto ativa tiver sido aplicada ao processo.
   - **Notificar somente**.

     Se este modo for selecionado, o Kaspersky Embedded Systems Security relatará exploits exibindo uma janela de encerramento. O processo comprometido continua a ser executado.

     Se o Kaspersky Embedded Systems Security detectar um exploit em um processo crítico enquanto o aplicativo estiver em execução no modo **Encerrar no exploit**, o componente forçará a mudança para o modo **Notificar somente**.

3. No bloco **Ações de prevenção**, defina as seguintes configurações:

   - **Notificar processos violados por meio do Serviço de terminal.**

     Se esta caixa de seleção for marcada, o Kaspersky Embedded Systems Security exibirá uma janela de encerramento com uma descrição explicando por que a proteção foi ativada e uma indicação do processo no qual uma tentativa de exploit foi detectada.

     Se a caixa de seleção for desmarcada, o Kaspersky Embedded Systems Security exibirá uma janela de encerramento quando uma tentativa de exploit ou o encerramento de um processo comprometido forem detectados. Uma janela de terminal é exibida, independentemente do status do Serviço de Kaspersky Security Exploit Prevention. A caixa de seleção é selecionada por padrão.

   - **Prevenir exploits de processos vulneráveis, mesmo com o Kaspersky Security Service desativado**.

     Se esta caixa de seleção for marcada, o Kaspersky Embedded Systems Security reduzirá o risco de exploração de vulnerabilidades nos processos que já foram iniciados, mesmo que o Kaspersky Security Service esteja em execução. O Kaspersky Embedded Systems Security não protegerá os processos adicionados depois que o Kaspersky Security Service for interrompido. Depois que o serviço for iniciado, a redução do impacto de exploits será interrompida para todos os processos.

     Se esta caixa de seleção for desmarcada, o Kaspersky Embedded Systems Security não protegerá os processos contra exploits quando o Kaspersky Security Service for interrompido.

     A caixa de seleção é selecionada por padrão.

4. Clique em **OK**.

O Kaspersky Embedded Systems Security salva e aplica as configurações de proteção da memória do processo definidas.

Adição de um processo para proteção

O componente Prevenção de Exploits protege vários processos por padrão. Você pode excluir processos do escopo da proteção desmarcando as caixas correspondentes na lista.

► *Para adicionar um processo à lista de processos protegidos:*

1. Abra a janela **Prevenção de Exploits** (consulte a seção "**Abertura das configurações de política para a Prevenção de Exploits**" na página 459).
2. Na guia **Processos protegidos**, clique no botão **Procurar**.

   A janela do Microsoft Windows Explorer é exibida.
3. Selecione o processo que você deseja adicionar à lista.
4. Clique no botão **Abrir**.

   O nome de processo é exibido na linha.
5. Clique no botão **Adicionar**.

   O processo será adicionado à lista de processos protegidos.
6. Selecione o processo adicionado.

7. Clique em **Definir técnicas de prevenção de exploits**.

   A janela **Técnicas de prevenção de exploits** é exibida.

8. Selecione uma das opções para aplicar as técnicas de redução de impacto:

   - **Aplicar todas as técnicas de prevenção de exploits disponíveis**.

     Se esta opção for selecionada, a lista não poderá ser editada. Todas as técnicas disponíveis para um processo são aplicadas por padrão.

   - **Aplicar técnicas de prevenção de exploits selecionadas**.

     Se esta opção for selecionada, é possível editar a lista de técnicas de redução de impacto aplicadas:

     a. Marque as caixas de verificação ao lado das técnicas que você deseja aplicar para proteger o processo selecionado.

     b. Marque ou desmarque a caixa de seleção **Aplicar técnica de Redução de superfície de ataque**.

9. Defina as configurações da técnica de Redução de superfície de ataque:

   - Digite os nomes dos módulos cuja inicialização será bloqueada do processo protegido no campo **Negar módulos**.
   - No campo **Não negar módulos se iniciados na Área de Internet**, marque as caixas de seleção ao lado das opções sob as quais você deseja permitir que módulos sejam iniciados:
     - Internet
     - Intranet local
     - Sites confiáveis
     - Sites restritos
     - Computador

     Essas configurações são aplicáveis apenas ao Internet Explorer®.

10. Clique em **OK**.

O processo é adicionado ao escopo da proteção da tarefa.

Gerenciamento da Prevenção de Exploits por meio do Console do Aplicativo

Nesta seção, aprenda como navegar pela interface do Console do Aplicativo e definir configurações do componente em um computador local.

Nesta seção

Navegação 463
Definição das configurações de proteção da memória do processo 463
Adição de um processo para proteção 464

Navegação

Aprenda como navegar para as configurações da tarefa requerida por meio da interface.

Nesta seção

Abertura das configurações gerais de Prevenção de Exploits 463
Abertura das configurações de proteção de processo de Prevenção de Exploits 463

Abertura das configurações gerais de Prevenção de Exploits

► *Para abrir a janela **Configurações de Prevenção de Exploits**:*

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security**.
2. Abra o menu de contexto e selecione a opção de menu **Prevenção de Exploits: configurações gerais**.

   A janela **Configurações de Prevenção de Exploits** é exibida.

Defina as configurações gerais para a Prevenção de Exploits conforme necessário.

Abertura das configurações de proteção de processo de Prevenção de Exploits

► *Para abrir a janela **Configurações de Proteção de processos**:*

1. Na árvore do Console do Aplicativo, selecione o nó **Kaspersky Embedded Systems Security**.
2. Abra o menu de contexto e selecione a opção de menu **Prevenção de Exploits: configurações de proteção de processos**.

   A janela **Configurações de proteção de processos** é exibida.

Defina as configurações de proteção da memória do processo.

Definição das configurações de proteção da memória do processo

► *Para adicionar um processo à lista de processos protegidos:*

1. Abra a janela Configurações de Prevenção de Exploits.
2. No bloco **Modo de Prevenção de Exploits**, defina as seguintes configurações:
   - **Prevenir exploits de processos vulneráveis**.

     Se esta caixa de seleção for marcada, o Kaspersky Embedded Systems Security reduzirá os riscos de exploração das vulnerabilidades dos processos da lista de processos protegidos.

     Se esta caixa de seleção for desmarcada, o Kaspersky Embedded Systems Security não protegerá os processos do computador contra exploits.

     Esta caixa é desmarcada por padrão.
   - **Encerrar no exploit**.

Se este modo for selecionado, o Kaspersky Embedded Systems Security encerrará um processo protegido após a detecção de uma tentativa de exploit se uma técnica de redução de impacto ativa tiver sido aplicada ao processo.

- **Notificar somente**.

  Se este modo for selecionado, o Kaspersky Embedded Systems Security relatará exploits exibindo uma janela de encerramento. O processo comprometido continua a ser executado.

  Se o Kaspersky Embedded Systems Security detectar um exploit em um processo crítico enquanto o aplicativo estiver em execução no modo **Encerrar no exploit**, o componente forçará a mudança para o modo **Notificar somente**.

3. No bloco **Ações de prevenção**, defina as seguintes configurações:

   - **Notificar processos violados por meio do Serviço de terminal.**

     Se esta caixa de seleção for marcada, o Kaspersky Embedded Systems Security exibirá uma janela de encerramento com uma descrição explicando por que a proteção foi ativada e uma indicação do processo no qual uma tentativa de exploit foi detectada.

     Se a caixa de seleção for desmarcada, o Kaspersky Embedded Systems Security exibirá uma janela de encerramento quando uma tentativa de exploit ou o encerramento de um processo comprometido forem detectados. Uma janela de terminal é exibida, independentemente do status do Serviço de Kaspersky Security Exploit Prevention. A caixa de seleção é selecionada por padrão.

   - **Prevenir exploits de processos vulneráveis, mesmo com o Kaspersky Security Service desativado**.

     Se esta caixa de seleção for marcada, o Kaspersky Embedded Systems Security reduzirá o risco de exploração de vulnerabilidades nos processos que já foram iniciados, mesmo que o Kaspersky Security Service esteja em execução. O Kaspersky Embedded Systems Security não protegerá os processos adicionados depois que o Kaspersky Security Service for interrompido. Depois que o serviço for iniciado, a redução do impacto de exploits será interrompida para todos os processos.

     Se esta caixa de seleção for desmarcada, o Kaspersky Embedded Systems Security não protegerá os processos contra exploits quando o Kaspersky Security Service for interrompido.

     A caixa de seleção é selecionada por padrão.

4. Na janela **Configurações de prevenção de exploits**, clique em **OK**.

O Kaspersky Embedded Systems Security salva e aplica as configurações de proteção da memória do processo definidas.

Adição de um processo para proteção

O componente Prevenção de Exploits protege vários processos por padrão. Você pode desmarcar os processos que não deseja proteger na lista de processos protegidos.

► *Para adicionar um processo à lista de processos protegidos:*

1. Abra a janela Configurações de proteção de processos.
2. Para adicionar um processo para protegê-los de violação e reduzir possíveis impactos de exploit, execute

as seguintes ações:

a. Clique no botão **Procurar**.

A janela **Abrir** padrão do Microsoft Windows é exibida.

b. Na janela exibida, selecione um processo que você deseja adicionar à lista.

c. Clique no botão **Abrir**.

d. Clique no botão **Adicionar**.

O processo será adicionado à lista de processos protegidos.

3. Selecione um processo na lista.
4. A configuração atual é exibida em **Configurações de proteção de processos**:
   - **Nome do processo**.
   - **Está em execução**.
   - **Técnicas de prevenção de exploits aplicadas**.
   - **Configurações de Redução da superfície de ataque**.
5. Para modificar as técnicas de prevenção de exploits aplicadas ao processo, selecione a guia **Técnicas de prevenção de exploits**.
6. Selecione uma das opções para aplicar as técnicas de redução de impacto:
   - **Aplicar todas as técnicas de prevenção de exploits disponíveis**.

     Se esta opção for selecionada, a lista não poderá ser editada. Todas as técnicas disponíveis para um processo são aplicadas por padrão.
   - **Aplicar técnicas de prevenção de exploits listadas para o processo**.

     Se esta opção for selecionada, é possível editar a lista de técnicas de redução de impacto aplicadas:

     a. Marque as caixas de verificação ao lado das técnicas que você deseja aplicar para proteger o processo selecionado.
7. Defina as configurações da técnica de Redução de superfície de ataque:
   - Digite os nomes dos módulos cuja inicialização será bloqueada do processo protegido no campo **Negar módulos**.
   - No campo **Não negar módulos se iniciados na Área de Internet**, marque as caixas de seleção ao lado das opções sob as quais você deseja permitir que módulos sejam iniciados:
     - Internet
     - Intranet local
     - Sites confiáveis
     - Sites restritos
     - Computador

     Essas configurações são aplicáveis apenas ao Internet Explorer®.
8. Clique em **OK**.

O processo é adicionado ao escopo da proteção da tarefa.

Técnicas de prevenção de exploits

Tabela 62. Técnicas de prevenção de exploits

Técnica de prevenção de exploits	Descrição
Prevenção Contra Execução de Dados (DEP, Data Execution Prevention)	A prevenção contra execução de dados bloqueia a execução do código arbitrário em áreas protegidas da memória.
Randomização do Layout do Espaço de Endereço (ASLR, Address Space Layout Randomization)	Altera o layout das estruturas de dados no espaço do endereço do processo.
Proteção contra Substituição do Gerenciador de Exceção Estruturada (SEHOP, Structured Exception Handler Overwrite Protection)	Substituição de registros de exceção ou substituição do gerenciador de exceção.
Alocação de Página Nula	Prevenção contra o redirecionamento do ponteiro nulo.
Verificação de Chamada de Rede LoadLibrary (Anti-ROP)	Proteção contra carregamento de DLLs de caminhos de rede.
Pilha Executável (Anti-ROP)	Bloqueio de execução não autorizada de áreas da pilha.
Verificação Anti-RET (Anti-ROP)	Verifica se a instrução CALL foi invocada de maneira segura.
Articulação Anti-Stack (Anti-ROP)	Proteção contra a relocalização do ponteiro de pilha ESP para um endereço executável.
Monitor de Acesso à Tabela de Endereço de Exportação (Monitor de Acesso EAT e Monitor de Acesso EAT através de Registrador de Depuração)	Proteção de acesso à leitura para a tabela de endereços de exportação para o kernel32.dll, kernelbase.dll e ntdll.dll
Alocação de heapspray (Heapspray)	Proteção contra a alocação de memória para executar um código malicioso.
Simulação do Fluxo de Execução (Contra Programação Direcionada por Retorno)	Detecção de cadeias suspeitas de instruções (possível gadget ROP) no componente de API do Windows.
Monitor de Chamada de Perfil de Intervalo (Proteção do Driver de Função Auxiliar (AFDP, Ancillary Function Driver Protection))	Proteção contra o escalamento de privilégios por uma vulnerabilidade no driver AFD (execução de código arbitrário no anel 0 através de uma chamada QueryIntervalProfile).
Redução da Superfície de Ataque (ASR)	Bloqueio da inicialização de suplementos vulneráveis por meio do processo protegido.
Contra o esvaziamento do processo (Hollowing)	Proteção contra criação e execução de cópias maliciosas de processos confiáveis.

Técnica de prevenção de exploits	Descrição
Contra AtomBombing (APC)	Exploração da tabela de átomo global via Chamadas de Procedimento Assíncrono (APC).
Contra CreateRemoteThread (RThreadLocal)	Outro processo criou uma thread no processo protegido.
Contra CreateRemoteThread (RThreadRemote)	O processo protegido criou uma thread em outro processo.

Integração com sistemas de terceiros

Esta seção descreve a integração do Kaspersky Embedded Systems Security com recursos e tecnologias de terceiros.

Neste capítulo

Monitoramento do desempenho. Contadores do Kaspersky Embedded Systems Security....468
Integração com WMI....484

Monitoramento do desempenho. Contadores do Kaspersky Embedded Systems Security

Esta seção fornece informações sobre os contadores do Kaspersky Embedded Systems Security: contadores de desempenho do Monitor do Sistema e contadores e interceptações SNMP.

Nesta seção

Contadores de desempenho do Monitor do Sistema....468
Contadores e interceptações SNMP do Kaspersky Embedded Systems Security....474

Contadores de desempenho do Monitor do Sistema

Esta seção contém informações sobre os contadores de desempenho do Monitor do Sistema do Microsoft Windows que são registrados pelo Kaspersky Embedded Systems Security durante a instalação.

Nesta seção

Sobre os contadores de desempenho do Kaspersky Embedded Systems Security....469
Número total de solicitações negadas....469
Número total de solicitações ignoradas....470
Número de solicitações não processadas devido à falta de recursos do sistema....471
Número de solicitações enviadas para serem processadas....471
Número médio de fluxos de triagem de interceptação de arquivos....472
Número máximo de fluxos de triagem de interceptação de arquivos....472
Número de elementos na fila de objetos infectados....473
Número de objetos processados por segundo....473

Sobre os contadores de desempenho do Kaspersky Embedded Systems Security

O componente **Contadores de desempenho** está incluído nos componentes instalados do Kaspersky Embedded Systems Security por padrão. O Kaspersky Embedded Systems Security registra os seus próprios contadores de desempenho para o Monitor do Sistema do Microsoft Windows durante a instalação.

Usando os contadores do Kaspersky Embedded Systems Security, você pode controlar o desempenho do aplicativo enquanto as tarefas de Proteção em tempo real são executadas. Você pode identificar locais problemáticos durante a execução com outros aplicativos e falhas de recursos. Você pode diagnosticar configurações indesejáveis e travamentos do Kaspersky Embedded Systems Security durante a operação.

Você pode visualizar os contadores de desempenho do Kaspersky Embedded Systems Security abrindo o console **Desempenho** no item **Administração** do Painel de Controle do Windows.

As seções a seguir listam as definições dos contadores, os intervalos recomendados para as leituras, os valores limite e recomendações de configurações do Kaspersky Embedded Systems Security caso os valores dos contadores os excedam.

Número total de solicitações negadas

Tabela 63. Número total de solicitações negadas

Nome	Número total de solicitações negadas
Definição	Número total de solicitações do driver de interceptação de arquivos para processar os objetos que não foram aceitos por processos do aplicativo; contado a partir do momento em que o Kaspersky Embedded Systems Security foi iniciado pela última vez. O aplicativo ignora objetos para os quais as solicitações para processamento são negadas pelos processos do Kaspersky Embedded Systems Security.
Finalidade	Este contador pode ajudá-lo a detectar: • Quedas de qualidade na Proteção em Tempo Real que afetam os processos de trabalho do Kaspersky Embedded Systems Security. • Interrupção da proteção em tempo real devido a falhas de triagem da interceptação de arquivos.
Valor normal / limite	0 / 1.
Intervalo de leitura recomendado	1 hora.

Recomendações de configuração caso o valor exceda o limite	O número de solicitações para objetos com processamento negado corresponde ao número de objetos ignorados. As situações que se seguem são possíveis, dependendo do comportamento do contador: • O contador mostra várias solicitações negadas durante um período prolongado de tempo: todos os processos do Kaspersky Embedded Systems Security são totalmente carregados, portanto, o Kaspersky Embedded Systems Security não pode verificar objetos. Para evitar ignorar objetos, aumente o número de processos do aplicativo para as tarefas de Proteção em tempo real. Você pode usar configurações do Kaspersky Embedded Systems Security como **Número máximo de processos ativos** e **Número de processos para a proteção em tempo real**. • O número de solicitações negadas excede de forma significativa o limite crítico e continua crescendo rapidamente: a interceptação travou. O Kaspersky Embedded Systems Security não está verificando os objetos ao acessar. Reinicie o Kaspersky Embedded Systems Security.

Número total de solicitações ignoradas

Tabela 64. Número total de solicitações ignoradas

Nome	Número total de solicitações ignoradas
Definição	O número total de pedidos do driver de interceptação de arquivos para processar objetos que foram recebidos pelo Kaspersky Embedded Systems Security mas que não geraram eventos de conclusão de processamento; esse número é contado a partir do momento em que o aplicativo foi iniciado pela última vez. Se um pedido de processamento de um objeto desse tipo aceito por um dos processos de trabalho não enviar um evento para conclusão do processamento, o driver vai transferir esse pedido para outro processo e o valor do contador **Número total de pedidos ignorados** aumentará em 1. Se o driver tiver percorrido todos os processos de trabalho e nenhum deles tiver recebido o pedido de processamento (por estar ocupado) ou enviado eventos para conclusão do processamento, o Kaspersky Embedded Systems Security vai ignorar esse objeto, pelo que o valor do contador **Número total de pedidos ignorados** aumentará em 1.
Finalidade	Esse contador permite detectar quebras no desempenho devido a falhas na interceptação.
Valor normal / limite	0 / 1
Intervalo de leitura recomendado	1 hora
Recomendações de configuração caso o valor exceda o limite	Se o valor do contador for diferente de zero, um ou vários fluxos de triagem de interceptação de arquivos foram congelados e estão inativos. O valor do contador corresponde ao número de fluxos atualmente inativos. Se a velocidade de verificação não for satisfatória, reinicie o Kaspersky Embedded Systems Security para restaurar os fluxos offline.

Número de solicitações não processadas devido à falta de recursos do sistema

Tabela 65. Número de solicitações não processadas devido à falta de recursos do sistema

Nome	Número de solicitações não processadas devido à falta de recursos.
Definição	Número total de solicitações do driver de interceptação de arquivos que não foram processados devido à falta de recursos do sistema (por exemplo, de RAM); contado a partir do momento em que o Kaspersky Embedded Systems Security foi iniciado pela última vez. O Kaspersky Embedded Systems Security ignora solicitações de objetos para processar que não sejam processados pelo driver de interceptação de arquivos.
Finalidade	Esse contador pode ser usado para detectar e eliminar qualidade potencialmente baixa na proteção em tempo real que ocorre devido a um volume reduzido nos recursos do sistema.
Valor normal / limite	0 / 1.
Intervalo de leitura recomendado	1 hora.
Recomendações de configuração caso o valor exceda o limite	Se o valor do contador for diferente de zero, os processos de trabalho do Kaspersky Embedded Systems Security precisam de mais RAM para processar solicitações. Os processos ativos de outros aplicativos podem estar usando toda a RAM disponível.

Número de solicitações enviadas para serem processadas

Tabela 66. Número de solicitações enviadas para serem processadas

Nome	Número de solicitações enviadas para serem processadas.
Definição	O número de objetos que aguardam processamento pelos processos em execução.
Finalidade	Este contador pode ser usado para rastrear a carga nos processos de trabalho do Kaspersky Embedded Systems Security e o nível geral de atividade de arquivos no computador.
Valor normal / limite	O valor do contador pode variar de acordo com o nível de atividade de arquivos do computador.
Intervalo de leitura recomendado	1 minuto
Recomendações de configuração caso o valor exceda o limite	Não

Número médio de fluxos de triagem de interceptação de arquivos

Tabela 67. Número médio de fluxos de triagem de interceptação de arquivos

Nome	Número médio de fluxos de triagem de interceptação de arquivos.
Definição	O número de fluxos de triagem de interceptação de arquivos em um processo e a média de todos os processos envolvidos no momento em tarefas de proteção em tempo real.
Finalidade	Esse contador pode ser usado para detectar e eliminar a baixa qualidade que ocorra na proteção em tempo real devido a carga completa nos processos do Kaspersky Embedded Systems Security.
Valor normal / limite	Varia / 40
Intervalo de leitura recomendado	1 minuto
Recomendações de configuração caso o valor exceda o limite	É possível criar até 60 fluxos de triagem de interceptação de arquivos em cada processo de trabalho. Se o valor do contador se aproximar de 60, haverá o risco de que nenhum dos processos de trabalho possa processar a próxima solicitação da fila a partir do driver de interceptação de arquivos e que o Kaspersky Embedded Systems Security ignore o objeto. Aumente o número de processos do Kaspersky Embedded Systems Security para tarefas de proteção em tempo real. Você pode usar configurações do Kaspersky Embedded Systems Security como **Número máximo de processos ativos** e **Número de processos para a Proteção em Tempo Real**.

Número máximo de fluxos de triagem de interceptação de arquivos

Tabela 68. Número máximo de fluxos de triagem de interceptação de arquivos

Nome	Número máximo de fluxos de triagem de interceptação de arquivos.
Definição	O número de fluxos de triagem de interceptação de arquivos em um processo e o máximo de todos os processos envolvidos no momento em tarefas de proteção em tempo real.
Finalidade	Esse contador permite detectar e eliminar quebras no desempenho devido a uma distribuição desequilibrada das cargas nos processos em execução.
Valor normal / limite	Varia / 40
Intervalo de leitura recomendado	1 minuto
Recomendações de configuração caso o valor exceda o limite	Se o valor desse contador exceder de forma significativa e contínua o valor do contador **Número médio de fluxos de interceptação de arquivos**, o Kaspersky Embedded Systems Security está distribuindo a carga de forma desequilibrada pelos processos em execução. Reinicie o Kaspersky Embedded Systems Security.

Número de elementos na fila de objetos infectados

Tabela 69. Número de elementos na fila de objetos infectados

Nome	Número de itens na fila de objetos infectados.
Definição	Número de objetos infectados atualmente aguardando processamento (desinfecção ou exclusão).
Finalidade	Este contador pode ajudá-lo a detectar: • Interrupção da Proteção em Tempo Real devido a possíveis falhas de triagem da interceptação de arquivos. • Sobrecarga de processos devido à distribuição não uniforme do tempo do processador entre diferentes processos de trabalho e o Kaspersky Embedded Systems Security. • Surtos de vírus.
Valor normal / limite	Esse valor pode ser diferente de zero enquanto o Kaspersky Embedded Systems Security está processando objetos infectados ou possivelmente infectados, mas regressará a zero após a conclusão do processamento / O valor permanece como diferente de zero durante um período de tempo prolongado.
Intervalo de leitura recomendado	1 minuto
Recomendações de configuração caso o valor exceda o limite	Se o valor do contador não retornar a zero durante um período de tempo prolongado: • O Kaspersky Embedded Systems Security não está processando objetos (talvez a triagem de interceptação de arquivos tenha travado). Reinicie o Kaspersky Embedded Systems Security. • Não existe tempo de processador suficiente para processar os objetos. Certifique-se de que o Kaspersky Embedded Systems Security obtenha tempo de processador adicional (por exemplo, reduzindo a carga de outros aplicativos no computador). • Ocorreu um surto de vírus. Um número muito elevado de objetos infectados ou possivelmente infectados na tarefa Proteção de Arquivos em Tempo Real é também um sinal de um surto de vírus. Você pode exibir informações sobre o número de objetos detectados nas estatísticas ou logs de tarefas.

Número de objetos processados por segundo

Tabela 70. Número de objetos processados por segundo

Nome	Número de objetos processados por segundo.
Definição	Número de objetos processados, dividido pelo tempo necessário para processar esses objetos (calculado em intervalos de tempo idênticos).

Finalidade	Esse contador reflete a velocidade do processamento de objetos; ele pode ser usado para detectar e eliminar pontos baixos no desempenho do computador que ocorrem devido a atribuição de tempo de processador insuficiente aos processos do Kaspersky Embedded Systems Security ou erros na operação do Kaspersky Embedded Systems Security.
Valor normal / limite	Varia / N.º
Intervalo de leitura recomendado	1 minuto.
Recomendações de configuração caso o valor exceda o limite	Os valores deste contador dependem dos valores definidos nas configurações do Kaspersky Embedded Systems Security e da carga no computador de processos de outros aplicativos. Observe o nível médio dos valores do contador por um longo período. Se o nível geral dos valores do contador diminuir, é possível uma das seguintes situações: • Os processos do Kaspersky Embedded Systems Security não têm tempo de processador suficiente para processar os objetos. Certifique-se de que o Kaspersky Embedded Systems Security obtenha tempo de processador adicional (por exemplo, reduzindo a carga de outros aplicativos no computador). • Ocorreu um erro no Kaspersky Embedded Systems Security (vários fluxos estão ociosos). Reinicie o Kaspersky Embedded Systems Security.

Contadores SNMP e interceptações do Kaspersky Embedded Systems Security

Esta seção contém informações sobre os contadores e interceptações do Kaspersky Embedded Systems Security.

Nesta seção

Sobre contadores e interceptações SNMP do Kaspersky Embedded Systems Security 474
Contadores SNMP do Kaspersky Embedded Systems Security 475
Interceptações SNMP do Kaspersky Embedded Systems Security 477

Sobre contadores e interceptações SNMP do Kaspersky Embedded Systems Security

Se você tiver incluído o componente Contadores e Interceptações SNMP no conjunto de componentes do Antivírus a ser instalado, você poderá visualizar os contadores e interceptações do Kaspersky Embedded Systems Security usando o Simple Network Management Protocol (SNMP).

Para exibir os Medidores e as interceptações do Kaspersky Embedded Systems Security na estação de trabalho do administrador, inicie o Serviço SNMP no computador protegido e os Serviços SNMP e de Interceptação SNMP na estação de trabalho do administrador.

Contadores SNMP do Kaspersky Embedded Systems Security

Esta seção contém tabelas com uma descrição das configurações para os contadores SNMP do Kaspersky Embedded Systems Security.

Nesta seção

Contadores de desempenho 475
Contadores de Quarentena 475
Contador de Backup 476
Contadores gerais 476
Contador de Atualização 476
Contadores de Proteção em Tempo Real 476

Contadores de desempenho

Tabela 71. Contadores de desempenho

Contador	Definição
currentRequestsAmount	Número de solicitações enviadas para serem processadas. (na página 471)
currentInfectedQueueLength	Número de elementos na fila de objetos infectados (consulte a seção "Número de elementos na fila de objetos infectados" na página 473)
currentObjectProcessingRate	Número de objetos processados por segundo (na página 473)
currentWorkProcessesNumber	Número atual de processos de trabalho usados pelo Kaspersky Embedded Systems Security

Contadores de Quarentena

Tabela 72. Contadores de Quarentena

Contador	Definição
totalObjects	Número de objetos atualmente na Quarentena
totalSuspiciousObjects	Número de objetos possivelmente infectados atualmente na Quarentena
currentStorageSize	Tamanho total dos dados na Quarentena (MB)

Contador de Backup

Tabela 73. Contador de Backup

Contador	Definição
currentBackupStorageSize	Tamanho total dos dados no Backup (MB)

Contadores gerais

Tabela 74. Contadores gerais

Contador	Definição
lastCriticalAreasScanAge	O período desde a última verificação completa das áreas críticas do computador (tempo decorrido em segundos desde a conclusão da última tarefa de *Verificação de áreas críticas*).
licenseExpirationDate	Data de expiração da licença se uma chave ativa ou chaves adicionais tiverem sido adicionadas, a data de expiração da licença associada à chave adicional é exibida.
currentApplicationUptime	O tempo que o Kaspersky Embedded Systems Security está em execução desde que foi iniciado pela última vez, em centenas de segundos.
currentFileMonitorTaskStatus	Status da tarefa de Proteção de Arquivos em Tempo Real: **Ativada** - em execução; **Desativada** - interrompido ou pausado.

Contador de Atualização

Tabela 75. Contador de Atualização

Contador	Definição
avBasesAge	“Idade” dos bancos de dados (tempo decorrido em centésimos de segundos desde a data de criação da última instalação dos bancos de dados atualizados).

Contadores de Proteção em Tempo Real

Tabela 76. Contadores de Proteção em Tempo Real

Contador	Definição
totalObjectsProcessed	Número total de objetos verificados desde a execução pela última vez da tarefa Proteção de Arquivos em Tempo Real
totalInfectedObjectsFound	Número total de objetos infectados e de outros detectados desde a última execução da tarefa de Proteção de arquivos em tempo real
totalSuspiciousObjectsFound	Número total de objetos possivelmente infectados detectados desde a última execução da tarefa de Proteção de arquivos em tempo real

Contador	Definição
totalVirusesFound	Número total de objetos verificados desde a última execução da tarefa de Proteção de arquivos em tempo real
totalObjectsQuarantined	Número total de objetos infectados, possivelmente infectados e outros objetos que foram colocados na Quarentena pelo Kaspersky Embedded Systems Security; calculado a partir do momento da última inicialização da tarefa de Proteção de arquivos em tempo real
totalObjectsNotQuarantined	Número total de objetos infectados ou possivelmente infectados que o Kaspersky Embedded Systems Security tentou colocar na Quarentena mas não conseguiu; calculado a partir da hora em que foi iniciada pela última vez a tarefa Proteção de Arquivos em Tempo Real
totalObjectsDisinfected	Número total de objetos infectados desinfectados pelo Kaspersky Embedded Systems Security; calculado a partir do momento em que a tarefa de Proteção de Arquivos em Tempo Real foi executada pela última vez
totalObjectsNotDisinfected	Número total de objetos infectados e de outros objetos que o Kaspersky Embedded Systems Security tentou desinfectar, mas não conseguiu; calculado a partir do momento da última inicialização da tarefa de Proteção de arquivos em tempo real
totalObjectsDeleted	Número total de objetos infectados, possivelmente infectados e outros objetos desinfectados pelo Kaspersky Embedded Systems Security; calculado a partir do momento da última inicialização da tarefa de Proteção de arquivos em tempo real
totalObjectsNotDeleted	Número total de objetos infectados, possivelmente infectados e de outros objetos que o Kaspersky Embedded Systems Security tentou desinfectar, mas não conseguiu; calculado a partir do momento da última inicialização da tarefa de Proteção de arquivos em tempo real
totalObjectsBackedUp	Número total de objetos infectados e outros objetos que foram colocados no Backup pelo Kaspersky Embedded Systems Security; calculado a partir do momento da última inicialização da tarefa de Proteção de arquivos em tempo real
totalObjectsNotBackedUp	Número total de objetos infectados e de outros objetos que o Kaspersky Embedded Systems Security tentou colocar no Backup, mas não conseguiu; calculado a partir do momento da última inicialização da tarefa de Proteção de arquivos em tempo real

Interceptações SNMP do Kaspersky Embedded Systems Security

As opções de interceptações SNMP no Kaspersky Embedded Systems Security são resumidas como se segue:

- eventThreatDetected: um objeto foi detectado.

  As opções da interceptação são as seguintes:

  - eventDateAndTime
  - eventSeverity

- computerName
- userName
- objectName
- threatName
- detectType
- detectCertainty

- eventBackupStorageSizeExceeds: Tamanho máximo do Backup excedido. O tamanho total de dados no Backup excedeu o valor especificado pelo **Tamanho máximo do Backup (MB)**. O Kaspersky Embedded Systems Security continua a fazer backup de objetos infectados.

  As opções da interceptação são as seguintes:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventThresholdBackupStorageSizeExceeds: limite de espaço disponível no backup atingido. O volume disponível no Backup atribuído pelo **Valor limite de espaço disponível (MB)** é igual ou inferior ao valor especificado. O Kaspersky Embedded Systems Security continua a fazer backup de objetos infectados.

  As opções da interceptação são as seguintes:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventQuarantineStorageSizeExceeds: tamanho máximo da Quarentena excedido. O tamanho total dos dados da Quarentena excedeu o valor especificado por **Tamanho máximo da Quarentena (MB)**. O Kaspersky Embedded Systems Security continua a colocar na Quarentena os objetos possivelmente infectados.

  As opções da interceptação são as seguintes:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventObjectNotQuarantined: erro de quarentena.

  As opções da interceptação são as seguintes:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - userName
  - computerName
  - objectName
  - storageObjectNotAddedEventReason

- eventObjectNotBackuped: erro ao salvar uma cópia de objeto no Backup.

  As opções da interceptação são as seguintes:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName
  - computerName
  - storageObjectNotAddedEventReason
- eventQuarantineInternalError: erro interno de Quarentena.

  As opções da interceptação são as seguintes:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventBackupInternalError: erro de Backup.

  As opções da interceptação são as seguintes:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventAVBasesOutdated: o banco de dados do antivírus está desatualizado. O número de dias desde a última execução da tarefa de atualização do banco de dados (tarefa local ou tarefa de grupo, ou tarefa para conjuntos de computadores) está sendo calculado.

  As opções da interceptação são as seguintes:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - dias
- eventAVBasesTotallyOutdated: o banco de dados do antivírus está obsoleto. O número de dias desde a última execução da tarefa de atualização do banco de dados (tarefa local ou tarefa de grupo, ou tarefa para conjuntos de computadores) está sendo calculado.

  As opções da interceptação são as seguintes:

  - eventSeverity
  - eventDateAndTime
  - eventSource

    - dias
- eventApplicationStarted: o Kaspersky Embedded Systems Security está sendo executado.

  As opções da interceptação são as seguintes:

    - eventSeverity
    - eventDateAndTime
    - eventSource
- eventApplicationShutdown: o Kaspersky Embedded Systems Security está interrompido.

  As opções da interceptação são as seguintes:

    - eventSeverity
    - eventDateAndTime
    - eventSource
- eventCriticalAreasScanWasntPerformForALongTime: as áreas críticas não são verificadas há muito tempo. Calculado como o número de dias desde a última conclusão da tarefa de Verificação de Áreas Críticas.

  As opções da interceptação são as seguintes:

    - eventSeverity
    - eventDateAndTime
    - eventSource
    - dias
- eventLicenseHasExpired: a licença expirou.

  As opções da interceptação são as seguintes:

    - eventSeverity
    - eventDateAndTime
    - eventSource
- eventLicenseExpiresSoon: a licença expira em breve. Calculado como o número de dias até a data de expiração da licença.

  As opções da interceptação são as seguintes:

    - eventSeverity
    - eventDateAndTime
    - eventSource
    - dias
- eventTaskInternalError: erro ao concluir a tarefa.

  As opções da interceptação são as seguintes:

    - eventSeverity
    - eventDateAndTime
    - eventSource

- errorCode
- knowledgeBaseId
- taskName

- eventUpdateError: erro de desempenho de tarefa de atualização.

  As opções da interceptação são as seguintes:

  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason

As descrições das opções de interceptações e seus possíveis valores de parâmetros são os seguintes:

- eventDateAndTime: data e hora do evento.
- eventSeverity: nível de importância.

  A opção pode ter os seguintes valores:

  - critical (1) – crítico
  - warning (2) – aviso
  - info (3) – informativo
- userName: um nome de usuário (por exemplo, o nome do usuário que tentou obter acesso a um arquivo infectado).
- computerName: nome do computador (por exemplo, o nome do computador a partir do qual um usuário tentou obter acesso a um arquivo infectado).
- eventSource: componente funcional em que o evento foi gerado.

  A opção pode ter os seguintes valores:

  - desconhecido (0) – componente funcional não conhecido
  - quarantine (1) – Quarentena
  - backup (2) – Backup
  - reporting (3) – Logs de tarefas
  - updates (4) – Atualização
  - realTimeProtection (5) – Proteção de Arquivos em Tempo Real
  - onDemandScanning (6) – Verificação por Demanda
  - product (7) – Evento relacionado com a operação do Kaspersky Embedded Systems Security como um todo, em vez da operação de componentes individuais
  - systemAudit (8) – log de auditoria do sistema
- eventReason: acionador de evento: o que provocou o evento.

  A opção pode ter os seguintes valores:

  - reasonUnknown(0) – o motivo é desconhecido

    - reasonInvalidSettings (1) – somente para eventos de Backup e Quarentena, é exibido se a Quarentena ou o Backup não estiver disponível (permissões de acesso insuficientes ou a pasta foi especificada incorretamente nas configurações da Quarentena -- por exemplo, um caminho de rede foi especificado). Nesse caso, o Kaspersky Embedded Systems Security usará a pasta padrão do Backup ou da Quarentena.
- objectName: um nome de objeto (por exemplo, nome do arquivo no qual o vírus foi detectado).
- threatName: o nome do objeto de acordo com a classificação da Enciclopédia de Vírus https://encyclopedia.kaspersky.com/knowledge/classification/. Esse nome é incluído no nome completo do objeto detectado que o Kaspersky Embedded Systems Security devolve ao detectar um objeto. Você pode exibir o nome completo de um objeto detectado no Log de tarefas (consulte a seção "Definições de configurações de log" na página 101).
- detectType: tipo de objeto detectado.

  A opção pode ter os seguintes valores:

    - undefined (0) – indefinido
    - virware – vírus clássicos e worms de rede
    - trojware – cavalos de Troia
    - malware – outros programas maliciosos
    - adware – software de publicidade
    - pornware – software de pornografia
    - riskware: aplicativos legítimos que podem ser usados por invasores para danificar os dados pessoais ou o computador do usuário
- detectCertainty: nível de certeza de detecção da ameaça.

  A opção pode ter os seguintes valores:

    - Suspeita (possivelmente infectado) – o Kaspersky Embedded Systems Security detectou uma correspondência parcial entre uma seção do código do objeto e a seção de código malicioso conhecida.
    - Certeza (infectado) – o Kaspersky Embedded Systems Security detectou uma correspondência total entre uma seção no código do objeto e a seção de código maliciosa conhecida.
- days: número de dias (por exemplo, o número de dias até a data de expiração da licença).
- errorCode: um código de erro.
- knowledgeBaseId: endereço de um artigo da base de dados de conhecimento (por exemplo, o endereço de um artigo que explica um erro em particular).
- taskName: um nome de tarefa.
- updaterErrorEventReason: um motivo para o erro de atualização.

  A opção pode ter os seguintes valores:

    - reasonUnknown(0) – o motivo é desconhecido
    - reasonAccessDenied – acesso negado
    - reasonUrlsExhausted – a lista de fontes de atualização colapsou
    - reasonInvalidConfig – arquivo de configuração inválido

- reasonInvalidSignature – assinatura inválida
- reasonCantCreateFolder – não é possível criar pasta
- reasonFileOperError – erro de arquivo
- reasonDataCorrupted – objeto corrompido
- reasonConnectionReset – conexão redefinida
- reasonTimeOut – o tempo limite de conexão expirou
- reasonProxyAuthError – erro de autenticação do servidor proxy
- reasonServerAuthError – erro de autenticação do servidor
- reasonHostNotFound – computador não encontrado
- reasonServerBusy – servidor indisponível
- reasonConnectionError – erro de conexão
- reasonModuleNotFound – objeto não encontrado
- reasonBlstCheckFailed(16) – erro ao verificar a lista negra de chaves. É possível que estivessem sendo publicadas atualizações ao banco de dados no momento da atualização; repita a atualização dentro de alguns minutos.

- storageObjectNotAddedEventReason: o motivo pelo qual o objeto não foi copiado para o Backup ou colocado na Quarentena.

  A opção pode ter os seguintes valores:

  - reasonUnknown(0) – o motivo é desconhecido
  - reasonStorageInternalError – erro de banco de dados; o Kaspersky Embedded Systems Security deve ser restaurado.
  - reasonStorageReadOnly – o banco de dados é somente-leitura; o Kaspersky Embedded Systems Security deve ser restaurado.
  - reasonStorageIOError – erro de entrada-saída: a) o Kaspersky Embedded Systems Security está corrompido, o Kaspersky Embedded Systems Security deve ser restaurado; b) o disco com os arquivos do Kaspersky Embedded Systems Security está corrompido.
  - reasonStorageCorrupted – o armazenamento está corrompido; o Kaspersky Embedded Systems Security deve ser restaurado.
  - reasonStorageFull – o banco de dados está cheio; é necessário espaço livre em disco.
  - reasonStorageOpenError – o arquivo de banco de dados não pode ser aberto; o Kaspersky Embedded Systems Security deve ser restaurado.
  - reasonStorageOSFeatureError – alguns recursos do sistema operacional não correspondem aos requisitos do Kaspersky Embedded Systems Security.
  - reasonObjectNotFound – o objeto que está sendo colocado na Quarentena não existe no disco.
  - reasonObjectAccessError – permissões insuficientes para usar o API de Backup: a conta sendo usada para executar a operação não tem permissões de Operador de Backup.
  - reasonDiskOutOfSpace – Não existe espaço suficiente no disco.

Integração com WMI

O Kaspersky Embedded Systems Security é compatível com a integração com o Windows Management Instrumentation (WMI): é possível usar sistemas cliente que usam WMI para receber dados via o padrão Web-Based Enterprise Management (WBEM) com o objetivo de reunir informações sobre o status do Kaspersky Embedded Systems Security e seus componentes.

Quando o Kaspersky Embedded Systems Security está instalado, ele registra o módulo proprietário no sistema, o que facilita a criação de um namespace Kaspersky Embedded Systems Security no namespace da raiz WMI no computador local. O namespace Kaspersky Embedded Systems Security permite trabalhar com classes e instâncias do Kaspersky Embedded Systems Security e suas propriedades.

Os valores de algumas propriedades de instâncias dependem dos tipos de tarefa.

A *tarefa não-periódica* é uma tarefa de aplicativo não limitada em termos de tempo e que pode estar constantemente em execução ou parada. Nenhum progresso de execução existe para tais tarefas. Os resultados da execução da tarefa são registrados em log constantemente enquanto a tarefa é executada como um evento único (por exemplo, a detecção de um objeto infectado por quaisquer tarefas de Proteção do Computador em Tempo Real). Este tipo de tarefa é gerenciado por meio de políticas do Kaspersky Security Center.

A *tarefa periódica* é uma tarefa de aplicativo limitada em termos de tempo e cujo progresso de execução é exibido em termos percentuais. Os resultados da tarefa são gerados quando ela é concluída e representados como um item único ou como um estado de aplicativo alterado (por exemplo, Atualização do Banco de Dados do aplicativo concluída, arquivos de configuração gerados para tarefas de geração de regra). Diversas tarefas periódicas do mesmo tipo podem estar sendo executadas em um único computador simultaneamente (três tarefas de verificação por demanda com escopos da verificação diferentes). As tarefas periódicas podem ser gerenciadas por meio do Kaspersky Security Center como tarefas de grupo.

Se você usar ferramentas para gerar consultas de namespace WMI e receber dados dinâmicos de namespaces WMI na sua rede corporativa, poderá receber informações sobre o estado de aplicativo atual (consulte a tabela abaixo).

Tabela 77. Informações sobre o estado do aplicativo

Propriedade da instância	Descrição	Valores
ProductName	Nome do aplicativo instalado.	Nome completo do aplicativo sem número da versão.
ProductVersion	Versão completa do aplicativo instalada	Número da versão do aplicativo completo, inclusive o número da compilação.
InstalledPatches	Conjunto de nomes de patch exibidos, implementados para o aplicativo.	Lista de reparos críticos instalados para o aplicativo.
IsLicenseInstalled	Estado de ativação do aplicativo.	Status da chave usada para ativar o aplicativo. Valores possíveis: • Falso - Uma chave ou o código de ativação não foi estabelecido no aplicativo. • Verdadeiro - Uma chave ou o código de ativação foi adicionado ao aplicativo.

Propriedade da instância	Descrição	Valores
LicenseDaysLeft	Exibe quantos dias restam até a expiração da licença atual.	Número de dias restantes até a expiração da licença atual. Valores possíveis não positivos: • 0 - Licença expirou • -1 - Incapaz de obter informações sobre a chave atual ou a chave especificada não pode ser usada para ativar o aplicativo (por exemplo, foi bloqueada com base em uma lista negra de chaves).
AVBasesDatetime	Carimbo de data/hora de uma versão de banco de dados do antivírus atual.	Data e hora da criação dos bancos de dados de antivírus atualmente em uso. Se o aplicativo instalado não usar bancos de dados do antivírus, o campo tem o valor “Não instalado”.
IsExploitPreventionEnabled	Estado do componente Prevenção de Exploits.	Status do componente Prevenção de Exploits. Valores possíveis: • Verdadeiro - O componente Prevenção de Exploits está ativo e fornece proteção. • Falso - O componente Prevenção de Exploits não fornece proteção. Por exemplo: desativado, não instalado, o Contrato de Licença foi violado.
ProtectionTasksRunning	Conjunto de tarefas de proteção em execução no momento.	Lista de proteção, controle e tarefas de monitoramento atualmente em execução. Este campo deve considerar todas as tarefas não periódicas em execução. Se nenhuma tarefa não periódica estiver em execução, o campo terá o valor "Não".
IsAppControlRunning	Estado da tarefa de Controle de Inicialização de Aplicativos.	Status da tarefa de Controle de Inicialização de Aplicativos. • Verdadeiro - a tarefa de Controle de Inicialização de Aplicativos está em execução. • Falso - O Controle de Inicialização de Aplicativos não está em execução ou o componente de Controle de Inicialização de Aplicativos não está instalado.

Propriedade da instância	Descrição	Valores
AppControlMode	Modo da tarefa de Controle de Inicialização de Aplicativos.	Descrição do status atual do componente Controle de Inicialização de Aplicativos e descreve o modo selecionado da tarefa correspondente. Valores possíveis: • Ativa - O modo **Ativa** é selecionado nas configurações de tarefa. • Somente estatísticas - O modo **Somente estatísticas** é selecionado nas configurações de tarefa. • Não instalado - O componente Controle de Inicialização de Aplicativos não está instalado
AppControlRulesNumber	O número total de regras de controle de inicialização de aplicativos.	O número de regras atualmente especificado nas configurações da tarefa de Controle de Inicialização de Aplicativos.
AppControlLastBlocking	O carimbo de data/hora do último bloqueio de inicialização de aplicativo pela tarefa de Controle de Inicialização de Aplicativos em qualquer modo.	Data e hora que o componente Controle de Inicialização de Aplicativos bloqueou pela última vez a inicialização de um aplicativo. Este campo inclui todos os aplicativos bloqueados, independentemente do modo da tarefa. Se nenhuma instância de inicialização de aplicativo bloqueada estiver registrada no momento em que a consulta WMI for processada, o campo recebe o valor “Não”.
PeriodicTasksRunning	O conjunto de tarefas periódicas atualmente em execução.	A lista de tarefas de Verificação por Demanda, Atualização e tarefas de tomada de inventário atualmente em execução. Este campo deve incluir todas as tarefas periódicas em execução. Se nenhuma tarefa periódica estiver sendo executada no momento, o campo recebe o valor "Não".
ConnectionState	O estado da conexão entre componente Provedor WMI e o Kaspersky Security Service (KAVFS).	Informações sobre o status da conexão entre o módulo do Provedor de WMI e o Kaspersky Security Service. Valores possíveis: • Êxito - a conexão foi estabelecida com êxito: o cliente WMI pode receber informações sobre o status de aplicativo. • Falha. Código de erro: <código> - A conexão não pode ser estabelecida devido a um erro com o código especificado.

Estes dados representam propriedades KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security, em que:

- KasperskySecurity_ProductInfo é o nome da classe do Kaspersky Embedded Systems Security
- ProductName=Kaspersky Embedded Systems Security é o parâmetro da chave do Kaspersky Embedded Systems Security

A instância é criada no namespace ROOT\Kaspersky\Security.

Trabalhar com o Kaspersky Embedded Systems Security na linha de comando

Esta seção descreve como trabalhar com o Kaspersky Embedded Systems Security na linha de comando.

Neste capítulo

Comandos da linha de comando 488

Códigos de retorno da linha de comando 515

Comandos da linha de comando

Você poderá executar comandos de gerenciamento básico do Embedded Systems Security na linha de comando do computador protegido, se tiver incluído o componente Utilitário de linha de comando na lista de recursos instalados durante a instalação do Kaspersky Embedded Systems Security.

Usando os comandos da linha de comando, você pode gerenciar apenas as funções que pode acessar de acordo com as permissões atribuídas a você no Kaspersky Embedded Systems Security.

Certos comandos do Kaspersky Embedded Systems Security são realizados das seguintes maneiras:

- Modo síncrono: o gerenciamento volta ao Console somente após a conclusão da execução do comando.
- Modo assíncrono: o gerenciamento volta ao Console imediatamente após a execução do comando.

► *Para interromper a execução de um comando no modo síncrono*

pressione o atalho **Ctrl+C** no teclado.

Observe as seguintes regras ao inserir comandos do Kaspersky Embedded Systems Security:

- Introduza modificadores e comandos usando letras maiúsculas e minúsculas.
- Delimite modificadores com o caractere de espaço.
- se o nome do arquivo/pasta cujo caminho você especificar como valor chave incluir um espaço, especifique o caminho do arquivo/pasta entre aspas, por exemplo: `"C:\TEST\test cpp.exe"`
- se necessário, use os marcadores de posição no nome do arquivo ou máscaras de caminho, por exemplo: “`C:\Temp\Temp*\`”, “`C:\Temp\Temp???.doc`”, “`C:\Temp\Temp*.doc`”

Você pode usar a linha de comandos para todo o conjunto de operações requeridas para gerenciamento e administração do Kaspersky Embedded Systems Security (consulte a tabela abaixo).

Tabela 78. Comandos do Kaspersky Embedded Systems Security

Comando	Descrição
KAVSHELL APPCONTROL (consulte a seção "Preenchendo a lista de regras de Controle de inicialização de aplicativos KAVSHELL APPCONTROL" na página 503)	Renova a lista de regras especificadas de acordo com o princípio de adição selecionado.
KAVSHELL APPCONTROL/CONFIG (consulte a seção "Gerenciamento da tarefa de Controle de Inicialização de Aplicativos KAVSHELL APPCONTROL /CONFIG" na página 500)	Controla o modo operacional da tarefa de Controle de Inicialização de Aplicativos
KAVSHELL APPCONTROL /GENERATE (consulte a seção "Gerador de Regras de Controle de Inicialização de Aplicativos KAVSHELL APPCONTROL /GENERATE" na página 501)	Inicia a tarefa do Gerador de Regras de Controle de Inicialização de Aplicativos.
KAVSHELL VACUUM (consulte a seção "Desfragmentação de arquivos de log do Kaspersky Embedded Systems Security. KAVSHELL VACUUM" na página 511)	Desfragmenta arquivos de log do Kaspersky Embedded Systems Security.
KAVSHELL PASSWORD	Gerencia as configurações de proteção de senha.
KAVSHELL HELP (consulte a seção "Exibindo a ajuda de comando do Kaspersky Embedded Systems Security. KAVSHELL HELP" na página 491)	Exibe a ajuda do comando para o Kaspersky Embedded Systems Security.
KAVSHELL START (consulte a seção "Iniciando e interrompendo o Kaspersky Security Service KAVSHELL START, KAVSHELL STOP" na página 491)	Inicia o serviço do Kaspersky Embedded Systems Security.
KAVSHELL STOP (consulte a seção "Iniciando e interrompendo o Kaspersky Security Service KAVSHELL START, KAVSHELL STOP" na página 491)	Interrompe o serviço do Kaspersky Embedded Systems Security.

Comando	Descrição
KAVSHELL SCAN (consulte a seção "Verificação da área selecionada. KAVSHELL SCAN" na página 492)	Cria e inicia uma tarefa de Verificação por Demanda temporária com o escopo da verificação e as configurações de segurança especificadas pelos modificadores do comando.
KAVSHELL SCANCRITICAL (consulte a seção "Iniciando a tarefa de Verificação de áreas críticas. KAVSHELL SCANCRITICAL" na página 496)	Inicia a tarefa do sistema de Verificação de áreas críticas.
KAVSHELL TASK (consulte a seção "Gerenciando a tarefa especificada de maneira assíncrona. KAVSHELL TASK" na página 497)	Inicia, pausa/reinicia, interrompe a tarefa selecionada de forma assíncrona, retorna o status/as estatísticas da tarefa atual.
KAVSHELL RTP (consulte a seção "Inicialização e interrupção de tarefas de Proteção em tempo real. KAVSHELL RTP" na página 499)	Executa ou interrompe todas as tarefas de Proteção em tempo real.
KAVSHELL UPDATE (consulte a seção "Iniciando a tarefa de Atualização do Banco de Dados do Kaspersky Embedded Systems Security. KAVSHELL UPDATE" na página 505)	Inicia a tarefa de atualização dos bancos do Kaspersky Embedded Systems Security com as configurações especificadas usando modificadores de comando.
KAVSHELL REVERTEM (consulte a seção "Revertendo atualizações do banco de dados do Kaspersky Embedded Systems Security. KAVSHELL ROLLBACK" na página 508)	Reverte os bancos para a versão anterior.
KAVSHELL LICENSE	Adicionar ou elimina as chaves. Exibe informações sobre as chaves adicionadas.
KAVSHELL TRACE (consulte a seção "Ativando, configurando e desativando o log de rastreamento. KAVSHELL TRACE" na página 509)	Ativa ou desativa o log de rastreamento, gerencia as configurações do log de rastreamento.
KAVSHELL DUMP (consulte a seção "Ativando e desativando a criação do arquivo de despejo. KAVSHELL DUMP" na página 512)	Ativa ou desativa os arquivos de despejo da memória de processo do Kaspersky Embedded Systems Security em caso de encerramento anormal de processos.

Comando	Descrição
KAVSHELL IMPORT (consulte a seção "Importando configurações. KAVSHELL IMPORT" na página 513)	Importa configurações gerais, funções e tarefas do Kaspersky Embedded Systems Security de um arquivo de configuração criado anteriormente.
KAVSHELL EXPORT (consulte a seção "Exportando configurações. KAVSHELL EXPORT" na página 514)	Exporta todas as configurações e as tarefas existentes do Kaspersky Embedded Systems Security para um arquivo de configuração.
KAVSHELL DEVCONTROL (consulte a seção "Preenchimento da lista de regras de Controle de Dispositivos. KAVSHELL DEVCONTROL" na página 504)	Adiciona à lista de regras de controle de dispositivos gerada de acordo com o método selecionado.

Exibindo a ajuda de comando do Kaspersky Embedded Systems Security. KAVSHELL HELP

Para obter a lista de todos os comandos do Kaspersky Embedded Systems Security, execute um dos comandos a seguir:

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Para obter uma descrição de um comando e sua sintaxe, execute um dos comandos a seguir:

```
KAVSHELL HELP <comando>

KAVSHELL <comando> /?
```

Exemplos de comando KAVSHELL HELP

Para exibir informações detalhadas sobre o comando KAVSHELL SCAN, execute o seguinte comando:

```
KAVSHELL HELP SCAN
```

Iniciando e interrompendo o Kaspersky Security Service KAVSHELL START, KAVSHELL STOP

Para executar o Kaspersky Security Service, execute o comando

```
KAVSHELL START
```

Por padrão, quando o Kaspersky Security Service é iniciado, as tarefas de Proteção de Arquivos em Tempo Real e Verificação na inicialização do sistema, bem como outras tarefas programadas para iniciar **Ao iniciar o aplicativo** serão iniciadas.

Para interromper o Kaspersky Security Service, execute o comando

```
KAVSHELL STOP
```

A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Verifica a área selecionada. KAVSHELL SCAN

Para iniciar uma tarefa para verificar áreas específicas do computador protegido use o comando `KAVSHELL SCAN`. Os modificadores de comando especificam o escopo da verificação e as configurações de segurança do nó selecionado.

A tarefa de Verificação por Demanda iniciada usando o comando `KAVSHELL SCAN` é uma tarefa temporária. Ela é exibida no Console do Aplicativo apenas enquanto é executada (não é possível visualizar as configurações da tarefa no Console do Aplicativo). O log de desempenho da tarefa é gerado simultaneamente. Ele é exibido em **Logs de tarefas** no Console do Aplicativo.

Ao especificar caminhos em tarefas de verificação para áreas específicas, você pode usar variáveis de ambiente. Se você usar a variável de ambiente especificada para o usuário, execute o comando `KAVSHELL SCAN` com as permissões para esse usuário.

O comando `KAVSHELL SCAN` é executado no modo síncrono.

Para iniciar uma tarefa de Verificação por Demanda existente a partir da linha de comando, use o comando KAVSHELL TASK (consulte a seção "Gerenciando a tarefa especificada de maneira assíncrona.Comando KAVSHELL TASK" na página 497).

Sintaxe do comando KAVSHELL SCAN

```
KAVSHELL SCAN <escopo da verificação>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:< caminho do
arquivo com a lista de escopos da verificação >] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>]
[/EM:<"máscaras">] [/ES:<tamanho>] [/ET:<número de segundos>] [/TZOFF]
[/OF:<SKIP|RESIDENT|SCAN[=<dias>] [NORECALL]>]
[/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<caminho para o
arquivo de log de tarefas>] [/ANSI] [/ALIAS:<alias da tarefa>]
```

O comando KAVSHELL SCAN tem chaves obrigatórias e opcionais (veja a tabela abaixo).

Exemplos do comando KAVSHELL SCAN

```
KAVSHELL SCAN Pasta56 D:\Pasta1\Pasta2\Pasta3\ C:\Pasta1\ C:\Pasta2\3.exe
"\\outro servidor\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
```

Tabela 79. Modificadores do comando KAVSHELL SCAN

Chave	Descrição
Escopo da verificação. Modificador obrigatório.	
<arquivos> <pastas> <caminho de rede>	Especifica o escopo da verificação - lista de arquivos, pastas, caminhos de rede e áreas predefinidas. Especifique os caminhos de rede no formato UNC (Universal Naming Convention). No exemplo seguinte, a pasta Pasta4 é especificada sem um caminho - ela está localizada na pasta a partir da qual você inicia o comando KAVSHELL: KAVSHELL SCAN Pasta4 Se o nome do objeto a ser verificado contiver espaços, ele deverá ser colocado entre aspas. Quando uma pasta for selecionada, o Kaspersky Embedded Systems Security também verificará todas as subpastas dessa pasta. Os símbolos * ou ? podem ser usados para verificar um grupo de arquivos.
/MEMORY	Verificar objetos da RAM
/SHARED	Verificar pastas compartilhadas do computador
/STARTUP	Verificar objetos de execução automática
/REMDRIVES	Verificar unidades removíveis
/FIXDRIVES	Verificar discos rígidos
/MYCOMP	Verificar todas as áreas do computador protegido
/L:<caminho do arquivo com a lista de escopos da verificação>	Nome do arquivo com a lista de escopos da verificação, incluindo o caminho completo do arquivo. Delimite os escopos da verificação nos arquivos usando quebras de linha. Você pode especificar áreas de verificação predefinidas tal como é exibido no seguinte exemplo de um arquivo com uma lista do escopo da verificação: C:\ D:\Docs*.doc E:\Meus Documentos /STARTUP /SHARED
Objetos verificados (Tipos de arquivos). Se você não especificar valores para esse modificador, o Kaspersky Embedded Systems Security vai verificar objetos pelo seu formato.	
/FA	Verificar todos os objetos
/FC	Verificar objetos por formato (por padrão). O Kaspersky Embedded Systems Security verifica somente o formato dos objetos incluídos na lista de formatos de objetos infetáveis.

Chave	Descrição
/FE	Verificar objetos por extensão. O Kaspersky Embedded Systems Security verifica somente objetos com extensões incluídas na lista de extensões de objetos infetáveis.
/NEWONLY	Verificar apenas arquivos novos e modificados. Se você não fornecer esse modificador, o Kaspersky Embedded Systems Security vai verificar todos os objetos.
Ação a ser executada em objetos infectados e outros. Se você não especificar valores para esse modificador, o Kaspersky Embedded Systems Security executará a ação **Ignorar**.	
DISINFECT	Desinfectar; ignorar se a desinfecção não for possível As configurações DISINFECT e DELETE são salvas na versão atual do Kaspersky Embedded Systems Security para garantir a compatibilidade com versões anteriores. Essas configurações podem ser utilizadas em vez dos comandos da chave /AI: e /AS: Neste caso, o Kaspersky Embedded Systems Security não processará os objetos possivelmente infectados.
DISINFDEL	Desinfectar; excluir se a desinfecção não for possível
DELETE	Excluir As configurações DISINFECT e DELETE são salvas na versão atual do Kaspersky Embedded Systems Security para garantir a compatibilidade com versões anteriores. Essas configurações podem ser utilizadas em vez dos comandos da chave /AI: e /AS: Neste caso, o Kaspersky Embedded Systems Security não processará os objetos possivelmente infectados.
REPORT	Enviar relatório (por padrão)
AUTO	Executar ação recomendada
/AS: **Ação a ser executada em objetos possivelmente infectados**/ Se você não especificar valores para esse modificador, o Kaspersky Embedded Systems Security executará a ação **Ignorar**.	
QUARANTINE	Quarentena
DELETE	Excluir
REPORT	Enviar relatório (por padrão)
AUTO	Executar ação recomendada
Exclusões	
/E:ABMSPO	Exclui objetos compostos dos seguintes tipos: A – arquivos compactados (verifica apenas arquivos compactados SFX) B – bancos de dados de e-mail M – e-mail sem formatação S – arquivos compactados e arquivos compactados SFX P – objetos compactados O – objetos OLE incorporados
/EM:<″máscaras″>	Excluir arquivos por máscara É possível especificar várias máscaras, por exemplo: EM:″*.txt;*.png; C\Videos*.avi″.

Chave	Descrição
/ET:<número de segundos>	Interrompe o processamento do objeto se ele continuar para além do número de segundos especificado pelo valor <número de segundos>. Por padrão, não há uma restrição de tempo.
/ES:<tamanho>	Não verificar objetos compostos maiores do que o tamanho (em MB) especificado pelo valor <tamanho>. Por padrão, o Kaspersky Embedded Systems Security verifica objetos de todos os tamanhos.
/TZOFF	Desativa exclusões da Zona Confiável
Configurações avançadas (Opções)	
/NOICHECKER	Desativa o uso da tecnologia iChecker (ativado por padrão)
/NOISWIFT	Desativa o uso da tecnologia iSwift (ativado por padrão)
/ANALYZERLEVEL:<intensidade da análise>	Ativa o Analisador Heurístico, configura o nível de análise. Estão disponíveis os seguintes níveis de análise heurística: 1 – superficial 2 – médio 3 – profundo Se você omitir o modificador, o Kaspersky Embedded Systems Security não usará o analisador heurístico.
/ALIAS:<alias da tarefa>	Permite atribuir a uma tarefa de Verificação por Demanda um nome temporário através do qual a tarefa pode ser acessada durante sua execução, por exemplo para visualizar as estatísticas usando o comando TASK. O alias da tarefa deve ser exclusivo entre os aliases de tarefas de todos os componentes funcionais do Kaspersky Embedded Systems Security. Se esse modificador não for especificado, é usado o nome temporário scan_<kavshell_pid>, por exemplo, scan_1234. No Console do Aplicativo, a tarefa recebe o nome Scan objects (<data e hora>), por exemplo, Scan objects 16/08/2007 17h13m14.
Configurações dos logs de tarefas (Configurações de relatórios)	

Chave	Descrição
/W:<caminho do arquivo de log de tarefas>	Se esta chave for especificada, o Kaspersky Embedded Systems Security salvará o arquivo de log de tarefas com o nome definido pelo valor da chave. O arquivo de log contém estatísticas de execução da tarefa, a hora em que ela foi iniciada e concluída (interrompida), além de informações sobre os eventos da tarefa. O log é usado para registrar eventos definidos pelas configurações do log de tarefas e pelo log de eventos do Kaspersky Embedded Systems Security no Visualizador de Eventos. É possível especificar o caminho absoluto ou relativo do arquivo de log. Se você especificar somente o nome de um arquivo sem especificar o caminho respetivo, o arquivo de log será criado na pasta atual. Ao reiniciar o comando com as mesmas configurações de log, o arquivo de log existente será substituído. O arquivo de log pode ser exibido enquanto uma tarefa está em execução. O log é exibido no nó Logs de tarefas do Console do Aplicativo. Se o Kaspersky Embedded Systems Security não conseguir criar o arquivo de log, ele não interromperá a execução do comando mas será exibida uma mensagem de erro.
/ANSI	A opção permite registrar os eventos no log de tarefas com a codificação ANSI. A opção ANSI não será aplicada se a opção W não for definida. Se a opção ANSI não for especificada, o log de tarefas é gerado usando a codificação UNICODE.

Iniciando a tarefa de Verificação de áreas críticas. KAVSHELL SCANCRITICAL

Use o comando `KAVSHELL SCANCRITICAL` para iniciar a tarefa do sistema Verificação por Demanda do sistema e Verificação de áreas críticas com as configurações definidas no Console do Aplicativo.

Sintaxe do comando KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<caminho para o arquivo de log de tarefas>]
```

Exemplos do comando KAVSHELL SCANCRITICAL

Para executar a tarefa de Verificação por Demanda e de Verificação de Áreas Críticas e salvar o log de tarefas scancritical.log na pasta atual, execute o seguinte comando:

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

Dependendo da sintaxe do modificador /W, você pode configurar a localização do log de tarefas (consulte a tabela abaixo).

Tabela 80. Sintaxe do modificador /W para o comando KAVSHELL SCANCRITICAL

Chave	Descrição
/W:<caminho do arquivo de log de tarefas>	Se esta chave for especificada, o Kaspersky Embedded Systems Security salvará o arquivo de log de tarefas com o nome definido pelo valor da chave. O arquivo de log contém estatísticas de execução da tarefa, a hora em que ela foi iniciada e concluída (interrompida), além de informações sobre os eventos da tarefa. O log é usado para registrar eventos definidos pelas configurações de logs de tarefas e pelo Log de Eventos do Aplicativo no Visualizador de Eventos. É possível especificar o caminho absoluto ou relativo do arquivo de log. Se você especificar somente o nome de um arquivo sem especificar o caminho respetivo, o arquivo de log será criado na pasta atual. Ao reiniciar o comando com as mesmas configurações de log, o arquivo de log existente será substituído. O arquivo de log pode ser exibido enquanto uma tarefa está em execução. O log é exibido no nó **Logs de tarefas** do Console do Aplicativo. Se o Kaspersky Embedded Systems Security não conseguir criar o arquivo de log, ele não interromperá a execução do comando mas será exibida uma mensagem de erro.

Gerenciando a tarefa especificada de maneira assíncrona. KAVSHELL TASK

Usando o comando `KAVSHELL TASK` você pode gerenciar a tarefa especificada: executar, pausar, continuar e interromper a tarefa especificada e visualizar o status e as estatísticas da tarefa atual. Este comando é executado no modo assíncrono.

A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Sintaxe do comando KAVSHELL TASK

```
KAVSHELL TASK [<alias do nome da tarefa> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Exemplos do comando KAVSHELL TASK

```
KAVSHELL TASK
```

```
KAVSHELL TASK on-access /START
```

```
KAVSHELL TASK user-task_1 /STOP
```

```
KAVSHELL TASK scan-computer /STATE
```

O comando `KAVSHELL TASK` pode ser executado sem modificadores ou com um ou vários modificadores

(consulte a tabela abaixo).

Tabela 81. Modificadores do comando KAVSHELL TASK

Chave	Descrição
Sem chaves	Mostra a lista de todas as tarefas existentes do Kaspersky Embedded Systems Security. A lista contém os campos: nome alternativo da tarefa, sua categoria (sistema ou personalizada) e o seu status atual.
<alias da tarefa>	Em vez do nome da tarefa, no comando SCAN TASK, use o alias da tarefa, um nome abreviado adicional atribuído pelo Kaspersky Embedded Systems Security às tarefas. Para visualizar os aliases de tarefa do Kaspersky Embedded Systems Security insira o comando KAVSHELL TASK sem modificadores
/START	Inicia a tarefa especificada no modo assíncrono.
/STOP	Interrompe a tarefa especificada.
/PAUSE	Pausa a tarefa especificada.
/RESUME	Reinicia a tarefa especificada no modo assíncrono.
/STATE	Retorna o status da tarefa atual (por exemplo, *Executando*, *Concluída*, *Pausada*, *Interrompida*, *Falhou*, *Iniciando*, *Recuperando*).
/STATISTICS	Obtém as estatísticas da tarefa - informações sobre o número de objetos processados a partir da hora de início da tarefa até agora.

Observe que nem todas as tarefas do Kaspersky Embedded Systems Security são totalmente compatíveis com essas chaves.

Os códigos de retorno do comando KAVSHELL TASK (consulte a seção "Códigos de retorno do comando KAVSHELL TASK" na página 517).

Registro do KAVFS como um processo protegido do sistema. KAVSHELL CONFIG

O comando `KAVSHELL CONFIG` permite controlar o registro do Kaspersky Security Service como um processo protegido do sistema (Processo protegido Superficial) usando o driver ELAM, instalado no sistema operacional

durante a instalação do aplicativo.

Sintaxe do comando KAVSHELL CONFIG

```
KAVSHELL CONFIG /PPL:<ON|OFF>
```

Tabela 82. Chaves do comando KAVSHELL CONFIG

Chave	Descrição
/PPL:ON	Registrar o Kaspersky Security Service como PPL.
/PPL:OFF	Remover o atributo de PPL do Kaspersky Security Service.

A aplicação executa o cancelamento do registro de serviço automaticamente quando alguma das seguintes ações é realizada:

- desinstalação do aplicativo
- atualização do aplicativo
- instalação de patch
- reparo dos componentes do aplicativo

Códigos de retorno do comando KAVSHELL CONFIG.

Inicialização e interrupção de tarefas de Proteção em Tempo Real. KAVSHELL RTP

Usando o comando `KAVSHELL RTP` você pode iniciar ou interromper todas as tarefas de proteção em tempo real.

> A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Sintaxe do comando KAVSHELL RTP

```
KAVSHELL RTP {/START | /STOP}
```

Exemplos do comando KAVSHELL RTP

Para executar tarefas de proteção em tempo real, execute o seguinte comando:

```
KAVSHELL RTP /START
```

O comando `KAVSHELL RTP` pode incluir qualquer dos dois modificadores obrigatórios (consulte a tabela abaixo).

Tabela 83. Modificadores do comando KAVSHELL RTP

Chave	Descrição
/START	Inicia todas as tarefas de Proteção em Tempo Real: Proteção de Arquivos em Tempo Real e Uso da KSN.
/STOP	Interrompe todas as tarefas de proteção em tempo real.

Gerenciamento da tarefa de Controle de Inicialização de Aplicativos KAVSHELL APPCONTROL /CONFIG

É possível usar o comando `KAVSHELL APPCONTROL /CONFIG` para configurar o modo em que a tarefa de Controle de Inicialização de Aplicativos executa e monitora o carregamento de módulos DLL.

Sintaxe do comando KAVSHELL APPCONTROL /CONFIG

```
 /config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config
/savetofile:<caminho completo para o arquivo XML>
```

Exemplos do comando KAVSHELL APPCONTROL /CONFIG

► *Para executar a tarefa de Controle de Inicialização de Aplicativos no modo **Ativa** sem carregar uma DLL e salvar as configurações da tarefa após a conclusão, execute o comando a seguir:*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

Você pode definir as configurações da tarefa de Controle de Inicialização de Aplicativos usando os parâmetros de linha de comando (consulte a tabela abaixo).

Tabela 84. Chaves de comando `KAVSHELL APPCONTROL /GENERATE`

Chave	Descrição
`/mode:<applyrules|statistics>`	Modo operacional da tarefa de Controle de Inicialização de Aplicativos. Você pode selecionar um dos seguintes modos: • ativa - aplicar regras de Controle de Inicialização de Aplicativos; • statistics - somente estatísticas
`/dll:<no|yes>`	Ativa ou desativa o monitoramento do carregamento de DLL.
`/savetofile: <caminho para arquivo XML>`	Exportar as regras especificadas no arquivo indicado no formato XML.
`/savetofile: <nome completo do arquivo xml>`	Salvar a lista de regras no arquivo.
`/savetofile: <nome completo do arquivo xml> /sdc`	Salvar a lista de regras de Controle de Distribuição de Software no arquivo.
`/clearsdc`	Excluir todas as regras de Controle de Distribuição de Software da lista.

Gerador de Regras de Controle de Inicialização de Aplicativos KAVSHELL APPCONTROL /GENERATE

Usando o comando `KAVSHELL APPCONTROL /GENERATE`, você pode gerar as listas de regras de Controle de inicialização de aplicativos.

A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Sintaxe do comando KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL /GENERATE <caminho para a pasta> | /source:<caminho para o arquivo com lista de pastas> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<usuário ou grupo de usuários>] [/export:<caminho para arquivo XML>] [/import:<a|r|m>] [/prefix:<prefixo para nomes de regras>] [/unique]
```

Exemplos do comando KAVSHELL APPCONTROL /GENERATE

- *Para gerar regras para arquivos a partir de pastas especificadas, execute o comando a seguir:*

  ```
  KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
  /export:c:\rules\appctrlrules.xml
  ```

- *Para gerar regras para arquivos executáveis de todas as extensões disponíveis na pasta especificada e, após a conclusão de tarefa, salvar as regras geradas no arquivo XML do arquivo especificado, execute o seguinte comando:*

  ```
  KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms
  /export:c\rules\appctrlrules.xml
  ```

Dependendo da sintaxe das chaves você pode definir as configurações de geração de regras automáticas da tarefa de Controle de Inicialização de Aplicativos (consulte a tabela abaixo).

Tabela 85. Chaves do comando `KAVSHELL APPCONTROL /GENERATE`

Chave	Descrição
Escopo de uso das regras de permissão	
<caminho da pasta>	Especifica o caminho da pasta com arquivos executáveis que necessitam de regras de permissão geradas automaticamente.
/source: <caminho para o arquivo com lista de pastas>	Especifica o caminho do arquivo TXT com a lista de pastas contendo arquivos executáveis que necessitam de regras de permissão geradas automaticamente.

/masks: <edms>	Especifica extensões de arquivos executáveis que necessitam de regras de permissão geradas automaticamente. Você pode incluir em arquivos de escopo de uso das regras as seguintes extensões: • e - Arquivos EXE • d - Arquivos DLL • m - Arquivos MSI • s - scripts
/runapp	Ao gerar regras de permissão, leva em consideração aplicativos em execução em um computador protegido no momento da execução da tarefa.
Ações ao gerar regras de permissão automaticamente	
/rules: <ch|cp|h>	Especifica ações a serem executadas durante a geração de regras de permissão de Controle de inicialização de aplicativos: • ch - usar certificado digital. Se o certificado estiver em falta, utilize o hash SHA256. • cp - usar o certificado digital. Se o certificado estiver em falta, use o caminho ao arquivo executável. • h - usar hash SHA256.
/strong	Usar o requerente e a impressão digital do certificado digital ao gerar automaticamente as regras de permissão de Controle de inicialização de aplicativos. O comando é executado se a chave /rules: <ch|cp> for especificada.
/user: <usuário ou grupo de usuários>	Especifica o nome de usuário ou de um grupo de usuários para os quais as regras serão aplicadas. O aplicativo controlará qualquer aplicativo executado pelo usuário e/ou grupo de usuários especificado.
Ações na conclusão do Gerador de Regras de Controle de Inicialização de Aplicativos	
/export: <path to XML file>	Salva as regras geradas no arquivo XML.
/unique	Adiciona informações sobre o computador com aplicativos instalados que são a base para a geração de regras de permissão de Controle de inicialização de aplicativos.
/prefix: <prefixo para nomes de regras>	Especifica o prefixo de nome para a geração de regras de permissão de controle de inicialização de aplicativos.

/import: <a|r|m>	Importa regras geradas para a lista de regras de controle de inicialização de aplicativos especificadas de acordo com o princípio de adição selecionado: • a - **Adicionar às regras existentes** (regras com configurações idênticas são duplicadas) • r - **Substituir as regras existentes** (regras com parâmetros idênticos não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único) • m - **Mesclar com as regras existentes** (regras com parâmetros idênticos não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único)

Preenchendo a lista de regras de Controle de inicialização de aplicativos KAVSHELL APPCONTROL

Utilizando `KAVSHELL APPCONTROL`, é possível adicionar regras do arquivo XML na lista de regras da tarefa de Controle de Inicialização de Aplicativos de acordo com o princípio selecionado e também excluir todas as regras definidas da lista.

A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Sintaxe do comando KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <caminho para arquivo XML> | /replace <caminho para arquivo XML> | /merge <caminho para arquivo XML> | /clear
```

Exemplos do comando KAVSHELL APPCONTROL

► *Para adicionar regras de um arquivo XML às regras já especificadas para a tarefa de Controle de Inicialização de Aplicativos de acordo com o princípio Adicionar às regras existentes, execute o seguinte comando:*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

Dependendo da sintaxe das chaves, você pode selecionar o princípio para adicionar novas regras um arquivo XML especificado a uma lista de regras definidas do Controle de inicialização de aplicativos (consulte a tabela abaixo).

Tabela 86. Chaves do comando KAVSHELL APPCONTROL

Chave	Descrição
/append <caminho para arquivo XML>	Renova a lista de regras de controle de inicialização de aplicativos com base em um arquivo XML especificado. Princípio de adição - **Adicionar às regras existentes** (regras com configurações idênticas são duplicadas).
/replace <caminho para arquivo XML>	Renova a lista de regras de controle de inicialização de aplicativos com base em um arquivo XML especificado. Princípio de adição - **Substituir as regras existentes** (regras com parâmetros idênticos não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único).
/merge <caminho para arquivo XML>	Renova a lista de regras de controle de inicialização de aplicativos com base em um arquivo XML especificado. Princípio de adição - **Mesclar com as regras existentes** (as novas regras não duplicam as regras já existentes).
/clear	Apaga a lista de regras de Controle de inicialização de aplicativos.

Preenchimento da lista de regras de Controle de Dispositivos. KAVSHELL DEVCONTROL

Utilizando `KAVSHELL DEVCONTROL` , é possível adicionar regras do arquivo XML à lista de regras da tarefa Controle de Dispositivos de acordo com o princípio selecionado e também excluir todas as regras definidas da lista.

A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Sintaxe do comando KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <caminho para arquivo XML> | /replace <caminho para arquivo XML> | /merge <caminho para arquivo XML> | /clear
```

Exemplos do comando KAVSHELL DEVCONTROL

► *Para adicionar regras de um arquivo XML às regras já especificadas para a tarefa Controle de Dispositivos de acordo com o princípio **Adicionar às regras existentes**, execute o seguinte comando:*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

Dependendo da sintaxe das chaves, você pode selecionar o princípio para adicionar novas regras e um arquivo XML especificado a uma lista de regras definidas do Controle de dispositivos (consulte a tabela abaixo).

Tabela 87. Chaves do comando KAVSHELL DEVCONTROL

Chave	Descrição
/append <caminho para arquivo XML>	Renova a lista de regras de controle de dispositivos com base em um arquivo XML especificado. Princípio de adição - **Adicionar às regras existentes** (regras com configurações idênticas são duplicadas).
/replace <caminho para arquivo XML>	Renova a lista de regras de controle de dispositivos com base em um arquivo XML especificado. Princípio de adição - **Substituir as regras existentes** (regras com parâmetros idênticos não são adicionadas; a regra é adicionada se pelo menos um parâmetro de regra for único).
/merge <caminho para arquivo XML>	Renova a lista de regras de controle de dispositivos com base em um arquivo XML especificado. Princípio de adição - **Mesclar com as regras existentes** (as novas regras não duplicam as regras já existentes).
/clear	Apaga a lista de regras de Controle de Dispositivos.

Iniciando a tarefa de atualização dos bancos de dados do Kaspersky Embedded Systems Security. KAVSHELL UPDATE

O comando KAVSHELL UPDATE pode ser usado para executar a atualização dos bancos de dados do Kaspersky Embedded Systems Security no modo assíncrono.

A tarefa de atualização dos bancos de dados do Kaspersky Embedded Systems Security executada usando o comando KAVSHELL UPDATE é uma tarefa temporária. Ela é exibida apenas no Console do Aplicativo ao ser executada. O log de tarefas é gerado simultaneamente. Ele é exibido em **Logs de tarefas** no Console do Aplicativo. As políticas do Kaspersky Security Center podem ser aplicadas às tarefas de atualização criadas e iniciadas usando o comando KAVSHELL UPDATE e as tarefas de atualização criadas no Console do Aplicativo. Para obter informações sobre o gerenciamento do Kaspersky Embedded Systems Security em computadores usando o Kaspersky Security Center, consulte a seção "Gerenciando o Kaspersky Embedded Systems Security usando o Kaspersky Security Center".

É possível usar variáveis de ambiente ao especificar o caminho da fonte de atualizações nesta tarefa. Se forem usadas variáveis de ambiente do usuário, execute o comando KAVSHELL UPDATE com as permissões para esse usuário.

Sintaxe do comando KAVSHELL UPDATE

```
KAVSHELL UPDATE < Caminho da fonte das atualizações | /AK | /KL> [/NOUSEKL]
[/PROXY:<address>:<porta>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<nome de usuário>]
[/PROXYPWD:<senha>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE]
```

```
[/TIMEOUT:<segundos>] [/REG:<código iso3166>] [/W:<caminho para arquivo de log de tarefas>] [/ALIAS:<alias da tarefa>]
```

O comando KAVSHELL UPDATE tem chaves obrigatórias e opcionais (veja a tabela abaixo).

Exemplos do comando KAVSHELL UPDATE

- *Para iniciar uma tarefa de atualização do banco de dados personalizada, execute o seguinte comando:*

```
KAVSHELL UPDATE
```

- *Para executar a tarefa de atualização do banco de dados usando os arquivos de atualização na pasta de rede \\server\databases, execute o seguinte comando:*

```
KAVSHELL UPDATE \\server\databases
```

- *Para iniciar uma tarefa de atualização do servidor FTP ftp://dnl-ru1.kaspersky-labs.com/ e registrar todos os eventos da tarefa no arquivo c:\update_report.log, execute o comando:*

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

- *Para baixar as atualizações do banco de dados do Kaspersky Embedded Systems Security do servidor de atualização da Kaspersky Lab, conecte-se à fonte de atualizações por meio de um servidor proxy (endereço do servidor proxy: proxy.company.com, porta: 8080). Para acessar o computador usando a autenticação NTLM integrada do Microsoft Windows com o nome de usuário: inetuser, senha: 123456, execute o seguinte comando:*

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

Tabela 88. Chaves do comando KAVSHELL UPDATE

Chave	Descrição
Fonte das atualizações (chave obrigatória). Especifique uma ou várias fontes. O Kaspersky Embedded Systems Security acessará as fontes na ordem em que elas forem listadas. Delimite as origens com um espaço.	
<caminho em formato UNC>	Fonte de atualização definida pelo usuário. Caminho da pasta de atualização de rede no formato UNC.
<URL>	Fonte de atualizações definida pelo usuário. Endereço do servidor HTTP ou FTP no qual a pasta de atualização está localizada.
<Pasta local>	Fonte de atualizações definida pelo usuário. Pasta no computador protegido.
/AK	Servidor de administração do Kaspersky Security Center como a fonte da atualização.
/KL	Servidores de atualização da Kaspersky Lab como fonte das atualizações.
/NOUSEKL	Não use os servidores de atualização da Kaspersky Lab se não houver outras fontes de atualização disponíveis (usadas por padrão).
Configurações do servidor proxy	

Chave	Descrição
/PROXY:<endereço>:<porta>	Nome de rede ou endereço IP do servidor proxy e sua porta. Se esta chave não for especificada, o Kaspersky Embedded Systems Security detectará automaticamente as configurações do computador proxy usado na rede local.
/AUTHTYPE:<0-2>	Esta chave especifica o método de autenticação para acessar o servidor proxy. Ele pode ter os seguintes valores: **0** – autenticação NTLM integrada do Microsoft Windows; o Kaspersky Embedded Systems Security fará contato com o servidor proxy sob a conta **Sistema local** (**SYSTEM**) **1** – autenticação NTLM integrada do Microsoft Windows; o Kaspersky Embedded Systems Security fará contato com o servidor proxy sob a conta com o nome de login e a senha especificados pelas chaves /PROXYUSER e /PROXYPWD **2** – autenticação com o nome de login e a senha especificados pelas chaves /PROXYUSER e /PROXYPWD (autenticação básica) Se não for exigida a autenticação para acessar o servidor proxy, não será necessário especificar uma chave.
/PROXYUSER:<nome de usuário>	O nome de usuário que será usado para acessar o servidor proxy. Se o valor da chave /AUTHTYPE:0 for especificado, as chaves /PROXYUSER:<nome de usuário> e /PROXYPWD:<senha> serão ignoradas.
/PROXYPWD:<senha>	A senha de usuário que será usada para acessar o servidor proxy. Se o valor da chave /AUTHTYPE:0 for especificado, as chaves /PROXYUSER:<nome de usuário> e /PROXYPWD:<senha> serão ignoradas. Se a chave /PROXYUSER for especificada e /PROXYPWD omitida, a senha será considerada como em branco.
/NOPROXYFORKL	Não usar as configurações do servidor proxy para se conectar aos servidores de atualização da Kaspersky Lab (usadas por padrão).
/USEPROXYFORCUSTOM	Usar as configurações do servidor proxy para se conectar às fontes de atualizações definidas pelo usuário (não usadas por padrão).
/USEPROXYFORLOCAL	Usar as configurações do servidor proxy para se conectar a fontes de atualização locais. Se não especificado, o valor **Ignorar servidor proxy para endereços locais** será aplicado.
Configurações gerais do servidor FTP e HTTP	
/NOFTPPASSIVE	Se esta chave for especificada, o Kaspersky Embedded Systems Security usará o modo de servidor FTP ativo para se conectar ao computador protegido. Se esta chave não for especificada, o Kaspersky Embedded Systems Security usará o modo de servidor FTP passivo, se possível.
/TIMEOUT:<número de segundos>	Tempo limite de conexão com o servidor FTP ou HTTP. Se você não especificar esta chave, o Kaspersky Embedded Systems Security usará o valor padrão: 10 segundos. O valor da chave deve ser um número inteiro.

Chave	Descrição
/REG:<código iso3166>	Configurações regionais. Esta chave é usada ao receber atualizações dos servidores de atualização da Kaspersky Lab. O Kaspersky Embedded Systems Security otimiza a carga da atualização no computador protegido por meio da seleção do servidor de atualização mais próximo. Como valor desta chave, especifique o código da letra do país onde está localizado o computador protegido, de acordo com a ISO 3166-1, por exemplo, /REG: gr ou /REG:RU. Se esta chave for omitida ou um código de país não existente for especificado, o Kaspersky Embedded Systems Security detectará a posição do computador protegido com base nas configurações regionais no computador onde o Console do Aplicativo está instalado.
/ALIAS:<alias da tarefa>	Esta chave permite atribuir um nome temporário à tarefa que pode ser usado para acessar a tarefa durante sua execução. Por exemplo, é possível exibir estatísticas da tarefa usando o comando TASK. O alias da tarefa deve ser exclusivo entre os aliases de tarefas de todos os componentes funcionais do Kaspersky Embedded Systems Security. Se essa chave não for especificada, é usado o nome temporário update_<kavshell_pid>, por exemplo, update_1234. No Console do Aplicativo, é atribuído à tarefa o nome Atualização do Banco de Dados (<data hora>), por exemplo, Atualização do Banco de Dados 16/08/2007 17h41m02.
/W:<caminho do arquivo de log de tarefas>	Se esta chave for especificada, o Kaspersky Embedded Systems Security salvará o arquivo de log de tarefas com o nome definido pelo valor da chave. O arquivo de log contém estatísticas de execução da tarefa, a hora em que ela foi iniciada e concluída (interrompida), além de informações sobre os eventos da tarefa. O log é usado para registrar eventos definidos pelas configurações do log de tarefas e pelo log de eventos do Kaspersky Embedded Systems Security no "Visualizador de Eventos". É possível especificar o caminho absoluto ou relativo do arquivo de log. Se for especificado apenas o nome do arquivo sem seu caminho, o arquivo de log será criado na pasta atual. Ao reiniciar o comando com as mesmas configurações de log, o arquivo de log existente será substituído. O arquivo de log pode ser exibido enquanto uma tarefa está em execução. O log é exibido no nó **Logs de tarefas** do Console do Aplicativo. Se o Kaspersky Embedded Systems Security não conseguir criar o arquivo de log, ele não interromperá a execução do comando ou exibirá uma mensagem de erro.

Códigos de retorno do comando KAVSHELL UPDATE (na página 518).

Revertendo atualizações do banco de dados do Kaspersky Embedded Systems Security. KAVSHELL ROLLBACK

O comando `KAVSHELL ROLLBACK` pode ser usado para executar uma tarefa do sistema de Reversão do banco de dados do Kaspersky Embedded Systems Security (reversão dos bancos de dados do Kaspersky Embedded Systems Security para a versão instalada anteriormente). O comando é executado de forma síncrona.

Sintaxe do comando:

```
KAVSHELL ROLLBACK
```

Códigos de retorno do comando KAVSHELL ROLLBACK (na página 519).

Gerenciando inspeção de log KAVSHELL TASK LOG-INSPECTOR

O comando `KAVSHELL TASK LOG-INSPECTOR` pode ser usado para monitorar a integridade do ambiente com base na análise do Log de Eventos do Windows.

Sintaxe do comando

```
KAVSHELL TASK LOG-INSPECTOR
```

Exemplos do comando

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Tabela 89. Modificadores do comando KAVSHELL TASK LOG-INSPECTOR

Chave	Descrição
/START	Inicia a tarefa especificada no modo assíncrono.
/STOP	Interrompe a tarefa especificada.
/STATE	Retorna o status da tarefa atual (por exemplo, *Executando*, *Concluída*, *Pausada*, *Interrompida*, *Falhou*, *Iniciando*, *Recuperando*).
/STATISTICS	Obtém as estatísticas da tarefa - informações sobre o número de objetos processados a partir da hora de início da tarefa até agora.

Códigos de retorno do comando KAVSHELL TASK LOG-INSPECTOR (consulte a seção "Códigos de retorno do comando KAVSHELL TASK LOG-INSPECTOR" na página 517).

Ativando, configurando e desativando o log de rastreamento. KAVSHELL TRACE

O comando `KAVSHELL TRACE` pode ser usado para ativar o log de rastreamento para todos os subsistemas do Kaspersky Embedded Systems Security e para configurar o nível de detalhe do log.

O Kaspersky Embedded Systems Security grava as informações nos arquivos de rastreamento e no arquivo de despejo no formulário não criptografado.

Sintaxe do comando KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<caminho da pasta do arquivo de log de rastreamento>
[/S:<tamanho máximo do log em megabytes>]
[/LVL:debug|info|warning|error|critical] | /OFF>
```

Se o log de rastreamento for mantido e você desejar alterar suas configurações, insira o comando `KAVSHELL TRACE` com a chave /ON e especifique as configurações do log de rastreamento com os valores das chaves /S e /LVL (veja a tabela abaixo).

Tabela 90. Chaves do comando KAVSHELL TRACE

Chave	Descrição
/ON	Ativa o log de rastreamento.
/F:<pasta com arquivos do log de rastreamento>	Esta chave especifica o caminho completo da pasta na qual os arquivos do log de rastreamento serão salvos (obrigatório). Se for especificado o caminho de uma pasta não existente, não será criado log de rastreamento. Caminhos para pastas em unidades de rede de outros computadores não podem ser especificados. Se um caractere de espaço for incluído no nome de uma pasta na qual você especifica o caminho como o valor da chave, coloque o caminho dessa pasta entre aspas, por exemplo: /F:"C\Trace Folder". As variáveis do ambiente do sistema podem ser usadas ao especificar o caminho dos arquivos de log de rastreamento; não são permitidas variáveis do ambiente do usuário.
/S: <tamanho máximo do arquivo de log em megabytes>	Esta chave define o tamanho máximo de um único arquivo de log de rastreamento. Assim que o arquivo de log atingir o nível máximo, o Kaspersky Embedded Systems Security começará a gravar informações em um novo arquivo; o arquivo de log anterior será salvo. Se o valor desta chave não for especificado, o tamanho máximo de um arquivo de log será 50 MB.
/LVL:debug|info|warning|error|critical	Esta chave configura o nível de detalhe do log, desde o valor máximo (**Todas as informações da depuração**) no qual todos os eventos são registrados no log, até o valor mínimo (**Eventos críticos**), no qual somente os eventos críticos são registrados. Se esta chave não for especificada, os eventos com o nível de detalhamento **Todas as informações da depuração** serão registrados no log de rastreamento.
/OFF	Esta chave desativa o log de rastreamento.

Exemplos do comando KAVSHELL TRACE

► *Para ativar o log de rastreamento usando o nível de detalhamento **Todas as informações da depuração** e o tamanho máximo de log de 200 MB, e salvar o arquivo de log na pasta C:\Pasta de Rastreamento, execute o comando:*

```
KAVSHELL TRACE /ON /F:"C:\Pasta de Rastreamento" /S:200
```

► *Para ativar o log de rastreamento usando o nível de detalhamento **Eventos importantes** e salvar o arquivo de log na pasta C:\Pasta de Rastreamento, execute o comando:*

```
KAVSHELL TRACE /ON /F:"C:\Pasta de Rastreamento" /LVL:warning
```

► *Para desativar o log de rastreamento:*

```
KAVSHELL TRACE /OFF
```

Códigos de retorno do comando KAVSHELL TRACE (consulte a seção "Códigos de retorno do comando KAVSHELL TRACE" na página 520).

Desfragmentação de arquivos de log do Kaspersky Embedded Systems Security. KAVSHELL VACUUM

Usando o comando `KAVSHELL VACUUM` você pode desfragmentar os arquivos de log do aplicativo. Ele permite evitar erros de sistema e do aplicativo devido ao armazenamento de um grande número de arquivos de log gerados com base nos eventos do aplicativo.

A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Recomenda-se aplicar o comando `KAVSHELL VACUUM` para otimizar o armazenamento de arquivos de log no caso de inicializações frequentes de tarefas de Verificação por Demanda e de atualização. Ao executar o comando, o Kaspersky Embedded Systems Security renova uma estrutura lógica dos arquivos de log de aplicativo que são armazenados em um computador protegido pelo caminho especificado.

Por padrão, os arquivos de log de aplicativo são armazenados em C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports. Se você tiver especificado manualmente outro caminho para o armazenamento de logs, o comando `KAVSHELL VACUUM` realizará a desfragmentação de arquivos na pasta que é especificada nas configurações de log do Kaspersky Embedded Systems Security.

O tamanho grande de arquivos em desfragmentação aumenta o período de execução do comando `KAVSHELL VACUUM`.

As tarefas de Proteção em Tempo Real e de Controle do Computador não estão disponíveis para serem executadas durante a execução do comando `KAVSHELL VACUUM`. O processo de desfragmentação em andamento restringe o acesso ao log do Kaspersky Embedded Systems Security e rejeita o registro de eventos em log. Para evitar a redução do nível de segurança, recomenda-se planejar com antecedência a execução do comando `KAVSHELL VACUUM` para um período de inatividade.

► *Para desfragmentar os arquivos de log do Kaspersky Embedded Systems Security, execute o comando seguinte:*

```
KAVSHELL VACUUM
```

A execução do comando é possível se iniciada com direitos de conta do administrador local.

Limpando a base iSwift. KAVSHELL FBRESET

O Kaspersky Embedded Systems Security usa a tecnologia iSwift, a qual permite que o aplicativo evite verificar novamente arquivos que não foram modificados desde a última verificação (**Usar a tecnologia iSwift**).

O Kaspersky Embedded Systems Security cria os arquivos klamfb.dat e klamfb2.dat na pasta de informações de volume %SYSTEMDRIVE%\System, contendo informações sobre os objetos limpos que já foram verificados. O arquivo klamfb.dat (klamfb2.dat) cresce com o número de arquivos verificados pelo Kaspersky Embedded Systems Security. O arquivo contém somente informações atuais sobre arquivos existentes no sistema: se um arquivo for removido, o Kaspersky Embedded Systems Security eliminará as informações sobre ele do klamfb.dat.

Para limpar um arquivo, use o comando `KAVSHELL FBRESET`.

Lembre-se sempre das seguintes instruções de operação do comando `KAVSHELL FBRESET`:

- Ao limpar o arquivo klamfb.dat por meio do comando KAVSHELL FBRESET, o Kaspersky Embedded Systems Security não pausa a proteção (ao contrário dos casos de exclusão manual de klamfb.dat).
- O Kaspersky Embedded Systems Security poderá aumentar a carga de trabalho do computador após os dados serem limpos no klamfb.dat. Nesse caso, o Kaspersky Embedded Systems Security verifica todos os arquivos acessados pela primeira vez desde a limpeza de klamfb.dat. Após a verificação, o Kaspersky Embedded Systems Security adiciona novamente ao arquivo klamfb.dat as informações sobre cada objeto verificado. No caso de novas tentativas de acessar o objeto, a tecnologia iSwift evitará que o arquivo seja verificado novamente, desde que ele permaneça inalterado.

A execução do comando `KAVSHELL FBRESET` está disponível apenas se a linha de comando for iniciada na conta SYSTEM.

Ativando e desativando a criação do arquivo de despejo. KAVSHELL DUMP

A criação de instantâneos (arquivo de despejo) para processos do Kaspersky Embedded Systems Security em casos de encerramento anormal de processos pode ser ativada ou desativada usando o comando `KAVSHELL DUMP` (consulte a tabela a seguir). É possível obter instantâneos adicionais da memória dos processos do Kaspersky Embedded Systems Security em andamento a qualquer momento.

Para que o arquivo de despejo seja criado com sucesso, o comando `KAVSHELL DUMP` deve ser executado na conta do sistema local (SYSTEM).

Sintaxe do comando KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<pasta com o arquivo de despejo>|/SNAPSHOT /F:< pasta com
```

```
o arquivo de despejo> / P:<pid> | /OFF>
```

Tabela 91. Chaves do comando KAVSHELL DUMP

Chave	Descrição
/ON	Ativa a criação do arquivo de despejo de memória do processo em casos de encerramento anormal.
/F:<caminho da pasta com arquivos de despejo>	Esta é uma chave obrigatória. Ela especifica o caminho da pasta na qual o arquivo de despejo será salvo. Caminhos para pastas em unidades de rede de outros computadores desprotegidos não podem ser especificados. As variáveis do ambiente do sistema podem ser usadas ao especificar o caminho da pasta com o arquivo de despejo da memória; não são permitidas variáveis do ambiente do usuário.
/SNAPSHOT	Obtém um instantâneo da memória do processo em andamento com um PID especificado e salva o arquivo de despejo na pasta cujo caminho é especificado pela chave /F.
/P	O identificador do processo, PID, é exibido no Gerenciador de Tarefas do Microsoft Windows.
/OFF	Desativa a criação arquivo de despejo de memória do processo em casos de encerramento anormal.

Códigos de retorno do comando KAVSHELL DUMP (consulte a seção "Códigos de retorno do comando KAVSHELL DUMP" na página 520).

Exemplos do comando KAVSHELL DUMP

► *Para ativar a criação do arquivo de despejo e salvá-lo na pasta C:\Pasta de Despejo, execute o comando:*

```
KAVSHELL DUMP /ON /F:"C:\Pasta de Despejo"
```

► *Para obter um despejo para o processo com ID 1234 na pasta C:/Despejos, execute o comando:*

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /F:1234
```

► *Para desativar a geração do arquivo de despejo, execute o comando:*

```
KAVSHELL DUMP /OFF
```

Importando configurações. KAVSHELL IMPORT

O comando `KAVSHELL IMPORT` permite importar as configurações do Kaspersky Embedded Systems Security, suas funções e tarefas a partir de um arquivo de configuração para uma cópia do Kaspersky Embedded Systems Security no computador protegido. É possível criar um arquivo de configuração usando o comando `KAVSHELL EXPORT`.

A senha pode ser necessária para executar o comando. Para digitar a senha atual, use a chave `[/pwd:<password>]`.

Sintaxe do comando KAVSHELL IMPORT

```
KAVSHELL IMPORT <nome do arquivo de configuração e caminho do arquivo>
```

Exemplos do comando KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Tabela 92. Chaves do comando KAVSHELL IMPORT

Chave	Descrição
<nome do arquivo de configuração e caminho do arquivo>	Nome do arquivo de configuração usado como fonte de importação das configurações. As variáveis do ambiente do sistema podem ser usadas ao especificar o caminho do arquivo; não são permitidas variáveis do ambiente do usuário.

Códigos de retorno do comando KAVSHELL IMPORT (consulte a seção "Códigos de retorno do comando KAVSHELL IMPORT" na página 521).

Exportando configurações. KAVSHELL EXPORT

O comando `KAVSHELL EXPORT` permite exportar todas as configurações do Kaspersky Embedded Systems Security e suas tarefas atuais para um arquivo de configuração para, depois, importá-las para cópias do Kaspersky Embedded Systems Security instaladas em outro computador.

Sintaxe do comando KAVSHELL EXPORT

```
KAVSHELL EXPORT <nome do arquivo de configuração e caminho do arquivo>
```

Exemplos do comando KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Tabela 93. Chaves do comando KAVSHELL EXPORT

Chave	Descrição
<nome do arquivo de configuração e caminho do arquivo>	Nome do arquivo de configuração que conterá as configurações. É possível atribuir qualquer extensão ao arquivo de configuração. As variáveis do ambiente do sistema podem ser usadas ao especificar o caminho do arquivo; não são permitidas variáveis do ambiente do usuário.

Códigos de retorno do comando KAVSHELL EXPORT (consulte a seção "Códigos de retorno do comando KAVSHELL EXPORT" na página 521).

Integração com Microsoft Operations Management Suite. KAVSHELL OMSINFO

Usando o comando KAVSHELL OMSINFO, é possível revisar o status do aplicativo e informações sobre ameaças

detectadas por bancos de dados de antivírus e pelo serviço da KSN. Os dados sobre ameaças são tomados dos logs de evento disponíveis.

Sintaxe do comando KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <caminho completo para arquivo gerado com nome do arquivo>
```

Exemplos do comando KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Tabela 94. Chaves do comando KAVSHELL OMSINFO

Chave	Descrição
<caminho do arquivo gerado com nome de arquivo>	Nome do arquivo gerado que conterá informações sobre status de aplicativo e ameaças detectadas.

Códigos de retorno da linha de comando

Nesta seção

Código de retorno dos comandos KAVSHELL START e KAVSHELL STOP 516
Código de retorno dos comandos KAVSHELL SCAN e KAVSHELL SCANCRITICAL 516
Códigos de retorno do comando KAVSHELL TASK LOG-INSPECTOR 517
Códigos de retorno do comando KAVSHELL TASK 517
Códigos de retorno do comando KAVSHELL RTP 518
Códigos de retorno do comando KAVSHELL UPDATE 518
Códigos de retorno do comando KAVSHELL ROLLBACK 519
Códigos de retorno do comando KAVSHELL LICENSE 519
Códigos de retorno do comando KAVSHELL TRACE 520
Códigos de retorno do comando KAVSHELL FBRESET 520
Códigos de retorno do comando KAVSHELL DUMP 520
Códigos de retorno do comando KAVSHELL IMPORT 521
Códigos de retorno do comando KAVSHELL EXPORT 521

Código de retorno dos comandos KAVSHELL START e KAVSHELL STOP

Tabela 95. Código de retorno dos comandos KAVSHELL START e KAVSHELL STOP

Código de retorno	Descrição
0	Operação concluída com êxito
-3	Erro de permissões
-5	Sintaxe de comando inválida
-6	Operação inválida (por exemplo, o serviço do Kaspersky Embedded Systems Security já está em execução ou já foi interrompido)
-7	Serviço não registrado
-8	A inicialização de Serviço automático está desativada.
-9	A tentativa de iniciar o computador em outra conta do usuário falhou (por padrão, o serviço do Kaspersky Embedded Systems Security é executado na conta do usuário Sistema local)
-99	Erro desconhecido

Código de retorno dos comandos KAVSHELL SCAN e KAVSHELL SCANCRITICAL

Tabela 96. Código de retorno dos comandos KAVSHELL SCAN e KAVSHELL SCANCRITICAL

Código de retorno	Descrição
0	Operação concluída com êxito (nenhuma ameaça detectada)
1	Operação cancelada
-2	Serviço não está em execução
-3	Erro de permissões
-4	Objeto não encontrado (arquivo com a lista de escopos da verificação não encontrado)
-5	Sintaxe de comando inválida ou escopo da verificação não definida
-80	Objetos infectados e outros detectados
-81	Objetos possivelmente infectados detectados
-82	Erros de processamento detectados
-83	Objetos não verificados detectados
-84	Objetos corrompidos detectados

Código de retorno	Descrição
-85	Falha ao criar o arquivo de log de tarefas
-99	Erro desconhecido
-301	Chave inválida

Códigos de retorno do comando KAVSHELL TASK LOG-INSPECTOR

Tabela 97. Código de retorno do comando KAVSHELL TASK LOG-INSPECTOR

Código de retorno	Descrição
0	Operação concluída com êxito
-6	Operação inválida (por exemplo, o serviço do Kaspersky Embedded Systems Security já está em execução ou já foi interrompido)
402	Tarefa já sendo executada (para modificador /STATE)

Códigos de retorno do comando KAVSHELL TASK

Tabela 98. Códigos de retorno do comando KAVSHELL TASK

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões
-4	Objeto não encontrado (tarefa não encontrada)
-5	Sintaxe de comando inválida
-6	Operação inválida (por exemplo, tarefa não está em execução, já em execução ou que não pode ser pausada)
-99	Erro desconhecido
-301	Chave inválida
401	Tarefa não sendo executada (para modificador /STATE)
402	Tarefa já sendo executada (para modificador /STATE)
403	Tarefa já pausada (para modificador /STATE)
-404	Erro ao executar a operação (a alteração no status da tarefa causou sua falha)

Códigos de retorno do comando KAVSHELL RTP

Tabela 99. Códigos de retorno do comando KAVSHELL RTP

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões
-4	Objeto não encontrado (uma das tarefas de proteção em tempo real ou todas as tarefas de proteção em tempo real não encontradas)
-5	Sintaxe de comando inválida
-6	Operação inválida (por exemplo, a tarefa já está em execução ou já foi interrompida)
-99	Erro desconhecido
-301	Chave inválida

Códigos de retorno do comando KAVSHELL UPDATE

Tabela 100. Códigos de retorno do comando KAVSHELL UPDATE

Código de retorno	Descrição
0	Operação concluída com êxito
200	Todos os objetos estão atualizados (os bancos de dados ou componentes do programa estão atualizados)
-2	Serviço não está em execução
-3	Erro de permissões
-5	Sintaxe de comando inválida
-99	Erro desconhecido
-206	Os arquivos de extensão estão ausentes da fonte especificada ou têm um formato desconhecido
-209	Erro ao conectar à fonte de atualização
-232	Erro de autenticação ao conectar ao servidor proxy
-234	Erro ao conectar o Kaspersky Security Center

Código de retorno	Descrição
-235	O Kaspersky Embedded Systems Security não foi autenticado ao conectar a fonte de atualização
-236	O banco de dados do aplicativo está corrompido
-301	Chave inválida

Códigos de retorno do comando KAVSHELL ROLLBACK

Tabela 101. Códigos de retorno do comando KAVSHELL ROLLBACK

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões
-99	Erro desconhecido
-221	Cópia de backup do banco de dados não encontrada ou corrompida
-222	Cópia de backup do banco de dados corrompida

Códigos de retorno do comando KAVSHELL LICENSE

Tabela 102. Códigos de retorno do comando KAVSHELL LICENSE

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Privilégios insuficientes para gerenciar chaves
-4	Chave com o número especificado não encontrada
-5	Sintaxe de comando inválida
-6	Operação inválida (chave já adicionada)
-99	Erro desconhecido
-301	Chave inválida
-303	A licença aplica-se a um aplicativo diferente

Códigos de retorno do comando KAVSHELL TRACE

Tabela 103. Códigos de retorno do comando KAVSHELL TRACE

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões
-4	Objeto não encontrado (caminho especificado como caminho para a pasta de logs de rastreamento não encontrado)
-5	Sintaxe de comando inválida
-6	Operação inválida (tentativa de execução do comando KAVSHELL TRACE /OFF se a criação de log de despejo já estiver desativada)
-99	Erro desconhecido

Códigos de retorno do comando KAVSHELL FBRESET

Tabela 104. Códigos de retorno do comando KAVSHELL FBRESET

Código de retorno	Descrição
0	Operação concluída com êxito
-99	Erro desconhecido

Códigos de retorno do comando KAVSHELL DUMP

Tabela 105. Códigos de retorno do comando KAVSHELL DUMP

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões
-4	Objeto não encontrado (caminho especificado como caminho para a pasta do arquivo de despejo não encontrado; processo com PID especificado não encontrado)
-5	Sintaxe de comando inválida

Código de retorno	Descrição
-6	Operação inválida (tentativa de execução do comando KAVSHELL DUMP/OFF se a criação de arquivo de despejo já estiver desativada)
-99	Erro desconhecido

Códigos de retorno do comando KAVSHELL IMPORT

Tabela 106. Códigos de retorno do comando KAVSHELL IMPORT

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões
-4	Objeto não encontrado (arquivo de configuração importável não encontrado)
-5	Sintaxe inválida
-99	Erro desconhecido
501	Operação concluída com êxito, no entanto ocorreu um erro/comentário durante a execução do comando, por exemplo, o Kaspersky Embedded Systems Security não importou parâmetros de algum componente funcional
-502	O arquivo sendo importando está ausente ou tem um formato não reconhecido
-503	Configurações incompatíveis (arquivo de configuração exportado a partir de um programa diferente ou de uma versão posterior e incompatível do Kaspersky Embedded Systems Security)

Códigos de retorno do comando KAVSHELL EXPORT

Tabela 107. Códigos de retorno do comando KAVSHELL EXPORT

Código de retorno	Descrição
0	Operação concluída com êxito
-2	Serviço não está em execução
-3	Erro de permissões
-5	Sintaxe inválida

Código de retorno	Descrição
-10	Não foi possível criar um arquivo de configuração (por exemplo, não existe acesso à pasta especificada no caminho para o arquivo)
-99	Erro desconhecido
501	Operação concluída com êxito, no entanto ocorreu um erro/comentário durante a execução do comando, por exemplo, o Kaspersky Embedded Systems Security não exportou parâmetros de algum componente funcional

Entrando em contato com o Suporte Técnico

Esta seção descreve as formas de receber suporte técnico e as condições em que ele está disponível.

Neste capítulo

Como obter suporte técnico 523

Obtenha suporte técnico por telefone 523

Suporte Técnico por meio do Kaspersky CompanyAccount 524

Usando arquivos de rastreamento e scripts do AVZ 524

Como obter suporte técnico

Se você não encontrar uma solução para seu problema na documentação do aplicativo ou em uma das fontes de informações sobre o aplicativo, é recomendado entrar em contato com o Suporte Técnico. Os especialistas do Suporte Técnico responderão a suas dúvidas sobre a instalação e o uso do aplicativo.

O suporte técnico só está disponível para os usuários que compraram uma licença comercial para o aplicativo. O suporte técnico não está disponível para os usuários com uma licença de avaliação.

Antes de entrar em contato com o Suporte Técnico, leia todas as regras do Suporte Técnico.

Você pode entrar em contato com o Suporte Técnico de uma das seguintes maneiras:

- Ligando para o Suporte Técnico.
- Enviando uma solicitação ao Suporte Técnico da Kaspersky Lab por meio do portal Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Obtenha suporte técnico por telefone

É possível ligar para especialistas de Suporte técnico da maior parte das regiões do mundo. Você pode encontrar informações sobre como obter suporte técnico na sua região e informações de contato do Suporte técnico no site do Suporte técnico da Kaspersky Lab (https://support.kaspersky.com.br/b2b/BR).

Antes de entrar em contato com o Suporte Técnico, leia todas as regras do Suporte Técnico (https://support.kaspersky.com/support/rules/pt_br).

Suporte Técnico por meio do Kaspersky CompanyAccount

O Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) é um portal para empresas que usam aplicativos da Kaspersky Lab. O Kaspersky CompanyAccount destina-se a facilitar a interação entre os usuários e os especialistas do Kaspersky Lab através de solicitações online. Com o Kaspersky CompanyAccount, é possível monitorar o andamento do processamento de solicitações eletrônicas pelos especialistas da Kaspersky Lab, além de armazenar um histórico de solicitações eletrônicas.

Você pode registrar todos os funcionários de sua organização em uma única conta de usuário no Kaspersky CompanyAccount. Uma única conta permite gerenciar de forma centralizada as solicitações eletrônicas de funcionários registrados para a Kaspersky Lab e também gerenciar os privilégios desses funcionários através do Kaspersky CompanyAccount.

O Web Kaspersky CompanyAccount está disponível nos seguintes idiomas:

- Inglês
- Espanhol
- Italiano
- Alemão
- Polonês
- Português
- Russo
- Francês
- Japonês

Para saber mais sobre o Kaspersky CompanyAccount, visite o site de Suporte Técnico https://support.kaspersky.com.br/faq/companyaccount_help.

Usando arquivos de rastreamento e scripts do AVZ

Após você reportar um problema aos especialistas de Suporte Técnico da Kaspersky Lab, eles poderão solicitar que você crie um relatório com informações sobre a operação do Kaspersky Embedded Systems Security e que o envie ao Suporte Técnico da Kaspersky Lab. Além disso, os especialistas do Suporte Técnico da Kaspersky Lab podem solicitar que você crie um arquivo de rastreamento. O arquivo de rastreamento permite monitorar o processo de como os comandos do aplicativo estão sendo executados, por etapas, para determinar o momento em que ocorre o erro na operação do aplicativo.

Após analisar os dados enviados, os especialistas do Suporte Técnico da Kaspersky Lab podem criar um script AVZ e enviá-lo para você. Com scripts AVZ, é possível analisar os processos ativos quanto à existência de ameaças, verificar o computador para detectar ameaças, desinfectar ou excluir arquivos infectados e criar relatórios de verificação do sistema.

Para um suporte e resolução de problemas de aplicativo mais eficientes, os especialistas do Suporte Técnico podem solicitar que você modifique a configuração do aplicativo temporariamente com objetivos de depuração durante o diagnóstico. Para isso, pode ser necessária a realização do seguinte:

- Ativação da funcionalidade que processa e armazena informações estendidas de diagnóstico.
- Controle detalhado das configurações de componentes individuais de software, que não estão disponíveis

por meio de elementos padrão da interface de usuário.

- Alteração das configurações de armazenamento e transmissão de informações de diagnóstico que foram processadas.
- Configuração da interceptação e registro de tráfego de rede em log.

Glossário

A

Analisador heurístico

Tecnologia de detecção de ameaças cujas informações ainda não foram adicionadas aos bancos de dados da Kaspersky Lab. O analisador heurístico detecta objetos cujo comportamento no sistema pode representar uma ameaça de segurança. Os objetos detectados pelo analisador heurístico são considerados como possivelmente infectados. Por exemplo, um objeto pode ser considerado possivelmente infectado se contiver sequências de comandos típicos de objetos maliciosos (abrir arquivo, gravar no arquivo).

Arquivo comprimido ou compactado

Um ou vários arquivos empacotados em um arquivo único por meio da compactação. Um aplicativo dedicado, chamado arquivador, é necessário para empacotar e desempacotar os dados.

Arquivo infectável

Um arquivo que, devido à sua estrutura ou ao seu formato, pode ser usado por criminosos como um "contêiner" para armazenar e distribuir código malicioso. Geralmente, estes são arquivos executáveis, com extensões como .com, .exe, e .dll. O risco da penetração de código malicioso em tais arquivos é bastante alto.

Atualização

Procedimento para substituir/adicionar novos arquivos (bancos de dados ou módulos do aplicativo) recuperados de servidores de atualização da Kaspersky Lab.

B

Backup

Armazenamento especial de cópias de backup de arquivos criadas antes da tentativa de desinfecção ou exclusão.

Bancos de dados de Antivírus

Bancos de dados que contêm informações sobre ameaças à segurança do computador conhecidas pela Kaspersky Lab na data de publicação dos bancos de dados de antivírus As entradas dos bancos de dados de antivírus permitem detectar código malicioso em objetos verificados. Os bancos de dados de Antivírus são criados pelos peritos da Kaspersky Lab e atualizados de hora em hora.

C

Chave ativa

Uma chave usada atualmente pelo aplicativo.

Configurações de tarefa

Configurações do aplicativo específicas para cada tipo de tarefa.

D

Desinfecção

Método de processamento de objetos infectados que resulta na recuperação completa ou parcial dos dados. Nem todos os objetos infectados podem ser desinfectados.

F

Falso positivo

Uma situação em que o aplicativo da Kaspersky Lab considera um objeto não infectado como infectado devido à semelhança de seu código com o código de um vírus.

G

Gravidade do evento

Propriedade de um evento encontrado durante a operação de um aplicativo da Kaspersky Lab. Há quatro níveis de gravidade:

- Evento crítico.
- Erro.
- Aviso.
- Informação.

Os eventos do mesmo tipo podem ter níveis de gravidade diferentes dependendo da situação na qual o evento ocorreu.

K

Kaspersky Security Network (KSN)

Uma infraestrutura de serviços na nuvem que fornece acesso ao banco de dados da Kaspersky Lab com informações constantemente atualizadas sobre a reputação de arquivos, recursos da web e software. A Kaspersky Security Network garante respostas mais rápidas por aplicativos da Kaspersky Lab a ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos positivos.

M

Máscara de arquivos

Representação de um nome de arquivo usando curingas. Os curingas padrão usados em máscaras de arquivos são * e ?, em que * representa qualquer número de caracteres e ? representa qualquer caractere.

N

Nível de segurança

O nível de segurança é definido como um conjunto predefinido de configurações de componentes do aplicativo.

O

Objeto infectado

Um objeto com uma porção de código que corresponde completamente a uma porção de código de um malware conhecido. A Kaspersky Lab não recomenda usar estes objetos.

Objeto OLE

Um objeto anexado ou incorporado a outro arquivo usando a tecnologia OLE (Object Linking and Embedding). Um exemplo de objeto OLE é uma planilha do Microsoft Excel® incorporada a um documento do Microsoft Word.

Objetos de inicialização

Grupo de aplicativos necessários para que o sistema operacional e o software instalados no computador iniciem e funcionem corretamente. Esses objetos são executados sempre que o sistema operacional é iniciado. Há vírus capazes de infectar tais objetos especificamente, podendo levar, por exemplo, ao bloqueio da inicialização do sistema operacional.

P

Período da licença

Período de tempo durante o qual você tem acesso aos recursos do aplicativo e direitos de uso dos serviços adicionais. Os serviços que você pode usar dependem do tipo da licença.

Política

Uma política determina as configurações de um aplicativo e gerencia a capacidade de configurar o aplicativo em computadores de um grupo de administração. Uma política individual deve ser criada para cada aplicativo. Você pode criar um número ilimitado de políticas diferentes para aplicativos instalados em computadores em cada grupo de administração, mas apenas uma política pode ser aplicada a cada aplicativo por vez dentro de um grupo de

administração.

Proteção em Tempo Real

Modo de operação do aplicativo no qual os objetos são verificados quanto à presença de código malicioso em tempo real.

O aplicativo intercepta todas as tentativas de abrir qualquer objeto (ler, escrever ou executar) e verifica o objeto para ameaças. Os objetos não infectados são transmitidos ao usuário; os objetos que contêm ameaças ou objetos possivelmente infectados são processados segundo as configurações da tarefa (desinfectado, excluído ou colocado em Quarentena).

Q

Quarentena

A pasta para onde o aplicativo da Kaspersky Lab move objetos possivelmente infectados que foram detectados. Os objetos são armazenados na Quarentena em formato criptografado para evitar qualquer impacto negativo no computador.

S

Servidor de Administração

Um componente do Kaspersky Security Center que armazena de modo centralizado informações sobre todos os aplicativos da Kaspersky Lab instalados na rede corporativa. Ele também pode ser usado para gerenciar tais aplicativos.

SIEM

Uma tecnologia que analisa eventos de segurança originados em vários dispositivos de rede e aplicativos.

Status da proteção

O status de proteção atual que reflete o nível da segurança do computador.

T

Tarefa

As funções executadas pelo aplicativo da Kaspersky Lab são implementadas como tarefas, por exemplo: Proteção de arquivos em tempo real, Verificação completa do computador e Atualização do Banco de dados.

Tarefa local

Uma tarefa definida e executada em um computador cliente único.

V

Vulnerabilidade

Uma falha no sistema operacional ou em um aplicativo que pode ser explorada por desenvolvedores de malware para penetrar no sistema operacional ou em aplicativos e corromper sua integridade. A presença de um grande número de vulnerabilidades em um sistema operacional torna-o pouco confiável, já que os vírus que penetrarem nele poderão causar problemas no próprio sistema operacional e nos aplicativos instalados.

AO Kaspersky Lab

A Kaspersky Lab é um fornecedor de renome mundial de sistemas de proteção de computadores contra várias ameaças digitais, incluindo ataques de vírus, malware, e-mail não solicitado (spam), ataques de rede e de hackers.

Em 2008, a Kaspersky Lab foi classificada como um dos quatro principais fornecedores de soluções de software de segurança de informações para o usuário final (IDC Worldwide Endpoint Security Revenue by Vendor). A Kaspersky Lab é o fornecedor preferencial de sistemas de proteção de computadores para usuários domésticos na Rússia (IDC Endpoint Tracker 2014).

A Kaspersky Lab foi fundada na Rússia em 1997. A partir daí, a organização se desenvolveu até se transformar em um grupo internacional de empresas com 38 escritórios em 33 países. A empresa emprega hoje mais de 3.000 especialistas qualificados.

Produtos. Os produtos da Kaspersky Lab oferecem proteção para todos os tipos de sistemas: de computadores domésticos a grandes redes corporativas.

A linha de produtos pessoais inclui aplicativos de segurança para computadores desktop, laptop e tablet, além de smartphones e outros dispositivos móveis.

A empresa oferece soluções para proteção e controle, e tecnologias para estações de trabalho e dispositivos móveis, máquinas virtuais, servidores de arquivos e servidores da web, gateways de correio e firewalls. O portfólio da empresa também inclui produtos especializados que fornecem proteção contra ataques de DDoS, proteção para sistemas de controle industriais e contra fraude financeira. Usadas em conjunto com ferramentas de gestão centralizadas, estas soluções asseguram a proteção automatizada eficaz de empresas e organizações de qualquer porte contra ameaças de computador. Os produtos da Kaspersky Lab são certificados pelos principais laboratórios de testes, compatíveis com aplicativos de diversos fornecedores de software e otimizados para funcionar na maioria das plataformas de hardware.

Os analistas de vírus da Kaspersky Lab trabalham incansavelmente. Todos os dias, eles descobrem centenas de milhares de novas ameaças de computador, criam ferramentas para detectá-las e desinfectá-las e incluem as assinaturas destas ameaças nos bancos de dados usados pelos aplicativos da Kaspersky Lab.

Tecnologias. Várias tecnologias que agora são parte integrante de modernas ferramentas antivírus foram originalmente desenvolvidas pela Kaspersky Lab. Não é nenhuma coincidência que muitos outros desenvolvedores usem o motor do Kaspersky Antivírus nos seus produtos, incluindo: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu e ZyXEL. Muitas das tecnologias inovadoras da empresa são patenteadas.

Realizações. Ao longo dos anos, a Kaspersky Lab recebeu centenas de prêmios por seus serviços no combate às ameaças de computador. Após testes e pesquisas realizadas pelo renomado laboratório de testes austríaco AV-Comparatives em 2014, a Kaspersky Lab ficou entre os dois principais fornecedores pelo número de certificados Advance+ obtidos e, ao final, recebeu o certificado de Melhor Classificação. Todavia, a principal realização da Kaspersky Lab é a fidelidade de seus usuários em todo o mundo. Os produtos e as tecnologias da empresa protegem mais de 400 milhões de usuários, e seus clientes corporativos somam mais de 270.000.

Site da Kaspersky Lab:	https://www.kaspersky.com.br
Enciclopédia de Vírus	https://securelist.com
Kaspersky VirusDesk:	https://virusdesk.kaspersky.com (para analisar arquivos e sites suspeitos)
Comunidade da Kaspersky Lab na Web:	https://community.kaspersky.com

Informações sobre código de terceiros

As informações sobre códigos de terceiros estão contidas no arquivo legal_notices.txt, na pasta de instalação do aplicativo.

Notificações de marcas registradas

As marcas registradas e marcas de serviço são propriedade de seus respectivos proprietários.

Intel e Pentium são marcas registradas da Intel Corporation nos Estados Unidos e/ou em outros países.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e em outros países.

Microsoft, Active Directory, Excel, Internet Explorer e Windows são marcas registradas da Microsoft Corporation nos Estados Unidos e em outros países.

UNIX é uma marca registrada nos Estados Unidos e em outros países, licenciada exclusivamente pela X/Open Company Limited.

Índice

A

Ação
objetos infectados 264
objetos suspeitos 264
Ações em objetos 264, 281, 404
Arquivo executável 264, 287, 316, 322, 324, 329
Arquivos compactados 264
Arquivos iSwift 187, 264, 404
Atualização
módulos de software 171
por programação 151, 177

B

Backup 194
Definindo configurações 199
excluindo objetos 198
restaurando objetos 196
Bancos de dados 171, 173
atualização automática 151, 173, 177
atualização manual 177
data de criação 161

C

Configuração
configurações de segurança 264, 404
tarefa 148, 177, 257, 281, 316, 322, 358, 364
Console 136, 143, 148
conexão 148
iniciar 219
Conteúdo das atualizações 181

D

Desinfecção de objetos 264
Dispositivos confiáveis 339

E

Eliminando o log de auditoria do sistema 203
Estatísticas 161
Exclusões do escopo da verificação 264
Executando tarefas ignoradas 151

F

Fonte de atualização 177, 181, 182

I

Ícone na área de notificação do tabuleiro do sistema 147
Interface do aplicativo 143
    ícone na área de notificação da barra de tarefas 147

J

Janela principal 143

L

Log de Eventos 201, 208

M

Modo de proteção 258

N

Negação padrão 339, 358

P

Pasta de armazenamento do backup 199
Pasta de logs 209
pasta para restauração
    Quarentena 192
Pasta para salvar atualizações 181
Programação de tarefas 151, 152
Proteção em Tempo Real 271

Q

Quarentena
    excluindo objetos 191
    exibindo objetos 185, 186
    limite de espaço disponível 192
    restauração de objetos 189
Quarentena e Backup 185

R

Regras 287, 340, 342, 344
    controle de dispositivos 340, 342, 344, 360, 361, 362, 363, 364
    controle de inicialização de aplicativos 287, 315, 316, 329, 332, 333, 334
Restaurando as configurações padrão 404
Restaurar objeto 189, 196

S

Servidor FTP 177, 181, 182
Servidor HTTP 173, 177, 181, 182
Servidor proxy 177

T

Tamanho máximo
    objeto verificado 264
    Quarentena 192

Tarefa 148, 149
Tipo de ameaça
ação 264

V

Verificação
nível de segurança 404
somente objetos novos e modificados 264
tempo máximo de verificação de objetos 264
Verificação de vírus de armazenamentos 187
Verificar fluxos NTFS alternativos 264