



# Ajuda do Websense Manager

Websense® Web Security  
Websense Web Filter

©1996–2008, Websense Inc.  
Todos os direitos reservados.  
10240 Sorrento Valley Rd., San Diego, CA 92121, EUA

Publicado em 2008  
Impresso nos EUA e na Irlanda

Os produtos e/ou métodos de uso descritos neste documento são cobertos pelos Números e Patentes nos EUA 5.983.270; 6.606.659; 6.947.985; 7.185.015; 7.194.464 e RE40.187 e outras patentes pendentes.

Este documento não pode, integral ou parcialmente, ser copiado, fotocopiado, reproduzido, traduzido ou reduzido para qualquer meio eletrônico ou formato legível por máquina sem o consentimento prévio por escrito da Websense Inc.

Foram realizados todos os esforços para garantir a exatidão deste manual. Porém, a Websense Inc. não apresenta garantias com relação a esta documentação e se isenta de quaisquer garantias implícitas de comerciabilidade e adequação a uma finalidade específica. A Websense Inc. não será responsável por qualquer erro ou por danos incidentais ou conseqüentes associados à disponibilização, ao desempenho ou ao uso desde manual ou dos exemplos incluídos. As informações nesta documentação estão sujeitas a alterações sem aviso prévio.

### **Marcas registradas**

Websense é uma marca registrada da Websense, Inc., nos EUA e em determinados mercados internacionais. A Websense possui muitas outras marcas não registradas nos EUA e internacionalmente. Todas as outras marcas registradas pertencem às respectivas empresas.

Microsoft, Windows, Windows NT, Windows Server e Active Directory são marcas comerciais ou registradas da Microsoft Corporation nos EUA e/ou em outros países.

Sun, Sun Java System e todas as marcas comerciais e logotipos baseados em Sun Java System são marcas comerciais ou registradas da Sun Microsystems, Inc. nos EUA e em outros países.

Mozilla e Firefox são marcas registradas da Mozilla Foundation nos EUA e em outros países.

eDirectory e Novell Directory Services são marcas registradas da Novell, Inc., nos EUA e em outros países.

Adobe, Acrobat e Acrobat Reader são marcas comerciais ou registradas da Adobe Systems Incorporated nos EUA e/ou em outros países.

Pentium é uma marca registrada da Intel Corporation.

Red Hat é uma marca registrada da Red Hat, Inc. nos EUA e em outros países. Linux é uma marca registrada de Linus Torvalds nos EUA e em outros países.

Este produto inclui software distribuído pela Apache Software Foundation (<http://www.apache.org>).

Copyright (c) 2000. The Apache Software Foundation. Todos os direitos reservados.

Outros nomes de produtos mencionados neste manual podem ser marcas comerciais ou registradas de suas respectivas empresas e são propriedade exclusiva dos respectivos fabricantes.

# Conteúdo

<b>Tópico 1</b>	<b>Primeiros Passos . . . . .</b>	<b>13</b>
	Visão geral . . . . .	14
	Trabalhando no Websense Manager . . . . .	14
	Fazendo logon no Websense Manager . . . . .	16
	Navegando no Websense Manager . . . . .	17
	Reverendo, salvando e descartando alterações. . . . .	19
	Hoje: Saúde, segurança e valor desde a meia-noite . . . . .	19
	Personalizando a página Hoje . . . . .	22
	Histórico: Últimos 30 dias . . . . .	22
	Tempo e largura de banda economizados . . . . .	24
	Personalizar a página Histórico. . . . .	25
	Sua assinatura . . . . .	26
	Gerenciando sua conta no Portal MyWebsense . . . . .	26
	Ativando o Websense Web Protection Services™ . . . . .	27
	Configurando as informações de sua conta. . . . .	28
	O Websense Master Database . . . . .	29
	Atualizações do banco de dados em tempo real . . . . .	30
	Atualizações de segurança em tempo real™. . . . .	30
	Configurando downloads do banco de dados . . . . .	31
	Testando a configuração da rede . . . . .	32
	Suporte Técnico da Websense . . . . .	32
<b>Tópico 2</b>	<b>Filtros de uso da Internet. . . . .</b>	<b>35</b>
	Filtragem de categorias e protocolos . . . . .	36
	Categorias especiais . . . . .	38
	Classes de risco . . . . .	39
	Grupos de protocolos de segurança. . . . .	41
	Instant Messaging Attachment Manager. . . . .	42
	Ações de filtragem . . . . .	42
	Usando o tempo da cota para limitar o acesso à Internet . . . . .	44
	Acesso com senha . . . . .	45
	Filtragem de pesquisa. . . . .	45
	Trabalhando com filtros . . . . .	46
	Criando um filtro de categoria . . . . .	47
	Editando um filtro de categoria. . . . .	48
	Criando um filtro de protocolo . . . . .	49

	Editando um filtro de protocolo . . . . .	50
	Filtros de categoria e protocolo definidos pelo Websense . . . . .	52
	Modelos de filtros de categoria e protocolo . . . . .	53
	Definindo configurações de filtragem do Websense . . . . .	54
<b>Tópico 3</b>	<b>Clientes . . . . .</b>	<b>57</b>
	Trabalhando com clientes. . . . .	58
	Trabalhando com computadores e redes . . . . .	59
	Trabalhando com usuários e grupos. . . . .	60
	Serviços de diretório . . . . .	60
	Windows NT Directory/Active Directory (Mixed Mode) . . . . .	61
	Windows Active Directory (Native Mode). . . . .	61
	Novell eDirectory e Sun Java System Directory. . . . .	63
	Configurações avançadas de diretório. . . . .	63
	Trabalhando com grupos LDAP personalizados . . . . .	64
	Adicionando ou editando um grupo LDAP personalizado . . . . .	65
	Adicionando um cliente . . . . .	66
	Pesquisando o serviço de diretório . . . . .	67
	Alterando configurações de cliente . . . . .	68
	Movendo clientes para funções . . . . .	68
<b>Tópico 4</b>	<b>Diretivas de filtragem da Internet. . . . .</b>	<b>71</b>
	A diretiva Padrão . . . . .	72
	Trabalhando com diretivas. . . . .	73
	Criando uma diretiva. . . . .	74
	Editando uma diretiva . . . . .	75
	Atribuindo uma diretiva aos clientes. . . . .	77
	Ordem de filtragem. . . . .	78
	Filtrando um site . . . . .	79
<b>Tópico 5</b>	<b>Páginas de bloqueio . . . . .</b>	<b>83</b>
	Mensagens de bloqueio de protocolo . . . . .	84
	Trabalhando com páginas de bloqueio. . . . .	85
	Personalizando a mensagem de bloqueio . . . . .	86
	Alterando o tamanho do quadro de mensagem . . . . .	87
	Alterando o logotipo exibido na página de bloqueio . . . . .	87
	Usando variáveis de conteúdo de página de bloqueio . . . . .	88
	Revertendo às páginas de bloqueio padrão . . . . .	89
	Criando mensagens de bloqueio alternativas . . . . .	90
	Usando uma página de bloqueio alternativa em outro computador. . . . .	90
<b>Tópico 6</b>	<b>Usando relatórios para avaliar diretivas de filtragem . . . . .</b>	<b>93</b>
	Visão geral de relatórios . . . . .	94
	O que é tempo de navegação na Internet? . . . . .	95

Relatórios de apresentação	96
Copiando um relatório de apresentação	99
Definindo o filtro de relatório	100
Selecionando clientes para um relatório	101
Selecionando categorias para um relatório	102
Selecionando protocolos para um relatório	103
Selecionando ações para um relatório	103
Definindo as opções de relatórios	104
Confirmando a definição do filtro de relatório	106
Trabalhando com favoritos	106
Gerando relatórios de apresentação	107
Agendando relatórios de apresentação	108
Definindo a programação	109
Selecionando relatórios para agendar	111
Definindo o intervalo de datas	111
Selecionando opções de saída	112
Exibindo a lista de trabalhos agendados	113
Exibindo o histórico de trabalhos	114
Relatórios investigativos	115
Relatórios de resumo	117
Relatórios de resumo em vários níveis	121
Relatórios de detalhes flexíveis	122
Colunas para relatórios de detalhes flexíveis	124
Relatórios de detalhe de atividade do usuário	126
Detalhes da atividade do usuário por dia	127
Detalhes da atividade do usuário por mês	128
Mapeamento de categorias	129
Relatórios padrão	131
Relatórios investigativos favoritos	132
Salvando um relatório como Favorito	133
Gerando ou excluindo um relatório Favorito	134
Modificando um relatório Favorito	134
Agendando relatórios investigativos	135
Gerenciando trabalhos programados de relatórios investigativos	138
Relatórios de valores atípicos	138
Saída para arquivo	139
Imprimindo relatórios investigativos	140
Acessando os relatórios próprios	141
<b>Tópico 7</b>	
<b>Análise de conteúdo com as opções em tempo real</b>	<b>143</b>
Download do banco de dados	144
Opções de verificação	145
Classificando conteúdo e verificando para identificar ameaças	146
Verificação de arquivos	147
Removendo conteúdo	148

	Refinando a verificação . . . . .	149
	Relatórios sobre a atividade de verificação em tempo real . . . . .	151
	Como a verificação em tempo real é registrada . . . . .	152
<b>Tópico 8</b>	<b>Filtrar Clientes Remotos . . . . .</b>	<b>155</b>
	Como o Remote Filtering funciona . . . . .	156
	Dentro da rede . . . . .	157
	Fora da rede . . . . .	158
	Identificando usuários remotos . . . . .	159
	Quando a comunicação com o servidor falha . . . . .	160
	Rede Virtual Privada (VPN, Virtual Private Network) . . . . .	161
	Definindo as configurações do Remote Filtering . . . . .	162
<b>Tópico 9</b>	<b>Refinar as diretivas de filtragem. . . . .</b>	<b>165</b>
	Restringindo usuários a uma lista definida de sites de Internet . . . . .	166
	Filtros de acesso limitado e precedência de filtragem. . . . .	166
	Criando um filtro de acesso limitado . . . . .	168
	Editando um filtro de acesso limitado. . . . .	168
	Adicionando sites pela página Editar diretiva. . . . .	170
	Copiando filtros e diretivas para funções. . . . .	170
	Criando componentes de filtro . . . . .	172
	Trabalhando com categorias. . . . .	173
	Editando categorias e seus atributos . . . . .	173
	Revisando todos os atributos de categorias personalizadas. . . . .	174
	Fazendo alterações de filtragem global de categorias . . . . .	175
	Renomeando uma categoria personalizada . . . . .	176
	Criando uma categoria personalizada . . . . .	176
	Filtrando com base em palavras-chave . . . . .	177
	Definindo palavras-chave . . . . .	179
	Redefinindo a filtragem de sites específicos. . . . .	180
	Definindo URLs não filtrados . . . . .	181
	Recategorizando URLs . . . . .	182
	Trabalhando com protocolos . . . . .	182
	Filtrando protocolos . . . . .	183
	Editando protocolos personalizados . . . . .	184
	Adicionando ou editando identificadores de protocolo . . . . .	185
	Renomeando um protocolo personalizado. . . . .	186
	Fazendo alterações de filtragem global de protocolos. . . . .	186
	Criando um protocolo personalizado . . . . .	187
	Adicionando a um protocolo definido pelo Websense . . . . .	189
	Usando o Bandwidth Optimizer para gerenciar a largura de banda. . . . .	189
	Configurando os limites padrão do Bandwidth Optimizer . . . . .	190
	Gerenciando o tráfego com base no tipo de arquivo . . . . .	191
	Trabalhando com tipos de arquivo . . . . .	193

Adicionando tipos de arquivo personalizados . . . . .	194
Adicionando extensões de arquivo a um tipo de arquivo . . . . .	194
Usando expressões regulares . . . . .	194
Usando a Caixa de ferramentas para verificar o comportamento de filtragem . . . . .	195
Categoria de URL . . . . .	196
Verificar diretiva . . . . .	196
Testar filtragem . . . . .	196
Acesso ao URL . . . . .	197
Investigar usuário . . . . .	197
Identificando um usuário para verificar diretiva ou testar filtragem	197
<b>Tópico 10</b> <b>Identificação do usuário . . . . .</b>	<b>199</b>
Identificação transparente . . . . .	199
Identificação transparente de usuários remotos . . . . .	200
Autenticação manual . . . . .	201
Configurando métodos de identificação de usuário . . . . .	202
Definindo regras de autenticação para máquinas específicas . . . . .	204
Definindo exceções para as configurações de identificação de usuário . . . . .	204
Revisando exceções para as configurações de identificação de usuário . . . . .	205
Autenticação manual segura . . . . .	207
Gerando chaves e certificados . . . . .	207
Ativando a autenticação manual segura . . . . .	208
Aceitando o certificado no navegador cliente . . . . .	209
DC Agent . . . . .	211
Configurando o DC Agent . . . . .	212
Logon Agent . . . . .	214
Configurando o Logon Agent . . . . .	215
RADIUS Agent . . . . .	217
Processando o tráfego RADIUS . . . . .	218
Configurando o ambiente RADIUS . . . . .	218
Configurando o RADIUS Agent . . . . .	219
Configurando o cliente RADIUS . . . . .	220
Configurando o servidor RADIUS . . . . .	221
eDirectory Agent . . . . .	222
Considerações especiais de configuração . . . . .	223
Configurando o eDirectory Agent . . . . .	224
Adicionando uma réplica do servidor eDirectory . . . . .	225
Configurando o eDirectory Agent para usar LDAP . . . . .	226
Habilitando consultas completas do Servidor eDirectory . . . . .	226
Configurando vários agentes . . . . .	228

	Definindo configurações diferentes para uma ocorrência do agente	230
	Parâmetros do arquivo INI	231
	Configurando um agente para ignorar determinados nomes de usuário	232
<b>Tópico 11</b>	<b>Administração delegada</b>	<b>235</b>
	Introdução às funções administrativas	236
	Introdução aos administradores	236
	Super administradores	237
	Administradores delegados	239
	Administradores em várias funções	240
	Introdução às funções administrativas	241
	Notificando administradores	243
	Tarefas dos administradores delegados	244
	Ver sua conta de usuário	245
	Ver a definição da sua função	245
	Adicionar clientes à página Clientes	246
	Criar diretivas e filtros	246
	Aplicar diretivas a clientes	248
	Gerar relatórios	248
	Habilitando o acesso ao Websense Manager	248
	Contas de diretório	249
	Contas de usuário do Websense	250
	Adicionando contas de usuário do Websense	251
	Alterando a senha de usuário do Websense	252
	Usando a administração delegada	252
	Adicionando funções	254
	Editando funções	254
	Adicionando administradores	257
	Adicionando clientes gerenciados	259
	Gerenciando conflitos entre funções	261
	Considerações especiais	261
	Vários administradores acessando o Websense Manager	263
	Definindo restrições de filtragem para todas as funções	264
	Criando uma Proteção de filtro	265
	Protegendo categorias	265
	Protegendo protocolos	266
<b>Tópico 12</b>	<b>Administração do Websense Server</b>	<b>269</b>
	Componentes de produtos Websense	270
	Componentes de filtragem	271
	Componentes de relatório	273
	Componentes de identificação de usuário	274
	Entendendo o Policy Database	275
	Trabalhando com o Policy Server	275

Adicionando e editando instâncias do Policy Server . . . . .	276
Trabalhando em um ambiente com vários Policy Servers . . . . .	276
Alterando o endereço IP do Policy Server . . . . .	277
Trabalhando com o Filtering Service . . . . .	279
Verificar detalhes do Filtering Service . . . . .	280
Verificar o status de download do Master Database . . . . .	280
Downloads do Master Database que podem ser retomados . . . . .	281
Exibindo e exportando o log de auditoria . . . . .	281
Parando e iniciando os serviços Websense . . . . .	283
Alertas . . . . .	284
Controle de inundação . . . . .	285
Configurando opções de alertas gerais . . . . .	285
Configurando alertas do sistema . . . . .	287
Configurando alertas de uso de categoria . . . . .	288
Adicionando alertas de uso de categoria . . . . .	288
Configurando alertas de uso de protocolo . . . . .	289
Adicionando alertas de uso de protocolo . . . . .	290
Verificando o status atual do sistema . . . . .	291
Fazendo backup e restaurando dados do Websense . . . . .	292
Programando backups . . . . .	294
Executando backups imediatos . . . . .	295
Mantendo os arquivos de backup . . . . .	296
Restaurando os dados do Websense . . . . .	296
Suspendendo backups programados . . . . .	297
Referência de comando . . . . .	298
<b>Tópico 13   Administração de relatórios . . . . .</b>	<b>299</b>
Planejando a sua configuração . . . . .	300
Gerenciando o acesso às ferramentas de relatórios . . . . .	300
Configuração básica . . . . .	301
Atribuindo categorias a classes de risco . . . . .	302
Configurando preferências de relatórios . . . . .	303
Configurando o Filtering Service para registro em log . . . . .	304
Utilitário Configuração do Log Server . . . . .	306
Configurando conexões do Log Server . . . . .	307
Configurando opções do servidor do banco de dados de log . . . . .	308
Configurando a conexão do banco de dados . . . . .	310
Configurando os arquivos de cache de log . . . . .	311
Configurando opções de consolidação . . . . .	312
Configurando o WebCatcher . . . . .	314
Autenticação do WebCatcher . . . . .	316
Interrompendo e iniciando o Log Server . . . . .	317

	Apresentando o banco de dados de log .....	317
	Trabalhos de banco de dados .....	318
	Administrando o banco de dados de log .....	319
	Configurações de administração do banco de dados de log .....	320
	Configurando opções de substituição .....	321
	Configurando o registro de URLs completos .....	322
	Configurando as opções de tempo de navegação na Internet ..	324
	Configurando opções de manutenção do banco de dados de log	325
	Configurando opções de partição do banco de dados de log...	327
	Configurando as partições disponíveis .....	328
	Visualizando logs de erros .....	329
	Configurando relatórios investigativos .....	330
	Conexão de banco de dados e padrões de relatórios .....	330
	Opções de exibição e saída .....	332
	Relatório próprio .....	334
<b>Tópico 14</b>	<b>Configuração da rede .....</b>	<b>337</b>
	Configuração de hardware .....	338
	Configuração do Network Agent .....	339
	Definindo as configurações globais .....	340
	Definindo as configurações locais .....	341
	Definindo as configurações de placa de rede .....	343
	Definindo as configurações de monitoramento para uma placa de rede .....	344
	Adicionando ou editando endereços IP .....	345
	Verificando a configuração do Network Agent .....	346
<b>Tópico 15</b>	<b>Solução de problemas .....</b>	<b>349</b>
	Problemas de instalação e assinatura .....	349
	O status do Websense indica um problema de assinatura .....	349
	Há usuários ausentes no Websense Manager após a atualização ..	350
	Problemas do Master Database .....	351
	O banco de dados de filtragem inicial está em uso .....	351
	O Master Database tem mais de 1 semana de idade .....	351
	Não é feito o download do Master Database .....	352
	Chave de assinatura .....	352
	Acesso à Internet .....	353
	Verificar as configurações de firewall e servidor proxy .....	353
	Espaço em disco insuficiente .....	354
	Memória insuficiente .....	355
	Aplicativos com restrições .....	356
	O download do Master Database não ocorre no horário correto...	356
	Entrando em contato com o suporte técnico para solucionar problemas de download do banco de dados .....	356
	Problemas de filtragem .....	357

O Filtering Service não está em execução . . . . .	357
O User Service não está disponível. . . . .	358
Os sites são categorizados incorretamente como Informática . . . .	359
Palavras-chave não estão sendo bloqueadas . . . . .	359
URLs de filtro de acesso personalizado ou limitado não são filtrados como esperado. . . . .	360
O usuário não pode acessar um protocolo ou um aplicativo como esperado. . . . .	360
Uma solicitação FTP não é bloqueada como esperado. . . . .	360
O software Websense não aplica as diretivas de usuário ou grupo. . . .	361
Os usuários remotos não são filtrados pela diretiva correta . . . . .	361
Problemas do Network Agent . . . . .	361
O Network Agent não está instalado. . . . .	361
O Network Agent não está em execução . . . . .	362
O Network Agent não está monitorando NICs . . . . .	362
O Network Agent não pode se comunicar com o Filtering Service . . . .	362
Atualizar informações de UID ou endereço IP do Filtering Service . . . . .	363
Problemas de identificação do usuário. . . . .	364
Solução de problemas do DC Agent. . . . .	365
Os usuários são filtrados incorretamente pela diretiva Padrão . . . .	365
Alterando as permissões do DC Agent e do User Service manualmente . . . . .	366
Solucionando problemas do Logon Agent . . . . .	366
Objetos de diretiva de grupo . . . . .	367
User Service em execução no Linux . . . . .	367
Visibilidade do controlador de domínio . . . . .	368
NetBIOS. . . . .	368
Problemas de perfil de usuário. . . . .	369
Solucionando problemas do eDirectory Agent . . . . .	369
Ativando o diagnóstico do eDirectory Agent . . . . .	370
O eDirectory Agent erra na contagem de conexões do eDirectory Server . . . . .	371
Executando o eDirectory Agent em modo de console. . . . .	371
Solucionando problemas do RADIUS Agent . . . . .	372
Executando o RADIUS Agent em modo de console. . . . .	372
Os usuários remotos não são solicitados a fazer autenticação manual. . . . .	373
Os usuários remotos não estão sendo filtrados corretamente . . . . .	373
Problemas com mensagens de bloqueio. . . . .	374
Nenhuma página de bloqueio aparece para um tipo de arquivo bloqueado . . . . .	374
Os usuários recebem um erro do navegador, e não uma página de bloqueio . . . . .	374
Uma página branca vazia aparece em vez de uma página de bloqueio . . . .	375

Mensagens de bloqueio de protocolo não são exibidas como esperado . . .	376
Uma mensagem de bloqueio de protocolo é exibida em vez de uma página de bloqueio . . . . .	376
Problemas de registro, mensagem de status e alerta. . . . .	377
Onde encontro as mensagens de erro dos componentes do Websense? . . . . .	377
Alertas de saúde do Websense . . . . .	377
Dois registros em log são gerados para uma única solicitação . . . . .	378
Problemas do Policy Server e do Policy Database. . . . .	378
Esqueci minha senha. . . . .	378
Não consigo fazer logon no Policy Server . . . . .	379
Falha do serviço Websense Policy Database ao iniciar . . . . .	379
Problemas de administração delegada . . . . .	380
Os clientes gerenciados não podem ser excluídos da função . . . . .	380
Mensagem de erro de logon informa que outra pessoa se conectou em minha máquina . . . . .	380
Alguns usuários não conseguem acessar um site na lista de URLs não filtrados . . . . .	381
Os sites recategorizados são filtrados de acordo com a categoria incorreta. . . . .	381
Não consigo criar um protocolo personalizado. . . . .	381
Problemas de relatório . . . . .	381
O Log Server não está em execução. . . . .	382
Nenhum Log Server está instalado para um Policy Server. . . . .	383
O banco de dados de log não foi criado . . . . .	383
O banco de dados de log não está disponível . . . . .	384
Tamanho do banco de dados de log . . . . .	385
O Log Server não está registrando dados no banco de dados de log. . . . .	385
Atualizando a senha de conexão do Log Server . . . . .	386
Configurando permissões de usuário para o Microsoft SQL Server 2005. . . . .	386
O Log Server não pode se conectar ao serviço de diretório . . . . .	387
Os dados sobre o tempo de navegação na Internet estão distorcidos. . . . .	388
A largura de banda é maior que o esperado . . . . .	388
Algumas solicitações de protocolo não estão sendo registradas. . . . .	388
Todos os relatórios estão vazios . . . . .	388
Partições de banco de dados . . . . .	389
SQL Server Agent job . . . . .	389
Configuração do Log Server . . . . .	389
Nenhum gráfico é exibido nas páginas Hoje ou Histórico . . . . .	390
Não é possível acessar determinados recursos de relatório. . . . .	390
A saída do Microsoft Excel não contém alguns dados de relatório . . . . .	390
Salvando a saída de relatórios de apresentação como HTML . . . . .	391
Problemas de pesquisa de relatórios investigativos . . . . .	391

Problemas gerais de relatórios investigativos . . . . .	392
Ferramentas de solução de problemas . . . . .	392
A caixa de diálogo Serviços do Windows. . . . .	392
O Windows Event Viewer. . . . .	393
O arquivo de log do Websense . . . . .	393

# 1

## Primeiros Passos

O software Websense oferece aos administradores de rede de todos os setores de atividades, desde negócios e educação até governo e outros, a possibilidade de controlar ou monitorar o tráfego de rede para a Internet.

- ◆ Minimizar o tempo que os funcionários gastam para acessar dados na Internet considerados objeccionáveis, inadequados ou não relacionados ao trabalho.
- ◆ Minimizar o uso inapropriado dos recursos da rede e a ameaça de medidas legais em decorrência de acesso inadequado.
- ◆ Acrescentar uma camada confiável de segurança à sua rede, protegendo-a contra spyware, malware, hackers e outras invasões.

A partir daqui, você pode obter informações sobre:

<b>Configuração básica do Websense</b>	<b>Implementação de filtragem de Internet</b>
<ul style="list-style-type: none"><li>• <i>Trabalhando no Websense Manager</i>, página 14</li><li>• <i>Sua assinatura</i>, página 26</li><li>• <i>O Websense Master Database</i>, página 29</li><li>• <i>Verificando a configuração do Network Agent</i>, página 346</li></ul>	<ul style="list-style-type: none"><li>• <i>Filtragem de categorias e protocolos</i>, página 36</li><li>• <i>Adicionando um cliente</i>, página 66</li><li>• <i>Trabalhando com diretivas</i>, página 73</li><li>• <i>Atribuindo uma diretiva aos clientes</i>, página 77</li></ul>

Você também pode aprender como:

<b>Avaliar sua configuração</b>	<b>Refinar as diretivas de filtragem</b>
<ul style="list-style-type: none"><li>• <i>Hoje: Saúde, segurança e valor desde a meia-noite</i>, página 19</li><li>• <i>Histórico: Últimos 30 dias</i>, página 22</li><li>• <i>Relatórios de apresentação</i>, página 96</li><li>• <i>Relatórios investigativos</i>, página 115</li><li>• <i>Usando a Caixa de ferramentas para verificar o comportamento de filtragem</i>, página 195</li></ul>	<ul style="list-style-type: none"><li>• <i>Criando uma categoria personalizada</i>, página 176</li><li>• <i>Redefinindo a filtragem de sites específicos</i>, página 180</li><li>• <i>Restringindo usuários a uma lista definida de sites de Internet</i>, página 166</li><li>• <i>Filtrando com base em palavras-chave</i>, página 177</li><li>• <i>Gerenciando o tráfego com base no tipo de arquivo</i>, página 191</li><li>• <i>Usando o Bandwidth Optimizer para gerenciar a largura de banda</i>, página 189</li></ul>

## Visão geral

---

Trabalhando em conjunto com dispositivos de integração — incluindo servidores proxy, firewalls, roteadores e appliances de cache — o software Websense oferece o mecanismo e as ferramentas de configuração para desenvolver, monitorar e aplicar diretivas de acesso à Internet.

Juntos, os componentes do Websense (descritos em *Componentes de produtos Websense*, página 270) fornecem recursos de filtragem de Internet, identificação de usuários, alertas, relatórios e solução de problemas.

A visão geral dos novos recursos incluídos nessa versão do software Websense pode ser encontrada nas [Notas de versão](#), disponíveis no [Portal de suporte do Websense](#).

Após a instalação, o software Websense aplicará a diretiva **Padrão** para monitorar o uso da Internet sem bloquear as solicitações. Esta diretiva controlará o acesso à Internet para todos os clientes na rede, até que você defina suas próprias diretivas e as atribua aos clientes. Mesmo depois de você ter criado suas configurações personalizadas para filtragem, a diretiva Padrão será aplicada sempre que o cliente não estiver sendo controlado por alguma outra diretiva. Consulte *A diretiva Padrão*, página 72, para obter mais informações.

O processo para criar filtros, adicionar clientes, definir diretivas e aplicar diretivas aos clientes está descrito em:

- ◆ [Filtros de uso da Internet](#), página 35
- ◆ [Clientes](#), página 57
- ◆ [Diretivas de filtragem da Internet](#), página 71

Uma ferramenta única e baseada em navegador — o Websense Manager — fornece a interface gráfica central para a configuração geral, o gerenciamento de diretivas e as funções de relatórios do software Websense. Consulte *Trabalhando no Websense Manager*, página 14, para obter mais informações.

Você pode definir os níveis de acesso ao Websense Manager para permitir que determinados administradores gerenciem apenas um grupo específico de clientes ou para permitir que indivíduos gerem relatórios sobre seu próprio uso de Internet. Consulte *Administração delegada*, página 235, para obter mais informações.

## Trabalhando no Websense Manager

---

Tópicos relacionados:

- ◆ [Fazendo logon no Websense Manager](#), página 16
- ◆ [Navegando no Websense Manager](#), página 17
- ◆ [Hoje: Saúde, segurança e valor desde a meia-noite](#), página 19
- ◆ [Histórico: Últimos 30 dias](#), página 22

O Websense Manager é a interface de configuração central usada para personalizar o comportamento de filtragem, monitorar o uso da Internet, gerar relatórios de uso de Internet e gerenciar as configurações e definições do software Websense. Esta ferramenta baseada na Web é compatível com dois navegadores:

- ◆ Microsoft Internet Explorer 7
- ◆ Mozilla Firefox 2

Embora seja possível iniciar o Websense Manager usando outros navegadores, dê preferência aos navegadores compatíveis para obter os recursos completos e a exibição adequada do aplicativo.

Para iniciar o Websense Manager, use um dos seguintes métodos:

- ◆ Em computadores com Windows:
  - Vá para **Iniciar >, Todos os programas, > Websense** e selecione **Websense Manager**.
  - Clique duas vezes no ícone do Websense Manager na área de trabalho.
- ◆ Abra um navegador compatível em qualquer computador de sua rede e digite:

```
https://<endereço IP>:9443/mng
```

Substitua o <endereço IP> com o endereço IP do computador do Websense Manager.

Se você não conseguir se conectar ao Websense Manager na porta padrão, consulte o arquivo **tomcat.log** no computador do Websense Manager (localizado por padrão no diretório **C:\Arquivos de programas\Websense\tomcat\logs\** ou **/opt/Websense/tomcat/logs/**) para verificar a porta.

Se estiver usando a porta correta e ainda assim não conseguir se conectar ao Websense Manager a partir de um computador remoto, verifique se o seu firewall permite a comunicação naquela porta.

É usada uma conexão SSL para comunicação segura baseada em navegadores com o Websense Manager. Esta conexão usa um certificado de segurança emitido pela Websense, Inc. Como os navegadores compatíveis não reconhecem a Websense, Inc., como uma Autoridade de Certificação conhecida, um erro de certificação será exibido da primeira vez que você iniciar o Websense Manager em um novo navegador. Para evitar a exibição desse erro, você pode instalar ou aceitar permanentemente o certificado no navegador. Consulte a [Base de conhecimentos Websense](#) para obter instruções.

Depois que o certificado de segurança for aceito, a página de logon do Websense Manager será exibida na janela do navegador (consulte [Fazendo logon no Websense Manager](#)).

## Fazendo logon no Websense Manager

Tópicos relacionados:

- ◆ [Trabalhando no Websense Manager](#)
- ◆ [Navegando no Websense Manager, página 17](#)
- ◆ [Hoje: Saúde, segurança e valor desde a meia-noite, página 19](#)
- ◆ [Histórico: Últimos 30 dias, página 22](#)

Após a instalação, o primeiro usuário que fizer logon no Websense Manager terá acesso administrativo total. O nome de usuário será **WebsenseAdministrator** e não poderá ser alterado. A senha do WebsenseAdministrator será configurada durante a instalação.

Para fazer logon, primeiro inicie o Websense Manager (consulte [Trabalhando no Websense Manager](#)). Na página de logon:

1. Selecione um **Policy Server** para gerenciar.  
Se o seu ambiente incluir apenas um Policy Server, ele será selecionado por padrão.
2. Selecione um **Tipo de conta**:
  - Para fazer logon usando uma conta de usuário do Websense, como o WebsenseAdministrator, clique em **Conta Websense** (padrão).
  - Para fazer logon usando suas credenciais de rede, clique em **Conta de rede**.
3. Insira o **Nome de usuário** e a **Senha**, e clique em **Logon**.

Você estará conectado ao Websense Manager.

- ◆ Se for o seu primeiro logon no Websense Manager, será oferecida a opção de iniciar o tutorial do Guia rápido. Se você não tiver experiência no uso do software Websense ou desta versão, é altamente recomendável que conclua o tutorial do Guia rápido.
- ◆ Se estiver usando administração delegada e tiver criado funções administrativas, talvez seja solicitado a selecionar uma função para gerenciar. Consulte [Administração delegada, página 235](#), para obter mais informações.

A seção do Websense Manager terminará 30 minutos após a última ação executada na interface do usuário (clique de uma página para outra, inserir informações, alterar o cache ou salvar alterações). Uma mensagem de aviso será exibida 5 minutos antes do encerramento da sessão.

- ◆ Se houver alterações na página que não estejam em cache ou que estejam pendentes em cache, as alterações serão perdidas quando a sessão terminar. Lembre-se de clicar em **OK** para colocar em cache e **Salvar tudo** para salvar e implementar todas as alterações.
- ◆ Se o Websense Manager for aberto em várias guias da mesma janela do navegador, todas as instâncias compartilharão a mesma sessão. Se o tempo limite da sessão for ultrapassado em uma guia, ele será ultrapassado em todas as guias.

- ◆ Se o Websense Manager for aberto em várias janelas do navegador no mesmo computador, as instâncias compartilharão a mesma sessão **se**:
    - Você estiver usando o Microsoft Internet Explorer e utilizar o atalho Ctrl-N para abrir uma nova instância do Websense Manager.
    - Você estiver usando o Mozilla Firefox.
- Se o tempo limite da sessão for ultrapassado em uma janela, ele será ultrapassado em todas as janelas.
- ◆ Se você iniciar várias janelas do Internet Explorer independentemente umas das outras e em seguida usá-las para fazer logon como administradores diferentes no Websense Manager, as janelas **não** compartilharão a sessão. Se o tempo limite de uma janela for ultrapassado, as outras não serão afetadas.

Se você fechar o navegador sem fazer logoff do Websense Manager ou se o computador remoto pelo qual estiver acessando o Websense Manager for encerrado inesperadamente, talvez você fique temporariamente bloqueado. O software Websense detectará esse problema em aproximadamente 2 minutos e encerrará a sessão interrompida, permitindo que você faça logon novamente.

## Navegando no Websense Manager

A interface do Websense Manager pode ser dividida em 4 áreas principais:

1. Banner do Websense
2. Painel de navegação esquerdo
3. Painel de atalho direito
4. Painel de conteúdo

The screenshot displays the Websense Manager web interface. At the top, there is a blue banner with the 'WebSecurity' logo, a status bar showing 'Policy Server: 192.168.247.43', and a user dropdown menu for 'Super Administrador' with a 'Logout' button. Below the banner, the interface is divided into several sections:

- Left Panel (Painel de navegação esquerdo):** Contains a 'Principal' menu with options like 'Status', 'Histórico', 'Alertas', 'Log de auditoria', 'Geração de relatórios', 'Gerenciamento de diretivas', 'Clientes', 'Diretivas', 'Filtros', 'Componentes do filtro', 'Administração delegada', and 'Proteção de filtro'.
- Top Right Panel (Painel de atalho direito):** Shows 'Nenhuma alteração detectada' with a 'Salvar tudo' button, 'Tarefas comuns' (Executar relatório, Criar diretiva, Recategorizar URL, Desbloquear URL, Sugerir nova categoria), and a 'Caixa de ferramentas' with dropdown menus for 'Categoria de URL', 'Verificar diretiva', 'Testar filtragem', 'Acesso ao URL', and 'Investigar usuário', along with a 'Portal de suporte' link.
- Main Content Area (Painel de conteúdo):**
  - Resumo do alerta de saúde:** Shows 'Nenhum problema detectado' with a green checkmark.
  - Valor de hoje:** A summary table with columns for 'Bloqueado' and 'Contadores'. Under 'Bloqueado', it lists 'Mal-intencionado: 0', 'Adulto: 0', and 'Spyware: 0'. Under 'Contadores', it lists 'Solicitações: 386', 'Bloqueado: 0', and 'RTSU: 20'.
  - Carga de filtragem atual:** A line graph showing the current filtering load over a 24-hour period, with peaks around 01:00, 06:00, and 09:00.
  - Principais riscos de segurança por solicitações:** A bar chart showing security risks by request category.
  - Principais categorias por solicitações:** A bar chart showing the top request categories, with 'Diversos' being the most frequent.

O **banner do Websense** exibe:

- ◆ Em qual **Policy Server** você está conectado no momento (consulte [Trabalhando com o Policy Server](#), página 275)
- ◆ Sua atual **Função** administrativa (consulte [Introdução às funções administrativas](#), página 236)
- ◆ Um botão de **Logoff** para quando você estiver pronto para encerrar sua sessão administrativa

O conteúdo exibido no Websense Manager variará de acordo com os privilégios concedidos ao usuário conectado. Para um usuário com privilégios somente de relatórios, por exemplo, não serão exibidas ferramentas de configuração de servidor ou de administração de diretivas. Consulte [Administração delegada](#), página 235, para obter mais informações.

Esta seção descreve as opções disponíveis para o WebsenseAdministrator e para outros usuários com privilégios de Super administradores.

O **painel de navegação esquerdo** tem duas guias: **Principal** e **Configurações**. Use a guia **Principal** para acessar status, relatórios, e recursos e funções de gerenciamento de diretivas. Use a guia **Configurações** para gerenciar sua conta Websense e executar tarefas globais de administração do sistema.

O **painel de atalho direito** contém links para ferramentas úteis e tarefas administrativas comuns. É aqui também que você pode rever e salvar quaisquer alterações que tenha feito no Websense Manager.

- ◆ A parte superior do painel de navegação indica se existem alterações em cache aguardando para serem salvas. Quando você estiver trabalhando no Websense Manager, a barra de Alterações indicará se existem ou não **Alterações pendentes**.

Na maioria dos casos, quando você executar uma tarefa no Websense Manager e clicar em **OK**, suas alterações serão colocadas em cache. (Às vezes, será necessário clicar em OK tanto na página subordinada quanto na página principal para colocar as alterações em cache.)

Após colocar as alterações em cache, clique em **Salvar tudo** para salvar e implementar as alterações. Para visualizar as alterações em cache antes de salvar (consulte [Revendo, salvando e descartando alterações](#), página 19), clique no botão **Exibir alterações pendentes**. É o botão menor à esquerda de Salvar tudo.

- ◆ A opção **Tarefas comuns** fornece atalhos para tarefas administrativas executadas com frequência. Clique em um item da lista para ir para a página onde a tarefa é executada.
- ◆ A **Caixa de ferramentas** contém ferramentas de pesquisa rápida que você pode usar para verificar a sua configuração de filtragem. Consulte [Usando a Caixa de ferramentas para verificar o comportamento de filtragem](#), página 195, para obter mais informações.

## Revendo, salvando e descartando alterações

Quando você executar uma tarefa no Websense Manager e, em seguida, clicar em **OK**, suas alterações serão colocadas em cache. Use a página **Exibir alterações pendentes** para rever as alterações em cache.



### Importante

Evite clicar duas ou três vezes no botão OK. Clicar várias vezes rapidamente no mesmo botão pode causar problemas no Mozilla Firefox, que só podem ser solucionados fechando e reabrindo o navegador.

As alterações em uma única área de funcionalidade são em geral agrupadas em uma única entrada na lista de cache. Por exemplo, se você adicionar 6 clientes e excluir 2 clientes, a lista de cache indicará apenas que foram feitas alterações em Clientes. As alterações em uma única página de Configurações, por outro lado, podem resultar em várias entradas na lista de cache. Isso ocorre quando uma única página de Configurações é usada para configurar várias funções do software Websense.

- ◆ Para salvar todas as alterações em cache, clique em **Salvar todas as alterações**.
- ◆ Para abandonar todas as alterações em cache, clique em **Cancelar todas as alterações**.

Após escolher Salvar tudo ou Cancelar tudo, a barra de Alterações no painel de atalho direito será atualizada adequadamente e você será levado de volta à última página que selecionou. Não existe a opção de desfazer para as funções de Salvar tudo ou Cancelar tudo.

Use o Log de auditoria para rever os detalhes das alterações feitas no Websense Manager. Consulte [Exibindo e exportando o log de auditoria, página 281](#), para obter mais informações.

## Hoje: Saúde, segurança e valor desde a meia-noite

Tópicos relacionados:

- ◆ [Navegando no Websense Manager, página 17](#)
- ◆ [Histórico: Últimos 30 dias, página 22](#)
- ◆ [Personalizando a página Hoje, página 22](#)
- ◆ [Alertas, página 284](#)

A página **Status > Hoje: Saúde, segurança e valor desde a meia-noite** será exibida primeiro quando você fizer logon no Websense Manager. Ela apresentará o status atual do seu software de filtragem e ilustrará graficamente a atividade de filtragem na

Internet por até 24 horas, começando à 00h01, de acordo com a hora da máquina do banco de dados de log.

Na parte superior da página, duas seções de resumo fornecem uma visão geral rápida do status atual:

- ◆ O **Resumo do alerta de saúde** mostra o status do software Websense. Se um erro ou aviso aparecer no resumo, clique na mensagem de alerta para abrir a página Alertas, onde encontrará informações mais detalhadas (consulte [Verificando o status atual do sistema](#), página 291).  
As informações no Resumo do alerta de saúde são atualizadas a cada 30 segundos.
- ◆ Em **Valor de Hoje**, veja exemplos de como a filtragem do Websense protegeu sua rede hoje, além do número total de solicitações da Internet negociadas e os totais de outras atividades importantes.

Abaixo das informações de resumo, até quatro gráficos fornecem informações sobre as atividades de filtragem. Estes gráficos estão disponíveis para os Super administradores e para os administradores delegados que tenham permissão para visualizar relatórios da página Hoje. Consulte [Editando funções](#), página 254.

As informações nestes gráficos são atualizadas a cada 2 minutos. Você talvez precise rolar para baixo para ver todos os gráficos.

Nome do Gráfico	Descrição
Carga de filtragem atual	Veja o volume de tráfego da Internet filtrado processado no banco de dados de log, mostrado em intervalos de 10 minutos.
Principais riscos de segurança por solicitações	Descubra as categorias de risco de segurança que receberam a maioria das solicitações hoje e determine se as diretivas de filtragem estão fornecendo a proteção certa para sua rede.
Principais categorias por solicitações	Veja as categorias que estão sendo mais acessadas hoje. Obtenha uma visão geral de alto nível das preocupações potenciais sobre segurança, largura de banda ou produtividade.
Aplicação de diretivas por classe de risco	Veja quantas solicitações para cada classe de risco foram permitidas e bloqueadas hoje (consulte <a href="#">Classes de risco</a> , página 39). Avalie se as diretivas atuais são eficazes ou se são necessárias alterações.
Principais protocolos por largura de banda	Saiba quais protocolos estão usando mais largura de banda na sua rede atualmente. Use estas informações para avaliar as necessidades de largura de banda e de possíveis alterações de diretivas.
Computadores que solicitam sites com risco de segurança	Descubra quais computadores acessaram sites com risco de segurança hoje. É recomendável verificar se essas máquinas não estão infectadas com vírus ou spyware.

Nome do Gráfico	Descrição
Principais usuários bloqueados	Veja quais usuários solicitaram a maior parte dos sites bloqueados hoje, obtendo informações úteis para a conformidade dos padrões de uso da Internet na empresa.
Principais sites não categorizados	Saiba quais sites não categorizados pelo Websense Master Database foram mais acessados hoje. Vá para <b>Tarefas comuns &gt; Recategorizar URL</b> para atribuir um site a uma categoria de filtragem.

Clique em qualquer gráfico de barras para abrir um relatório investigativo com mais detalhes.

Três botões serão exibidos acima da página:

- ◆ **Download do banco de dados**, disponível somente para Super administradores, abre a página para visualizar os downloads do Master Database ou iniciar um download (consulte *Verificar o status de download do Master Database*, página 280).
- ◆ **Personalizar**, disponível somente para Super administradores, abre uma página onde você pode alterar os gráficos que serão exibidos na página (consulte *Personalizando a página Hoje*, página 22).
- ◆ **Imprimir**, disponível para todos os administradores, abre uma janela secundária com uma versão imprimível dos gráficos exibidos na página Hoje. Use as opções do navegador para imprimir esta página, que omite todas as opções de navegação encontradas na janela principal do Websense Manager.

Abaixo dos gráficos de atividade e filtragem na Internet, o **Resumo do Filtering Service** mostra o status de cada Filtering Service associado ao Policy Server atual. Clique no endereço IP do Filtering Service para visualizar mais informações sobre a instância do Filtering Service.

Por motivos de segurança, a sessão do Websense Manager será encerrada após 30 minutos de inatividade. Porém, você poderá optar por continuar a monitorar os dados de filtragem e alerta: marque **Continuar a monitorar o status de Hoje, Histórico e Alertas sem tempo limite** na parte inferior da página Hoje. As informações sobre estas três páginas continuarão sendo atualizadas normalmente, até que você feche o navegador ou navegue para outra página do Websense Manager.



### Importante

Se você habilitar a opção de monitoração e permanecer nas páginas Hoje, Histórico e Alertas por mais de 30 minutos, a tentativa de navegar para outra página do Websense Manager fará você voltar à página de logon.

Se habilitar esta opção, lembre-se de salvar as alterações em cache antes de terminar o período de 30 minutos de tempo limite.

## Personalizando a página Hoje

Tópicos relacionados:

- ◆ [Hoje: Saúde, segurança e valor desde a meia-noite](#), página 19
- ◆ [Personalizar a página Histórico](#), página 25

Use a página **Hoje > Personalizar** para selecionar até quatro gráficos para a página Status > Hoje. Somente Super administradores com permissões incondicionais de diretivas (inclusive WebsenseAdministrator) podem personalizar a página Hoje.

Os gráficos que você selecionar serão exibidos na página Hoje de todos os Super administradores e dos administradores delegados que tiverem permissão para visualizar gráficos na página Hoje. Consulte [Editando funções](#), página 254.

Alguns gráficos exibem informações potencialmente confidenciais, como nomes de usuários ou endereços IP. Certifique-se de que os gráficos selecionados sejam adequados para todos os administradores que puderem visualizá-los.

Para selecionar gráficos, marque ou desmarque a caixa de seleção ao lado do nome do gráfico. Quando terminar de marcar as seleções, clique em **OK** para voltar à página Hoje e visualizar os gráficos. Para voltar à página Hoje sem fazer alterações, clique em **Cancelar**.

Para uma breve descrição das informações exibidas em cada gráfico, consulte [Hoje: Saúde, segurança e valor desde a meia-noite](#), página 19.

## Histórico: Últimos 30 dias

---

Tópicos relacionados:

- ◆ [Hoje: Saúde, segurança e valor desde a meia-noite](#), página 19
- ◆ [Navegando no Websense Manager](#), página 17
- ◆ [Personalizar a página Histórico](#), página 25

Use a página **Status > Histórico: Últimos 30 Dias** para obter uma visão geral do comportamento de filtragem para até os últimos 30 dias. Os gráficos da página são atualizados diariamente à 00h01 para incorporar dados do dia anterior, como determinado pela hora da máquina do banco de dados de log.

O período exato abrangido pelos gráficos e tabelas de resumo dependerá de quanto tempo o software Websense esteve filtrando. Durante o primeiro mês da instalação do software Websense, a página mostrará os dados do número de dias desde que ele foi instalado. Depois disso, os relatórios abrangerão os 30 dias anteriores ao dia de hoje.

As **Estimativas de valor** na parte superior da página fornecem uma estimativa da economia de tempo e de largura de banda proporcionada pelo software Websense, bem como um resumo das solicitações bloqueadas de categorias que são importantes para muitas empresas.

Passa o mouse sobre o item **Tempo** ou **Largura de banda** (em Salvo) para obter uma explicação de como a estimativa foi calculada (consulte [Tempo e largura de banda economizados](#), página 24). Você pode clicar em **Personalizar** para alterar o modo como os valores são calculados.

A área **Solicitações bloqueadas** ilustra adicionalmente como o software Websense protegeu sua rede, listando várias categorias de interesse para muitas empresas e mostrando o número total de solicitações bloqueadas para cada uma delas durante um período.

Dependendo das permissões de relatório concedidas para a função, os administradores delegados talvez não visualizem os gráficos descritos abaixo. Consulte [Editando funções](#), página 254.

A página também inclui até quatro gráficos com destaques de filtragem. Você talvez precise rolar para baixo para ver todos os gráficos. As informações nos gráficos são atualizadas uma vez ao dia. Clique em um gráfico para iniciar um relatório investigativo com mais detalhes.

Nome do gráfico	Descrição
Atividade na Internet por solicitações	Reveja o número de solicitações da Internet filtradas processado no banco de dados de log a cada dia.
Principais riscos de segurança por solicitações	Veja quais categorias de Risco de segurança foram acessadas recentemente e determine se as diretivas de filtragem estão fornecendo a proteção certa para sua rede.
Principais categorias por solicitações	Veja quais categorias foram mais acessadas. Obtenha uma visão geral de alto nível das preocupações potenciais sobre segurança, largura de banda ou produtividade.
Principais sites não categorizados	Descubra quais sites não categorizados pelo Websense Master Database foram mais acessados. Vá para <b>Tarefas comuns &gt; Recategorizar URL</b> para atribuir um site a uma categoria de filtragem.
Principais protocolos por largura de banda	Saiba quais protocolos usaram mais largura de banda na sua rede recentemente. Use essas informações para avaliar as necessidades de largura de banda e as possíveis alterações de diretiva.
Aplicação de diretivas por classe de risco	Veja quantas solicitações para cada classe de risco foram permitidas e bloqueadas recentemente (consulte <a href="#">Classes de risco</a> , página 39). Avalie se as diretivas atuais são eficazes ou se são necessárias alterações.

Nome do gráfico	Descrição
Principais usuários bloqueados	Veja quais usuários tiveram mais solicitações de Internet bloqueadas. Obtenha informações úteis para a conformidade dos padrões de uso da Internet na sua empresa.
Resumo de aplicação de diretivas	Obtenha uma visão geral das solicitações permitidas, das solicitações bloqueadas a sites na classe Risco de segurança e das bloqueadas a outros sites recentemente. Considere quais aspectos de filtragem precisam de uma avaliação mais detalhada.

Dois botões são exibidos acima da página:

- ◆ **Personalizar**, disponível somente para Super administradores, abre uma página onde você pode alterar os gráficos que serão exibidos na página e alterar como as estimativas de economia serão calculadas (consulte [Personalizar a página Histórico](#), página 25).
- ◆ **Imprimir**, disponível para todos os administradores, abre uma janela secundária com uma versão imprimível dos gráficos exibidos na página Histórico. Use as opções do navegador para imprimir esta página, que omite todas as opções de navegação encontradas na janela principal do Websense Manager.

## Tempo e largura de banda economizados

Além da segurança aprimorada que a filtragem do Websense oferece, ela também ajuda a reduzir o tempo e a largura de banda perdidos em decorrência de atividade improdutiva na Internet.

A seção Salvo da área Estimativas de valor apresenta uma estimativa dessa economia de tempo e de largura de banda. Estes valores são calculados do seguinte modo:

- ◆ Tempo economizado: multiplique o **tempo típico usado por visita** pelos **sites bloqueados**. Inicialmente, o software Websense usa um valor padrão, como o número médio de segundos que um usuário passa visualizando um site da Web solicitado. O valor de sites bloqueados representa o número total de solicitações bloqueadas durante o intervalo de tempo especificado na página Histórico.
- ◆ Largura de banda economizada: multiplique a **largura de banda típica usada por visita** pelo número de **sites bloqueados**. Inicialmente, o software Websense usa um valor padrão, como o número médio de bytes consumidos pelo site da Web médio. O valor de sites bloqueados representa o número total de solicitações bloqueadas durante o intervalo de tempo especificado na página Histórico.

Consulte [Personalizar a página Histórico](#), página 25, para obter informações sobre como alterar os valores usados nesses cálculos para refletir o uso em sua empresa.

## Personalizar a página Histórico

Tópicos relacionados:

- ◆ [Histórico: Últimos 30 dias](#), página 22
- ◆ [Personalizando a página Hoje](#), página 22

Use a página **Histórico** > **Personalizar** para determinar quais gráficos serão exibidos na página Status > Histórico e para determinar como a economia de tempo e de largura de banda será calculada.

Marque a caixa de seleção ao lado do nome de cada gráfico, até 4, que você deseja incluir na página Histórico. Para uma descrição breve de cada gráfico, consulte [Histórico: Últimos 30 dias](#), página 22. Somente Super administradores com permissões incondicionais de diretivas (inclusive WebsenseAdministrator) podem personalizar os gráficos da página Histórico.

Alguns gráficos exibem informações potencialmente confidenciais, como nomes de usuários. Certifique-se de que os gráficos selecionados sejam adequados para todos os administradores que puderem visualizá-los.

Tanto Super administradores quanto administradores delegados podem personalizar o modo como a economia de tempo e de largura de banda é calculada. Os administradores delegados acessam esses campos clicando no link **Personalizar** no pop-up que descreve os cálculos de economia de tempo e de largura de banda.

Insira novas medidas da média de tempo e de largura de banda para usar como base de cálculo:

Opção	Descrição
Média de segundos salvos por página bloqueada	Insira o número médio de segundos que sua empresa estima que um usuário passe visualizando páginas individuais. O software Websense multiplica esse valor pelo número de páginas bloqueadas para determinar a economia de tempo mostrada na página Histórico.
Média de largura de banda [KB] economizada por página bloqueada	Insira o tamanho médio, em kilobytes (KB), das páginas visualizadas. O software Websense multiplica esse valor pelo número de páginas bloqueadas para determinar a economia de largura de banda mostrada na página Histórico.

Quando terminar de fazer as alterações, clique em **OK** para voltar à página Histórico e visualizar os novos gráficos ou as estimativas de tempo e de largura de banda. Para voltar à página Histórico sem fazer alterações, clique em **Cancelar**.

## Sua assinatura

---

As assinaturas do Websense são distribuídas em termos de clientes. Um cliente é um usuário ou um computador em sua rede.

Quando você adquire uma assinatura, uma chave de assinatura é enviada por e-mail. Cada chave é válida para uma única instalação do Websense Policy Server. Se você instalar vários Policy Servers, precisará de uma chave separada para cada um deles.

Antes de começar a filtragem, você precisará inserir uma chave de assinatura válida (consulte [Configurando as informações de sua conta](#), página 28). Isso permitirá o download do Master Database (consulte [O Websense Master Database](#), página 29), que habilita o software Websense para filtrar clientes.

Depois do primeiro download bem-sucedido do banco de dados, o Websense Manager exibirá o número de clientes incluídos em sua assinatura.

O software Websense mantém uma tabela de assinaturas de clientes filtrados a cada dia. A tabela de assinaturas é limpa todas as noites. A primeira vez que o cliente fizer uma solicitação na Internet depois de a tabela ser limpa fará seu endereço IP ser inserido na tabela.

Quando o número de clientes listados na tabela alcançar o nível da assinatura, qualquer cliente anteriormente não-listado que solicitar acesso à Internet excederá a assinatura. Se isso ocorrer, o cliente que exceder o nível de assinatura será bloqueado inteiramente na Internet ou receberá acesso não filtrado à Internet, dependendo da configuração definida. Do mesmo modo, quando a assinatura expirar, todos os clientes serão inteiramente bloqueados ou não filtrados, dependendo da configuração.

Para configurar o comportamento de filtragem quando uma assinatura for excedida ou expirar, consulte [Configurando as informações de sua conta](#), página 28.

Para configurar o software Websense para enviar avisos por e-mail quando a assinatura aproximar-se de seu limite ou excedê-lo, consulte [Configurando alertas do sistema](#), página 287.

O número de categorias filtradas dependerá de sua assinatura do Websense. O software Websense filtrará todos os sites em todas as categorias ativadas em sua aquisição.

## Gerenciando sua conta no Portal MyWebsense

A Websense, Inc., mantém um portal para clientes em [www.mywebsense.com](http://www.mywebsense.com) que você pode utilizar para acessar atualizações de produtos, patches, novidades sobre os produtos, avaliações e recursos de suporte técnico para seu software Websense.

Quando você criar uma conta, será solicitado que insira todas as chaves da assinatura do Websense. Isso ajudará a garantir seu acesso a informações, alertas e patches importantes para seu produto e sua versão do Websense.

Depois que tiver uma conta no MyWebsense, se você não conseguir fazer logon no Websense Manager por não lembrar da senha do WebsenseAdministrator,

simplesmente clique em **Esqueci minha senha** na página de logon do Websense Manager. Você será solicitado a fazer logon no MyWebsense, e receberá instruções para gerar e ativar uma nova senha.



### Importante

Quando você pedir uma nova senha, a chave de assinatura que selecionar no portal MyWebsense precisará corresponder à chave inserida na página Conta do Websense Manager.

Vários membros de sua empresa podem criar logons no MyWebsense associados à mesma chave de assinatura.

Para acessar o portal MyWebsense pelo Websense Manager, vá para **Ajuda > MyWebsense**.

## Ativando o Websense Web Protection Services™

As assinaturas do Websense Web Security incluem acesso aos Websense Web Protection Services: SiteWatcher™, BrandWatcher™ e ThreatWatcher™. Depois de ativados, esses serviços atuarão para proteger os sites da Web, as marcas e os servidores Web de sua empresa.

Serviço	Descrição
SiteWatcher	Alerta quando os sites da Web de sua empresa são infectados com códigos maliciosos, permitindo que você adote medidas imediatas para proteger os clientes existentes e potenciais, bem como os parceiros que visitem o site.
BrandWatcher	<ul style="list-style-type: none"> <li>Alerta quando os sites ou marcas de sua empresa são alvos de ataques de phishing ou keylogging.</li> <li>Fornecer inteligência de segurança de Internet, detalhes dos ataques e outras informações relacionadas à segurança, para que você possa tomar providências, notificar os clientes e minimizar qualquer impacto de relações públicas.</li> </ul>
ThreatWatcher	<ul style="list-style-type: none"> <li>Fornecer uma "visão do ponto de vista dos hackers" do servidor Web de sua empresa, verificando-o para identificar vulnerabilidades conhecidas e ameaças potenciais.</li> <li>Reporta os níveis de risco e oferece recomendações em um portal baseado na Web.</li> <li>Ajuda a impedir ataques maliciosos em servidores Web antes que ocorram.</li> </ul>

Faça logon no portal MyWebsense para ativar o Websense Protection Services. Depois que o ThreatWatcher estiver ativado, faça logon no MyWebsense para acessar os relatórios de ameaças para servidores Web registrados.

## Configurando as informações de sua conta

Tópicos relacionados:

- ◆ [Sua assinatura, página 26](#)
- ◆ [Configurando downloads do banco de dados, página 31](#)
- ◆ [Trabalhando com protocolos, página 182](#)

Use a página **Configurações > Conta** para entrar e visualizar as informações sobre a assinatura e alterar a senha do WebsenseAdministrator, utilizada para acessar o Websense Manager. WebsenseAdministrator é a conta administrativa mestre padrão usada para gerenciar o software Websense.

Também é aqui que você pode habilitar o software Websense para enviar dados de uso de protocolos para a Websense, Inc., anonimamente. Estas informações poderão ser usadas para atualizar o Websense Master Database, uma coleção de mais de 36 milhões de sites de Internet e mais de 100 definições de protocolo (consulte [O Websense Master Database, página 29](#), para obter mais informações).

1. Depois de instalar o software Websense ou quando receber uma nova chave de assinatura, use o campo **Chave de assinatura** para inserir a chave.  
Depois que você inserir a nova chave de assinatura e clicar em OK, o download do Master Database começará automaticamente.
2. Após o primeiro download do Master Database, as seguintes informações serão exibidas:

Chave expira em	Data final da sua assinatura atual. Após essa data, você precisará renovar a assinatura para continuar a fazer download do Master Database e filtragem de sua rede.
Usuários da rede com assinatura	Número de usuários na rede que podem ser filtrados.
Usuários remotos com assinatura	Número de usuários que podem ser filtrados fora da rede (requer o recurso opcional Remote Filtering).

3. Selecione **Bloquear usuários quando a assinatura vencer ou for excedida** para:
  - Bloquear todo o acesso à Internet para todos os usuários quando a assinatura vencer.
  - Bloquear todo o acesso à Internet de usuários que excedam o número de usuários com assinatura.

Se esta opção não estiver selecionada, os usuários terão acesso não filtrado à Internet nessas ocasiões.
4. Para alterar a senha do WebsenseAdministrator, primeiro forneça a senha atual e depois insira e confirme a nova senha.
  - A senha deve ter de 4 a 25 caracteres. Ela faz distinção entre maiúsculas e minúsculas, e pode incluir letras, números, caracteres especiais e espaços.

- É recomendável criar uma senha forte para a conta WebsenseAdministrator. A senha deve ter no mínimo 8 caracteres e incluir pelo menos uma letra maiúscula, uma letra minúscula, um número e um caractere especial.
5. Marque **Enviar dados de categoria e protocolo à Websense, Inc.** para que o software Websense colete dados de uso sobre as categorias e protocolos definidos pelo Websense, e os envie anonimamente para a Websense, Inc.
- Esses dados de uso ajudam a Websense, Inc., a aprimorar continuamente os recursos de filtragem do software Websense.

## O Websense Master Database

Tópicos relacionados:

- ◆ [Atualizações do banco de dados em tempo real](#), página 30
- ◆ [Atualizações de segurança em tempo real™](#), página 30
- ◆ [Filtragem de categorias e protocolos](#), página 36
- ◆ [Trabalhando com o Filtering Service](#), página 279
- ◆ [Verificar o status de download do Master Database](#), página 280
- ◆ [Downloads do Master Database que podem ser retomados](#), página 281

O Websense Master Database contém as definições de categoria e protocolo que fornecem a base de filtragem do conteúdo de Internet (consulte [Filtragem de categorias e protocolos](#), página 36).

- ◆ As **Categorias** são usadas para agrupar sites da Web (identificados pelo URL e pelo endereço IP) com conteúdo semelhante.
- ◆ As definições de **Protocolo** agrupam os protocolos de comunicação na Internet usados para fins semelhantes, como transferência de arquivos ou envio de mensagens instantâneas.

Uma versão limitada do banco de dados de filtragem é instalada durante a instalação do software Websense, mas recomenda-se fazer download do Master Database completo assim que possível para habilitar os recursos totais de filtragem da Internet. Para fazer download do Master Database pela primeira vez, insira sua chave de assinatura na página **Configurações > Conta** (consulte [Configurando as informações de sua conta](#), página 28).

Se o software Websense precisar passar por um proxy para fazer download, utilize também a página **Configurações > Download do banco de dados** para configurar as definições do proxy (consulte [Configurando downloads do banco de dados](#), página 31).

O processo de download do banco de dados completo poderá levar poucos minutos ou mais de 60 minutos, dependendo de fatores como velocidade de conexão de Internet, largura de banda, memória disponível e espaço livre em disco.

Após o download inicial, o software Websense fará download das alterações no banco de dados de acordo com o agendamento definido por você (consulte [Configurando downloads do banco de dados](#), página 31). Como o Master Database é atualizado freqüentemente, por padrão, os downloads do banco de dados são agendados para acontecer diariamente.

Se o Master Database for de mais de 14 dias atrás, o software Websense não filtrará solicitações de Internet.

Para iniciar um download de banco de dados a qualquer momento ou para visualizar o status do último download do banco de dados, a data do último download ou o número da versão atual do banco de dados, vá para **Status > Hoje** e clique em **Download do banco de dados**.

## Atualizações do banco de dados em tempo real

Além dos downloads agendados, o software Websense faz atualizações de emergência dos bancos de dados quando necessário. A atualização em tempo real pode ser usada, por exemplo, para recategorizar um site que tenha sido temporariamente categorizado de modo incorreto. Essas atualizações garantem que os sites e protocolos sejam filtrados de forma adequada.

O software Websense verifica as atualizações do banco de dados a cada hora.

As atualizações mais recentes são listadas na página **Status > Alertas** (consulte [Verificando o status atual do sistema](#), página 291).

## Atualizações de segurança em tempo real™

Além de receber as atualizações do banco de dados em tempo real padrão, os usuários do Websense Web Security poderão habilitar Atualizações de segurança em tempo real para receber atualizações do Master Database relacionadas à segurança assim que elas forem publicadas pela Websense, Inc.

As Atualizações de segurança em tempo real fornecem uma camada adicional de proteção contra ameaças à segurança da Internet. A instalação dessas atualizações assim que elas são publicadas reduz a vulnerabilidade a novos golpes de phishing (fraude de identidade), aplicativos nocivos e códigos maliciosos que infectam os principais sites ou aplicativos da Web.

O Filtering Service verifica as atualizações de segurança a cada 5 minutos. Porém, como as atualizações são enviadas apenas quando ocorrem ameaças à segurança, as alterações efetivas são eventuais e tendem a não interromper a atividade normal da rede.

Use a página **Configurações > Download do banco de dados** para habilitar Atualizações de segurança em tempo real (consulte [Configurando downloads do banco de dados](#), página 31).

## Configurando downloads do banco de dados

Tópicos relacionados:

- ◆ [Configurando as informações de sua conta](#), página 28
- ◆ [O Websense Master Database](#), página 29
- ◆ [Verificar o status de download do Master Database](#), página 280

Use a página **Configurações > Download do banco de dados** para definir o agendamento para downloads automáticos do Master Database. Forneça também informações importantes sobre qualquer servidor proxy ou firewall pelo qual o software Websense tenha que passar para fazer download do banco de dados.

1. Selecione os **Dias de download** para downloads automáticos.

Você precisa fazer download do Master Database pelo menos a cada 14 dias para que o software Websense continue filtrando ininterruptamente. Se você desmarcar todos os dias de download, o software Websense tentará automaticamente fazer download quando o banco de dados tiver completado 7 dias.



**Obs.:**

Os dias de download estarão desabilitados quando as Atualizações de segurança em tempo real estiver habilitadas (consulte [Etapa 3](#)). Os downloads são executados automaticamente todos os dias para garantir que o banco de dados padrão mais atualizado esteja disponível para as atualizações de segurança.

2. Selecione a hora inicial (**De**) e a hora final (**Até**) do **Cronograma de download**. Se nenhuma hora for selecionada, o download do banco de dados ocorrerá entre 21h (9 horas da noite) e 6h (6 horas da manhã).

O software Websense selecionará uma hora aleatória durante esse período para entrar em contato com o servidor do Master Database. Para configurar alertas de falhas de download, consulte [Configurando alertas do sistema](#), página 287.



**Obs.:**

Depois do download do Master Database ou das atualizações, o uso da CPU pode alcançar 90% enquanto o banco de dados estiver sendo carregado na memória local.

3. (*Websense Web Security*) Selecione **Habilitar Atualizações de segurança em tempo real** para que o software Websense verifique as atualizações de segurança para o Master Database a cada 5 minutos. Quando uma atualização de segurança for detectada, seu download ocorrerá imediatamente.

As atualizações de segurança em tempo real protegem rapidamente a sua rede contra a vulnerabilidade a ameaças como novos golpes de phishing (fraude de identidade), aplicativos nocivos e códigos maliciosos que infectam os principais sites ou aplicativos da Web.

4. Selecione **Usar servidor proxy ou firewall** se o software Websense precisar acessar a Internet passando por um servidor proxy ou de um firewall de proxy (diferente do produto de integração com o qual o software Websense se comunica) para fazer download do Master Database. Em seguida, configure o seguinte:

Nome ou IP do servidor	Insira o endereço IP ou o nome do computador que está hospedando o servidor proxy ou firewall.
Porta	Insira o número da porta pela qual o download do banco de dados deve passar (o padrão é 8080).

5. Se o servidor proxy ou firewall configurado na etapa 4 exigir autenticação para acessar a Internet, selecione **Usar autenticação** e, em seguida, insira o **Nome de usuário** e a **Senha** que o software Websense deverá usar para ter acesso à Internet.



**Obs.:**

Se a opção Usar autenticação estiver selecionada, o servidor proxy ou firewall precisará estar configurado para aceitar texto não criptografado ou autenticação básica para habilitar os downloads do Master Database.

Por padrão, o nome do usuário e a senha são codificados para corresponder ao conjunto de caracteres da região da máquina do Policy Server. Esta codificação pode ser configurada manualmente na página **Configurações > Serviços de diretório** (consulte [Configurações avançadas de diretório](#), página 63).

## Testando a configuração da rede

---

Para que a filtragem de solicitações de Internet ocorra, o software Websense precisa conhecer o tráfego de Internet de/para os computadores em sua rede. Use o Detector de tráfego de rede para garantir que essa comunicação de Internet esteja visível para o software de filtragem. Consulte [Verificando a configuração do Network Agent](#), página 346, para obter instruções.

Se o detector de tráfego não conseguir ver todos os segmentos de sua rede, consulte [Configuração da rede](#), página 337, para obter instruções de configuração.

## Suporte Técnico da Websense

---

A Websense, Inc., tem um compromisso com a satisfação do cliente. Vá ao site do Suporte Técnico da Websense a qualquer momento para obter informações sobre a

versão mais recente, acessar a Base de conhecimentos, a documentação do produto ou criar uma solicitação de suporte.

[www.websense.com/SupportPortal/](http://www.websense.com/SupportPortal/)

O tempo de resposta para solicitações on-line durante o horário comercial é de aproximadamente 4 horas. As solicitações fora do horário comercial serão respondidas no dia útil seguinte.

Também está disponível o atendimento por telefone. Para respostas rápidas e eficazes no atendimento telefônico, tenha em mãos o seguinte:

- ◆ Chave de assinatura do Websense
- ◆ Acesso ao Websense Manager
- ◆ Acesso aos computadores que executam o Filtering Service e o Log Server, e ao servidor do banco de dados (Microsoft SQL Server ou MSDE)
- ◆ Permissão para acessar o banco de dados do Websense
- ◆ Familiaridade com a sua arquitetura de rede, ou acesso a um especialista
- ◆ Especificações de computadores que executam Filtering Service e Websense Manager
- ◆ Uma lista de outros aplicativos que estão sendo executados no computador do Filtering Service

Para problemas graves, talvez sejam necessárias informações adicionais.

O atendimento telefônico padrão está disponível durante o horário comercial normal, de segunda-feira a sexta-feira, nos seguintes números:

- ◆ San Diego, Califórnia, EUA: **+1 858.458.2940**
- ◆ Londres, Inglaterra: **+44 (0) 1932 796244**

Consulte o site de suporte listado acima para ver o horário de funcionamento e outras opções de suporte.

Os clientes no Japão devem entrar em contato com seus distribuidores para um serviço mais rápido.



# 2

## Filtros de uso da Internet

Tópicos relacionados:

- ◆ [Filtragem de categorias e protocolos](#), página 36
- ◆ [Trabalhando com filtros](#), página 46
- ◆ [Definindo configurações de filtragem do Websense](#), página 54
- ◆ [Diretivas de filtragem da Internet](#), página 71
- ◆ [Refinar as diretivas de filtragem](#), página 165

O acesso do usuário à Internet é controlado por diretivas. Uma diretiva é uma programação que informa ao software Websense como e quando filtrar o acesso a sites da Web e aplicativos da Internet. Em termos mais simples, as diretivas são formadas por:

- ◆ **Filtros de categoria**, usados para aplicar ações (Permitir, Bloquear) a categorias de sites da Web.
- ◆ **Filtros de protocolo**, usados para aplicar ações a aplicativos da Internet e a protocolos não-HTTP.
- ◆ Uma programação que determina quando cada filtro é aplicado.

A filtragem baseada em diretivas permite que você atribua aos clientes (usuários, grupos e computadores da rede) diferentes níveis de acesso à Internet. Primeiro, crie filtros para definir restrições exatas de acesso à Internet e, depois, utilize-os para construir uma diretiva.

Na primeira vez em que é instalado, o software Websense cria uma diretiva **Padrão** e a utiliza para começar a monitorar solicitações da Internet assim que uma chave de assinatura é inserida (consulte [A diretiva Padrão](#), página 72). Inicialmente, a diretiva Padrão permite todas as solicitações.



---

**Obs.:**

No caso de atualização de uma versão anterior do software Websense, as configurações das diretivas existentes são preservadas. Depois da atualização, revise suas diretivas para ter certeza de que ainda são apropriadas.

---

Para aplicar restrições de filtragem distintas a diferentes clientes, defina filtros de categoria. Você poderia definir o seguinte:

- ◆ Um filtro de categoria que bloqueie o acesso a todos os sites da Web, exceto àqueles das categorias Negócios e economia, Educação e Notícias e mídia.
- ◆ Um segundo filtro de categoria que permita todos os sites da Web, exceto os que representem um risco de segurança e os que contenham material para adultos.
- ◆ Um terceiro filtro de categoria que monitore o acesso a sites da Web sem bloqueá-los (consulte [Criando um filtro de categoria](#), página 47)

Para acompanhar esses filtros de categoria, você poderia definir:

- ◆ Um filtro de protocolo que bloqueie o acesso a grupos de protocolos de streaming media, mensagens instantâneas e bate-papo, Compartilhamento de arquivos P2P e Proxy Avoidance.
- ◆ Um segundo filtro de protocolo que permita todos os protocolos não-HTTP, exceto os que estiverem associados a proxy avoidance.
- ◆ Um terceiro filtro de protocolo que permita todos os protocolos não-HTTP (consulte [Criando um filtro de protocolo](#), página 49).

Após definir um conjunto de filtros que correspondam às regras de acesso à Internet da sua organização, você poderá adicioná-los a diretivas e aplicá-los aos clientes (consulte [Diretivas de filtragem da Internet](#), página 71).

## Filtragem de categorias e protocolos

---

O Websense Master Database organiza sites da Web semelhantes (identificados por URLs e endereços IP) em **categorias**. Cada categoria tem um nome descritivo, como Material para adultos, Jogos de azar ou Compartilhamento de arquivos P2P. Você também pode criar suas próprias categorias personalizadas para grupos de sites que sejam de interesse específico da sua organização (consulte [Criando uma categoria personalizada](#), página 176). Juntas, as categorias do Master Database e as definidas pelo usuário formam a base da filtragem na Internet.

A Websense, Inc. não faz julgamentos de valor sobre as categorias ou os sites no Master Database. As categorias são desenvolvidas para criar agrupamentos úteis de sites que sejam de interesse dos assinantes. O objetivo não é caracterizar qualquer site ou grupo de sites, ou as pessoas ou interesses que os publicam, e as categorias não devem ser interpretadas desta forma. Da mesma forma, os rótulos vinculados às categorias do Websense são formas abreviadas e práticas e não têm por finalidade transmitir qualquer opinião ou atitude (nem devem ser criados com essa finalidade) aprovando ou não o assunto ou os sites classificados.

A lista atualizada de categorias do Master Database está disponível em:

[www.websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php](http://www.websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php)

Para sugerir que um site seja incluído no Master Database, clique em **Sugerir nova categoria** no painel de atalho do lado direito do Websense Manager ou acesse:

[www.websense.com/SupportPortal/SiteLookup.aspx](http://www.websense.com/SupportPortal/SiteLookup.aspx)

Depois de fazer logon no portal MyWebsense, você acessará a ferramenta Site Lookup and Category Suggestion (Pesquisa no site e sugestão de categoria).

Quando cria um **filtro de categoria** no Websense Manager, você escolhe quais categorias deseja bloquear e quais deseja permitir.

Além de abranger categorias de URL, o Websense Master Database também contém grupos de protocolos usados para gerenciar tráfego não-HTTP da Internet. Cada grupo de protocolos define tipos semelhantes de protocolos de Internet (como FTP ou IRC) e aplicativos (como AOL Instant Messenger ou BitTorrent). As definições são verificadas e atualizadas todas as noites.

Assim como acontece com as categorias, você também pode definir protocolos personalizados para utilizá-los na filtragem de Internet.

A lista atualizada de protocolos do Master Database está disponível em:

[www.websense.com/global/en/ProductsServices/MasterDatabase/ProtocolCategories.php](http://www.websense.com/global/en/ProductsServices/MasterDatabase/ProtocolCategories.php)

Ao criar um **filtro de protocolo**, você escolhe quais protocolos deseja bloquear e quais deseja permitir.



**Obs.:**

Para habilitar a filtragem baseada em protocolos, é necessário que o Network Agent esteja instalado.

Alguns protocolos definidos pelo Websense permitem o bloqueio de tráfego de saída da Internet destinado a um servidor externo (por exemplo, um servidor específico de mensagens instantâneas). Somente os protocolos definidos pelo Websense com números de portas atribuídos dinamicamente poderão ser bloqueados como tráfego de saída.

### Novas categorias e protocolos

Quando novas categorias e novos protocolos são adicionados ao Master Database, é designada a cada um deles uma ação de filtragem padrão, como **Permitir** ou **Bloquear** (consulte *Ações de filtragem*, página 42).

- ◆ A ação padrão é aplicada a todos os filtros ativos de categoria e protocolo (consulte *Trabalhando com filtros*, página 46). Para alterar a maneira como a categoria ou o protocolo é filtrado, edite os filtros ativos.
- ◆ A ação padrão baseia-se no feedback sobre se os sites ou protocolos em questão são ou não geralmente considerados apropriados aos negócios.

Você pode configurar o Websense para gerar um alerta do sistema e notificá-lo toda vez que novas categorias ou protocolos forem adicionados ao Master Database. Para obter mais informações, consulte *Alertas*, página 284.

## Categorias especiais

O Master Database contém categorias especiais para ajudar a gerenciar tipos específicos de uso da Internet. As categorias a seguir estão disponíveis em todas as edições do software Websense:

- ◆ A categoria **Eventos especiais** é usada para classificar sites considerados como tópicos importantes. Isso ajuda a gerenciar aumentos repentinos relacionados a eventos no tráfego da Internet. Por exemplo, o site oficial da Copa do Mundo normalmente pode aparecer na categoria Esportes, mas ser transferido para a categoria Eventos especiais durante as finais do campeonato.  
As atualizações na categoria Eventos especiais são adicionadas ao Master Database durante os downloads programados. Os sites permanecem nessa categoria durante um curto período de tempo, após o qual são transferidos para outra categoria ou são excluídos do Master Database.
- ◆ A categoria **Produtividade** tem como objetivo evitar comportamentos de perda de tempo.
  - Anúncios
  - Download de freeware/software
  - Mensagens Instantâneas
  - Corretagem de ações on-line
  - Pay-to-Surf
- ◆ A categoria **Largura de banda** concentra-se na economia de largura da banda da rede.
  - Rádio e TV pela Internet
  - Telefonia pela Internet
  - Compartilhamento de arquivos P2P
  - Armazenamento/backup pessoal em rede
  - Streaming Media

O Websense Web Security inclui outras categorias de segurança:

- ◆ O **Websense Security Filtering** (também conhecido simplesmente como **Security**) concentra-se em sites da Internet que contêm código malicioso e são capazes de enganar os programas de detecção de vírus. Por padrão, os sites desta categoria são bloqueados.
  - Redes bot
  - Keyloggers
  - Websites nocivos
  - Phishing e outras fraudes
  - Softwares potencialmente indesejados
  - Spyware
- ◆ A **Proteção estendida** concentra-se nos sites da Web que provavelmente contêm código malicioso. Por padrão, os sites nas subcategorias Exposição elevada e Exploits emergentes são bloqueados.

- A subcategoria **Exposição elevada** contém sites que camuflam sua verdadeira natureza ou identidade ou, ainda, com elementos que sugerem uma intenção potencialmente maliciosa.
- A subcategoria **Exploits emergentes** contém sites identificados como hospedeiros de código de exploit conhecido e potencial.
- A subcategoria **Conteúdo potencialmente perigoso** inclui sites que provavelmente apresentam conteúdo pouco útil ou inútil.

O grupo Proteção estendida filtra sites da Web potencialmente maliciosos com base na *reputação*. A reputação do site baseia-se em sinais anteriores de atividade potencialmente maliciosa. Um invasor poderia mirar em um URL que contivesse erros ortográficos comuns, por exemplo, ou que tivesse outras semelhanças com um URL legítimo. Esse site, então, poderia ser usado para distribuir malware a usuários antes de os filtros tradicionais poderem ser atualizados para identificar o site como malicioso.

Quando a pesquisa de segurança do Websense detecta uma ameaça potencial, ela é adicionada à categoria Proteção estendida até o Websense estar totalmente certo sobre a classificação final do site.

## Classes de risco

Tópicos relacionados:

- ◆ [Atribuindo categorias a classes de risco](#), página 302
- ◆ [Relatórios de apresentação](#), página 96
- ◆ [Relatórios investigativos](#), página 115

O Websense Master Database agrupa as categorias em **classes de risco**. As classes de risco sugerem tipos ou níveis possíveis de vulnerabilidades geradas pelos sites que estão no grupo de categorias.

As classes de risco são usadas principalmente na geração de relatórios. As páginas Hoje e Histórico contêm gráficos que exibem a atividade na Internet por classe de risco. É possível gerar relatórios de apresentação ou relatórios investigativos organizados por classe de risco.

As classes de risco também podem ser úteis na criação de filtros de risco. Por exemplo, inicialmente, o filtro de categoria Segurança básica bloqueia todas as categorias padrão na classe Risco de segurança. Você poderá usar os agrupamentos da classe de risco como uma diretriz quando estiver criando seus próprios filtros de categoria; isso irá ajudá-lo a determinar se uma categoria deve ser permitida, bloqueada ou limitada de alguma forma.

O software Websense contém cinco classes de risco, que são listadas a seguir. Por padrão, o software Websense agrupa as seguintes categorias em cada classe de risco.

- ◆ Uma categoria pode aparecer em várias classes de risco ou não ser atribuída a nenhuma classe de risco.
- ◆ Os agrupamentos podem ser alterados periodicamente no Master Database.

### **Responsabilidade legal**

Material para adultos (inclusive Conteúdo adulto, Lingerie e roupas de banho, Nudez, Sexo)  
Largura de banda > Compartilhamento de arquivos P2P  
Jogos de azar  
Ilegal ou questionável  
Tecnologia da Informação > Hacking e Proxy Avoidance  
Militantes e extremistas  
Racismo e ódio  
Mau gosto  
Violência  
Armas

### **Perda de largura de banda de rede**

Largura de banda (inclusive Rádio e TV pela Internet, Telefonia pela Internet, Compartilhamento de arquivos P2P, Armazenamento/backup pessoal em rede, Streaming Media)  
Entretenimento > Serviços de Download de MP3 e Áudio  
Produtividade > Anúncios e download de freeware e software

### **Uso empresarial**

Negócios e economia (inclusive Informações e serviços financeiros)  
Educação > Materiais educacionais e Materiais de referência  
Governo (inclusive Militares)  
Tecnologia da Informação (inclusive Segurança da Informação, Portais e mecanismos de pesquisa e sites de tradução de URLs)  
Viagens  
Veículos

### **Risco de segurança**

Largura de banda > Compartilhamento de arquivos P2P  
Proteção estendida (inclusive Exposição elevada, Exploits emergentes e Conteúdo potencialmente perigoso) [*Websense Web Security*]  
Tecnologia da Informação > Hacking e Proxy Avoidance  
Produtividade > Download de freeware/software  
Segurança (inclusive Redes bot, Keyloggers, Websites nocivos, Phishing e outras fraudes, Softwares potencialmente indesejados e Spyware)

## Perda de produtividade

Aborto (inclusive Pró-escolha e Pró-vida)  
 Material para adultos > Educação sexual  
 Grupos de defesa  
 Largura de banda > Rádio e TV pela Internet, Compartilhamento de arquivos P2P e Streaming Media)  
 Drogas (inclusive Abuso de drogas, Maconha, Remédios com receita e Suplementos e compostos não regulados)  
 Educação (inclusive Instituições culturais e Instituições educacionais)  
 Entretenimento (inclusive Serviços de Download de MP3 e Áudio)  
 Jogos de azar  
 Jogos  
 Governo > Organizações políticas  
 Saúde  
 Tecnologia da Informação > Web Hosting  
 Comunicação na Internet (inclusive Email geral, Email organizacional, Mensagens de texto e mídia e Bate-papo)  
 Procura de emprego  
 Notícias e mídia (inclusive Periódicos alternativos)  
 Produtividade (inclusive Download de freeware/software, Mensagens instantâneas, Quadros de mensagens e fóruns, Corretagem de ações on-line, Pay-to-Surf)  
 Religião (inclusive Religiões não tradicionais, Ocultismo e folclore e Religiões tradicionais)  
 Compras (inclusive Leilões na Internet e Imóveis)  
 Organizações sociais (inclusive Organizações de profissionais e trabalhadores, Organizações filantrópicas e de serviços e Organizações sociais e associações)  
 Sociedade e estilo de vida (inclusive Álcool e tabaco, Gays, lésbicas ou bissexuais, Hobbies, Classificados pessoais e encontros, Restaurantes e jantares e Relacionamento sociais e sites pessoais)  
 Eventos especiais  
 Esportes (inclusive Clubes de caça esportiva e armas)  
 Viagens  
 Veículos

Os Super administradores podem alterar as categorias designadas a cada classe de risco na página **Configurações > Classe de risco** (consulte [Atribuindo categorias a classes de risco](#), página 302).

## Grupos de protocolos de segurança

Além das categorias Segurança e Proteção estendida, o Websense Web Security contém dois protocolos desenvolvidos para ajudar na detecção de spyware e de conteúdo ou código malicioso transmitido na Internet.

- ◆ O grupo de protocolos **Tráfego malicioso** inclui o protocolo **Redes bot**, que tem por objetivo bloquear tráfego de comando e controle gerado por um bot que tenta se conectar com uma rede bot para fins maliciosos.
- ◆ O grupo de protocolos **Tráfego malicioso (somente monitoramento)** é usado para identificar tráfego que pode estar associado a um software malicioso.
  - O protocolo **Worms de email** monitora tráfego SMTP de saída que pode ser gerado por um ataque de worm por email.
  - O protocolo **Outros tráfegos maliciosos** monitora tráfego de entrada ou saída suspeito de conexão com aplicativos maliciosos.

Por padrão, o grupo de protocolos Tráfego malicioso está bloqueado e pode ser configurado em seus filtros de protocolos (consulte [Editando um filtro de protocolo](#), página 50). Os protocolos de Tráfego malicioso (somente monitoramento) podem ser registrados para fins de relatórios, mas não é possível aplicar nenhuma outra ação de filtragem.

## Instant Messaging Attachment Manager

O Instant Messaging (IM) Attachment Manager é um recurso opcional. Se assiná-lo, você poderá restringir o compartilhamento de arquivos com clientes de mensagens instantâneas, inclusive de AOL/ICQ, Microsoft (MSN) e Yahoo. Dessa forma, você permite o tráfego de mensagens instantâneas, mas bloqueia a transferência de anexos por esses clientes.

Arquivos anexos em mensagens instantâneas é um grupo de protocolos que contém definições para vários clientes de mensagens instantâneas. Quando o IM Attachment Manager está habilitado, esses protocolos aparecem na lista de protocolos em todos os filtros de protocolos habilitados, bem como na página Editar protocolos.

A filtragem de anexos de mensagens instantâneas pode ser aplicada tanto ao tráfego interno quanto ao externo. Para habilitar a filtragem de tráfego interno, acesse a página **Configurações > Network Agent > Configurações globais** e defina a parte da sua rede que será monitorada (consulte [Definindo as configurações globais](#), página 340).

## Ações de filtragem

---

Os filtros de categoria e protocolo designam uma **ação** a cada categoria ou protocolo. É essa ação que o software de filtragem da Websense adota em resposta a uma solicitação da Internet de um cliente. Estas são as ações que se aplicam tanto às categorias quanto aos protocolos:

- ◆ **Bloquear** a solicitação. Os usuários recebem uma página ou mensagem de bloqueio e não conseguem exibir o site ou usar o aplicativo da Internet.
- ◆ **Permitir** a solicitação. Os usuários conseguem exibir o site ou usar o aplicativo da Internet.

- ◆ Avaliar o uso atual de **largura de banda** antes de bloquear ou permitir a solicitação. Quando esta ação está habilitada e o uso da largura de banda atinge um limite específico, as próximas solicitações da Internet a uma categoria ou protocolo específico são bloqueadas. Consulte [Usando o Bandwidth Optimizer para gerenciar a largura de banda](#), página 189.

Ações adicionais podem ser aplicadas somente a categorias.



**Obs.:**

As opções Confirmar e Cota não devem ser usadas quando clientes individuais (usuários, grupos e computadores) são gerenciados por vários Policy Servers.

As informações de tempo associadas a esses recursos não são compartilhadas entre os Policy Servers e é possível que seja concedido aos clientes mais ou menos acesso à Internet do que você pretendia.

- ◆ **Confirmar** – os usuários recebem uma página de bloqueio, solicitando que confirmem se o site está sendo acessado para fins de negócios. Se o usuário clicar em **Continuar**, ele poderá ver o site.

Um clique no botão Continuar ativa um temporizador. Durante o período de tempo configurado (por padrão, 60 segundos), o usuário pode visitar outros sites da categoria Confirmar sem receber outra página de bloqueio. Quando esse período de tempo terminar, o usuário receberá uma página de bloqueio ao tentar acessar qualquer outro site da categoria Confirmar.

O tempo padrão pode ser alterado na página **Configurações > Filtragem**.

- ◆ **Cota** – os usuários recebem uma página de bloqueio, perguntando se desejam usar o tempo da cota para acessar o site. Se o usuário clicar em **Utilizar cota de tempo**, ele poderá ver o site.

Um clique no botão Utilizar cota de tempo inicializa dois temporizadores: um temporizador de sessão de cota e um temporizador de alocação de cota total.

- Se o usuário solicitar mais sites de cota durante um período de **sessão** padrão (10 minutos é o padrão), ele poderá acessar esses sites sem receber outra página de bloqueio.
- O tempo de cota **total** é alocado em uma base diária. Depois que o tempo for consumido, cada cliente deverá esperar até o dia seguinte para poder acessar os sites das categorias da cota. A alocação de cota diária padrão (60 minutos é o padrão) é definida na página **Configurações > Filtragem**. As alocações de cota diária também podem ser concedidas aos clientes em uma base individual. Para obter mais informações, consulte [Usando o tempo da cota para limitar o acesso à Internet](#), página 44,.
- ◆ **Bloquear palavras-chave** – quando você definir palavras-chave e habilitar o bloqueio por palavras-chave, os usuários que estiverem solicitando acesso a um site cujo URL contém uma palavra-chave bloqueada não terão permissão para acessar esse site. Consulte [Filtrando com base em palavras-chave](#), página 177.

- ◆ **Bloquear tipos de arquivo** – quando o bloqueio por tipo de arquivo estiver habilitado, os usuários que estiverem tentando fazer download de um arquivo cujo tipo está bloqueado receberão uma página de bloqueio. Nesse caso, o download do arquivo não será feito. Consulte [Gerenciando o tráfego com base no tipo de arquivo, página 191](#).

## Usando o tempo da cota para limitar o acesso à Internet

Quando um usuário clica em Utilizar cota de tempo, ele consegue ver sites de qualquer categoria de cota até a sessão da cota terminar. O tempo da sessão de cota padrão (configurado na página **Configurações > Filtragem**) é 10 minutos.



### Obs.:

A opção Cota não deve ser usada quando clientes individuais são gerenciados por vários Policy Servers.

As informações de tempo associadas a esse recurso não são compartilhadas entre os Policy Servers e é possível que seja concedido aos clientes mais ou menos acesso à Internet do que você pretendia.

Quando a sessão de cota termina, uma solicitação para um site de cota resulta em outra mensagem de bloqueio de cota. Os usuários que ainda não tiverem esgotado sua alocação de cota diária poderão iniciar uma nova sessão de cota.

Quando o tempo de cota está configurado, o software Websense usa uma lista de prioridade para determinar como responder quando um usuário solicita um site de uma categoria de cota. O software procura o tempo de cota configurado para:

1. O usuário
2. O computador ou cliente da rede
3. Os grupos a que o usuário pertence

Se um usuário for membro de vários grupos, o software Websense concederá o tempo de cota de acordo com a configuração **Utilizar bloqueio mais restritivo** definida na página **Configurações > Filtragem** (consulte [Definindo configurações de filtragem do Websense, página 54](#)).

4. Tempo de cota padrão

Os applets de Internet (por exemplo, applets Java ou Flash) podem não responder conforme esperado às restrições de tempo da cota. Mesmo que seja acessado de um site com restrição por cota, um applet que seja executado no navegador pode continuar sendo executado além do tempo configurado da sessão de cota.

Isso acontece porque o download desses applets é todo feito em um computador cliente, sendo executado como aplicativo, ou seja, sem se comunicar de volta com o servidor host original. No entanto, se o usuário clicar no botão Atualizar do navegador, o software Websense detectará a comunicação com o servidor host e bloqueará a solicitação de acordo com as restrições de cota aplicáveis.

## Acesso com senha

O Acesso com senha permite que usuários com senhas válidas acessem sites bloqueados pelo Websense. Ela pode ser concedida a clientes individuais (usuários, grupos, computadores ou redes).

Quando a opção de acesso com senha está habilitada, as mensagens de bloqueio do Websense apresentam um campo de senha. Os clientes que digitarem uma senha válida poderão acessar sites bloqueados durante um período de tempo específico.

**Obs.:**

A opção de acesso com senha não deve ser usada quando clientes individuais são gerenciados por vários Policy Servers.

As informações de tempo associadas a esse recurso não são compartilhadas entre os Policy Servers e é possível que seja concedido aos clientes mais ou menos acesso à Internet do que você pretendia.

A opção de acesso com senha é habilitada na página **Configurações > Filtragem** (consulte [Definindo configurações de filtragem do Websense](#), página 54).

Os privilégios de acesso com senha são concedidos a clientes específicos na página **Gerenciamento de diretivas > Clientes** (consulte [Adicionando um cliente](#), página 66, ou [Alterando configurações de cliente](#), página 68).

## Filtragem de pesquisa

A filtragem de pesquisa é um recurso oferecido por alguns mecanismos de pesquisa que ajuda a limitar o número de resultados de pesquisa inadequados que são exibidos aos usuários.

De um modo geral, os resultados dos mecanismos de pesquisa na Internet podem incluir miniaturas associadas aos sites que correspondem aos critérios de pesquisa. Se essas miniaturas estiverem associadas a sites bloqueados, o software Websense impede os usuários de acessarem o site completo, mas não impede que o mecanismo de pesquisa exiba a imagem.

Quando você habilita a filtragem de pesquisa, o software Websense ativa um recurso do mecanismo de pesquisa que impede a exibição de miniaturas associadas a sites bloqueados nos resultados da pesquisa. A habilitação da filtragem de pesquisa afeta tanto os clientes de filtragem locais quanto os remotos.

A Websense, Inc. mantém um banco de dados de mecanismos de pesquisa com recursos da filtragem de pesquisa. Quando um mecanismo de pesquisa é adicionado ou removido do banco de dados, é gerado um alerta (consulte [Alertas](#), página 284).

A filtragem de pesquisa é habilitada na página **Configurações > Filtragem**. Consulte [Definindo configurações de filtragem do Websense](#), página 54, para obter mais informações.

## Trabalhando com filtros

---

Tópicos relacionados:

- ◆ [Filtragem de categorias e protocolos](#), página 36
- ◆ [Diretivas de filtragem da Internet](#), página 71
- ◆ [Criando um filtro de categoria](#), página 47
- ◆ [Criando um filtro de protocolo](#), página 49
- ◆ [Criando um filtro de acesso limitado](#), página 168

Utilize a página **Gerenciamento de diretivas > Filtros** no Websense Manager para exibir, criar e modificar filtros de categoria e protocolo, bem como para trabalhar com outras ferramentas de filtragem.

A página Filtros está dividida em três seções principais:

- ◆ Os **filtros de categoria** determinam quais categorias serão bloqueadas e quais serão permitidas.
- ◆ Os **filtros de protocolo** determinam quais protocolos não-HTTP serão bloqueados e quais serão permitidos.  
Para habilitar a filtragem baseada em protocolos, é necessário que o Network Agent esteja instalado.
- ◆ Os **filtros de acesso limitado** definem uma lista restritiva de sites da Web permitidos (consulte [Restringindo usuários a uma lista definida de sites de Internet](#), página 166).

Os filtros de categoria, protocolo e acesso limitado são os fundamentos das **diretivas**. Cada diretiva é formada por no mínimo um filtro de categoria ou um filtro de acesso limitado e por um filtro de protocolo, aplicado a clientes selecionados em uma programação específica.

- ◆ Para revisar ou editar um filtro existente de categoria, protocolo ou acesso limitado, clique no nome do filtro. Para obter mais informações, consulte:
  - [Editando um filtro de categoria](#), página 48
  - [Editando um filtro de protocolo](#), página 50
  - [Editando um filtro de acesso limitado](#), página 168
- ◆ Para criar um novo filtro de categoria, protocolo ou acesso limitado, clique em **Adicionar**. Para obter mais informações, consulte:
  - [Criando um filtro de categoria](#), página 47
  - [Criando um filtro de protocolo](#), página 49
  - [Criando um filtro de acesso limitado](#), página 168

Para duplicar um filtro existente, marque a caixa de seleção ao lado do nome do filtro e clique em **Copiar**. A cópia recebe o nome do filtro original com um número anexo,

para fins de exclusividade, e é adicionada à lista de filtros. Edite a cópia da mesma maneira que faria com qualquer outro filtro.

Se você tiver criado funções de administração delegada (consulte [Administração delegada](#), página 235), os Super administradores poderão copiar as diretivas criadas para outras funções para serem usadas por administradores delegados.

Para copiar filtros em outra função, marque primeiro a caixa de seleção ao lado do nome do filtro e clique em **Copiar para função**. Consulte [Copiando filtros e diretivas para funções](#), página 170, para obter mais informações.

## Criando um filtro de categoria

Tópicos relacionados:

- ◆ [Trabalhando com filtros](#), página 46
- ◆ [Editando um filtro de categoria](#), página 48

Utilize a página **Gerenciamento de diretivas > Filtros > Adicionar filtro de categoria** para criar um novo filtro de categoria. Você pode trabalhar a partir de um modelo predefinido ou criar uma cópia de um filtro de categoria existente para usar como base para o novo filtro.

1. Insira um nome exclusivo em **Nome do filtro**. O nome de diretiva deve ter de 1 a 50 caracteres e não pode incluir nenhum destes caracteres:  
 \* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,  
 Os nomes de filtro podem incluir espaços, traços e apóstrofes.
2. Insira uma **Descrição** resumida do filtro. Essa descrição aparece ao lado do nome do filtro na seção Filtros de categoria da página Filtros; deve explicar a finalidade do filtro.  
 As restrições de caracteres aplicáveis a nomes de filtro também são aplicadas a descrições, com 2 exceções: as descrições podem incluir pontos (.) e vírgulas (,).
3. Selecione uma entrada na lista suspensa para determinar se usará um modelo ou criará uma cópia de um filtro existente. Para obter mais informações sobre modelos, consulte [Modelos de filtros de categoria e protocolo](#), página 53.
4. Para ver e editar o novo filtro, clique em **OK**. O filtro é adicionado à lista **Filtros de categoria** na página Filtros.

Para personalizar o filtro, clique no nome dele e passe para a seção [Editando um filtro de categoria](#).

## Editando um filtro de categoria

Tópicos relacionados:

- ◆ [Filtragem de categorias e protocolos](#), página 36
- ◆ [Ações de filtragem](#), página 42
- ◆ [Usando o tempo da cota para limitar o acesso à Internet](#), página 44
- ◆ [Acesso com senha](#), página 45
- ◆ [Trabalhando com filtros](#), página 46
- ◆ [Trabalhando com categorias](#), página 173

Utilize a página **Gerenciamento de diretivas > Filtros > Editar filtro de categoria** para fazer alterações nos filtros de categoria existentes.



### Importante

Quando você edita um filtro de categoria, as alterações afetam cada diretiva que aplica o filtro.

As diretivas que aplicam um filtro de categoria com o mesmo nome em outra função de administração delegada não são afetadas.

O nome e a descrição do filtro aparecem na parte superior da página.

- ◆ Clique em **Renomear** para alterar o nome do filtro.
- ◆ Basta digitar no campo **Descrição** para alterar a descrição do filtro.

O número ao lado de **Diretivas que usam este filtro** indica quantas diretivas usam o filtro selecionado. Se o filtro de categoria estiver habilitado, clique em **Ver diretivas** para ver uma lista de diretivas que aplicam o filtro.

A parte inferior da página mostra uma lista de categorias e as ações aplicadas no momento a cada uma delas.

1. Selecione uma entrada na lista **Categorias** para ver informações sobre a categoria ou para alterar a ação de filtragem associada à categoria selecionada.
2. Antes de fazer alterações na ação aplicada a uma categoria, utilize a seção **Detalhes da categoria** para revisar quaisquer atributos especiais associados à categoria.
  - Para revisar URLs recategorizados ou não filtrados designados à categoria, se houver, clique em **Consulte URLs personalizados nesta categoria**. Consulte [Redefinindo a filtragem de sites específicos](#), página 180.
  - Para avaliar palavras-chave designadas à categoria, clique em **Consulte palavras-chave nesta categoria**. Consulte [Filtrando com base em palavras-chave](#), página 177.

- Para avaliar expressões comuns utilizadas para definir palavras-chave ou URLs personalizados para a categoria, clique em **Consulte expressões regulares nesta categoria**.
3. Utilize os botões na parte inferior da lista de categorias para alterar a ação aplicada à categoria selecionada. Para obter mais informações sobre as ações disponíveis, consulte [Ações de filtragem](#), página 42.  
Os administradores delegados não poderão alterar a ação associada a categorias que tiverem sido bloqueadas por um Super administrador. Consulte [Definindo restrições de filtragem para todas as funções](#), página 264, para obter mais informações.
  4. Utilize as caixas de seleção à direita da lista Categorias para aplicar ações de filtragem avançadas à categoria selecionada:
    - Para alterar o modo como as palavras-chave são usadas na filtragem da categoria selecionada, marque ou desmarque a opção **Bloquear palavras-chave**. Consulte [Filtrando com base em palavras-chave](#), página 177
    - Para determinar se os usuários podem acessar determinados tipos de arquivos dos sites na categoria selecionada, marque ou desmarque a opção **Bloquear tipos de arquivo**. Consulte [Gerenciando o tráfego com base no tipo de arquivo](#), página 191.  
Se você tiver optado por bloquear tipos de arquivo, selecione um ou mais tipos para serem bloqueados.
    - Para especificar se o acesso aos sites da categoria é limitado com base em determinados limites de banda, marque ou desmarque a opção **Bloquear com o Bandwidth Optimizer**. Consulte [Usando o Bandwidth Optimizer para gerenciar a largura de banda](#), página 189.  
Se você tiver optado pelo bloqueio com base na largura de banda, especifique os limites a serem usados.
  5. Repita as etapas de 1 a 3 para fazer alterações nas ações de filtragem aplicadas a outras categorias.
  6. Depois de editar o filtro, clique em **OK** para armazenar suas alterações em cache e retornar à página Filtros. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Para ativar um novo filtro de categoria, adicione-o a uma diretiva e designe-a a clientes. Consulte [Diretivas de filtragem da Internet](#), página 71.

## Criando um filtro de protocolo

Tópicos relacionados:

- ◆ [Filtragem de categorias e protocolos](#), página 36
- ◆ [Ações de filtragem](#), página 42
- ◆ [Editando um filtro de protocolo](#), página 50
- ◆ [Trabalhando com protocolos](#), página 182

Utilize a página **Gerenciamento de diretivas > Filtros > Adicionar filtro de protocolo** para definir um novo filtro de protocolo. Você pode trabalhar a partir de um modelo predefinido ou criar uma cópia de um filtro de protocolo existente para usar como base para o novo filtro.

1. Insira um nome exclusivo em **Nome do filtro**. O nome de diretiva deve ter de 1 a 50 caracteres e não pode incluir nenhum destes caracteres:

\* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

Os nomes de filtro podem incluir espaços, traços e apóstrofes.

2. Insira uma **Descrição** resumida do filtro. Essa descrição aparece ao lado do nome do filtro na seção Filtros de protocolo da página Filtros; deve explicar a finalidade do filtro.

As restrições de caracteres aplicáveis a nomes de filtro também são aplicadas a descrições, com 2 exceções: as descrições podem incluir pontos (.) e vírgulas (,).

3. Selecione uma entrada na lista suspensa para determinar se usará um modelo (consulte [Modelos de filtros de categoria e protocolo](#), página 53) ou fará uma cópia de um filtro existente como base para o novo filtro.
4. Para ver e editar o novo filtro, clique em **OK**. O filtro é adicionado à lista **Filtros de protocolo** na página Filtros.

Para concluir a personalização do novo filtro, passe para a seção [Editando um filtro de protocolo](#).

## Editando um filtro de protocolo

Tópicos relacionados:

- ◆ [Filtragem de categorias e protocolos](#), página 36
- ◆ [Criando um filtro de protocolo](#), página 49
- ◆ [Ações de filtragem](#), página 42
- ◆ [Trabalhando com protocolos](#), página 182
- ◆ [Usando o Bandwidth Optimizer para gerenciar a largura de banda](#), página 189

Utilize a página **Gerenciamento de diretivas > Filtros > Editar filtro de protocolo** para fazer alterações nos filtros de protocolo existentes.



### Importante

As alterações feitas aqui afetarão todas as diretivas que aplicam esse filtro.

As diretivas que aplicam um filtro de protocolo com o mesmo nome em uma outra função de administração delegada não são afetadas.

---

O nome e a descrição do filtro aparecem na parte superior da página.

- ◆ Clique em **Renomear** para alterar o nome do filtro.
- ◆ Basta digitar no campo **Descrição** para alterar a descrição do filtro.

O número ao lado de **Diretivas que usam este filtro** indica quantas diretivas usam o filtro selecionado. Se o filtro de protocolo estiver habilitado, clique em **Ver diretivas** para ver uma lista de diretivas que aplicam o filtro.

A parte inferior da página mostra uma lista de protocolos e as ações aplicadas no momento a cada uma delas.

Para alterar o modo como os protocolos são filtrados e registrados:

1. Selecione um protocolo na lista **Protocolos**. As ações de filtragem avançadas do protocolo selecionado aparecem à direita da lista.
2. Utilize os botões **Permitir** e **Bloquear** localizados na parte inferior da lista Protocolos para alterar a ação aplicada ao protocolo selecionado.



**Obs.:**

O software Websense pode bloquear solicitações de protocolos baseados em TCP, mas não solicitações de protocolos baseados em UDP.

Alguns aplicativos utilizam mensagens baseadas em TCP e em UDP. Se uma solicitação de rede original de um aplicativo for feita via TCP e depois outros dados forem enviados via UDP, o software Websense bloqueará a solicitação TCP inicial e, conseqüentemente, o tráfego UDP.

As solicitações UDP poderão ser registradas como bloqueadas, mesmo quando forem permitidas.

Para aplicar a mesma ação aos outros protocolos no grupo de protocolos selecionado, clique em **Aplicar ao grupo**.

3. Se você quiser que informações sobre o uso do protocolo selecionado fiquem disponíveis para fins de alerta ou relatórios, marque a caixa de seleção **Registrar dados de protocolo em log**.
4. Para definir limites de largura de banda para uso deste protocolo, clique em **Bloquear com o Bandwidth Optimizer** e especifique os limites de banda a serem usados. Consulte [Usando o Bandwidth Optimizer para gerenciar a largura de banda, página 189](#), para obter mais informações.
5. Depois de editar o filtro, clique em **OK** para armazenar suas alterações em cache e retornar à página Filtros. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Para ativar um novo filtro de protocolo, adicione-o a uma diretiva e aplique-a a clientes (consulte [Diretivas de filtragem da Internet](#), página 71).



**Obs.:**

Você pode criar diretivas que comecem a aplicar um filtro de protocolo em um dado momento. Se os usuários iniciarem uma sessão de protocolo antes de esse filtro entrar em efeito, poderão continuar acessando o protocolo durante o tempo em que a sessão durar, mesmo que seja bloqueado pelo filtro. Quando um usuário terminar a sessão, as solicitações adicionais para o protocolo serão bloqueadas.

## Filtros de categoria e protocolo definidos pelo Websense

O software Websense contém várias amostras de filtros de categoria e protocolo. Você pode utilizar esses filtros como estão ou modificá-los para adaptá-los às suas necessidades de filtragem. Caso você não precise dos filtros predefinidos, muitos deles também podem ser apagados.

Estes são os filtros de categoria predefinidos:

- ◆ Básico
- ◆ Segurança básica
- ◆ Bloquear tudo
- ◆ Padrão
- ◆ Somente monitoramento
- ◆ Permitir tudo

Os filtros de categoria Bloquear tudo e Permitir tudo não aparecem na página Filtros, embora possam ser adicionados a diretivas. Esses filtros desempenham uma função especial na filtragem e não pode ser excluídos nem editados. Quando uma solicitação da Internet é filtrada, o software Websense verifica se o filtro Bloquear tudo ou Permitir tudo se aplica, antes de executar quaisquer outras verificações de filtragem (consulte [Filtrando um site](#), página 79).

Estes são os filtros de protocolo predefinidos:

- ◆ Segurança básica
- ◆ Padrão
- ◆ Somente monitoramento
- ◆ Permitir tudo

Assim como seu filtro de categoria equivalente, o filtro de protocolo Permitir tudo não aparece na página Filtros e não pode ser editado nem excluído. Quando uma filtragem é realizada, ele também é priorizado.

Os filtros de protocolo e de categoria Padrão podem ser editados, mas não podem ser excluídos. Em ambientes de atualização, se houver falhas na diretiva Padrão, os filtros Padrão serão usados para filtrar solicitações para as quais nenhuma diretiva se aplicar.

## Modelos de filtros de categoria e protocolo

Quando você cria um novo filtro de categoria ou protocolo, um ponto de partida pode ser fazer uma cópia de um filtro existente na página Filtros, selecionar um filtro existente como modelo na página Adicionar filtro ou usar um **modelo** de filtro.

O software Websense contém cinco modelos de filtro de categoria:

- ◆ **Somente monitoramento e Permitir tudo** permitem todas as categorias.
- ◆ **Bloquear tudo** bloqueia todas as categorias.
- ◆ **Básico** bloqueia as categorias que foram bloqueadas mais freqüentemente e permite as demais.
- ◆ **Padrão** aplica ações Bloquear, Permitir, Continuar e Cota a categorias.
- ◆ **Segurança básica** bloqueia somente categorias padrão da classe Risco de segurança (consulte [Classes de risco](#), página 39).

O software Websense também contém três modelos de filtro de protocolo:

- ◆ **Somente monitoramento e Permitir tudo** permitem todos os protocolos.
- ◆ **Segurança básica** bloqueia os protocolos de Compartilhamento de arquivos P2P e de Proxy Avoidance, bem como Arquivos anexos em mensagens instantâneas (caso tenha sido contratado) e Tráfego malicioso (Websense Web Security).
- ◆ **Padrão** bloqueia os protocolos de mensagens instantâneas/bate-papo, bem como Compartilhamento de arquivos P2P, Proxy Avoidance e Arquivos anexos em mensagens instantâneas (caso tenham sido contratados) e Tráfego malicioso (Websense Web Security).

Embora possa modificar ou excluir a maioria dos filtros de categoria e protocolo definidos pelo Websense, você não pode editar nem remover modelos. Da mesma forma, embora você possa criar tantos filtros personalizados quanto sejam necessários, não poderá criar novos modelos.

Como os modelos não podem ser modificados, eles sempre permitem remeter às ações de filtragem originais aplicadas por filtros definidos pelo Websense. Por exemplo, os modelos de filtros de categoria e protocolo Típico aplicam as mesmas ações que os filtros de categoria e protocolo Padrão. Isso quer dizer que você sempre pode restaurar a configuração de filtragem original do Websense criando filtros que utilizem os padrões de modelo.

Para obter instruções sobre como usar um modelo para criar um novo filtro, consulte [Criando um filtro de categoria](#), página 47, ou [Criando um filtro de protocolo](#), página 49.

## Definindo configurações de filtragem do Websense

---

Tópicos relacionados:

- ◆ [Filtragem de categorias e protocolos](#), página 36
- ◆ [Clientes](#), página 57
- ◆ [Páginas de bloqueio](#), página 83
- ◆ [Ações de filtragem](#), página 42
- ◆ [Acesso com senha](#), página 45
- ◆ [Ordem de filtragem](#), página 78
- ◆ [Usando o Bandwidth Optimizer para gerenciar a largura de banda](#), página 189
- ◆ [Filtrando com base em palavras-chave](#), página 177

Utilize a página **Configurações > Filtragem** para definir as configurações básicas de vários recursos de filtragem.

Em **Bandwidth Optimizer**, insira as informações necessárias para filtrar o uso da Internet com base na largura de banda disponível. Para obter mais informações sobre filtragem baseada em largura de banda, consulte [Usando o Bandwidth Optimizer para gerenciar a largura de banda](#), página 189.

1. Para especificar uma **velocidade de conexão à Internet**, proceda de uma das seguintes formas:
  - Selecione uma velocidade padrão na lista suspensa.
  - Insira a velocidade da rede, em kilobits por segundo, no campo de texto.
2. Utilize o campo **Largura de banda padrão para rede** para inserir um limite padrão (um percentual do tráfego total da rede) a ser usado quando a filtragem baseada na largura de banda da rede estiver habilitada.
3. Utilize o campo **Largura de banda padrão por protocolo** para inserir um limite padrão que deverá ser usado quando a filtragem baseada na largura de banda do protocolo estiver ativa.

Utilize a seção **Filtragem geral** para determinar como os usuários são filtrados quando várias diretivas de grupo se aplicam, especificar opções de pesquisa por palavras-chave e definir um comportamento de acesso com senha, continuação e sessão de cota.

1. Para determinar como os usuários serão filtrados quando várias diretivas de grupo se aplicarem, marque ou desmarque a opção **Usar diretiva de grupo mais restritiva** (consulte [Ordem de filtragem](#), página 78).
  - Quando a opção estiver selecionada, será adotada a diretiva que se aplicar à configuração de filtragem mais restritiva. Em outras palavras, se uma diretiva de grupo aplicável bloquear o acesso a uma categoria e outra permitir o acesso, a solicitação de um site nessa categoria será bloqueada.

- Quando a opção não estiver selecionada, será usada a configuração mais permissiva.
2. Selecione uma das seguintes **Opções de pesquisa por palavra-chave** (consulte [Filtrando com base em palavras-chave](#), página 177).

Somente CGI	Bloqueia os sites quando palavras-chave aparecem em strings de consulta CGI (depois de “?” em um endereço da Web). Exemplo: <b>search.yahoo.com/search?p=test</b> Quando esta opção está selecionada, o software Websense não procura palavras-chave antes do ponto de interrogação (“?”).
Somente URL	Bloqueia sites quando palavras-chave aparecem no URL. Se o endereço solicitado contiver uma string de consulta CGI, o software Websense procurará palavras-chave até o ponto de interrogação (“?”).
URL e CGI	Bloqueia sites quando palavras-chave aparecem em qualquer parte no endereço. Se houver uma string de consulta CGI, o software Websense procurará palavras-chave antes e depois do ponto de interrogação (“?”).
Desabilitar bloqueio de palavras-chave	Tenha cuidado. A seleção da opção <b>Desabilitar bloqueio de palavras-chave</b> desabilita o bloqueio de palavra-chave, mesmo quando a opção <b>Bloquear palavras-chave</b> está selecionada em um filtro de categoria.

3. No campo **Tempo limite de substituição da senha**, insira o número máximo de segundos (até 3600; o padrão é 60) durante os quais um usuário pode acessar sites em todas as categorias depois de selecionar o acesso com senha (consulte [Acesso com senha](#), página 45).
4. No campo **Tempo limite para continuação**, insira o número máximo de segundos (até 3600; o padrão é 60) durante os quais um usuário que clicar em Continuar poderá acessar sites nas categorias controladas pela ação Confirmar (consulte [Ações de filtragem](#), página 42).
5. No campo **Duração da sessão de cota**, insira o intervalo (até 60 minutos, o padrão é 10) durante os quais os usuários poderão visitar sites nas categorias limitadas por cotas (consulte [Usando o tempo da cota para limitar o acesso à Internet](#), página 44).

Uma sessão começa quando o usuário clica no botão Utilizar cota de tempo.

6. Especifique o **Tempo de cota padrão por dia** (até 240 minutos; o padrão é 60) para todos os usuários.

Para alterar o tempo de cota de usuários específicos, acesse a página **Diretivas > Clientes**.

Quando você fizer alterações na duração da sessão de cota e no tempo de cota padrão por dia, o valor de **Sessões de cota padrão por dia** será calculado e exibido.

Utilize a seção **Mensagens de bloqueio** para inserir o URL ou caminho até a página de bloqueio HTML alternativa que você criou para o quadro superior de mensagens de

bloqueio baseadas em navegador (consulte *Criando mensagens de bloqueio alternativas*, página 90).

- ◆ É possível usar páginas separadas para os diferentes protocolos: **FTP**, **HTTP** (inclusive **HTTPS**) e **Gopher**.
- ◆ Deixe esses campos em branco para usar a mensagem de bloqueio fornecida pelo software Websense ou uma versão personalizada dessa mensagem (consulte *Personalizando a mensagem de bloqueio*, página 86).

No **Search Filtering**, selecione **Habilitar filtragem de pesquisa** para que o software Websense ative uma configuração criada em determinados mecanismos de busca. Dessa forma, as miniaturas e demais conteúdo explícito associado a sites bloqueados não aparecerão nos resultados de pesquisa (consulte *Filtragem de pesquisa*, página 45).

Os mecanismos de pesquisa a que esse recurso oferece suporte são exibidos na parte inferior da seção.

Quando terminar de definir as configurações de filtragem, clique em **OK** para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

# 3

## Clientes

Você pode personalizar o modo como o software Websense filtra solicitações de computadores ou de usuários específicos, adicionando-os como **clientes** no Websense Manager. Os clientes podem ser:

- ◆ **Computadores:** Computadores individuais da rede definidos pelo endereço IP.
- ◆ **Redes:** Grupos de computadores definidos coletivamente como um intervalo de endereços IP.
- ◆ **Usuários:** Contas de usuário, grupo ou domínio em um serviço de diretório suportado.

Inicialmente, o software Websense filtra todos os clientes da mesma maneira, usando a diretiva **Padrão** (consulte [A diretiva Padrão, página 72](#)). Quando adiciona um cliente à página Clientes no Websense Manager, você pode designá-lo a uma diretiva de filtragem específica.

Caso seja possível aplicar várias diretivas, como acontece quando uma diretiva é designada ao usuário e outra ao computador, o software Websense procede da seguinte forma para determinar qual diretiva será aplicada:

1. Aplique a diretiva atribuída ao **usuário** que está fazendo a solicitação. Se essa diretiva não contiver filtros programados no momento da solicitação, utilize a próxima diretiva aplicável.
2. Se não houver uma diretiva específica de usuário ou a diretiva não contiver filtros ativos no momento da solicitação, procure uma diretiva atribuída ao **computador** (primeiro) ou à **rede** (segundo) de onde a solicitação foi feita.
3. Se não houver uma diretiva específica do computador ou da rede, ou a diretiva não contiver filtros ativos no momento da solicitação, procure uma diretiva atribuída a qualquer **grupo** a que o usuário pertença. Se o usuário pertencer a vários grupos, o software Websense considerará todas as diretivas de grupo que se aplicarem (consulte [Ordem de filtragem, página 78](#)).
4. Se não houver uma diretiva de grupo, procure uma diretiva atribuída ao **domínio** (OU) do usuário.
5. Se não for encontrada uma diretiva aplicável ou a diretiva não aplicar um filtro de categoria no momento da solicitação, aplique a diretiva **Padrão** da função a que o cliente foi designado.

Para obter mais informações sobre como o software Websense aplica diretivas de filtragem aos clientes, consulte [Filtrando um site, página 79](#).

## Trabalhando com clientes

Tópicos relacionados:

- ◆ [Clientes](#), página 57
- ◆ [Trabalhando com computadores e redes](#), página 59
- ◆ [Trabalhando com usuários e grupos](#), página 60
- ◆ [Adicionando um cliente](#), página 66
- ◆ [Alterando configurações de cliente](#), página 68

Utilize a página **Gerenciamento de diretivas > Clientes** para ver informações sobre clientes existentes, adicionar, editar ou excluir clientes, ou mover clientes para uma função de administração delegada.

Se for um administrador delegado, você deverá adicionar clientes à sua lista de clientes gerenciados para vê-los na página Clientes. Consulte [Adicionando um cliente](#), página 66, para obter instruções.

Os clientes dividem-se em três grupos:

- ◆ **Diretório**, que inclui usuários, grupos e domínios do seu serviço de diretório (consulte [Trabalhando com usuários e grupos](#), página 60).
- ◆ **Redes**, intervalos de endereços IP dentro da rede filtrada que podem ser controlados por uma única diretiva (consulte [Trabalhando com computadores e redes](#), página 59).
- ◆ **Computadores**, computadores individuais na rede filtrada, identificados pelo endereço IP (consulte [Trabalhando com computadores e redes](#), página 59).

Clique no sinal de mais (+) ao lado do tipo de cliente para ver uma lista de clientes existentes do tipo selecionado. Cada listagem de clientes informa o seguinte:

- ◆ O nome do cliente, o endereço IP ou o intervalo de endereços IP.
- ◆ A **diretiva** que está atribuída ao cliente. A diretiva **Padrão** é usada até outra ser atribuída (consulte [Diretivas de filtragem da Internet](#), página 71).
- ◆ Se o cliente pode ou não usar um **acesso com senha** para ver sites bloqueados (consulte [Acesso com senha](#), página 45).
- ◆ Se o cliente tem uma quantidade personalizada de **tempo de cota** alocada (consulte [Usando o tempo da cota para limitar o acesso à Internet](#), página 44).

Para encontrar um cliente específico, navegue até o nó apropriado na árvore.

Para editar configurações de autenticação, diretiva do cliente, acesso com senha e tempo de cota, selecione um ou mais clientes na lista e clique em **Editar**. Consulte [Alterando configurações de cliente](#), página 68, para obter mais informações.

Para adicionar um cliente ou aplicar uma diretiva a um cliente gerenciado que não está aparecendo na página Clientes, clique em **Adicionar**. Em seguida, passe para a seção [Adicionando um cliente](#), página 66, para obter mais informações.

Se você tiver criado funções de administração delegada (consulte [Administração delegada](#), página 235), os Super administradores poderão mover seus clientes para outras funções. Primeiro marque a caixa de seleção ao lado da entrada do cliente e, em seguida, clique em **Mover para função**. Quando um cliente é transferido para uma função de administração delegada, a diretiva e os filtros aplicados a ele são copiados para a função. Consulte [Movendo clientes para funções](#), página 68, para obter mais informações.

Se você tiver configurado o software Websense para se comunicar com um serviço de diretório baseado em LDAP, o botão **Gerenciar grupos LDAP personalizados** aparecerá na barra de ferramentas na parte superior da página. Clique neste botão para adicionar ou editar grupos com base em um atributo LDAP (consulte [Trabalhando com grupos LDAP personalizados](#), página 64).

Para remover um cliente do Websense Manager, selecione-o e clique em **Excluir**.

## Trabalhando com computadores e redes

Tópicos relacionados:

- ◆ [Trabalhando com clientes](#), página 58
- ◆ [Trabalhando com usuários e grupos](#), página 60
- ◆ [Adicionando um cliente](#), página 66
- ◆ [Atribuindo uma diretiva aos clientes](#), página 77

No Websense Manager, um **computador** é o endereço IP (por exemplo, 10.201.3.1) associado a um computador filtrado. Uma **rede** é o intervalo de endereços IP (por exemplo, 10.201.3.2 - 10.201.3.44) associado a um grupo de computadores filtrados.

Você pode designar diretivas a clientes de computador e rede da mesma forma que faria com clientes de usuário, grupo ou domínio.

- ◆ Atribua uma diretiva a um **computador**, por exemplo, que não exija que os usuários façam logon ou que possa ser acessado por usuários com contas de convidado.
- ◆ Atribua uma diretiva a uma **rede** para aplicar a mesma diretiva de filtragem a vários computadores ao mesmo tempo.

Quando uma diretiva é designada a um computador ou a uma rede, ela é aplicada a qualquer usuário que esteja conectado ao computador filtrado, **a menos que** você tenha a designado ao usuário conectado. Essa diretiva de computador ou de rede prevalece sobre quaisquer outras diretivas de **grupo** aplicáveis ao usuário.

## Trabalhando com usuários e grupos

Tópicos relacionados:

- ◆ [Trabalhando com clientes](#), página 58
- ◆ [Serviços de diretório](#), página 60
- ◆ [Trabalhando com grupos LDAP personalizados](#), página 64
- ◆ [Trabalhando com computadores e redes](#), página 59
- ◆ [Adicionando um cliente](#), página 66
- ◆ [Atribuindo uma diretiva aos clientes](#), página 77

Para aplicar diretivas a usuários específicos e a grupos na sua rede, configure o software Websense para acessar seu serviço de diretório a fim de obter informações sobre o objeto de diretório (usuário, grupo, domínio e unidade organizacional).

O software Websense pode se comunicar com o Windows NT Directory/Active Directory (Mixed Mode) e com o Windows Active Directory, o Novell eDirectory e o Sun Java System Directory acessados via LDAP (Lightweight Directory Access Protocol).



**Obs.:**

Quando você usa um serviço de diretório baseado em LDAP, não há suporte para nomes de usuário duplicados. Confira se o mesmo nome de usuário não aparece em mais de um domínio.

Além disso, se você estiver usando o Windows Active Directory ou o Sun Java System Directory, os nomes de usuário com senhas em branco não serão suportados. Certifique-se de que senhas tenham sido atribuídas a todos os usuários.

O Websense User Service transmite informações do serviço de diretório para o Policy Server e o Filtering Service para serem usadas na aplicação de diretivas de filtragem.

A Websense, Inc. recomenda a instalação do User Service em um computador com Windows (embora ele possa residir em em um computador com Linux). Geralmente, esse é o mesmo computador em que o Policy Server está instalado.

Para configurar o software Websense a fim de se comunicar com seu serviço de diretório, consulte [Serviços de diretório](#).

## Serviços de diretório

Um serviço de diretório é uma ferramenta que armazena informações sobre usuários e recursos de uma rede. Para poder adicionar clientes de usuário (usuários, grupos,

domínios ou unidades organizacionais) ao Websense Manager, você deverá primeiro configurar o software Websense para recuperar informações no serviço de diretório.

Utilize a página **Configurações > Serviços de diretório** para identificar o serviço de diretório usado na sua rede. Você só pode definir configurações para um único tipo de serviço de diretório por Policy Server.

Primeiro, selecione um serviço de diretório na lista Diretórios. A seleção que você fizer determinará quais configurações aparecerão na página.

Para obter instruções sobre configuração, consulte a seção apropriada:

- ◆ [Windows NT Directory/Active Directory \(Mixed Mode\)](#), página 61
- ◆ [Windows Active Directory \(Native Mode\)](#), página 61
- ◆ [Novell eDirectory e Sun Java System Directory](#), página 63

## Windows NT Directory/Active Directory (Mixed Mode)

Se o seu serviço de diretório for Windows NT Directory ou Active Directory em Mixed Mode, não será necessária configuração adicional.

Em raras circunstâncias, se você estiver usando outro serviço de diretório, talvez precise fornecer informações adicionais nessa tela. Isso só ocorrerá quando:

- ◆ O DC Agent estiver sendo usado para identificação transparente (consulte [DC Agent](#), página 211)
- e
- ◆ o User Service for executado em um computador com Linux.

Se essa for a sua configuração, forneça as credenciais administrativas listadas no Windows NT Directory/Active Directory (Mixed Mode). Caso contrário, os campos de credenciais administrativas aparecerão desabilitados.

## Windows Active Directory (Native Mode)

O Windows Active Directory armazena informações do usuário em um ou mais *catálogos globais*. O catálogo global permite que usuários e aplicativos localizem objetos (usuários, grupos e assim por diante) em um domínio do Active Directory.

Para que o software Websense possa se comunicar com o Active Directory no Native Mode, você deve fornecer informações sobre os servidores do catálogo global na sua rede.

1. Clique em **Adicionar** ao lado da lista de servidores de catálogo global. A página Adicionar servidor de catálogo global aparecerá.
2. Utilize o campo **IP ou nome do servidor** para identificar o servidor de catálogo global:
  - Se houver vários servidores de catálogo global configurados para failover, insira o nome de domínio DNS.

- Se os servidores de catálogo global não estiverem configurados para failover, insira o endereço IP ou nome de host (caso a resolução de nome esteja habilitada na rede) do servidor a ser adicionado.
3. Insira a **porta** que o software Websense deverá usar para se comunicar com o catálogo global (por padrão, **3268**).
  4. Se preferir, insira o **contexto raiz** que o software Websense deverá usar para procurar informações do usuário. Se você fornecer um valor, ele deverá ser um contexto válido no seu domínio.
    - Caso tenha especificado a porta de comunicação 3268 ou 3269, você não precisará fornecer um contexto raiz.
    - Caso a porta especificada seja 389 ou 636, forneça um contexto raiz.
    - Se o contexto raiz for deixado em branco, o software Websense iniciará a procura no nível mais alto do serviço de diretório.



**Obs.:**

Evite usar o mesmo nome de usuário em mais de um domínio. Se o software Websense encontrar nomes de contas duplicados para um usuário, não será possível identificar o usuário claramente.

---

5. Especifique qual conta administrativa o software Websense deve usar para recuperar o nome do usuário e informações sobre o caminho no serviço de diretório. É necessário que essa conta possa consultar e ler a partir do serviço de diretório, mas ela não precisa ser capaz de fazer alterações nele nem ser um administrador de domínio.

Selecione **Nome distinto por componente** ou **Nome completo distinto** para especificar como você prefere inserir as informações da conta.

- Se tiver escolhido a opção Nome distinto por componente, insira o **nome de exibição**, a **senha** da conta, a **pasta da conta** e o **nome do domínio DNS** da conta administrativa. Utilize o formulário de nome comum (cn) do nome de usuário administrativo, e não o formulário de ID de usuário (uid).



**Obs.:**

O campo **Pasta da conta** não suporta valores com a tag da unidade organizacional (ou) (por exemplo, *ou=Finance*). Se o nome da conta administrativa contiver a tag ou, insira o nome completo distinto dessa conta.

---

- Se você tiver escolhido a opção Nome completo distinto, insira o nome distinto como uma única string no campo **Nome distinto do usuário** (por exemplo, *cn=Admin, cn=Users, ou=InfoSystems, dc=company, dc=net*) e especifique a **senha** dessa conta.
6. Clique em **OK**.
  7. Repita o processo acima para cada servidor de catálogo global.
  8. Clique em **Configurações avançadas de diretório** e vá para a seção *Configurações avançadas de diretório*, página 63.

## Novell eDirectory e Sun Java System Directory

Para recuperar informações do serviço de diretório, o software Websense requer o nome distinto, o contexto raiz e a senha de uma conta de usuário com privilégios administrativos.

1. Insira o endereço IP do serviço de diretório no campo **IP do servidor**.
2. Insira o número da **porta** que o software Websense usará para se comunicar com o diretório. O padrão é 389.
3. Se o diretório exigir privilégios de administrador para acesso somente leitura, insira o **nome distinto do administrador** e a **senha**.
4. Se preferir, insira o **contexto raiz** que o software Websense deverá usar para procurar informações do usuário. Por exemplo, *o=domain.com*.

A limitação do contexto aumenta a velocidade e a eficiência na recuperação de informações do usuário.



### Obs.:

Evite usar o mesmo nome de usuário em mais de um domínio. Se o software Websense encontrar nomes de contas duplicados para um usuário, não será possível identificar o usuário claramente.

5. Clique em **Configurações avançadas de diretório** e vá para a seção *Configurações avançadas de diretório*, página 63.

## Configurações avançadas de diretório

Tópicos relacionados:

- ◆ [Windows Active Directory \(Native Mode\)](#), página 61
- ◆ [Novell eDirectory e Sun Java System Directory](#), página 63

Essas configurações podem ser usadas para definir:

- ◆ O modo como o software Websense pesquisa no serviço de diretório para localizar informações de usuários, grupos e domínios.
- ◆ Se o software Websense utiliza uma conexão criptografada para se comunicar com o serviço de diretório.
- ◆ O conjunto de caracteres que o software Websense utiliza para codificar informações LDAP.

Defina essas configurações, conforme necessário, para qualquer serviço de diretório baseado em LDAP.

1. Se você utilizar tipos de classes de objetos personalizados (nomes de atributo) no serviço de diretório, selecione a opção **Usar filtros personalizados**. As strings de filtros padrão aparecerão nos campos Filtros.
2. Edite as strings de filtros existentes, substituindo os tipos de classes de objetos específicos do seu diretório. Por exemplo, se o seu diretório usa um tipo de classe de objeto como **dept** em vez de **ou** (unidade organizacional), insira um novo valor no campo Filtro de pesquisa de domínios.

Os atributos sempre têm strings que são usadas na pesquisa do conteúdo do serviço de diretório. Os filtros personalizados fornecem a funcionalidade descrita aqui.

- **Filtro de pesquisa de usuários** determina como o User Service pesquisa os usuários.
  - **Filtro de pesquisa de grupos** determina como o User Service pesquisa os grupos.
  - **Filtro de pesquisa de domínios** determina como o User Service pesquisa domínios e unidades organizacionais.
  - **Filtro de pesquisa de grupos do usuário** determina como o User Service associa usuários a grupos.
3. Para proteger as comunicações entre o software Websense e seu serviço de diretório, selecione **Usar SSL**.
  4. Para determinar qual conjunto de caracteres o software Websense usará para codificar informações LDAP, selecione **UTF-8** ou **MBCS**.

O MBCS, ou conjunto de caracteres multibyte, costuma ser usado para codificar idiomas do Leste Asiático, como chinês, japonês e coreano.
  5. Clique em **OK** para armazenar suas alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Trabalhando com grupos LDAP personalizados

---

Tópicos relacionados:

- ◆ [Trabalhando com usuários e grupos](#), página 60
- ◆ [Serviços de diretório](#), página 60
- ◆ [Adicionando ou editando um grupo LDAP personalizado](#), página 65

Utilize a página **Gerenciar Grupos LDAP personalizados** para gerenciar grupos personalizados com base nos atributos definidos no seu serviço de diretório. Esta

opção só estará disponível se você tiver configurado o software Websense para se comunicar com um serviço de diretório baseado em LDAP.



### Importante

Quando você adiciona grupos LDAP personalizados ao Websense Manager, as definições de grupo são armazenadas pelo Policy Server ativo e não afetam outras instâncias do Policy Server. Para adicionar grupos LDAP personalizados a vários Policy Servers, utilize o Websense Manager para fazer logon em cada Policy Server e inserir as informações.

Se você adicionar grupos LDAP personalizados e alterar serviços de diretório ou mudar a localização do serviço de diretório, os grupos existentes se tornarão inválidos. Você precisará adicionar os grupos novamente e, depois, definir cada um como um cliente.

- ◆ Para adicionar um grupo, clique em **Adicionar** (consulte [Adicionando ou editando um grupo LDAP personalizado](#), página 65).
- ◆ Para alterar uma entrada na lista, clique no respectivo nome de grupo (consulte [Adicionando ou editando um grupo LDAP personalizado](#)).
- ◆ Para remover uma entrada, primeiro selecione-a e, em seguida, clique em **Excluir**.

Quando terminar de fazer as alterações nos grupos LDAP personalizados, clique em **OK** para armazená-las em cache e retornar à página anterior. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Adicionando ou editando um grupo LDAP personalizado

Utilize a página **Adicionar grupo LDAP personalizado** para definir um grupo no Websense Manager baseado em qualquer atributo que você tenha definido no seu serviço de diretório. Utilize a página **Editar grupo LDAP personalizado** para fazer alterações em uma definição existente.



### Importante

Se você adicionar grupos LDAP personalizados e alterar serviços de diretório ou mudar a localização do serviço de diretório, os grupos existentes se tornarão inválidos. Você precisará adicionar os grupos novamente e, depois, definir cada um como um cliente.

1. Insira ou altere o **nome do grupo**. Utilize um nome descritivo para indicar claramente a finalidade do grupo LDAP.

Os nomes dos grupos não diferenciam maiúsculas e minúsculas e devem ser exclusivos.

2. Insira ou altere a descrição que define esse grupo no seu serviço de diretório. Por exemplo:

(WorkStatus=parttime)

Neste exemplo, **WorkStatus** é um atributo de usuário que indica o status de trabalho e **parttime** é um valor que indica se o funcionário trabalha em horário parcial.

3. Clique em **OK** para retornar à página Gerenciar grupos LDAP personalizados. A entrada nova ou revisada aparecerá na lista.
4. Adicione ou edite outra entrada ou clique em **OK** para armazenar as alterações em cache e retornar à página anterior. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Adicionando um cliente

---

Tópicos relacionados:

- ◆ [Trabalhando com clientes](#), página 58
- ◆ [Trabalhando com computadores e redes](#), página 59
- ◆ [Trabalhando com usuários e grupos](#), página 60
- ◆ [Pesquisando o serviço de diretório](#), página 67
- ◆ [Alterando configurações de cliente](#), página 68

Utilize a página **Gerenciamento de diretivas > Clientes > Adicionar clientes** para adicionar clientes de usuário, grupo, computador e rede ao Websense Manager. Assim, você poderá atribuir uma diretiva a eles.

Se estiver conectado com uma função de administração delegada, você só poderá adicionar clientes que aparecerem na sua lista de clientes gerenciados. No processo de inclusão de clientes gerenciados na página Clientes, você precisa atribuir a eles uma diretiva.

1. Identifique um ou mais clientes:
  - Para adicionar um cliente de usuário, grupo ou domínio, navegue até a árvore **Diretório** para localizar entradas no seu serviço de diretório. Se estiver usando um serviço de diretório baseado em LDAP, você também poderá clicar em **Pesquisar** para habilitar uma ferramenta de pesquisa de diretório (consulte [Pesquisando o serviço de diretório](#), página 67).
  - Para adicionar um cliente de computador ou rede, insira um **endereço IP** ou **intervalo de endereços IP**. Não é possível haver sobreposição de duas definições de rede, mas um cliente de rede pode incluir um endereço IP identificado separadamente como um cliente de computador. No caso de sobreposição, a diretiva atribuída ao computador prevalecerá em relação à atribuída à rede.

2. Clique no botão de seta (>) para adicionar cada cliente à lista **Clientes selecionados**.  
Para remover uma entrada da lista Clientes selecionados, selecione o cliente e clique em **Remover**.
3. Selecione uma **diretiva** para atribuir a todos os clientes da lista Clientes selecionados.
4. Quando terminar, clique em **OK** para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Os clientes são adicionados à lista apropriada na página **Gerenciamento de diretivas > Clientes**. Para alterar a diretiva atribuída a um ou mais clientes ou definir mais configurações de cliente, selecione cada entrada de cliente e clique em **Editar**. Consulte [Alterando configurações de cliente](#), página 68, para obter mais informações.

## Pesquisando o serviço de diretório

Se tiver configurado o software Websense para se comunicar com um serviço de diretório baseado em LDAP, você poderá usar uma função de pesquisa para identificar usuários que serão adicionados como clientes ao Websense Manager. A pesquisa também está disponível para adicionar administradores e clientes gerenciados a funções de administração delegada.

Para pesquisar um serviço de diretório a fim de recuperar informações sobre usuários, grupos ou unidades organizacionais, faça o seguinte:

1. Clique em **Pesquisar**.
2. Insira o **nome** (completo ou parcial) do usuário, do grupo ou da unidade organizacional.
3. Utilize a lista **Tipo** para indicar o tipo da entrada de diretório (usuário, grupo, unidade organizacional ou tudo) que você deseja localizar.  
Em um serviço de diretório muito grande, a seleção de **Tudo** pode fazer com que a pesquisa demore muito tempo.
4. Navegue pela árvore **Contexto da pesquisa** para especificar qual parte do diretório deverá ser pesquisada. Um contexto mais exato ajuda a acelerar a pesquisa.
5. Clique em **Ir**.  
É exibida uma lista de resultados de pesquisa.
6. Selecione uma ou mais entradas nos resultados da pesquisa e clique na seta para a direita (>) para adicionar cada seleção como cliente ou administrador.
7. Clique em **Nova pesquisa** para inserir outro conjunto de critérios de pesquisa.
8. Clique em **Procurar** para voltar a navegar pelo diretório.
9. Quando você terminar de fazer alterações, clique em **OK** para armazená-las em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Alterando configurações de cliente

---

Utilize a página **Gerenciamento de diretivas > Clientes > Editar cliente** para alterar configurações de diretiva e de autenticação de um ou mais clientes. Se você selecionar vários clientes antes de clicar em Editar, as alterações de configuração que fizer na página Editar cliente serão aplicadas a todos esses clientes.

1. Selecione uma **diretiva** para aplicar aos clientes selecionados. Até outra diretiva ser atribuída, é a diretiva Padrão que controla os clientes.
2. Para permitir que usuários substituam uma página de bloqueio do Websense por meio da inserção de uma senha, clique em **Ativado** em Acesso com senha. Em seguida, insira a senha e confirme-a.

Para remover privilégios de acesso com senha de um cliente, clique em **Desativado**.

3. Para alocar determinado período de **tempo de cota** aos clientes selecionados, clique em **Personalizado** e insira o número de minutos de cota que serão atribuídos.

Para retornar às configurações de cota padrão, clique em **Padrão**.

4. Clique em **OK** para armazenar suas alterações em cache e voltar à página Clientes. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

As novas configurações de cliente aparecem como parte da listagem de clientes na página **Gerenciamento de diretivas > Clientes**.

## Movendo clientes para funções

---

Os Super administradores podem usar a página **Mover o cliente para função** para mover um ou mais clientes para uma função de administração delegada. Depois que um cliente for movido, ele aparecerá na lista Clientes gerenciados na página Clientes na função de destino.

- ◆ A diretiva aplicada ao cliente na função Super administradores e os filtros que a aplicam são copiados para a função de administração delegada.
- ◆ Os administradores delegados podem alterar as diretivas aplicadas a seus clientes gerenciados.
- ◆ As restrições de Proteção de filtro não afetam os clientes gerenciados por Super administradores, mas afetam os gerenciados em funções de administração delegada.
- ◆ Se um grupo, domínio ou unidade organizacional for adicionado a uma função como cliente gerenciado, os administradores delegados nessa função poderão atribuir diretivas a usuários individuais nesse grupo, domínio ou unidade organizacional.

- ◆ Se uma rede (intervalo de endereços IP) for adicionada a uma função como um cliente gerenciado, os administradores delegados nessa função poderão atribuir diretivas a computadores individuais nessa rede.
- ◆ Não é possível mover o mesmo cliente para várias funções.

Para mover os clientes selecionados para uma função de administração delegada:

1. Utilize a lista suspensa **Selecionar função** para selecionar uma função de destino.
2. Clique em **OK**.  
Uma caixa de diálogo pop-up indica que os clientes selecionados estão sendo movidos. Esse processo pode levar alguns instantes.
3. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Se os administradores delegados na função selecionada estiverem conectados com um acesso de diretiva durante o processo de mover, eles precisarão fazer logout do Websense Manager e, em seguida, fazer logon novamente para verem os novos clientes em suas listas de clientes gerenciados.



# 4

## Diretivas de filtragem da Internet

Tópicos relacionados:

- ◆ [Filtros de uso da Internet](#), página 35
- ◆ [Clientes](#), página 57
- ◆ [A diretiva Padrão](#), página 72
- ◆ [Trabalhando com diretivas](#), página 73
- ◆ [Ordem de filtragem](#), página 78

As diretivas controlam o acesso dos usuários à Internet. Uma diretiva consiste em:

- ◆ Filtros de categoria, usados para aplicar ações (Permitir, Bloquear) a categorias de site da Web (consulte [Filtragem de categorias e protocolos](#), página 36)
- ◆ Filtros de acesso limitado, usados para permitir acesso apenas a uma lista restrita de sites da Web (consulte [Restringindo usuários a uma lista definida de sites de Internet](#), página 166)
- ◆ Filtros de protocolo, usados para aplicar ações a protocolos de Internet (consulte [Filtragem de categorias e protocolos](#), página 36)
- ◆ Uma programação que determina quando cada filtro de categoria ou de acesso limitado e filtro de protocolo serão aplicados

A instalação de um novo software Websense inclui 3 diretivas predefinidas:

- ◆ **Padrão** filtra o acesso à Internet de todos os clientes não regidos por outra diretiva. O software Websense começa a aplicar essa diretiva assim que uma chave de assinatura é inserida (consulte [A diretiva Padrão](#), página 72).
- ◆ **Irrestrito** fornece acesso ilimitado à Internet. Por padrão, esta diretiva não é aplicada a clientes.
- ◆ **Exemplo - Usuário padrão** mostra como vários filtros de categoria e de protocolo podem ser aplicados a uma diretiva para fornecer diversos graus de restrição de filtragem em momentos diferentes. Esta diretiva é usada no Tutorial do guia rápido - novo usuário para demonstrar o processo de edição de uma diretiva e sua aplicação aos clientes.

Use qualquer uma dessas diretivas no estado em que se encontra, edite-a de acordo com sua organização ou crie suas próprias diretivas.

## A diretiva Padrão

---

Tópicos relacionados:

- ◆ [Diretivas de filtragem da Internet](#), página 71
- ◆ [Trabalhando com diretivas](#), página 73
- ◆ [Ordem de filtragem](#), página 78

Após a instalação do software Websense, a diretiva **Padrão** começará a monitorar o uso da Internet assim que você inserir sua chave de assinatura. Inicialmente, a diretiva Padrão permite todas as solicitações.



**Obs.:**

As configurações de diretiva existentes serão preservadas quando for feito upgrade de uma versão anterior do software Websense. Após o upgrade, verifique suas diretivas para garantir que elas ainda estejam adequadas.

---

Quando você criar e aplicar suas próprias diretivas de filtragem, a diretiva Padrão continuará atuando como uma rede de proteção, filtrando o acesso à Internet de qualquer cliente não regido por outra diretiva.

Em uma nova instalação, a diretiva Padrão deverá fornecer cobertura de filtragem da Internet (aplicar uma combinação de filtros de categoria ou de acesso limitado e, se aplicável, filtros de protocolo) 24 horas por dia, 7 dias por semana.



**Importante**

Os usuários que estiverem fazendo upgrade de uma versão anterior do software Websense poderão ter uma diretiva Padrão que não abranja todos os períodos. Não é necessário alterar a diretiva Padrão. Entretanto, se você editar a diretiva futuramente, o software Websense não permitirá salvar as alterações até que todos os períodos tenham sido cumpridos.

---

Edite a diretiva Padrão, conforme necessário, para atender às necessidades de sua organização. Essa diretiva não poderá ser excluída.

## Trabalhando com diretivas

Tópicos relacionados:

- ◆ [Diretivas de filtragem da Internet, página 71](#)
- ◆ [Criando uma diretiva](#)
- ◆ [Editando uma diretiva](#)
- ◆ [Filtros de uso da Internet](#)
- ◆ [Refinar as diretivas de filtragem](#)

Use a página **Gerenciamento de diretivas > Diretivas** para verificar as informações de diretiva existentes. Essa página também funciona como ponto de início para adicionar, editar e excluir diretivas, copiar diretivas em funções de administração delegada (apenas Super administradores) e imprimir informações detalhadas sobre sua configuração de diretiva.

A página Diretivas inclui uma lista de diretivas existentes. A lista inclui um nome e uma descrição de cada diretiva, além do número de clientes de usuário, de rede e de computador aos quais essa diretiva foi atribuída.

- ◆ Para adicionar uma diretiva, clique em **Adicionar** e consulte [Criando uma diretiva, página 74](#), para obter mais informações.
- ◆ Para editar uma diretiva, clique no nome de diretiva na lista e consulte [Editando uma diretiva, página 75](#), para obter mais informações.
- ◆ Para ver quais clientes são filtrados pela diretiva, clique em um número na coluna Usuários, Redes ou Computadores. As informações do cliente são exibidas em uma caixa de diálogo pop-up.

Para imprimir uma lista de todas as suas diretivas e respectivos componentes, incluindo filtros, categorias e protocolos personalizados, palavras-chave, URLs personalizados e expressões regulares, clique em **Imprimir diretivas em arquivo**. Esse recurso cria uma planilha detalhada com informações de diretiva no formato Microsoft Excel. Sua finalidade é permitir que especialistas em recursos humanos, gerentes e outras pessoas com autoridade de supervisão verifiquem as informações de diretiva de filtragem de maneira conveniente.

Se você tiver criado funções de administração delegada (consulte [Administração delegada, página 235](#)), os Super administradores poderão copiar as diretivas criadas para outras funções para serem usadas por administradores delegados. Os filtros aplicados pela diretiva também serão copiados.



**Obs.:**

Como os administradores delegados são regidos pela Proteção de filtro, os filtros de Permitir tudo e as diretivas que os aplicam não podem ser copiados para funções.

Para copiar diretivas para outra função, marque primeiro a caixa de seleção ao lado do nome da diretiva e clique em **Copiar para função**. Consulte [Copiando filtros e diretivas para funções](#), página 170, para obter mais informações.

## Criando uma diretiva

Tópicos relacionados:

- ◆ [Diretivas de filtragem da Internet](#), página 71
- ◆ [Trabalhando com diretivas](#), página 73
- ◆ [Editando uma diretiva](#), página 75
- ◆ [Trabalhando com filtros](#), página 46
- ◆ [Restringindo usuários a uma lista definida de sites de Internet](#), página 166

Use a página **Gerenciamento de diretivas > Diretivas > Adicionar diretiva** para criar uma nova diretiva personalizada.

1. Insira um nome exclusivo em **Nome da diretiva**. O nome de diretiva deve ter 1 a 50 caracteres e não pode incluir nenhum destes caracteres:

\* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

Os nomes de diretiva podem incluir espaços, traços e apóstrofes.

2. Insira uma **Descrição** para a diretiva. A descrição deve ser clara e detalhada para auxiliar no gerenciamento de diretivas a longo prazo.

As restrições de caracteres aplicáveis a nomes de diretivas também são aplicadas a descrições, com 2 exceções: as descrições podem incluir pontos (.) e vírgulas (,).

3. Para usar uma diretiva existente como base da nova diretiva, marque a caixa de seleção **Basear em uma diretiva existente** e selecione uma diretiva na lista suspensa.

Para iniciar com uma diretiva vazia, deixe a caixa de seleção desmarcada.

4. Clique em **OK** para colocar suas alterações em cache e ir para a página Editar diretiva.

Use a página Editar diretiva para concluir a definição da nova diretiva. Consulte [Editando uma diretiva](#), página 75.

## Editando uma diretiva

Tópicos relacionados:

- ◆ [Diretivas de filtragem da Internet](#), página 71
- ◆ [Trabalhando com diretivas](#), página 73
- ◆ [Criando uma diretiva](#), página 74
- ◆ [Trabalhando com filtros](#), página 46
- ◆ [Restringindo usuários a uma lista definida de sites de Internet](#), página 166

Use a página **Gerenciamento de diretivas > Diretivas > Editar diretiva** para fazer alterações em uma diretiva existente ou para concluir a definição de uma nova diretiva.

Use a parte superior da página para editar o nome e a descrição da diretiva:

- ◆ Clique em **Renomear** para alterar o nome da diretiva.
- ◆ Basta digitar no campo **Descrição** para alterar a descrição do filtro.

Embaixo da descrição da diretiva, o campo **Clientes** lista a quantidade de clientes de cada tipo (usuário, computador e rede) que são filtrados no momento por essa diretiva. Para ver quais clientes são controlados pela diretiva, clique no link que corresponde ao tipo de cliente apropriado.

Para atribuir essa diretiva a mais clientes, clique em **Aplicar a clientes** na barra de ferramentas localizada na parte superior da página e consulte [Atribuindo uma diretiva aos clientes](#), página 77.

Use a área **Definição da diretiva** para definir os filtros que serão aplicados por essa diretiva em momentos diferentes:

1. Clique em **Adicionar** para adicionar um bloqueio de tempo à programação.
2. Use as colunas **Início** e **Fim** na tabela Programação para definir o período de cobertura desse bloqueio de tempo.

Para definir a filtragem para um período que ultrapassa a meia-noite (por exemplo, 17:00 às 8:00), adicione dois bloqueios de tempo à programação: um que abranja o período desde a hora inicial até a meia-noite e outro que abranja o período desde a meia-noite até a hora final.

A diretiva **Exemplo - Usuário padrão**, incluída com o software Websense, demonstra como definir um período de filtragem que ultrapasse a meia-noite.

3. Use a coluna **Dias** para definir os dias da semana que serão incluídos nesse bloqueio de tempo. Para selecionar os dias de uma lista, clique na seta para baixo no lado direito da coluna. Quando terminar de selecionar os dias, clique na seta para cima.
4. Use a coluna **Filtro de categoria/acesso limitado** para selecionar um filtro a ser aplicado durante esse bloqueio de tempo.

Para adicionar um novo filtro a ser aplicado a essa diretiva, selecione **Criar filtro de categoria** ou **Criar filtro de acesso limitado**. Consulte [Criando um filtro de categoria, página 47](#), ou [Criando um filtro de acesso limitado, página 168](#), para obter instruções.

- Use a coluna **Filtro de protocolo** para selecionar um filtro de protocolo a ser aplicado durante esse bloqueio de tempo.

Para adicionar um novo filtro a ser aplicado a essa diretiva, selecione **Criar filtro de protocolo**. Consulte [Criando um filtro de protocolo, página 49](#), para obter instruções.

- Repita as etapas 1 a 5 para adicionar outros bloqueios de tempo à programação.

Quando qualquer bloqueio de tempo da programação é selecionado, a parte inferior da página Editar diretivas mostra os filtros aplicados durante esse bloqueio de tempo.

Cada listagem de filtros inclui:

- ◆ O tipo de filtro (filtro de categoria, filtro de acesso limitado ou filtro de protocolo)
- ◆ O nome e a descrição do filtro
- ◆ O conteúdo do filtro (categorias ou protocolos com ações aplicadas ou uma lista de sites permitidos)
- ◆ O número de diretivas que aplicam o filtro selecionado
- ◆ Os botões que podem ser usados para editar o filtro

Quando você edita um filtro na página, as alterações afetam cada diretiva que aplica o filtro. Antes de editar um filtro aplicado por várias diretivas, clique no link **Número de diretivas que usam este filtro** para ver exatamente quais diretivas serão afetadas.

Os botões exibidos na parte inferior da listagem de filtros dependem do tipo de filtro:

Tipo de filtro	Botões
<b>filtro de categoria</b>	<ul style="list-style-type: none"> <li>• Use o botão <b>Permitir, Bloquear, Confirmar</b> ou <b>Cota</b> para alterar a ação aplicada às categorias selecionadas (consulte <a href="#">Ações de filtragem, página 42</a>).</li> <li>• Para alterar a ação aplicada a uma categoria pai e a todas as suas subcategorias, primeiro altere a ação aplicada à categoria pai e, em seguida, clique em <b>Aplicar a subcategorias</b>.</li> <li>• Para ativar o bloqueio de palavras-chave, de tipos de arquivo ou um bloqueio baseado na largura de banda, clique em <b>Avançado</b>.</li> </ul>

Tipo de filtro	Botões
<b>filtros de acesso limitado</b>	<ul style="list-style-type: none"> <li>• Use o botão <b>Adicionar sites</b> e <b>Adicionar expressões</b> para adicionar os URLs, endereços IP ou expressões regulares permitidas (consulte <a href="#">Restringindo usuários a uma lista definida de sites de Internet</a>, página 166).</li> <li>• Para remover um site do filtro, marque a caixa de seleção ao lado do URL, do endereço IP ou da expressão e, em seguida, clique em <b>Excluir</b>.</li> </ul>
<b>filtro de protocolo</b>	<ul style="list-style-type: none"> <li>• Use o botão <b>Permitir</b> ou <b>Bloquear</b> para alterar a ação aplicada aos protocolos selecionados (consulte <a href="#">Ações de filtragem</a>, página 42).</li> <li>• Para alterar a ação aplicada a todos os protocolos de um grupo, altere a ação aplicada a qualquer protocolo do grupo e, em seguida, clique em <b>Aplicar ao grupo</b>.</li> <li>• Para registrar dados do protocolo selecionado ou habilitar o bloqueio com base na largura de banda, clique em <b>Avançado</b>.</li> </ul>

Quando terminar de editar uma diretiva, clique em **OK** para armazenar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Atribuindo uma diretiva aos clientes

Tópicos relacionados:

- ◆ [Diretivas de filtragem da Internet](#), página 71
- ◆ [Criando uma diretiva](#), página 74
- ◆ [Editando uma diretiva](#), página 75
- ◆ [Clientes](#), página 57
- ◆ [Adicionando um cliente](#), página 66

Use a página **Diretivas > Editar diretiva > Aplicar diretiva a clientes** para atribuir a diretiva selecionada aos clientes.

A lista Clientes mostra todos os clientes de usuário, de computador e de rede disponíveis, bem como a diretiva atribuída atualmente a cada um deles.

Marque a caixa de seleção ao lado de cada cliente a ser filtrado pela diretiva selecionada e, em seguida, clique em **OK** para voltar à página Editar diretiva. Clique em **OK** novamente para armazenar suas alterações em cache.

Clique em **Salvar tudo** para solicitar que o software Websense inicie o uso da nova diretiva para filtrar as solicitações dos clientes selecionados.

## Ordem de filtragem

---

O software Websense usa vários filtros, aplicados em uma ordem específica, para determinar se os dados da Internet solicitados serão permitidos, bloqueados ou limitados.

Para cada solicitação recebida, o software Websense:

1. Verifica a conformidade da assinatura, assegurando que a assinatura esteja atual e o número de clientes com assinatura não tenha sido excedido.
2. Determina a diretiva a ser aplicada, pesquisando nesta ordem:
  - a. Diretiva atribuída ao **usuário**.
  - b. Diretiva atribuída ao **endereço IP** (computador ou rede) da máquina usada.
  - c. Diretivas atribuídas aos **grupos** aos quais o usuário pertence.
  - d. Diretivas atribuídas ao **domínio** do usuário.
  - e. A diretiva **Padrão**.A primeira diretiva aplicável encontrada é usada.
3. Filtra a solicitação de acordo com as restrições da diretiva.

Em alguns casos, um usuário pertence a mais de um grupo ou domínio e nenhuma diretiva de usuário, de computador ou de rede é aplicável. Nesses casos, o software Websense verifica as diretivas atribuídas a cada um dos grupos do usuário.

- ◆ Se todos os grupos tiverem a mesma diretiva, o software Websense filtrará a solicitação de acordo com ela.
- ◆ Se um dos grupos tiver outra diretiva, o software Websense filtrará a solicitação de acordo com a seleção **Utilizar bloqueio mais restritivo** na página **Configurações > Filtragem**.

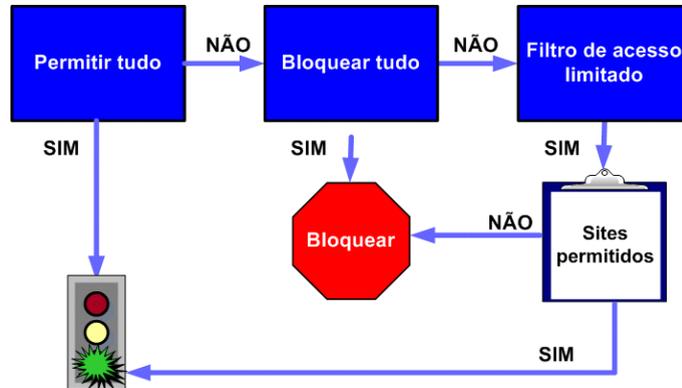
Se a opção **Utilizar bloqueio mais restritivo** estiver marcada e qualquer uma das diretivas aplicáveis bloquear o acesso à categoria solicitada, o software Websense bloqueará o site.

Se a opção não estiver marcada e qualquer uma das diretivas aplicáveis permitir o acesso à categoria solicitada, o software Websense permitirá o site.

Se uma das diretivas aplicáveis executar um filtro de acesso limitado, a opção **Utilizar bloqueio mais restritivo** poderá ter efeitos diferentes do esperado. Consulte [Filtros de acesso limitado e precedência de filtragem](#), página 166.

## Filtrando um site

O software Websense avalia as restrições de diretiva conforme a seguir para determinar se o site solicitado deve ser permitido ou bloqueado.

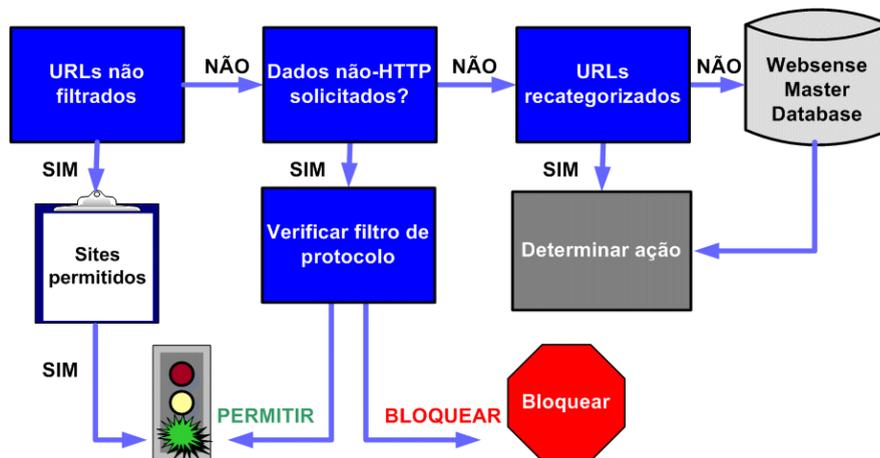


1. Determina qual **filtro de categoria** ou **filtro de acesso limitado** será aplicado pela diretiva para o dia e o horário atuais.
  - Se o filtro de categoria ativo for **Permitir tudo**, permita o site.
  - Se o filtro de categoria ativo for **Bloquear tudo**, bloqueie o site.
  - No caso de um **filtro de acesso limitado**, verifique se ele contém o URL ou o endereço IP. Se ele contiver, permita o site. Caso contrário, bloqueie o site.

- Se qualquer outro filtro de categoria for aplicado, continue na etapa 2.

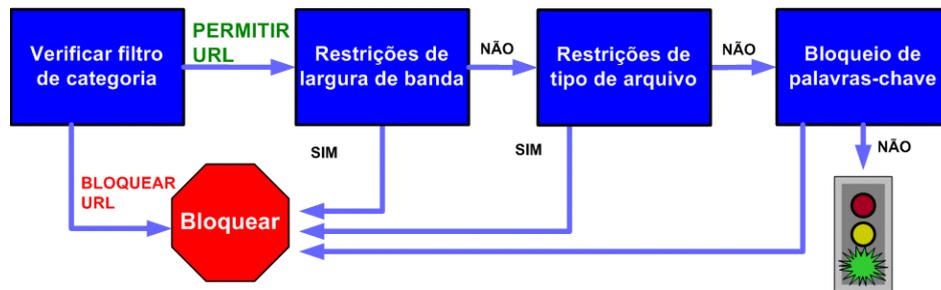
**Obs.:**

O software Websense filtra os URLs acessados do cache de um mecanismo de pesquisa da Internet da mesma forma que qualquer outro URL. Os URLs armazenados dessa maneira são filtrados de acordo com as diretivas ativas para suas categorias. Os registros de log dos URLs em cache mostram o URL inteiro armazenado em cache, incluindo qualquer parâmetro de mecanismo de pesquisa.



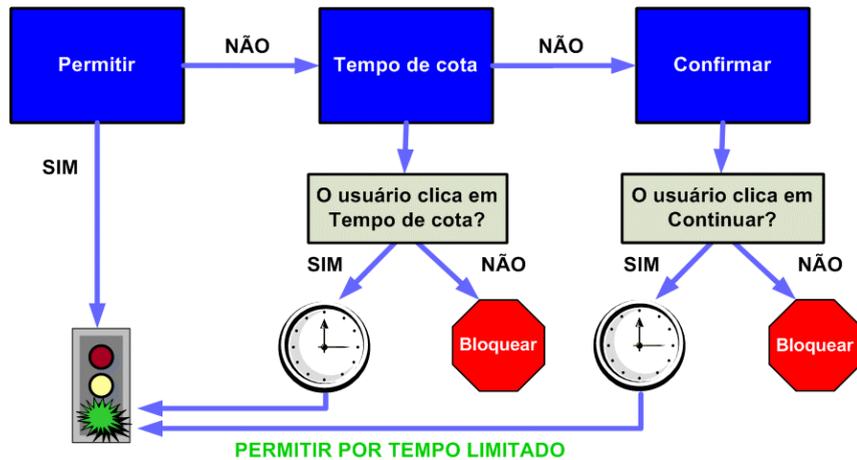
- Tenta fazer a correspondência do site com uma entrada na lista **URLs não filtrados**.
  - Se o URL aparecer na lista, permita o site.
  - Caso contrário, continue na etapa 3.
- Verifica o **filtro de protocolo** ativo e determina se há algum protocolo não-HTTP associado à solicitação.
  - Se houver, aplique as configurações de filtragem de protocolo aos dados que possivelmente serão transmitidos.
  - Caso contrário, continue na etapa 4.
- Tenta fazer a correspondência do site com uma entrada na lista **URLs recategorizados**.
  - Se for feita a correspondência, identifique a categoria referente ao site e vá para a etapa 6.
  - Caso contrário, continue na etapa 5.
- Tenta fazer a correspondência do site com uma entrada no **Master Database**.
  - Se o URL aparecer no Master Database, identifique a categoria referente ao site e continue na etapa 6.

- Se não for feita nenhuma correspondência, categorize o site como Diversos/ Não categorizado e continue na etapa 6.



- Verifica o filtro de categoria ativo e identifica a ação aplicada à categoria que contém o site solicitado.
  - Se a ação for **Bloquear**, bloqueie o site.
  - Se qualquer outra ação for aplicada, continue na etapa 7.
- Verifica se há configurações do **Bandwidth Optimizer** no filtro de categoria ativo (consulte *Usando o Bandwidth Optimizer para gerenciar a largura de banda*, página 189).
  - Se o uso da largura de banda atual exceder qualquer limite configurado, bloqueie o site.
  - Se o uso da largura de banda atual não exceder os limites especificados ou se nenhuma ação baseada na largura de banda for aplicável, continue na etapa 8.
- Verifica se há restrições de **tipo de arquivo** aplicadas à categoria ativa (consulte *Gerenciando o tráfego com base no tipo de arquivo*, página 191).
  - Se o site contiver arquivos cujas extensões estejam bloqueadas, bloqueie o acesso a eles. Se o próprio site incluir um tipo de arquivo bloqueado, bloqueie o acesso ao site.
  - Se o site não contiver arquivos com extensões bloqueadas, vá para a etapa 9.
- Verifica se há **palavras-chave** bloqueadas no caminho do URL e de CGI se o bloqueio de palavras-chave estiver habilitado (consulte *Filtrando com base em palavras-chave*, página 177).
  - Se for encontrada uma palavra-chave bloqueada, bloqueie o site.

- Caso contrário, continue na etapa 10.



10. Trata o site de acordo com a ação aplicada à categoria.

- **Permitir:** permite o site.
- **Limitar por cota:** exibe a mensagem de bloqueio com uma opção para exibir o site usando um tempo de cota ou voltar para a página anterior.
- **Confirmar:** exibe a mensagem de bloqueio com a opção para exibir o site para fins de trabalho.

O software Websense continuará até que o site solicitado esteja bloqueado ou seja explicitamente permitido. Quando isso ocorrer, ele não tentará nenhuma outra filtragem. Por exemplo, se um site solicitado pertencer a uma categoria bloqueada e contiver uma palavra-chave bloqueada, o software Websense bloqueará o site no nível de categoria sem verificar o filtro de palavras-chave. Em seguida, o Log Server registrará a solicitação como bloqueada devido a uma categoria bloqueada, e não por causa de uma palavra-chave.



**Obs.:**

Os usuários com privilégios de acesso com senha podem acessar os sites da Internet, independentemente do motivo de bloqueio do site.

# 5

## Páginas de bloqueio

Tópicos relacionados:

- ◆ *Mensagens de bloqueio de protocolo*, página 84
- ◆ *Trabalhando com páginas de bloqueio*, página 85
- ◆ *Criando mensagens de bloqueio alternativas*, página 90
- ◆ *Usando uma página de bloqueio alternativa em outro computador*, página 90

Quando o software Websense bloqueia um site da Web, exibe uma página de bloqueio no navegador do cliente. Se o site estiver bloqueado porque pertence a uma categoria na classe Risco de segurança (consulte *Classes de risco*, página 39), uma versão especial da página de bloqueio é exibida.

Por padrão, uma página de bloqueio consiste em 3 seções principais.

A imagem mostra uma interface de usuário de uma página de bloqueio. No topo, há um cabeçalho com um ícone de erro e o texto "Conteúdo bloqueado pela sua empresa". Abaixo disso, há um "quadro superior" com campos "Motivo:" e "URL:". O "quadro inferior" contém o texto "Opções:" seguido de uma mensagem e um botão "Voltar".

**Conteúdo bloqueado pela sua empresa** ← cabeçalho

**Motivo:** Esta categoria Websense é filtrada: Conteúdo adulto. ← quadro superior

**URL:** http://www.playboy.com/

**Opções:** Clique em [mais informações](#) para saber mais sobre a sua diretiva de acesso.

Clique em **Voltar** ou use o botão de voltar do navegador para retornar à página an  
Voltar ← quadro inferior

- ◆ O **cabeçalho** explica que o site foi bloqueado.
- ◆ O **quadro superior** contém uma mensagem de bloqueio que mostra o URL solicitado e o motivo por que o URL foi bloqueado.
- ◆ O **quadro inferior** apresenta quaisquer opções disponíveis para o usuário, como a opção de voltar à página anterior ou clicar no botão Continuar ou Utilizar cota de tempo para exibir o site.

As páginas de bloqueio são construídas a partir de arquivos HTML. O software Websense inclui páginas de bloqueio padrão. Você pode usar esses arquivos padrão ou criar versões personalizadas.

- ◆ Personalizar os arquivos padrão para alterar a mensagem de bloqueio (consulte [Trabalhando com páginas de bloqueio](#), página 85).
- ◆ Configurar o software Websense para usar mensagens de bloqueio (padrão ou personalizadas) hospedadas em um servidor Web remoto (consulte [Usando uma página de bloqueio alternativa em outro computador](#), página 90).

## Mensagens de bloqueio de protocolo

---

Tópicos relacionados:

- ◆ [Trabalhando com páginas de bloqueio](#), página 85
- ◆ [Criando mensagens de bloqueio alternativas](#), página 90
- ◆ [Usando uma página de bloqueio alternativa em outro computador](#), página 90

Quando um usuário ou aplicativo solicita um protocolo bloqueado não-HTTP, o software Websense exibe uma mensagem de bloqueio de protocolo.

Porém, quando um usuário solicita um site bloqueado de FTP, HTTPS ou Gopher em um navegador, e a solicitação passa por um proxy, uma página de bloqueio baseada em HTML é exibida no navegador.

Se um aplicativo solicita o protocolo bloqueado, o usuário também pode receber uma mensagem de erro do aplicativo, indicando que não pode ser executado. As mensagens de erro de aplicativo não são geradas pelo software Websense.

Alguma configuração do sistema pode ser necessária para exibir mensagens de bloqueio de protocolo em computadores com Windows:

- ◆ Para exibir uma mensagem de bloqueio de protocolo em computadores clientes executando Windows NT, XP ou 200x, o serviço Windows Messenger deve estar habilitado. Este serviço é desabilitado por padrão. Você pode usar a caixa de diálogo Serviços do Windows para descobrir se o serviço está sendo executado em um determinado computador (consulte [A caixa de diálogo Serviços do Windows](#), página 392).
- ◆ Para exibir mensagens de bloqueio de protocolo em um computador com Windows 98, você deve iniciar **winpopup.exe**, localizado no diretório do Windows. Execute o aplicativo a partir do prompt de comando ou configure-o para início automático, copiando-o para a pasta Inicializar.

As mensagens de bloqueio de protocolo não são exibidas em computadores com Linux. As páginas de bloqueio em HTML são exibidas em todos os sistemas operacionais.

Se a filtragem de protocolos estiver habilitada, o software Websense filtra solicitações de protocolo, mesmo que as mensagens de bloqueio de protocolo não estejam configuradas para exibição em computadores clientes.

## Trabalhando com páginas de bloqueio

Tópicos relacionados:

- ◆ [Mensagens de bloqueio de protocolo](#), página 84
- ◆ [Personalizando a mensagem de bloqueio](#), página 86
- ◆ [Criando mensagens de bloqueio alternativas](#), página 90
- ◆ [Usando uma página de bloqueio alternativa em outro computador](#), página 90

Os arquivos usados para criar páginas de bloqueio do Websense são armazenados no diretório **Websense\BlockPages\en\Default**:

- ◆ O arquivo **master.html** constrói o quadro de informação para a página de bloqueio e usa um dos seguintes arquivos para exibir opções apropriadas no quadro inferior.

Nome do arquivo	Conteúdo
blockFrame.html	Texto e botão (opção Voltar) para sites em categorias bloqueadas.
continueFrame.html	Texto e botões para sites em categorias às quais a ação <b>Confirmar</b> é aplicada.
quotaFrame.html	Texto e botões para sites em categorias às quais a ação <b>Cota</b> é aplicada.
moreInfo.html	Conteúdo para a página que aparece quando um usuário clica no link <b>Mais informações</b> na página de bloqueio.

- ◆ **block.html** contém o texto para o quadro superior da mensagem de bloqueio, que explica que o acesso é restrito, lista o site solicitado e descreve por que o site é restrito.

## Personalizando a mensagem de bloqueio

Tópicos relacionados:

- ◆ [Alterando o tamanho do quadro de mensagem](#), página 87
- ◆ [Alterando o logotipo exibido na página de bloqueio](#), página 87
- ◆ [Usando variáveis de conteúdo de página de bloqueio](#), página 88
- ◆ [Revertendo às páginas de bloqueio padrão](#), página 89

Você pode fazer uma cópia dos arquivos da página de bloqueio padrão e usar a cópia para personalizar o quadro superior da página de bloqueio que os usuários recebem.

- ◆ Adicione informações sobre as políticas de uso da Internet de sua empresa.
  - ◆ Forneça um método para contatar Recursos Humanos ou um administrador do Websense sobre as políticas de uso da Internet.
1. Navegue para o diretório de página de bloqueio do Websense:  
`<caminho de instalação>\BlockPages\en\Default`
  2. Copie os arquivos da página de bloqueio para o diretório de página de bloqueio personalizado:

`<caminho de instalação>\BlockPages\en\Custom`



### Obs.:

**Não** modifique os arquivos da mensagem de bloqueio original no diretório **BlockPages\en\Default**. Copie-os para o diretório **BlockPages\en\Custom** e depois modifique as cópias.

---

3. Abra o arquivo em um editor de texto, como Notepad ou vi.



### Aviso

Use um editor de texto puro para editar arquivos de mensagem de bloqueio. Alguns editores de HTML modificam o código HTML, o que pode corromper os arquivos e causar problemas para exibição das mensagens de bloqueio.

---

4. Modifique o texto. Os arquivos contêm comentários que orientam você para fazer alterações.

**Não** modifique os tokens (delimitados pelos símbolos \$\* e \*\$) ou a estrutura do código HTML. Eles habilitam o software Websense a exibir informações específicas na mensagem de bloqueio.

5. Salve o arquivo.
6. Reinicie o Filtering Service (consulte [Parando e iniciando os serviços Websense](#), página 283, para obter instruções).

## Alterando o tamanho do quadro de mensagem

Dependendo de quais informações você deseja fornecer na mensagem de bloqueio, a largura padrão da mensagem de bloqueio e a altura do quadro superior podem não ser apropriados. Para alterar esses parâmetros de tamanho no arquivo **master.html**:

1. Copie **master.html** do diretório **Websense\BlockPages\en\Default** para **Websense\BlockPages\en\Custom**.
2. Abra o arquivo em um editor de texto, como Notepad ou vi (e não em um editor de HTML).
3. Para alterar a largura do quadro de mensagem, edite a seguinte linha:  

```
<div style="border: 1px solid #285EA6;width: 600px...">
```

 Altere o valor do parâmetro **width** (largura), conforme necessário.
4. Para fazer o quadro superior da mensagem rolar, a fim de exibir informações adicionais, edite a seguinte linha:  

```
<iframe src="$*WS_BLOCKMESSAGE_PAGE*$*WS_SESSIONID*$" ... scrolling="no" style="width:100%; height: 6em;">
```

 Altere o valor do parâmetro **scrolling** (rolagem) para **auto** a fim de exibir uma barra de rolagem quando o texto da mensagem excede a altura do quadro.  
 Você também pode alterar o valor do parâmetro **height** (altura) para alterar a altura do quadro.
5. Salve e feche o arquivo.
6. Reinicie o Filtering Service para implementar a alteração (consulte [Parando e iniciando os serviços Websense](#), página 283).

## Alterando o logotipo exibido na página de bloqueio

O arquivo **master.html** também inclui o código HTML usado para exibir um logotipo do Websense na página de bloqueio. Para substituir com o logotipo da sua empresa:

1. Copie os arquivos da página de bloqueio do diretório **Websense\BlockPages\en\Default** para **Websense\BlockPages\en\Custom**, se ainda não foram copiados.
2. Copie um arquivo de imagem que contenha o logotipo da sua organização para o mesmo local.
3. Abra **master.html** em um editor de texto, como Notepad ou vi (e não em um editor de HTML), e edite a seguinte linha para substituir o logotipo do Websense com o logotipo da sua empresa.  

```

```

  - Substitua **wslogo\_block\_page.png** com o nome do arquivo de imagem que contém o logotipo da sua empresa.
  - Substitua os valores do parâmetro **title** (título) para refletir o nome de sua empresa.
4. Salve e feche o arquivo.

- Reinicie o Filtering Service para implementar a alteração (consulte *Parando e iniciando os serviços Websense*, página 283).

## Usando variáveis de conteúdo de página de bloqueio

As variáveis de conteúdo controlam as informações exibidas em páginas de bloqueio em HTML. As seguintes variáveis são incluídas com o código da mensagem de bloqueio padrão.

Nome da variável	Conteúdo exibido
WS_DATE	Data atual
WS_USERNAME	Nome do usuário atual (excluindo o nome do domínio)
WS_USERDOMAIN	Nome de domínio para o usuário atual
WS_IPADDR	Endereço IP do computador de origem da solicitação
WS_WORKSTATION	Nome de máquina do computador bloqueado (se nenhum nome estiver disponível, o endereço IP é exibido)

Para usar uma variável, insira o nome da variável entre os símbolos \$\* \*\$ no comando HTML apropriado:

```
<p id="NomeDeUsuario">*$WS_USERNAME*$</p>
```

Aqui, *WS\_USERNAME* é a variável.

O código da mensagem de bloqueio inclui variáveis adicionais, descritas abaixo. Algumas dessas variáveis podem ser úteis para criar suas próprias mensagens de bloqueio personalizadas. Ao ver essas variáveis em arquivos de mensagem de bloqueio definidos pelo Websense, porém, **não** os modifique. Como o Filtering Service usa essas variáveis ao processar solicitações bloqueadas, elas devem permanecer no local.

Nome da variável	Objetivo
WS_URL	Exibe o URL solicitado
WS_BLOCKREASON	Exibe por que o site foi bloqueado (ou seja, qual ação de filtragem foi aplicada)
WS_ISSECURITY	Indica se o site solicitado pertence a qualquer das categorias padrão na classe Risco de segurança. Quando TRUE (verdadeiro), a página de bloqueio de segurança é exibida.
WS_PWOVERRIDECGIDATA	Preenche um campo de entrada no código HTML da página de bloqueio com informações sobre o uso do botão <b>Acesso com senha</b>
WS_QUOTA_CGIDATA	Preenche um campo de entrada no código HTML da página de bloqueio com informações sobre o uso do botão <b>Utilizar cota de tempo</b>

Nome da variável	Objetivo
WS_PASSWORDOVERRIDE_BEGIN, WS_PASSWORDOVERRIDE_END	Envolvido na ativação da funcionalidade de acesso com senha
WS_MOREINFO	Exibe informações detalhadas (mostradas depois que o link <b>Mais informação</b> é clicado) sobre por que o site solicitado foi bloqueado
WS_POLICYINFO	Indica qual política rege o cliente solicitante
WS_MOREINFOCGIDATA	Envia dados ao Filtering Service sobre o uso do link <b>Mais informações</b>
WS_QUOTATIME	Exibe a quantidade de cota de tempo restante para o cliente solicitante
WS_QUOTAINTERVALTIME	Exibe a duração da sessão de cota configurada para o cliente solicitante
WS_QUOTABUTTONSTATE	Indica se o botão <b>Utilizar cota de tempo</b> está habilitado ou desabilitado para uma solicitação específica
WS_SESSIONID	Atua como um identificador interno associado com uma solicitação
WS_TOPFRAMESIZE	Indica o tamanho (como porcentagem) da parte superior de uma página de bloqueio enviada por um servidor de bloqueio personalizado, se houver algum configurado
WS_BLOCKMESSAGE_PAGE	Indica a fonte a ser usada para o quadro superior de uma página de bloqueio
WS_CATEGORY	Exibe a categoria do URL bloqueado
WS_CATEGORYID	O identificador exclusivo para a categoria de URL solicitada

## Revertendo às páginas de bloqueio padrão

Se os usuários experimentarem erros depois que você implementar páginas de bloqueio personalizadas, você pode restaurar as mensagens de bloqueio padrão da seguinte forma:

1. Exclua todos os arquivos do diretório **Websense\BlockPages\en\Custom**. Por padrão, o software Websense voltará a usar os arquivos no diretório Padrão.
2. Reinicie o Filtering Service (consulte [Parando e iniciando os serviços Websense](#), página 283).

## Criando mensagens de bloqueio alternativas

---

Tópicos relacionados:

- ◆ [Trabalhando com páginas de bloqueio](#), página 85
- ◆ [Personalizando a mensagem de bloqueio](#), página 86

Você pode criar seus próprios arquivos HTML para fornecer o texto que aparece no quadro superior da página de bloqueio. Use arquivos HTML existentes, crie cópias alternativas a partir do zero ou faça cópias de **block.html** para usar como modelo.

- ◆ Crie uma mensagem de bloqueio diferente para cada um de 3 protocolos: HTTP, FTP e Gopher.
- ◆ Hospede os arquivos na máquina do Websense ou em seu servidor Web interno (consulte [Usando uma página de bloqueio alternativa em outro computador](#), página 90).

Depois de criar arquivos de mensagem de bloqueio alternativos, você deve configurar o software Websense para exibir as novas mensagens (consulte [Definindo configurações de filtragem do Websense](#), página 54). Durante este processo, você pode especificar qual mensagem é usada para cada um dos protocolos configuráveis.

## Usando uma página de bloqueio alternativa em outro computador

---

Tópicos relacionados:

- ◆ [Trabalhando com páginas de bloqueio](#), página 85
- ◆ [Personalizando a mensagem de bloqueio](#), página 86
- ◆ [Criando mensagens de bloqueio alternativas](#), página 90

Em vez de usar páginas de bloqueio do Websense e personalizar apenas a mensagem no quadro superior, você pode criar suas próprias páginas de bloqueio em HTML e hospedá-las em um servidor Web interno.



**Obs.:**

É possível armazenar páginas de bloqueio em um servidor Web externo. Se, porém, esse servidor hospeda um site listado no Master Database, e o site está em uma categoria bloqueada, a página de bloqueio será bloqueada.

---

Algumas empresas usam páginas de bloqueio alternativas e remotas para ocultar a identidade do servidor Websense.

A página de bloqueio remota pode ser qualquer arquivo em HTML; não precisa seguir o formato das páginas de bloqueio padrão do Websense. Usar este método para criar páginas de bloqueio, porém, impede que você use as funções Continuar, Utilizar cota de tempo e Acesso com senha disponíveis nas páginas de bloqueio definidas pelo Websense (padrão ou personalizadas).

Quando os arquivos estiverem no local, edite o arquivo **eimserver.ini** para apontar para a nova página de bloqueio.

1. Páre os serviços Websense Filtering Service e Policy Server, nessa ordem (consulte *Parando e iniciando os serviços Websense*, página 283).
2. No computador do Filtering Service, navegue até o diretório **bin** do Websense (por padrão, \Program Files\Websense\bin ou /opt/websense/bin).
3. Crie uma cópia de backup do arquivo **eimserver.ini** e armazene em outro diretório.
4. Abra o arquivo **eimserver.ini** em um editor de texto e localize a seção **[WebsenseServer]** (no alto do arquivo).
5. Digite o nome de host ou o endereço IP do servidor que hospeda a página de bloqueio no seguinte formato:

```
UserDefinedBlockPage=http://<nome do host ou endereço IP>
```

A parte de protocolo do URL (http://) é obrigatória.

6. Salve o arquivo e feche o editor de texto.
7. Reinicie o Websense Policy Server e o Websense Filtering Service, nessa ordem.

Quando os serviços estiverem inicializados, o usuário recebe a página de bloqueio hospedada no computador alternativo.



# 6

## Usando relatórios para avaliar diretivas de filtragem

Tópicos relacionados:

- ◆ [Visão geral de relatórios](#), página 94
- ◆ [Relatórios de apresentação](#), página 96
- ◆ [Relatórios investigativos](#), página 115
- ◆ [Acessando os relatórios próprios](#), página 141

O Websense Manager pode fornecer diversas ferramentas de relatórios para uso ao avaliar a eficácia de suas diretivas de filtragem. (O Websense Manager e os componentes de relatório do Websense devem estar instalados em servidores Windows.)

- ◆ A página **Hoje** aparece primeiro quando você abre o Websense Manager. Mostra o status operacional do software Websense e pode exibir gráficos de atividades de filtragem na rede a partir da meia-noite. (Consulte [Hoje: Saúde, segurança e valor desde a meia-noite](#), página 19.)
- ◆ A página **Histórico** mostra gráficos de atividades de filtragem na rede para até 30 dias, dependendo da quantidade de informações no banco de dados de log. Esses gráficos não incluem as atividades de hoje. (Consulte [Histórico: Últimos 30 dias](#), página 22.)
- ◆ **Relatórios de apresentação e relatórios investigativos** oferecem muitas opções para gerar, personalizar e agendar relatórios. Consulte [Visão geral de relatórios](#), página 94, para obter mais informações.

Se a sua empresa instalou o Websense Manager em um servidor Linux, ou escolheu o programa de relatórios Websense Explorer for Linux em vez dos componentes de relatório para Windows, as opções de relatórios não aparecem no Websense Manager. Nenhum gráfico de filtragem de Internet aparecerá nas páginas Hoje e Histórico. Consulte o *Explorer for Linux Administrator's Guide* para obter informações sobre como instalar o programa e gerar relatórios.

## Visão geral de relatórios

---

Tópicos relacionados:

- ◆ [Usando relatórios para avaliar diretivas de filtragem](#), página 93
- ◆ [Relatórios de apresentação](#), página 96
- ◆ [Relatórios investigativos](#), página 115
- ◆ [Acessando os relatórios próprios](#), página 141

Além dos gráficos que aparecem nas páginas Hoje e Histórico, o software Websense oferece duas opções de relatórios: relatórios de apresentação e relatórios investigativos.



**Obs.:**

Em empresas que usam administração delegada, alguns administradores talvez não possam acessar todos os recursos de relatórios. Consulte [Administração delegada](#), página 235.

**Relatórios de apresentação** oferecem uma lista de definições de relatórios. Alguns são relatórios em tabelas, outros combinam um gráfico de barras e uma tabela. Para gerar um relatório de apresentação:

1. Selecione um relatório na lista.
2. Clique em **Executar**.
3. Selecione o intervalo de datas.
4. Clique em **Executar agora**.

Além de gerar gráficos predefinidos, você pode copiá-los e aplicar um filtro de relatório personalizado que identifica clientes, categorias, protocolos ou ações específicas para inclusão. Marque as definições de relatórios que usa com frequência como Favoritos para facilitar sua localização.

Você pode agendar qualquer relatório de apresentação para execução em uma hora específica ou em um ciclo de repetição. Consulte [Relatórios de apresentação](#), página 96, para obter detalhes.

**Relatórios investigativos** permitem navegar nos dados de registros de forma interativa. A página principal mostra um gráfico de barras em nível de resumo das atividades por classe de risco. Clique nos diferentes elementos da página para atualizar o gráfico ou obter outra exibição dos dados.

- ◆ Clique no nome da classe de risco e selecione um nível maior de detalhes com relação à classe de risco. Por exemplo, você pode optar por mostrar a atividade por usuário para a classe de risco Responsabilidade legal.
- ◆ Clique em um nome de usuário no gráfico resultante para exibir mais detalhes sobre o usuário.

- ◆ Escolha outra opção na lista **Uso da Internet por** para alterar o gráfico de barras de resumo.
- ◆ Preencha os campos acima do gráfico de barras para exibir dois níveis de informações simultaneamente. Por exemplo, começando com um gráfico de resumo de categorias, você poderia escolher **10, Usuário** e **5** para exibir a atividade para os 5 principais usuários nas 10 principais categorias.
- ◆ Clique em uma barra ou em um número para abrir um relatório detalhado para o item (classe de risco, categoria, usuário ou outro).
- ◆ Clique em **Relatórios favoritos** para salvar um formato de relatório especialmente útil para uso futuro ou para gerar um Favorito salvo anteriormente.

As possibilidades são quase infinitas. Consulte *Relatórios investigativos*, página 115, para obter detalhes sobre as muitas formas como você pode exibir dados de uso da Internet.

## O que é tempo de navegação na Internet?

Tópicos relacionados:

- ◆ *Trabalhos de banco de dados*, página 318
- ◆ *Configurando as opções de tempo de navegação na Internet*, página 324

Você pode gerar relatórios de apresentação e relatórios investigativos com base no tempo de navegação na Internet (IBT), a quantidade de tempo que uma pessoa passa acessando sites da Web. Nenhum software pode informar a quantidade exata de tempo que alguém passa visualizando um site específico depois que está aberto. Alguém pode abrir um site, visualizá-lo durante alguns segundos e depois atender o telefone antes de solicitar outro site. Outra pessoa poderia passar vários minutos lendo cada site em detalhes antes de passar para o seguinte.

O software Websense inclui um trabalho de banco de dados de log para calcular o tempo de navegação na Internet (IBT), usando uma fórmula baseada em determinados valores configuráveis. Este trabalho é executado uma vez ao dia. Portanto, as informações de tempo de navegação podem estar atrasadas em relação aos dados de registro.

Para os cálculos de tempo de navegação, uma sessão de Internet começa quando um usuário abre um navegador. Continua enquanto o usuário solicita sites da Web adicionais pelo menos a cada 3 minutos. (Este limite de tempo de leitura padrão é configurável.)

A sessão de Internet termina quando mais de 3 minutos passam antes que o usuário solicite outro site. O software Websense calcula o total tempo da sessão, começando com a hora da primeira solicitação e terminando 3 minutos depois da última solicitação.

Uma nova sessão começa se o usuário faz solicitações adicionais após mais de 3 minutos. Em geral, o tempo de navegação de um usuário consiste em várias sessões a cada dia.

Consulte *Trabalhos de banco de dados*, página 318, e *Configurando as opções de tempo de navegação na Internet*, página 324, para obter informações sobre o trabalho de tempo de navegação na Internet e as opções de configuração associadas.

## Relatórios de apresentação

---

Tópicos relacionados:

- ◆ [Copiando um relatório de apresentação](#), página 99
- ◆ [Copiando um relatório de apresentação](#), página 99
- ◆ [Trabalhando com favoritos](#), página 106
- ◆ [Gerando relatórios de apresentação](#), página 107
- ◆ [Agendando relatórios de apresentação](#), página 108
- ◆ [Exibindo a lista de trabalhos agendados](#), página 113

A página **Geração de relatórios > Relatórios de apresentação** apresenta uma lista de gráficos predefinidos e relatórios em tabelas, cada um mostrando informações específicas do banco de dados de log (consulte [Apresentando o banco de dados de log](#), página 317). Selecione um relatório neste Catálogo de relatórios para exibir uma breve descrição.

Você pode copiar um relatório predefinido e personalizar o filtro de relatórios, especificando quais clientes, categorias, protocolos e ações devem ser incluídos. Os relatórios que são usados com frequência podem ser marcados como Favoritos para ajudar você a localizá-los com mais rapidez.

Execute qualquer relatório agora ou programe relatórios selecionados para execução posterior ou periódica. Escolha o formato de saída e distribua os relatórios agendados para um grupo de destinatários selecionados.

Se você gerar um relatório diretamente da página Relatórios de apresentação em formato HTML, o relatório não é salvo quando você vai para outra página. Se você gerar e imediatamente exibir um relatório em formato PDF ou XLS, o relatório não é salvo quando você fecha o programa de visualização (Adobe Reader ou Microsoft Excel).

Como alternativa, você pode optar por salvar o arquivo PDF ou XLS, em vez de exibi-lo imediatamente, ou usar a opção Salvar no programa de exibição. Nestes casos, certifique-se de excluir ou mover arquivos de relatórios periodicamente para evitar problemas de espaço em disco.

Os relatórios agendados são salvos automaticamente no seguinte diretório:

```
<caminho_de_instalacao>\ReportingOutput
```

O caminho de instalação padrão é C:\Arquivos de Programas\WebSense.

Quando um relatório de apresentação agendado for executado, o arquivo de relatório é encaminhado para os destinatários como um anexo de e-mail denominado **presentationreport\_0**. O número é incrementado, de acordo com o número de relatórios anexos. Observe que o nome do anexo não corresponde ao nome do arquivo armazenado no diretório ReportingOutput. Para localizar um relatório especificado neste diretório, pesquise arquivos criados na data em que o trabalho agendado foi executado.

Os relatórios são excluídos automaticamente do diretório ReportingOutput após 15 dias. Se você quer manter os relatórios durante um período mais longo, inclua-os em sua rotina de backup ou agende-os e salve os arquivos enviados por e-mail em um local padrão que permita armazenamento de longo prazo.

Dependendo do número de relatórios que você gerar diariamente, os arquivos de relatórios podem ocupar quantidades consideráveis de espaço em disco. Certifique-se de que exista espaço em disco adequado disponível no computador do WebSense Manager. Se o diretório ReportingOutput ficar grande demais antes da exclusão automática dos arquivos, você pode excluir os arquivos manualmente.

O software WebSense gera o relatório no formato que você escolher: PDF (Adobe Reader), XLS (Microsoft Excel) ou HTML. Se você escolher o formato HTML, o relatório é exibido no painel de conteúdo do WebSense Manager. Esses relatórios não podem ser impressos ou salvos em arquivo. Para imprimir ou salvar um relatório em arquivo, escolha o formato de saída PDF ou XLS.

Se você escolher o formato PDF ou XLS, terá a opção de salvar o arquivo de relatório em disco ou exibi-lo em uma janela separada.



#### **Importante**

Para exibir relatórios de apresentação em formato PDF, o Adobe Reader v7.0 ou mais recente deve estar instalado no computador a partir do qual você está acessando o WebSense Manager.

Para exibir relatórios de apresentação em formato XLS, o Microsoft Excel 2003 ou mais recente deve estar instalado no computador a partir do qual você está acessando o WebSense Manager.

---

Na página Relatórios de apresentação, navegue no Catálogo de relatórios e selecione um relatório de interesse. Em seguida, use os controles na página para executar o

relatório, criar uma cópia para a qual você pode personalizar o filtro de relatório, e mais.

<b>Botão</b>	<b>Ação</b>
Mostrar somente favoritos	<p>Selecione esta opção para limitar o Catálogo de relatórios a exibir apenas os relatórios marcados como Favoritos.</p> <p>Desmarque esta opção para restaurar a lista completa de relatórios.</p>
Editar filtro de relatório	<p>Disponível apenas quando uma cópia de um relatório predefinido é selecionada, esta opção permite selecionar categorias, protocolos, usuários e ações para inclusão no relatório. Consulte <a href="#">Copiando um relatório de apresentação</a>, página 99.</p>
Copiar	<p>Faz uma cópia do relatório selecionado e adiciona ao Catálogo de relatórios como um relatório personalizado. Consulte <a href="#">Copiando um relatório de apresentação</a>, página 99.</p> <p>Selecione o relatório personalizado e defina parâmetros específicos para ele, clicando em <b>Editar filtro de relatório</b>.</p>
Favorito	<p>Marca o relatório selecionado como um Favorito ou remove a designação de Favorito. Consulte <a href="#">Trabalhando com favoritos</a>, página 106.</p> <p>O Catálogo de relatórios mostra um símbolo de estrela ao lado do nome do relatório para qualquer relatório marcado como Favorito. Use a caixa de seleção <b>Mostrar somente favoritos</b> para controlar quais relatórios aparecem no Catálogo de relatórios.</p>
Excluir	<p>Exclui a cópia do relatório selecionado do Catálogo de relatórios. Você não pode excluir relatórios predefinidos instalados com o software.</p> <p>Se o relatório excluído aparece em trabalhos agendados, continuará a ser gerado com esses trabalhos.</p>
Executar	<p>Gera o relatório selecionado depois que você definir o intervalo de datas e o formato de saída. Consulte <a href="#">Gerando relatórios de apresentação</a>, página 107.</p> <p>Para controlar outros aspectos de um relatório personalizado (copiar de um relatório predefinido), consulte <a href="#">Copiando um relatório de apresentação</a>, página 99.</p> <p>Para agendar o relatório para executar em outro horário ou com uma programação repetida, clique em Agendador.</p>

Os botões acima da página fornecem opções adicionais para relatórios de apresentação.

Botão	Ação
Fila detrabalhos	Exibe uma página listando trabalhos agendados que foram criados, junto com o status de cada trabalho. Consulte <a href="#">Exibindo a lista de trabalhos agendados</a> , página 113
Agendador	Permite definir um trabalho que contém um ou mais relatórios para execução em um horário específico ou em uma programação repetida. Consulte <a href="#">Agendando relatórios de apresentação</a> , página 108.

## Copiando um relatório de apresentação

Tópicos relacionados:

- ◆ [Definindo o filtro de relatório](#), página 100
- ◆ [Relatórios de apresentação](#), página 96

Inicialmente, a página **Relatórios de apresentação** mostra um Catálogo de relatórios que lista todos os relatórios predefinidos instalados com o software. Você pode gerar qualquer desses relatórios para um período de tempo específico, selecionando o relatório e clicando em Executar.

Esses relatórios predefinidos também funcionam como modelos que podem ser copiados para criar um filtro de relatório personalizado. Crie um filtro de relatório para controlar elementos como quais usuários, categorias, protocolos e ações devem ser incluídos quando você gerar um relatório a partir da cópia.

Depois de copiar um relatório e editar o filtro de relatório, você pode copiar o novo relatório para criar variações com base na cópia.

1. Selecione qualquer relatório no Catálogo de relatórios.
2. Clique em **Copiar**.  
Uma duplicata do nome do relatório aparece no Catálogo de relatórios, com um código anexo para indicar que é uma cópia.
3. Selecione a cópia no Catálogo de relatórios e clique em **Editar filtro de relatório** para modificar os elementos do relatório. Consulte [Definindo o filtro de relatório](#), página 100.

## Definindo o filtro de relatório

Tópicos relacionados:

- ◆ [Copiando um relatório de apresentação, página 99](#)
- ◆ [Gerando relatórios de apresentação, página 107](#)

Os filtros de relatório permitem controlar quais informações são incluídas em um relatório. Por exemplo, você pode optar por limitar um relatório a clientes, categorias, classes de risco ou protocolos selecionados, ou mesmo ações de filtragem selecionadas (permitir, bloquear, e assim por diante). Você também pode definir um novo nome e descrição para a entrada no Catálogo de relatórios, especificar um logotipo personalizado para aparecer, e definir outras opções gerais pelo filtro de relatório.



### Obs.:

Usar um logotipo personalizado requer alguma preparação antes de definir o filtro de relatório. Você deve criar a imagem desejada em um formato gráfico compatível e posicionar o arquivo no local apropriado. Consulte [Personalizando o logotipo do relatório, página 105](#).

---

As opções específicas disponíveis no filtro dependem do relatório selecionado. Por exemplo, se você selecionou um relatório de informações de grupo, como Principais grupos bloqueados por solicitações, pode controlar quais grupos aparecem no relatório, mas não pode escolher usuários individuais.

O filtro para relatórios predefinidos não pode ser alterado. Você pode editar o filtro para uma cópia de um relatório predefinido:

1. Selecione um relatório no Catálogo de relatórios.  
Se o botão Editar filtro de relatório está desativado, continue com etapa 2.  
Se o botão Editar filtro de relatório está ativado, pule para a etapa 3.
2. Clique em **Copiar** para fazer uma cópia que você pode personalizar.  
Uma duplicata do nome do relatório aparece no Catálogo de relatórios, com um código anexo para indicar que é uma cópia.
3. Clique no botão **Editar filtro de relatório**.  
A página Filtro de relatório é aberta, com guias separadas para administrar diferentes elementos do relatório. Selecione os itens que deseja em cada guia, depois clique em **Próximo** para ir para a próxima guia. Para obter instruções detalhadas, consulte:
  - [Selecionando clientes para um relatório, página 101](#)
  - [Selecionando categorias para um relatório, página 102](#)
  - [Selecionando protocolos para um relatório, página 103](#)
  - [Selecionando ações para um relatório, página 103](#)

- [Definindo as opções de relatórios](#), página 104
- 4. Na guia **Confirmar**, escolha se deseja executar ou agendar o relatório, além de salvar o filtro de relatório. Consulte [Confirmando a definição do filtro de relatório](#), página 106.

## Selecionando clientes para um relatório

Tópicos relacionados:

- ◆ [Selecionando categorias para um relatório](#), página 102
- ◆ [Selecionando protocolos para um relatório](#), página 103
- ◆ [Selecionando ações para um relatório](#), página 103
- ◆ [Definindo as opções de relatórios](#), página 104
- ◆ [Confirmando a definição do filtro de relatório](#), página 106

A guia **Clientes** da página Relatórios de apresentação > Filtro de relatório permite controlar quais clientes estão incluídos no relatório. Você pode selecionar apenas um tipo de cliente para cada relatório. Por exemplo, você não pode selecionar alguns usuários e alguns grupos para o mesmo relatório.

Quando a definição de relatório especifica um tipo de cliente específico, você pode escolher clientes daquele tipo ou clientes que representam um grupo maior. Por exemplo, se você está definindo um filtro para um relatório baseado em principais grupos bloqueados por solicitações, pode selecionar grupos, domínios ou unidades organizacionais para o relatório, mas não pode selecionar usuários individuais.

Não são necessárias seleções nesta guia se você deseja reportar sobre todos os clientes relevantes.

1. Selecione um tipo de cliente na lista suspensa.
2. Defina o número máximo de resultados da pesquisa na lista **Limitar pesquisa**.  
Dependendo do tráfego em sua empresa, pode haver grandes números de usuários, grupos ou domínios no banco de dados de log. Esta opção administra o tamanho da lista de resultados, e o tempo necessário para exibir os resultados da pesquisa.
3. Digite um ou mais caracteres para pesquisa e clique em **Pesquisar**.  
Use o asterisco (\*) como curinga para indicar caracteres ausentes. Por exemplo, J\*a poderia retornar Júlia, Janaína, Juliana, Joana, e assim por diante.  
Defina suas seqüências de caracteres de pesquisa com cuidado, para garantir que todos os resultados desejados estejam incluídos no número selecionado para limitação da pesquisa.
4. Destaque uma ou mais entradas na lista de resultados e clique no botão de seta para a direita (>) para movê-los para a lista **Selecionados**.
5. Repita as etapas 2-4 conforme necessário para fazer pesquisas adicionais e acrescentar mais clientes à lista Selecionados.

- Depois de fazer as seleções, clique em **Próximo** para abrir a guia Categorias. Consulte [Selecionando categorias para um relatório](#), página 102.

## Selecionando categorias para um relatório

Tópicos relacionados:

- ◆ [Selecionando clientes para um relatório](#), página 101
- ◆ [Selecionando protocolos para um relatório](#), página 103
- ◆ [Selecionando ações para um relatório](#), página 103
- ◆ [Definindo as opções de relatórios](#), página 104
- ◆ [Confirmando a definição do filtro de relatório](#), página 106

A guia **Categorias** da página Relatórios de apresentação > Filtro de relatório permite controlar as informações incluídas no relatório com base em categorias ou classes de risco. Consulte [Classes de risco](#), página 39.

Não são necessárias seleções nesta guia se você deseja reportar sobre todas as categorias ou classes de risco relevantes.

- Selecione uma classificação: **Categoria** ou **Classe de risco**.

Expanda uma categoria principal para exibir suas subcategorias. Expanda uma classe de risco para consultar uma lista das categorias designadas atualmente para a classe de risco.

Se o relatório associado é para uma classe de risco específica, apenas a classe de risco relevante e as categorias que representa estão disponíveis para seleção.



**Obs.:**

Se você selecionar um subconjunto de categorias para a classe de risco nomeada no relatório, considere modificar o título do relatório para refletir suas seleções.

- Marque a caixa de seleção para cada categoria ou classe de risco que será incluída no relatório.

Use os botões **Selecionar tudo** e **Limpar tudo** abaixo da lista para minimizar o número de seleções individuais necessárias.

- Clique no botão de seta para a direita (>) para mover suas seleções para a lista **Selecionadas**.

Quando você marca uma classe de risco, clicar na seta para a direita coloca todas as categorias associadas na lista Selecionadas.

- Depois que todas as seleções estiverem concluídas, clique em **Próximo** para abrir a guia Protocolos. Consulte [Selecionando protocolos para um relatório](#), página 103.

## Selecionando protocolos para um relatório

Tópicos relacionados:

- ◆ [Selecionando clientes para um relatório](#), página 101
- ◆ [Selecionando categorias para um relatório](#), página 102
- ◆ [Selecionando ações para um relatório](#), página 103
- ◆ [Definindo as opções de relatórios](#), página 104
- ◆ [Confirmando a definição do filtro de relatório](#), página 106

A guia **Protocolos** da página Relatórios de apresentação > Filtro de relatório permite controlar quais protocolos são incluídos no relatório.

Não são necessárias seleções nesta guia se você deseja reportar sobre todos os protocolos relevantes.

1. Expanda e contraia os grupos de protocolos com o ícone ao lado do nome do grupo.
2. Marque a caixa de seleção para cada protocolo que será incluído no relatório. Use os botões **Selecionar tudo** e **Limpar tudo** abaixo da lista para minimizar o número de seleções individuais necessárias.
3. Clique no botão de seta para a direita (>) para mover suas seleções para a lista **Selecionadas**.
4. Depois que todas as seleções estiverem concluídas, clique em **Próximo** para abrir a guia Ações. Consulte [Selecionando ações para um relatório](#), página 103.

## Selecionando ações para um relatório

Tópicos relacionados:

- ◆ [Selecionando clientes para um relatório](#), página 101
- ◆ [Selecionando categorias para um relatório](#), página 102
- ◆ [Selecionando protocolos para um relatório](#), página 103
- ◆ [Definindo as opções de relatórios](#), página 104
- ◆ [Confirmando a definição do filtro de relatório](#), página 106

A guia **Ações** da página Relatórios de apresentação > Filtro de relatório permite controlar quais ações de filtragem (por exemplo, permitidas pelo filtro de acesso limitado, bloqueadas por cota) são incluídas no relatório. Se o relatório especifica um tipo de ação específico, como Bloqueadas, você fica limitado a selecionar ações daquele tipo para o relatório.

Não são necessárias seleções nesta guia se você deseja reportar sobre todas as ações relevantes.

1. Expanda e contraia os grupos de ações com o ícone ao lado do nome do grupo.
2. Marque a caixa de seleção para cada ação que será incluída no relatório.  
Use os botões **Selecionar tudo** e **Limpar tudo** abaixo da lista para minimizar o número de seleções individuais necessárias.
3. Clique no botão de seta para a direita (>) para mover suas seleções para a lista **Selecionadas**.
4. Depois que todas as seleções estiverem concluídas, clique em **Próximo** para abrir a guia Opções. Consulte [Definindo as opções de relatórios](#), página 104.

## Definindo as opções de relatórios

Tópicos relacionados:

- ◆ [Personalizando o logotipo do relatório](#), página 105
- ◆ [Selecionando clientes para um relatório](#), página 101
- ◆ [Selecionando categorias para um relatório](#), página 102
- ◆ [Selecionando protocolos para um relatório](#), página 103
- ◆ [Selecionando ações para um relatório](#), página 103
- ◆ [Definindo as opções de relatórios](#), página 104
- ◆ [Confirmando a definição do filtro de relatório](#), página 106

Use a guia **Opções** da página Relatórios de apresentação > Filtro de relatório para configurar diversos aspectos do relatório.

1. Modifique o **Nome do catálogo de relatórios** que aparece no Catálogo de relatórios. O nome pode ter até 85 caracteres.  
Este nome não aparece no relatório em si; é usado apenas para identificar a combinação única de formato de relatório e filtro no Catálogo de relatórios.
2. Modifique o **Título do relatório** que aparece no relatório. O título pode ter até 85 caracteres.
3. Modifique a **Descrição** que aparece no Catálogo de relatórios. A descrição pode ter até 336 caracteres.  
A descrição deve ajudar você a identificar esta combinação única de formato de relatório e filtro no Catálogo de relatórios.
4. Selecione um logotipo para aparecer no relatório.  
Todos os arquivos de imagem suportados no diretório apropriado são listados. Consulte [Personalizando o logotipo do relatório](#), página 105.
5. Marque a caixa de seleção **Salvar como favorito** para que o relatório seja listado como Favorito.  
O Catálogo de relatórios mostra um símbolo de estrela ao lado dos relatórios Favoritos. Você pode selecionar **Mostrar somente favoritos** na página Catálogo de relatórios para reduzir o número de relatórios listados, o que permite ir mais rápido para um relatório específico.

6. Marque a caixa de seleção **Mostrar somente principal** e digite um número de 1 a 20 para limitar o número de itens incluídos no relatório.

Esta opção aparece apenas se o relatório selecionado está formatado como um relatório N primeiros, para exibição de um número de itens limitado. A limitação de itens depende do relatório. Por exemplo, para o relatório Principais categorias visitadas, esta entrada determina quantas categorias são incluídas no relatório.

7. Depois que todas as entradas e seleções estiverem concluídas, clique em **Próximo** para abrir a guia Confirmar. Consulte [Confirmando a definição do filtro de relatório, página 106](#).

### Personalizando o logotipo do relatório

Os relatórios de apresentação predefinidos exibem o logotipo do Websense no canto superior esquerdo. Quando você copia um relatório predefinido e define seu filtro de relatório, pode escolher outro logotipo.

1. Crie um arquivo de imagens em um dos seguintes formatos:

- .bmp
- .gif
- .jif
- .jpe
- .jpg
- .jpeg
- .png
- .tiff

2. Use no máximo 25 caracteres para o nome do arquivo de imagens, incluindo a extensão.
3. Coloque o arquivo de imagens no seguinte diretório:

```
<caminho_de_instalacao>\Manager\ReportingTemplates\images
```

O caminho de instalação padrão é C:\Arquivos de Programas\Websense.

Todos os arquivos de imagens suportados neste diretório aparecem automaticamente na lista suspensa na guia Opções da página Filtro de relatório. A imagem é dimensionada automaticamente para ajuste no espaço alocado para o logotipo. (Consulte [Definindo as opções de relatórios, página 104](#).)



#### Obs.:

Não remova imagens que estão ativas nos filtros de relatórios a partir deste diretório. Se o arquivo de logotipo especificado estiver ausente, não é possível gerar o relatório.

## Confirmando a definição do filtro de relatório

Tópicos relacionados:

- ◆ [Selecionando clientes para um relatório](#), página 101
- ◆ [Selecionando categorias para um relatório](#), página 102
- ◆ [Selecionando protocolos para um relatório](#), página 103
- ◆ [Selecionando ações para um relatório](#), página 103
- ◆ [Definindo as opções de relatórios](#), página 104

A guia **Confirmar** da página Relatórios de apresentação > Filtro de relatório exibe o nome e a descrição que aparecerão no Catálogo de relatórios, e permite escolher como prosseguir.

### 1. Revise **Nome** e **Descrição**.

Se forem necessárias alterações, clique em **Voltar** para voltar à guia Opções, onde você pode fazer essas alterações. (Consulte [Definindo as opções de relatórios](#), página 104.)

### 2. Indique como você quer prosseguir:

Opção	Descrição
Salvar	Salva o filtro de relatório e volta ao Catálogo de relatórios. Consulte <a href="#">Relatórios de apresentação</a> , página 96.
Salvar e executar	Salva o filtro de relatório e abre a página Executar relatório. Consulte <a href="#">Gerando relatórios de apresentação</a> , página 107.
Salvar e programar	Salva o filtro de relatório e abre a página Agendar relatório. Consulte <a href="#">Agendando relatórios de apresentação</a> , página 108.

### 3. Clique em **Concluir** para implementar a seleção feita na etapa 2.

## Trabalhando com favoritos

Tópicos relacionados:

- ◆ [Relatórios de apresentação](#), página 96
- ◆ [Gerando relatórios de apresentação](#), página 107
- ◆ [Agendando relatórios de apresentação](#), página 108

Você pode marcar qualquer relatório de apresentação, predefinido ou personalizado, como um Favorito. Use esta opção para identificar os relatórios que você gera com mais frequência e quer poder localizar rapidamente no Catálogo de relatórios.

1. Na página **Relatórios de apresentação**, destaque um relatório que você gera com frequência e quer poder localizar rapidamente.
2. Clique em **Favorito**.  
Um símbolo de estrela aparece ao lado dos nomes de relatórios favoritos na lista, permitindo que você os identifique rapidamente quando todos os relatórios são mostrados.
3. Marque a caixa de seleção **Mostrar somente favoritos** acima do Catálogo de relatórios para limitar a lista aos marcados como Favoritos. Desmarque esta caixa de seleção para restaurar a lista completa de relatórios.

Se as suas necessidades mudarem e um relatório Favorito não estiver mais sendo usado com frequência, você pode remover a designação de Favorito.

1. Destaque um relatório que tem o símbolo de estrela de Favorito.
2. Clique em **Favorito**.  
O símbolo de estrela é removido do nome do relatório no Catálogo de relatórios. Agora, o relatório é omitido da lista se você escolher **Mostrar somente favoritos**.

## Gerando relatórios de apresentação

Tópicos relacionados:

- ◆ [Relatórios de apresentação, página 96](#)
- ◆ [Agendando relatórios de apresentação, página 108](#)

Gerar um único relatório imediatamente envolve as etapas mostradas abaixo.



**Obs.:**

Antes de gerar um relatório em formato PDF, o Adobe Reader v7.0 ou mais recente deve estar instalado no computador a partir do qual você está acessando o Websense Manager.

Antes de gerar um relatório em formato XLS, o Microsoft Excel 2003 ou mais recente deve estar instalado no computador a partir do qual você está acessando o Websense Manager.

Se o software apropriado não estiver instalado, você tem a opção de salvar o arquivo.

Para criar trabalhos com um ou mais relatórios para executar uma vez ou em um ciclo de repetição com o recurso de programação de relatórios de apresentação. Consulte [Agendando relatórios de apresentação, página 108](#).

1. Na página **Relatórios de apresentação**, destaque um relatório na árvore do Catálogo de relatórios e clique em **Executar**.

2. Selecione a **Data inicial** e a **Data final** para os dados do relatório.
3. Selecione um **Formato de saída** para o relatório.

Formato	Descrição
PDF	Portable Document Format. Os arquivos PDF são visualizados no Adobe Reader.
HTML	HyperText Markup Language. Os arquivos HTML podem ser visualizados diretamente no navegador Internet Explorer ou Firefox.
XLS	Planilha em Excel. Os arquivos XLS são visualizados no Microsoft Excel.

4. Se você selecionou um relatório **N primeiros**, escolha quantos itens serão incluídos no relatório.
5. Clique em **Executar**.  
Os relatórios em HTML aparecem no painel de conteúdo. Se você selecionou a saída em PDF ou XLS, terá a opção de abrir o relatório em uma janela separada ou salvar o relatório em disco.
6. Para imprimir um relatório, use a opção imprimir do programa que exibe o relatório.  
Para obter melhores resultados, gere a saída em PDF ou XLS para impressão. Em seguida, use as opções de impressão no Adobe Reader ou Microsoft Excel, respectivamente.

Você pode salvar um relatório com saída em formato PDF ou XLS usando o recurso Salvar no Adobe Reader ou Microsoft Excel.

## Agendando relatórios de apresentação

Tópicos relacionados:

- ◆ [Relatórios de apresentação, página 96](#)
- ◆ [Gerando relatórios de apresentação, página 107](#)
- ◆ [Exibindo a lista de trabalhos agendados, página 113](#)
- ◆ [Copiando um relatório de apresentação, página 99](#)

Você pode executar relatórios de apresentação conforme são necessários ou usar a página **Relatórios de apresentação > Agendador** para criar trabalhos que definem uma programação para executar um ou mais relatórios.

Os relatórios gerados por trabalhos agendados são distribuídos para um ou mais destinatários via e-mail. Ao criar trabalhos agendados, considere se o seu servidor de e-mail será capaz de administrar o tamanho e a quantidade de arquivos de relatório anexos.

Para acessar o Agendador:

- ◆ Clique no botão **Agendador** no alto da página Relatórios de apresentação (acima do Catálogo de relatórios).
- ◆ Ao adicionar ou editar um filtro de relatório para um relatório, escolha **Salvar e programar** na guia Confirmar e clique em **Concluir**. (Consulte [Copiando um relatório de apresentação](#), página 99.)
- ◆ Clique no link do nome do trabalho na página Fila de trabalhos para editar um trabalho.
- ◆ Clique em **Adicionar** na página Fila de trabalhos para criar um novo trabalho.

A página Agendador contém diversas guias para selecionar os relatórios que serão executados e agendar a execução. Para obter instruções detalhadas, consulte:

- ◆ [Definindo a programação](#), página 109
- ◆ [Selecionando relatórios para agendar](#), página 111
- ◆ [Definindo o intervalo de datas](#), página 111
- ◆ [Selecionando opções de saída](#), página 112

Depois de criar trabalhos, você pode exibir uma lista de trabalhos, com status e outras informações úteis. Consulte [Exibindo a lista de trabalhos agendados](#), página 113.

## Definindo a programação

Tópicos relacionados:

- ◆ [Agendando relatórios de apresentação](#), página 108
- ◆ [Selecionando relatórios para agendar](#), página 111
- ◆ [Selecionando opções de saída](#), página 112
- ◆ [Definindo o intervalo de datas](#), página 111

Defina um trabalho de relatórios para ocorrer uma vez ou em um ciclo de repetição na guia **Agendar** da página Relatórios de apresentação >.



### Obs.:

É recomendável agendar trabalhos de relatório em diferentes dias e horários, para evitar a sobrecarga do banco de dados de log e a redução do desempenho para registros e relatórios interativos.

1. Digite um **Nome do trabalho** que identifique este trabalho agendado de forma única.

2. Selecione um **Padrão de recorrência** e **Opções de recorrência** para o trabalho. As opções específicas disponíveis dependem do padrão selecionado.

Padrão	Opções
Uma Vez	Digite a data exata em que o trabalho será executado ou clique no ícone para selecionar em um calendário.
Diário	Não estão disponíveis opções de recorrência adicionais.
Semanal	Marque a caixa de seleção para cada dia da semana em que o trabalho será executado.
Mensal	Digite as datas durante o mês para execução do trabalho. As datas devem ser um número entre 1 e 31, e devem ser separadas por vírgulas (1,10,20). Para executar o trabalho em datas consecutivas a cada mês, digite uma data inicial e uma data final, separadas por um hífen (3-5).

3. Em **Agendar horário**, defina a hora inicial para execução do trabalho. O trabalho começa de acordo com a hora do computador que está executando o Websense Manager.



**Obs.:**

Para começar a gerar relatórios agendados hoje, selecione uma hora tarde o suficiente para que você possa concluir a definição do trabalho antes da hora inicial.

4. Em **Agendar período**, selecione uma data para começar o trabalho, e uma opção para concluir o trabalho.

Opção	Descrição
Sem data final	O trabalho continua a ser executado de acordo com a programação estabelecida, indefinidamente. Para cancelar o trabalho em alguma ocasião no futuro, edite ou exclua o trabalho. Consulte <a href="#">Exibindo a lista de trabalhos agendados</a> , página 113.
Terminar depois de	Selecione o número de vezes para executar o trabalho. Depois daquele número de ocorrências, o trabalho não será executado novamente, mas fica na Fila de trabalhos até ser excluído. Consulte <a href="#">Exibindo a lista de trabalhos agendados</a> , página 113.
Terminar em	Define a data em que o trabalho pára de ser executado. Não será executado na data ou posteriormente.

5. Clique em **Próximo** para abrir a guia Geração de relatórios. Consulte [Selecionando relatórios para agendar](#), página 111.

## Selecionando relatórios para agendar

Tópicos relacionados:

- ◆ [Agendando relatórios de apresentação](#), página 108
- ◆ [Definindo a programação](#), página 109
- ◆ [Selecionando opções de saída](#), página 112
- ◆ [Definindo o intervalo de datas](#), página 111

Use a guia **Selecionar relatório** da página > Agendador de relatórios de apresentação para escolher relatórios para o trabalho.

1. Destaque um relatório para este trabalho na árvore do Catálogo de relatórios.
2. Clique no botão de seta para a direita (>) para mover o relatório para a lista **Selecionados**.
3. Repita as etapas 1 e 2 até que todos os relatórios para este trabalho apareçam na lista **Selecionados**.
4. Clique em **Próximo** para abrir a guia Intervalo de datas. Consulte [Definindo o intervalo de datas](#), página 111.

## Definindo o intervalo de datas

Tópicos relacionados:

- ◆ [Agendando relatórios de apresentação](#), página 108
- ◆ [Definindo a programação](#), página 109
- ◆ [Selecionando relatórios para agendar](#), página 111
- ◆ [Selecionando opções de saída](#), página 112

Use a guia **Intervalo de datas** da página > Agendador de relatórios de apresentação para definir o intervalo de datas para o trabalho. As opções disponíveis dependem de sua seleção para **Intervalo de datas**.

Intervalo de datas	Descrição
Todas as datas	Os relatórios incluem todas as datas disponíveis no banco de dados de log. Não são necessárias entradas adicionais. Quando esta opção é usada para repetir trabalhos, poderá haver informações duplicadas em relatórios em execuções separadas.

Intervalo de datas	Descrição
Datas específicas	Escolha as datas exatas para início ( <b>De</b> ) e fim ( <b>Até</b> ) para os relatórios neste trabalho. Esta opção é ideal para trabalhos executados apenas uma vez. Escolher esta opção para uma programação repetida resulta em relatórios duplicados.
Datas relativas	Use as listas suspensas para escolher o número de períodos que serão reportados (Este, Último, Últimos 2, e assim por diante), e o tipo de período (Dias, Semanas ou Meses). Por exemplo, o trabalho poderia abranger as Últimas 2 semanas ou Este mês. Semana representa uma semana de calendário, de domingo a domingo. Mês representa um mês de calendário. Por exemplo, Esta semana produz um relatório de domingo até hoje; Este mês produz um relatório do primeiro dia do mês até hoje; Semana passada produz um relatório do domingo anterior até sábado; e assim por diante. Esta opção é ideal para trabalhos executados em uma programação repetida. Permite administrar quantos dados aparecem em cada relatório, e minimiza a duplicação de dados em relatórios em execuções separadas.

Depois de definir o intervalo de datas para o trabalho, clique em **Próximo** para exibir a guia Saída. Consulte [Selecionando opções de saída](#), página 112.

## Selecionando opções de saída

Tópicos relacionados:

- ◆ [Agendando relatórios de apresentação](#), página 108
- ◆ [Definindo a programação](#), página 109
- ◆ [Selecionando relatórios para agendar](#), página 111
- ◆ [Definindo o intervalo de datas](#), página 111

Depois de selecionar os relatórios para um trabalho, use a guia **Saída** para selecionar o formato de saída e as opções de distribuição.

1. Selecione o formato de arquivo para o relatório concluído.

Formato	Descrição
PDF	Portable Document Format. Os destinatários devem ter o Adobe Reader v7.0 ou mais recente para exibir os relatórios em PDF.
XLS	Planilha em Excel. Os destinatários devem ter o Microsoft Excel 2003 ou mais recente para exibir os relatórios em XLS.

2. Digite endereços de e-mail para distribuição do relatório.

Digite cada endereço em uma linha separada.

3. Marque a caixa de seleção **Personalizar assunto e corpo de e-mail**, se desejado. Em seguida, digite o texto personalizado para **Assunto e Corpo** do e-mail de distribuição deste trabalho.
4. Clique em **Salvar trabalho** para salvar e implementar a definição de trabalho, e exiba a página Fila de trabalhos.
5. Revise este trabalho e qualquer outro trabalho agendado. Consulte [Exibindo a lista de trabalhos agendados](#), página 113.

## Exibindo a lista de trabalhos agendados

Tópicos relacionados:

- ◆ [Relatórios de apresentação](#), página 96
- ◆ [Agendando relatórios de apresentação](#), página 108
- ◆ [Selecionando opções de saída](#), página 112
- ◆ [Agendando relatórios investigativos](#), página 135

A página **Relatórios de apresentação > Fila de trabalhos** lista os trabalhos agendados criados para relatórios de apresentação. A lista fornece o status de cada trabalho, e também informações básicas sobre o trabalho; por exemplo, com que frequência é executado. Nesta página, você pode adicionar e excluir trabalhos agendados, suspender um trabalho temporariamente, e mais.

(Para revisar trabalhos agendados para relatórios investigativos, consulte [Gerenciando trabalhos programados de relatórios investigativos](#), página 138.)

A lista fornece as seguintes informações para cada trabalho.

Coluna	Descrição
Nome do trabalho	O nome atribuído quando o trabalho foi criado.
Estado	Um dos seguintes: <ul style="list-style-type: none"> <li>• ATIVADO indica um trabalho que é executado de acordo com o padrão de recorrência estabelecido.</li> <li>• DESATIVADO indica um trabalho que está inativo e não é executado.</li> </ul>
Recorrência	O padrão de recorrência (Uma vez, Diário, Semanal, Mensal) definido para este trabalho.
Histórico	Clique no link <b>Detalhes</b> para abrir a página Histórico de trabalhos para o trabalho selecionado. Consulte <a href="#">Exibindo o histórico de trabalhos</a> , página 114.
Próxima programação	Data e hora para a próxima execução.
Proprietário	O nome de usuário do administrador que agendou o trabalho.

Use as opções na página para administrar os trabalhos. Alguns dos botões requerem que você primeiro marque a caixa de seleção ao lado do nome de cada trabalho que deve ser incluído.

Opção	Descrição
Link de nome do trabalho	Abre a página Agendador, onde você pode editar a definição do trabalho. Consulte <a href="#">Agendando relatórios de apresentação</a> , página 108.
Adicionar trabalho	Abre a página Agendador, onde você pode definir um novo trabalho. Consulte <a href="#">Agendando relatórios de apresentação</a> , página 108.
Excluir	Exclui da Fila de trabalhos todos os trabalhos que foram marcados na lista. Depois que um trabalho foi excluído, não pode ser restaurado.  Para interromper temporariamente a execução de um trabalho específico, use o botão <b>Desativar</b> .
Executar agora	Começa imediatamente a executar os trabalhos que foram marcados na lista. Isso é em acréscimo às execuções agendadas regularmente.
Ativar	Reativa trabalhos desativados que foram marcados na lista. O trabalho começa a ser executado de acordo com a programação estabelecida.
Desativar	Interrompe a execução de trabalhos ativados que foram marcados na lista. Use para suspender temporariamente um trabalho que talvez deseje restaurar no futuro.

## Exibindo o histórico de trabalhos

Tópicos relacionados:

- ◆ [Agendando relatórios de apresentação](#), página 108
- ◆ [Exibindo a lista de trabalhos agendados](#), página 113

Use a página **Relatórios de apresentação > Fila de trabalhos > Histórico de trabalhos** para exibir informações sobre tentativas recentes de executar um trabalho selecionado. A página lista cada relatório separadamente, fornecendo as seguintes informações.

Coluna	Descrição
Nome do relatório	Título impresso no relatório.
Data inicial	Data e hora em que o relatório começou a ser executado.
Data final	Data e hora em que o relatório foi concluído.
Status	Indicador de se o relatório foi bem-sucedido ou falhou.
Mensagem	Informações relevantes sobre o trabalho, como se o relatório foi encaminhado por e-mail com êxito.

## Relatórios investigativos

Tópicos relacionados:

- ◆ [Relatórios de resumo](#), página 117
- ◆ [Relatórios de resumo em vários níveis](#), página 121
- ◆ [Relatórios de detalhes flexíveis](#), página 122
- ◆ [Relatórios de detalhe de atividade do usuário](#), página 126
- ◆ [Relatórios padrão](#), página 131
- ◆ [Relatórios investigativos favoritos](#), página 132
- ◆ [Agendando relatórios investigativos](#), página 135
- ◆ [Relatórios de valores atípicos](#), página 138
- ◆ [Saída para arquivo](#), página 139
- ◆ [Conexão de banco de dados e padrões de relatórios](#), página 330

Use a página **Geração de relatórios > Relatórios investigativos** para analisar a atividade de filtragem de Internet de forma interativa.

Inicialmente, a página principal de Relatórios investigativos mostra um relatório de resumo de atividade por classe de risco. Trabalhe na exibição do relatório de resumo, clicando nos links e elementos disponíveis para explorar áreas de interesse e obter informações gerais sobre o uso de Internet em sua empresa. Consulte [Relatórios de resumo](#), página 117.

Relatórios de resumo em vários níveis (consulte [Relatórios de resumo em vários níveis](#), página 121) e relatórios de detalhes flexíveis (consulte [Relatórios de detalhes flexíveis](#), página 122) permitem analisar as informações de diferentes perspectivas.

Outros recursos de exibição de relatórios e relatórios investigativos podem ser acessados a partir de links no alto da página. Consulte a tabela abaixo para uma lista de links e os recursos que acessam. (Nem todos os links estão disponíveis em todas as páginas.)

Opção	Ação
Usuário por dia/mês	Exibe uma caixa de diálogo que permite definir um relatório de atividades de um usuário específico, abrangendo um dia ou um mês. Para obter mais informações, consulte <a href="#">Relatórios de detalhe de atividade do usuário</a> , página 126.
Relatórios padrão	Exibe uma lista de relatórios predefinidos, para que você possa ver rapidamente uma combinação específica de dados. Consulte <a href="#">Relatórios padrão</a> , página 131.
Relatórios favoritos	Permite salvar o relatório atual como Favorito, e exibe uma lista de Favoritos existentes, que você pode gerar ou agendar. Consulte <a href="#">Relatórios investigativos favoritos</a> , página 132.

Opção	Ação
Fila detrabalhos	Exibe a lista de trabalhos de relatórios investigativos agendados. Consulte <a href="#">Agendando relatórios investigativos</a> , página 135.
Exibir valores atípicos	Exibe relatórios mostrando o uso da Internet que é significativamente diferente da média. Consulte <a href="#">Relatórios de valores atípicos</a> , página 138.
Opções	Exibe a página para selecionar outro banco de dados de log para relatórios. A página Opções também permite personalizar determinados recursos de relatórios, como o período de tempo inicialmente mostrado em relatórios de resumo e as colunas padrão para relatórios de detalhes. Consulte <a href="#">Conexão de banco de dados e padrões de relatórios</a> , página 330.
	Clique neste botão, à direita dos campos de Pesquisa, para exportar o relatório atual para um arquivo de planilha compatível com Microsoft Excel. Você é solicitado a abrir ou salvar o arquivo. Para abrir o arquivo, o Microsoft Excel 2003 ou mais recente deve estar instalado. Consulte <a href="#">Saída para arquivo</a> , página 139.
	Clique neste botão, à direita dos campos de Pesquisa, para exportar o relatório atual para um arquivo PDF compatível com Adobe Reader. Você é solicitado a abrir ou salvar o arquivo. Para abrir o arquivo, o Adobe Reader versão 7.0 ou mais recente deve estar instalado. Consulte <a href="#">Saída para arquivo</a> , página 139.

Lembre-se de que os relatórios limitam-se às informações que foram registradas no banco de dados de log. Se você desativar o registro para nomes de usuário, endereços IP ou categorias selecionadas (consulte [Configurando o Filtering Service para registro em log](#), página 304), essas informações não poderão ser incluídas. De forma semelhante, se você desativar o registro para determinados protocolos (consulte [Editando um filtro de protocolo](#), página 50), as solicitações para esses protocolos não ficam disponíveis. Se você deseja que os relatórios incluam o nome de domínio (www.domínio.com) e o caminho para uma página específica no domínio (/produtos/produtoA), deve registrar URLs completas (consulte [Configurando o registro de URLs completos](#), página 322).

Os relatórios investigativos do Websense são limitados pelo processador e pela memória disponível no computador que executa o Websense Manager, e também por alguns recursos de rede. A geração de alguns relatórios grandes pode demorar muito. A mensagem de progresso inclui uma opção para salvar o relatório como Favorito, para que você possa programá-lo para execução em outra ocasião. Consulte [Agendando relatórios investigativos](#), página 135.

## Relatórios de resumo

Tópicos relacionados:

- ◆ [Relatórios de resumo em vários níveis](#), página 121
- ◆ [Relatórios de detalhes flexíveis](#), página 122
- ◆ [Relatórios de detalhe de atividade do usuário](#), página 126
- ◆ [Relatórios padrão](#), página 131
- ◆ [Relatórios investigativos favoritos](#), página 132
- ◆ [Agendando relatórios investigativos](#), página 135
- ◆ [Relatórios de valores atípicos](#), página 138
- ◆ [Saída para arquivo](#), página 139

Inicialmente, a página relatórios investigativos fornece um relatório de resumo de uso para todos os usuários por classe de risco, mostrando a atividade do dia atual no banco de dados de log. A medição para este gráfico de barras inicial é Ocorrências (quantas vezes o site foi solicitado). Para configurar o período de tempo para este relatório de resumo inicial, consulte [Conexão de banco de dados e padrões de relatórios](#), página 330.

Altere rapidamente as informações incluídas no relatório ou aprofunde nos detalhes do relatório, clicando nos diversos links e opções disponíveis na página.

1. Selecione uma das seguintes opções na lista **Medição**.

Opção	Descrição
Ocorrências	Quantas vezes o URL foi solicitado. Dependendo de como o Log Server é configurado, podem ser acessos reais, com um registro separado para cada elemento separado de um site solicitado, ou visitas, que combina os diferentes elementos do site em um único registro. Consulte <a href="#">Configurando os arquivos de cache de log</a> , página 311.
Largura de banda [KB]	A quantidade de dados, em quilobytes, contidos na solicitação inicial do usuário e na resposta do website. É o total combinado dos valores Enviados e Recebidos. Lembre-se de que alguns produtos de integração não enviam estas informações para o software Websense. Dois exemplos são Check Point FireWall-1 e Cisco PIX Firewall. Se a sua integração não envia estas informações, e o Websense Network Agent está instalado, ative a opção <b>Log de solicitações HTTP (registro de log aprimorado)</b> para que a placa de rede apropriada ative os relatórios sobre as informações de largura de banda. Consulte <a href="#">Definindo as configurações de placa de rede</a> , página 343.

Opção	Descrição
Enviados [KB]	O número de quilobytes enviados como a solicitação da Internet. Representa a quantidade de dados transmitidos, que podem ser uma solicitação simples para um URL ou um envio mais significativo, se o usuário está se registrando em um website, por exemplo.
Recebidos [KB]	O número de quilobytes recebidos em resposta à solicitação. Inclui todos os textos, imagens e scripts que compõem o site.  Para sites que estão bloqueados, o número de quilobytes varia de acordo com o software que está criando o registro. Quando o Websense Network Agent cria os registros, o número de bytes recebidos para um site bloqueado representa o tamanho da página de bloqueio do Websense.  Se o registro é criado pelo Websense Security Gateway, como resultado de verificação em tempo real, os quilobytes recebidos representam o tamanho da página verificada. Consulte <a href="#">Análise de conteúdo com as opções em tempo real</a> , página 143, para obter mais informação sobre a verificação em tempo real.  Se outro produto de integração cria os registros, os quilobytes recebidos para um site bloqueado podem ser zero (0), podem representar o tamanho da página de bloqueio, ou podem ser um valor obtido a partir do site solicitado.
Tempo de navegação	Uma estimativa do tempo dedicado a visualizar o site. Consulte <a href="#">O que é tempo de navegação na Internet?</a> , página 95.

2. Altere o agrupamento primário do relatório, selecionando uma opção na lista **Uso da Internet por** acima do relatório.

As opções variam de acordo com o conteúdo do banco de dados de log e determinadas considerações de rede. Por exemplo, se existe apenas um grupo ou domínio no banco de dados de log, os Grupos e os Domínios não aparecem nesta lista. De forma semelhante, se existem muitos usuários (mais de 5.000) ou grupos (mais de 3.000), essas opções não aparecem. (Alguns desses limites podem ser configurados. Consulte [Opções de exibição e saída](#), página 332.)

3. Clique em um nome na coluna da esquerda (ou na seta ao lado do nome) para exibir uma lista de opções, como por usuário, por domínio ou por ação.

As opções listadas são semelhantes às listadas em **Uso da Internet por**, personalizadas para serem um subconjunto significativo do conteúdo exibido atualmente.



**Obs.:**

Às vezes, uma opção, como Usuário ou Grupo, aparece em letras vermelhas. Neste caso, selecionar essa opção pode produzir um relatório muito grande, cuja geração demorará muito. Considere aprofundar mais os detalhes antes de selecionar a opção.

4. Selecione uma dessas opções para gerar um novo relatório de resumo mostrando as informações selecionadas para a entrada associada.  
Por exemplo, em um relatório de resumo de Classe de risco, clicar em Usuário na classe de risco Responsabilidade legal gera um relatório da atividade de cada usuário na classe de risco Responsabilidade legal.
5. Clique em uma nova entrada na coluna da esquerda e selecione uma opção para ver mais detalhes sobre o item específico.
6. Use as setas ao lado de um cabeçalho de coluna para alterar a ordem de classificação do relatório.
7. Controle o relatório de resumo com as seguintes opções acima do gráfico. Em seguida, aprofunde em detalhes relacionados, clicando nos elementos do novo relatório.

Opção	Ação
Caminho de relatório (Usuário > Dia)	Ao lado da lista <b>Uso da Internet por</b> está um caminho que mostra as seleções criadas no relatório atual. Clique em qualquer link no caminho para voltar a essa exibição dos dados.
Exibir	<p>Selecione um período para o relatório: Um dia, Uma semana, Um mês ou Tudo. O relatório é atualizado para exibir dados para o período selecionado.</p> <p>Use os botões de seta adjacentes para percorrer os dados disponíveis, um período (dia, semana, mês) de cada vez.</p> <p>À medida que você muda esta seleção, os campos <b>Exibir de</b> são atualizados para refletir o período de tempo que está sendo exibido.</p> <p>O campo <b>Exibir</b> exibe Personalizado, em vez de um período de tempo, se você escolher uma data específica nos campos Exibir de ou na caixa de diálogo Favoritos.</p>
Exibir de... até...	<p>As datas nestes campos são atualizadas automaticamente para refletir o período de tempo que está sendo exibido quando você faz alterações no campo <b>Exibir</b>.</p> <p>Como alternativa, digite datas inicial e final exatas para os relatórios ou clique no ícone de calendário para selecionar as datas desejadas.</p> <p>Clique no botão de seta para a direita adjacente para atualizar o relatório depois de selecionar as datas.</p>
Gráfico de pizza / Gráfico de barras	<p>Quando o gráfico de barras estiver ativo, clique em <b>Gráfico de pizza</b> para exibir o relatório de resumo atual como um gráfico de pizza. Clique na etiqueta da fatia para exibir as mesmas opções que estão disponíveis quando você clica em uma entrada na coluna esquerda do gráfico de barras.</p> <p>Quando o gráfico de pizza estiver ativo, clique em <b>Gráfico de barras</b> para exibir o relatório de resumo atual como um gráfico de barras.</p>
Tela cheia	Selecione esta opção para exibir o relatório investigativo em uma janela separada, sem os painéis de navegação esquerdo e direito.

Opção	Ação
Anônimo / nomes	<p>Clique em <b>Anônimo</b> para que os relatórios exibam um número de identificação do usuário atribuído internamente sempre que um nome de usuário deveria ter aparecido.</p> <p>Quando os nomes estão ocultos, clique em <b>Nomes</b> para exibir os nomes de usuário nestes locais.</p> <p>Em algumas circunstâncias, os nomes de usuário não podem ser exibidos. Para obter mais informações, consulte <a href="#">Configurando o Filtering Service para registro em log</a>, página 304.</p> <p>Se você clicar em Anônimo e depois passar para outra visualização dos dados, como a exibição de detalhes ou valores atípicos, os nomes de usuário permanecem ocultos no novo relatório. Porém, para voltar à exibição de resumo com os nomes ocultos, você deve usar os links no alto do relatório, e não as trilhas no banner.</p> <p>Se administradores individuais nunca devem ter acesso a nomes de usuário em relatórios, atribua uma função em que as permissões de relatório impeçam a visualização de nomes de usuário em relatórios investigativos e o acesso a relatórios de apresentação.</p>
Procurar por	<p>Selecione um elemento de relatório na lista e digite um valor, integral ou parcialmente, para a pesquisa na caixa de texto adjacente.</p> <p>Clique no botão de seta adjacente para iniciar a pesquisa e exibir resultados.</p> <p>Digitar um endereço IP parcial, como 10.5., pesquisa em todas as sub-redes, 10.5.0.0 até 10.5.255.255 neste exemplo.</p>

8. Adicione um subconjunto de informações para todas as entradas, ou para entradas selecionadas, na coluna esquerda, criando um relatório de resumo em vários níveis. Consulte [Relatórios de resumo em vários níveis](#), página 121.
9. Crie um relatório em tabelas para um item específico na coluna esquerda, clicando no número adjacente ou na barra de medições. Este relatório detalhado pode ser modificado para atender as suas necessidades específicas. Consulte [Relatórios de detalhes flexíveis](#), página 122.

## Relatórios de resumo em vários níveis

Tópicos relacionados:

- ◆ [Relatórios investigativos](#), página 115
- ◆ [Relatórios de resumo](#), página 117
- ◆ [Relatórios de detalhes flexíveis](#), página 122
- ◆ [Relatórios de detalhe de atividade do usuário](#), página 126
- ◆ [Relatórios padrão](#), página 131
- ◆ [Relatórios investigativos favoritos](#), página 132
- ◆ [Agendando relatórios investigativos](#), página 135
- ◆ [Relatórios de valores atípicos](#), página 138
- ◆ [Saída para arquivo](#), página 139

Os relatórios de resumo em vários níveis mostram um segundo nível de informações para complementar as informações primárias exibidas. Por exemplo, se a exibição primária mostra classes de risco, você pode definir um segundo nível para saber quais categorias foram mais solicitadas em cada classe de risco. Como outro exemplo, se o relatório primário mostra solicitações para cada categoria, você poderia mostrar as 5 principais categorias e os 10 usuários que fizeram mais solicitações para cada.

Use as configurações imediatamente acima do relatório de resumo para criar um relatório de resumo em vários níveis.

Selecionar os primeiros  por  e exibir  resultados

1. Na lista **Selecionar os primeiros**, escolha um número para designar quantas entradas primárias (coluna da esquerda) serão reportadas. O relatório resultante inclui as entradas primárias com os maiores valores. (Isso mostra as datas mais antigas, se Dia for a entrada primária.)  
Como alternativa, marque a caixa de seleção ao lado das entradas individuais desejadas na coluna da esquerda para reportar apenas essas entradas. O campo **Selecionar os primeiros** exibe **Personalizado**.
2. Na lista **por**, escolha as informações secundárias para o relatório.
3. No campo **Exibir**, escolha o número de resultados secundários que serão reportados para cada entrada primária.
4. Clique em **Exibir resultados** para gerar o relatório de resumo em vários níveis. O relatório de resumo é atualizado para mostrar apenas o número selecionado de entradas primárias. Abaixo da barra para cada entrada primária, uma lista de entradas secundárias aparece.
5. Use as setas ao lado de um cabeçalho de coluna para alterar a ordem de classificação do relatório.

Para voltar a um relatório de resumo com um único nível, selecione outra opção em **Uso da Internet por**. Como alternativa, clique nas entradas primárias ou secundárias e selecione uma opção para gerar um novo relatório investigativo dessas informações.

## Relatórios de detalhes flexíveis

Tópicos relacionados:

- ◆ [Relatórios investigativos](#), página 115
- ◆ [Relatórios de resumo](#), página 117
- ◆ [Relatórios de resumo em vários níveis](#), página 121
- ◆ [Relatórios investigativos favoritos](#), página 132
- ◆ [Agendando relatórios investigativos](#), página 135
- ◆ [Relatórios de valores atípicos](#), página 138
- ◆ [Saída para arquivo](#), página 139
- ◆ [Conexão de banco de dados e padrões de relatórios](#), página 330
- ◆ [Colunas para relatórios de detalhes flexíveis](#), página 124

Os relatórios de detalhes fornecem uma exibição em tabelas das informações no banco de dados de log. Acesse a exibição de relatório de detalhes na página principal depois de visualizar um relatório de resumo para o qual deseja mais detalhes.

Você pode solicitar uma exibição de detalhes a partir de qualquer linha. Porém, ao solicitar um relatório de detalhes baseado em ocorrências, é melhor começar em uma linha que mostra menos de 100.000 ocorrências. Se houver mais de 100.000 ocorrências para uma linha específica, o valor de ocorrências é exibido em vermelho para alertar você de que a geração de um relatório detalhado pode demorar.

A exibição do relatório de detalhes é considerada *flexível*, porque permite criar seu próprio relatório. Você pode adicionar ou excluir colunas de informação, e alterar a ordem das colunas exibidas. As informações são classificadas de acordo com a ordem das colunas. Você pode até inverter a ordem de classificação em cada coluna, de crescente para decrescente, ou vice-versa.

Os relatórios investigativos do Websense são limitados pelo processador e pela memória disponível no computador que executa o Websense Manager, e também por alguns recursos de rede. As solicitações para relatórios grandes podem atingir o tempo limite. Quando você solicita um relatório grande, recebe opções para gerar o relatório sem tempos limites.



### Importante

Em qualquer lista suspensa ou de valores, algumas opções podem aparecer em vermelho. O vermelho indica que selecionar a opção poderá resultar em um relatório muito grande. Em geral, é mais eficaz aprofundar mais os detalhes antes de selecionar a opção.

---

1. Gerar um relatório de resumo ou em vários níveis na página principal de relatórios investigativos. (Consulte [Relatórios de resumo](#), página 117, ou [Relatórios de resumo em vários níveis](#), página 121.)
2. Aprofundar nos resultados para foco nas informações de interesse imediato.  
Ao gerar um relatório com base em ocorrências, é melhor aprofundar para uma entrada que mostre menos de 100.000 ocorrências antes de abrir a exibição de relatório de detalhes.
3. Clique no número ou na barra na linha que você quer explorar em mais detalhes. Para incluir várias linhas em um relatório, marque a caixa de seleção para cada linha antes de clicar no número ou na barra em uma linha.  
Uma mensagem pop-up mostra o progresso enquanto o relatório de detalhes é carregado.



**Obs.:**

Se a geração do relatório demorar muito, considere salvá-lo como um relatório Favorito, clicando no link na mensagem Carregando, e agendando para execução posterior. Consulte [Relatórios investigativos favoritos](#), página 132.

4. Revise as informações no relatório inicial.  
As colunas padrão variam, dependendo se você está reportando ocorrências, largura de banda ou tempo de navegação, e das seleções na página Opções. (Consulte [Conexão de banco de dados e padrões de relatórios](#), página 330.)
5. Clique em **Modificar relatório** no alto da página.  
A lista **Relatório atual** na caixa de diálogo Modificar relatório mostra quais colunas aparecem no relatório de detalhes atual.
6. Selecione um nome de coluna nome na lista **Colunas disponíveis** ou **Relatório atual**, e clique nos botões de seta para a direita (>) ou seta para a esquerda (<) para mover a coluna para a outra lista.  
Escolha no máximo 7 colunas para o relatório. A coluna que mostra a medida (ocorrências, largura de banda, tempo de navegação) do relatório inicial de resumo sempre aparece como a coluna da direita. Não aparece como opção ao modificar o relatório.  
Consulte [Colunas para relatórios de detalhes flexíveis](#), página 124, para uma lista das colunas disponíveis, e uma descrição de cada.
7. Selecione um nome de coluna na lista **Relatório atual** e use os botões de seta para cima e para baixo para alterar a ordem das colunas.  
A coluna no alto da lista Relatório atual torna-se a coluna da esquerda no relatório.

8. Clique no link **Resumo** ou **Detalhe** acima do relatório para alternar entre as duas exibições.

Opção	Descrição
Resumo	Você deve remover a coluna Hora para exibir um relatório de resumo. Os relatórios de resumo agrupam em uma única entrada todos os registros que compartilham um elemento comum. O elemento especificado varia, de acordo com as informações no relatório. Tipicamente, a coluna mais à direita antes da medida mostra o elemento resumido.
Detalhe	A opção Detalhe exibe cada registro como uma linha separada. A coluna Hora pode ser exibida.

9. Clique em **Enviar** para gerar o relatório definido.
10. Use as seguintes opções para modificar o relatório exibido.
- Use as opções de **Exibir** acima do relatório para alterar o período de tempo incluído no relatório.
  - Clique na seta para cima ou para baixo em um cabeçalho de coluna para reverter a ordem de classificação para a coluna e os dados associados.
  - Use os links **Próximo** e **Anterior** acima e abaixo do relatório para exibir páginas adicionais do relatório, se houver. Por padrão, cada página contém 100 linhas, que podem ser ajustadas para adequação às suas necessidades. Consulte [Opções de exibição e saída](#), página 332.
  - Clique no URL para abrir o website solicitado em uma nova janela.
11. Clique em **Relatório favorito** se quiser salvar o relatório para poder gerá-lo periodicamente com rapidez (consulte [Salvando um relatório como Favorito](#), página 133).

## Colunas para relatórios de detalhes flexíveis

Tópicos relacionados:

- ◆ [Relatórios de detalhes flexíveis](#), página 122
- ◆ [Relatórios investigativos favoritos](#), página 132
- ◆ [Agendando relatórios investigativos](#), página 135

A tabela abaixo descreve as colunas disponíveis para relatórios de detalhes (consulte [Relatórios de detalhes flexíveis](#), página 122).

Nem todas as colunas estão disponíveis em todas as ocasiões. Por exemplo, se a coluna Usuário é exibida, Grupo não está disponível; se Categoria é exibida, Classe de risco não está disponível.

Nome da coluna	Descrição
Usuário	Nome do usuário que fez a solicitação. As informações do usuário devem estar disponíveis no banco de dados de log para inclusão em relatórios. As informações de grupo não estão disponíveis em relatórios baseados em usuários.
Dia	Data em que a solicitação foi feita.
Nome de host em URL	Nome de domínio (também denominado nome de host) do site solicitado.
Domínio	Domínio do serviço de diretório para o cliente baseado em diretório (usuário ou grupo, domínio ou unidade organizacional) que fez a solicitação.
Grupo	Nome do grupo ao qual o solicitador pertence. Os nomes de usuários individuais não são fornecidos em relatórios baseados em grupos. Se o usuário que solicitou o site pertence a mais de um grupo no serviço de diretório, o relatório lista vários grupos nesta coluna.
Classe de risco	Classe de risco associada com a categoria à qual o site solicitado pertence. Se a categoria está em várias classes de risco, todas as classes de risco relevantes são listadas. Consulte <a href="#">Atribuindo categorias a classes de risco</a> , página 302.
Objeto de diretório	Caminho de diretório para o usuário que fez a solicitação, excluindo o nome do usuário. Tipicamente, isso resulta em várias linhas para o mesmo tráfego, porque cada usuário pertence a vários caminhos. Se você está usando um serviço de diretório não-LDAP, esta coluna não está disponível.
Disposição	Ação que o software Websense recebe como resultado da solicitação; por exemplo, categoria permitida ou categoria bloqueada.
Servidor de origem	Endereço IP do computador que está enviando solicitações ao Filtering Service. É o computador que está executando o produto de integração ou o Websense Network Agent.
Protocolo	Protocolo da solicitação.
Grupo de protocolo	Grupo do Master Database em que o protocolo solicitado recai.
IP de origem	Endereço IP do computador de onde a solicitação foi feita.
IP de destino	Endereço IP do site solicitado.
URL completo	Nome de domínio e caminho para o site solicitado (exemplo: <a href="http://www.meudominio.com/produtos/itemum/">http://www.meudominio.com/produtos/itemum/</a> ). Se você não está registrando URLs completos, esta coluna fica vazia. Consulte <a href="#">Configurando o registro de URLs completos</a> , página 322.
Mês	Mês de calendário em que a solicitação foi feita.

Nome da coluna	Descrição
Porta	Porta TCP/IP pela qual o usuário se comunicou com o site.
Largura de banda	<p>A quantidade de dados, em kilobytes, contidos na solicitação inicial do usuário e na resposta do website. É o total combinado dos valores Enviados e Recebidos.</p> <p>Lembre-se de que alguns produtos de integração não enviam estas informações para o software Websense. Dois exemplos são Check Point FireWall-1 e Cisco PIX Firewall. Se a sua integração não envia estas informações, e o Websense Network Agent está instalado, ative a opção <b>Log de solicitações HTTP (registro de log aprimorado)</b> para que a placa de rede apropriada ative os relatórios sobre as informações de largura de banda. Consulte <a href="#">Definindo as configurações de placa de rede, página 343</a>.</p>
Bytes enviados	O número de bytes enviados como a solicitação da Internet. Representa a quantidade de dados transmitidos, que podem ser uma solicitação simples para um URL ou um envio mais significativo, se o usuário está se registrando em um website, por exemplo.
Bytes recebidos	<p>O número de bytes recebidos da Internet em resposta à solicitação. Inclui todos os textos, imagens e scripts que compõem o site.</p> <p>Para sites que estão bloqueados, o número de bytes varia de acordo com o software que está criando o registro de log. Quando o Websense Network Agent cria os registros, o número de bytes recebidos para um site bloqueado representa o tamanho da página de bloqueio.</p> <p>Se o registro de log é criado pelo Websense Security Gateway, como resultado de verificação em tempo real, os bytes recebidos representam o tamanho da página verificada. Consulte <a href="#">Análise de conteúdo com as opções em tempo real, página 143</a>, para obter mais informações sobre a verificação em tempo real.</p> <p>Se outro produto de integração cria os registros, os bytes recebidos para um site bloqueado podem ser zero (0), podem representar o tamanho da página de bloqueio, ou podem ser um valor obtido a partir do site solicitado.</p>
Hora	Hora em que o site foi solicitado, no formato HH:MM:SS, usando um relógio de 24 horas.
Categoria	Categoria sob a qual a solicitação foi filtrada. Pode ser uma categoria do Websense Master Database ou uma categoria personalizada.

## Relatórios de detalhe de atividade do usuário

Tópicos relacionados:

- ◆ [Relatórios investigativos, página 115](#)

Clique no link **Usuário por dia/mês** para gerar um relatório de Detalhes da atividade do usuário. Este relatório fornece uma interpretação gráfica da atividade de Internet do usuário para um único dia ou um mês completo.

Primeiro, gere um relatório para um usuário específico para um dia selecionado. A partir desse relatório, você pode gerar um relatório da atividade do mesmo usuário para um mês completo. Para obter instruções detalhadas, consulte:

- ◆ [Detalhes da atividade do usuário por dia](#), página 127
- ◆ [Detalhes da atividade do usuário por mês](#), página 128

## Detalhes da atividade do usuário por dia

Tópicos relacionados:

- ◆ [Relatórios investigativos](#), página 115
- ◆ [Relatórios de detalhe de atividade do usuário](#), página 126
- ◆ [Detalhes da atividade do usuário por mês](#), página 128

O relatório Detalhes da atividade do usuário por dia fornece uma exibição mais aprofundada da atividade de um usuário específico em um dia.

1. Selecione **Usuário por dia/mês** no alto da página principal. A caixa de diálogo Detalhes do usuário por dia aparecerá.
2. Digite um nome de usuário, ou uma parte do nome, no campo **Pesquisar usuário** e clique em **Pesquisar**.

A pesquisa exibe uma lista de rolagem com até 100 nomes de usuário correspondentes do banco de dados de log.

3. Faça uma seleção na lista **Selecionar usuário**.
4. No campo **Selecionar dia**, aceite a data da última atividade que aparece por padrão ou escolha outra data.  
Você pode digitar a nova data ou clicar no ícone de calendário para selecionar uma data. A caixa de seleção de calendário indica o intervalo de datas coberto pelo banco de dados de log ativo.
5. Clique em **Ir para Usuário por dia** para consultar um relatório detalhado de atividade para o usuário na data solicitada.

O relatório inicial mostra uma linha de tempo da atividade do usuário em incrementos de 5 minutos. Cada solicitação aparece como um ícone, que corresponde a uma categoria do Websense Master Database. Um único ícone representa todas as categorias personalizadas. (A cor dos ícones corresponde ao grupo de risco mostrado nos relatórios de atividade do usuário por mês. Consulte [Detalhes da atividade do usuário por mês](#), página 128.)

Coloque o mouse sobre um ícone para mostrar a hora exata, a categoria e a ação para a solicitação associada.

Use os controles listados abaixo para modificar a exibição do relatório ou ver uma legenda.

Opção	Descrição
Dia anterior / Dia seguinte	Exibe a atividade de Internet deste usuário para o dia de calendário anterior ou seguinte.
Exibição de tabela	Exibe uma lista de cada URL solicitado, fornecendo a data e a hora da solicitação, a categoria e a ação adotada (bloqueada, permitida ou outro).
Exibição detalhada	Exibição gráfica inicial do relatório.
Agrupar ocorrências similares / Exibir todas as ocorrências	Combina em uma única linha todas as solicitações que ocorreram em intervalos de 10 segundos e têm domínio, categoria e ação iguais. Isso resulta em uma exibição mais curta e resumida da informação. O limite de tempo padrão é 10 segundos. Se você precisar alterar este valor, consulte <a href="#">Opções de exibição e saída, página 332</a> . Depois que você clicar no link, ele se torna Exibir todas as ocorrências, que restaura a lista original de cada solicitação.
Controle de exibição de categorias	Exibe uma lista de cada categoria no relatório atual, mostrando o nome da categoria e o ícone que representa a categoria. Controla quais categorias aparecem no relatório, marcando as caixas de seleção para as categorias que serão incluídas. Em seguida, clique em <b>Aceitar</b> para atualizar o relatório de acordo com as suas seleções.

6. Clique em **Detalhes da atividade do usuário por mês**, acima do relatório, para exibir a atividade do mesmo usuário para o mês completo. Consulte [Detalhes da atividade do usuário por mês, página 128](#), para obter mais informações.

## Detalhes da atividade do usuário por mês

Tópicos relacionados:

- ◆ [Relatórios investigativos, página 115](#)
- ◆ [Relatórios de detalhe de atividade do usuário, página 126](#)
- ◆ [Detalhes da atividade do usuário por dia, página 127](#)
- ◆ [Mapeamento de categorias, página 129](#)

Quando o relatório Detalhes da atividade do usuário por dia está aberto, você pode alternar para ver a atividade mensal para o usuário.

1. Abra um relatório Detalhes da atividade do usuário por dia. Consulte [Detalhes da atividade do usuário por dia, página 127](#).

2. Clique em **Detalhes da atividade do usuário por mês** no alto.  
O novo relatório exibe uma imagem de calendário, com a área de cada dia mostrando pequenos blocos coloridos que representam a atividade de Internet do usuário para o dia. As solicitações para sites em categorias personalizadas são mostradas como blocos cinza.
3. Clique em **Legenda de categorias do banco de dados** no alto à esquerda para ver como as cores representam risco potencial de baixo para alto para o site solicitado.  
As atribuições de categorias são fixas e não podem ser alteradas. Consulte [Mapeamento de categorias](#), página 129.
4. Clique em **Anterior** ou **Próximo** para exibir a atividade de Internet deste usuário para o mês anterior ou próximo.

## Mapeamento de categorias

Tópicos relacionados:

- ◆ [Relatórios investigativos](#), página 115
- ◆ [Relatórios de detalhe de atividade do usuário](#), página 126
- ◆ [Detalhes da atividade do usuário por mês](#), página 128

A seguinte lista identifica quais categorias são representadas por cada uma das cores nos relatórios Atividade do usuário por dia e Atividade do usuário por mês.

Lembre-se de que os nomes de categorias no Master Database estão sujeitas a alterações. Adicionalmente, as categorias podem ser adicionadas ou excluídas em qualquer ocasião.

Cor	Categorias
Cinza	Categorias personalizadas Tráfego não-HTTP
Azul escuro	<b>Negócios e economia</b> e todas as subcategorias <b>Educação</b> e todas as subcategorias <b>Saúde</b> <b>Tecnologia da Informação</b> , incluindo os Mecanismos de pesquisa e portais, e as subcategorias de Web Hosting <b>Diversos</b> subcategorias Redes de entrega de conteúdo, Conteúdo dinâmico, Imagens (mídia), Servidores de imagem e Endereços IP privados <b>Produtividade</b> /Anúncios

Cor	Categorias
Azul claro	<p><b>Drogas/Remédios</b> com receita</p> <p><b>Governo</b> e a subcategoria Militares</p> <p><b>Tecnologia da Informação/Sites</b> de tradução de URLs</p> <p><b>Diversos</b>, somente a categoria principal</p> <p><b>Notícias e mídia</b>, somente a categoria principal</p> <p><b>Eventos especiais</b></p>
Amarelo Verde	<p><b>Aborto</b> e todas as subcategorias</p> <p><b>Material para adultos/Educação</b> sexual</p> <p><b>Largura de banda</b>, incluindo as subcategorias Rádio e TV pela Internet, Armazenamento/backup pessoal em rede, e Streaming media.</p> <p><b>Entretenimento</b> e a subcategoria MP3</p> <p><b>Jogos</b></p> <p><b>Governo/Organizações</b> diretivas</p> <p><b>Tecnologia da Informação/Segurança</b> de informática</p> <p><b>Comunicação pela Internet/Webmail</b></p> <p><b>Diversos/Servidores</b> para download de arquivos</p> <p><b>Diversos/Erros</b> de rede</p> <p><b>Notícias e mídia/Periódicos</b> alternativos</p> <p><b>Produtividade</b>, incluindo as subcategorias Mensagens instantâneas, Quadros de mensagens e clubes, Corretagem de ações on-line</p> <p><b>Religião</b> e suas subcategorias Religiões não tradicionais, ocultismo e folclore, Religiões tradicionais</p> <p><b>Segurança</b>, somente a categoria principal</p> <p><b>Compras</b> e todas as subcategorias</p> <p><b>Organizações sociais</b> e todas as subcategorias</p> <p><b>Sociedade e estilo de vida</b>, incluindo as subcategorias Gays, lésbicas ou bissexuais, Hobbies, Websites pessoais, e Restaurantes e jantares</p> <p><b>Esportes</b> e todas as subcategorias</p> <p><b>Viagens</b></p> <p><b>Definidos pelo Usuário</b></p> <p><b>Veículos</b></p>

Cor	Categorias
Laranja	<b>Material adulto</b> /Nudez <b>Grupos de defesa</b> <b>Largura de banda</b> /Telefonia pela Internet <b>Drogas</b> e as subcategorias Abuso de drogas, Maconha, Suplementos e Compostos não regulamentados. <b>Tecnologia da Informação</b> /Proxy Avoidance <b>Comunicação pela Internet</b> e sua subcategoria Bate-papo <b>Pesquisa de emprego</b> <b>Diversos</b> /Não categorizado <b>Produtividade</b> e as subcategorias Download de freeware e software, e Pay-to-Surf <b>Religião</b> <b>Sociedade e estilos de vida</b> e as subcategorias Álcool e tabaco, Anúncios pessoais e Namoro <b>Mau gosto</b> <b>Armas</b>
Vermelho	<b>Material para adultos</b> e estas subcategorias: conteúdo adulto, lingerie e roupas de banho, e sexo <b>Largura de banda</b> /Compartilhamento de arquivos -a-ponto (P2P) <b>Jogos de azar</b> <b>Ilegal ou questionável</b> <b>Tecnologia da Informação</b> /Hacking <b>Militantes e extremistas</b> <b>Racismo e ódio</b> <b>Segurança</b> e as subcategorias Keyloggers, Websites maliciosos, Phishing, e Spyware <b>Violência</b>

## Relatórios padrão

Tópicos relacionados:

- ◆ [Relatórios investigativos](#), página 115
- ◆ [Relatórios investigativos favoritos](#), página 132
- ◆ [Agendando relatórios investigativos](#), página 135

Os relatórios padrão permitem exibir um conjunto de informações específico rapidamente, sem usar o processo de aprofundamento.

1. Clique no link **Relatórios padrão** na página principal de Relatórios investigativos.

- Escolha o relatório que contém a informação desejada. Os seguintes relatórios estão disponíveis.

---

#### **Níveis de atividade mais altos**

- Quais usuários têm mais ocorrências?
- Os 10 primeiros usuários para os 10 URLs mais visitados
- Atividade dos 5 primeiros usuários em Compras, Entretenimento e Esportes
- 5 primeiros URLs para as 5 categorias mais votadas

---

#### **O mais alto consumo de largura de banda**

- Quais grupos estão consumindo a maior quantidade de largura de banda?
- Grupos consumindo a maior quantidade de largura de banda em Mídia
- Relatório de URL detalhado sobre usuários por perda de largura de banda
- Os 10 primeiros grupos das categorias de largura de banda

---

#### **Mais tempo online**

- Quais usuários passaram mais tempo on-line
- Quais usuários dedicaram mais tempo em sites de categorias de produtividade

---

#### **Mais bloqueados**

- Quais usuários foram bloqueados mais vezes?
- Quais sites foram bloqueados mais vezes?
- Relatório de URL detalhado sobre usuários que foram bloqueados
- 10 categorias mais bloqueadas

---

#### **O mais alto risco de segurança**

- As primeiras categorias representam um risco de segurança
- Os primeiros usuários do protocolo P2P
- Principais usuários de sites em categorias de segurança
- URLs para as primeiras 10 máquinas com atividade de spyware

---

#### **Responsabilidade legal**

- Risco de responsabilidade legal por categoria
  - Os primeiros usuários em categorias Adultas
- 

- Exiba o relatório que aparece.
- Salve o relatório como Favorito se deseja executá-lo periodicamente. Consulte [Relatórios investigativos favoritos](#), página 132.

## **Relatórios investigativos favoritos**

Tópicos relacionados:

- ◆ [Relatórios investigativos](#), página 115
- ◆ [Agendando relatórios investigativos](#), página 135

Você pode salvar a maioria dos relatórios investigativos como **Favoritos**. Isso inclui relatórios que você gera aprofundando para informações específicas, relatórios padrão e relatórios de detalhes que você modificou para atender as suas necessidades específicas. Em seguida, execute o relatório Favorito em qualquer ocasião ou agende-o para execução em dias e horas específicos.

Em empresas que usam administração delegada, a permissão para salvar e programar Favoritos é definida pelo Super administrador. Os administradores que recebem esta permissão podem executar e agendar apenas os Favoritos que salvaram; não têm acesso a Favoritos salvos por outros administradores.

Para obter instruções detalhadas sobre como trabalhar com relatórios Favoritos, consulte:

- ◆ [Salvando um relatório como Favorito](#), página 133
- ◆ [Gerando ou excluindo um relatório Favorito](#), página 134
- ◆ [Modificando um relatório Favorito](#), página 134

## Salvando um relatório como Favorito

Tópicos relacionados:

- ◆ [Relatórios investigativos favoritos](#), página 132
- ◆ [Modificando um relatório Favorito](#), página 134

Use o seguinte procedimento para salvar um relatório como Favorito.

1. Gere um relatório investigativo com o formato e as informações desejadas.
2. Clique em **Relatórios favoritos**.
3. Aceite ou modifique o nome exibido pelo Websense Manager.  
O nome pode conter letras, números e sublinhados (\_). Não podem ser usados espaços em branco ou outros caracteres especiais.
4. Clique em **Adicionar**.  
O nome do relatório é adicionado à lista de Favoritos.
5. Selecione um relatório nesta lista. Em seguida, selecione uma opção para administrar o relatório. Dependendo da opção escolhida, consulte:
  - [Gerando ou excluindo um relatório Favorito](#), página 134
  - [Agendando relatórios investigativos](#), página 135

## Gerando ou excluindo um relatório Favorito

Tópicos relacionados:

- ◆ [Relatórios investigativos favoritos](#), página 132
- ◆ [Modificando um relatório Favorito](#), página 134

Você pode gerar um relatório Favorito em qualquer ocasião ou apagar um relatório que ficou obsoleto.

1. Clique em **Relatórios favoritos** para exibir uma lista de relatórios salvos como favoritos.



**Obs.:**

Se a sua empresa usa administração delegada, esta lista não inclui relatórios favoritos salvos por outros administradores.

---

2. Selecione o relatório desejado na lista.

Se o relatório desejado não foi salvo como Favorito, consulte [Salvando um relatório como Favorito](#), página 133.

3. Dependendo de sua necessidade:

- Clique em **Executar agora** para gerar e exibir o relatório selecionado imediatamente.
- Clique em **Agendar** para agendar a relatório para executar depois ou periodicamente. Consulte [Agendando relatórios investigativos](#), página 135 para obter mais informações.
- Clique em **Excluir** para remover o relatório da lista Favoritos.

## Modificando um relatório Favorito

Tópicos relacionados:

- ◆ [Relatórios investigativos](#), página 115
- ◆ [Relatórios investigativos favoritos](#), página 132

Você pode criar facilmente um novo relatório Favorito que é semelhante a um relatório Favorito existente, da seguinte forma.

1. Clique em **Relatórios favoritos** para exibir uma lista de relatórios salvos como favoritos.

**Obs.:**

Se a sua empresa usa administração delegada, esta lista não inclui relatórios favoritos salvos por outros administradores.

2. Selecione e execute o relatório Favorito existente que é mais semelhante ao novo relatório que você quer criar. (Consulte *Gerando ou excluindo um relatório Favorito*, página 134.)
3. Modifique o relatório exibido conforme desejado.
4. Clique em **Relatórios favoritos** para salvar a exibição revisada como um relatório Favorito com um novo nome. (Consulte *Salvando um relatório como Favorito*, página 133.)

## Agendando relatórios investigativos

Tópicos relacionados:

- ◆ *Relatórios investigativos favoritos*, página 132
- ◆ *Salvando um relatório como Favorito*, página 133
- ◆ *Gerenciando trabalhos programados de relatórios investigativos*, página 138

Você deve salvar um relatório investigativo como Favorito antes de poder agendá-lo para execução posterior ou em um ciclo de repetição. Quando o trabalho de relatório agendado for executado, os relatórios resultantes são enviados por e-mail aos destinatários designados. Ao criar trabalhos agendados, considere se o seu servidor de e-mail será capaz de administrar o tamanho e a quantidade de arquivos de relatório anexos.

Os arquivos de relatórios agendados são salvos no seguinte diretório:

```
<caminho_de_instalacao>\webroot\Explorer\<nome>\
```

O caminho de instalação padrão é C:\Arquivos de Programas\WebSense. Se o trabalho agendado tem apenas um destinatário, <nome> é a primeira parte do endereço de e-

mail (antes da @). No caso de vários destinatários, os relatórios são salvos em um diretório chamado Outro.



**Obs.:**

Os relatórios salvos a partir de um trabalho repetido usam o mesmo nome em todas as ocasiões. Se você quiser salvar arquivos para um período mais longo do que um ciclo único, altere o nome do arquivo ou copie o arquivo para outro local.

Dependendo do tamanho e do número de relatórios agendados, este diretório poderia ficar muito grande. Limpe o diretório periodicamente, eliminando arquivos de relatórios desnecessários.

1. Salvar um ou mais relatórios como Favoritos. (Consulte [Salvando um relatório como Favorito](#), página 133).
2. Clique em **Relatórios favoritos** para exibir uma lista de relatórios salvos como favoritos.



**Obs.:**

Se a sua empresa usa funções de administração delegada, esta lista não inclui relatórios favoritos salvos por outros administradores.

3. Destaque até 5 relatórios para execução como parte do trabalho.
4. Clique em **Agendar** para criar um trabalho de relatório agendado e forneça as informações solicitadas na página Agendar relatório.

É recomendável programar trabalhos de relatório em diferentes dias e horários, para evitar a sobrecarga do banco de dados de log e a redução do desempenho para registros e relatórios interativos.

<b>Campo</b>	<b>Descrição</b>
Recorrência	Selecione a frequência (Uma vez, Diário, Semanal, Mensal) para execução do trabalho de relatório.
Data inicial	Escolha o dia da semana ou a data de calendário para executar o trabalho pela primeira (ou única) vez.
Hora de execução	Defina a hora do dia para executar o trabalho.
Enviar por e-mail para	Use o campo <b>Endereços de e-mail adicionais</b> para adicionar os endereços apropriados à lista. Destaque um ou mais endereços de e-mail para receber os relatórios do trabalho. (Certifique-se de desmarcar os e-mails que não devem receber os relatórios.)
Endereços de e-mail adicionais	Digite um endereço de e-mail e clique em <b>Adicionar</b> para colocá-lo na lista <b>Enviar por e-mail para</b> . O novo endereço de e-mail é destacado automaticamente com os outros endereços de e-mail selecionados.

<b>Campo</b>	<b>Descrição</b>
Personalizar assunto do e-mail e corpo do texto	Marque esta caixa de seleção para personalizar suas linhas de assunto de notificação e o texto do corpo do e-mail. Se esta caixa não está marcada, o assunto e o texto padrão são usados.
Assunto do e-mail	Digite o texto para aparecer como linha de assunto do e-mail quando relatórios agendados são distribuídos. O assunto do e-mail padrão é: Trabalho programado de relatórios investigativos
Texto do e-mail	Digite texto para ser adicionado à mensagem de e-mail para distribuição de relatórios agendados. O e-mail fica conforme aparece abaixo, com o seu texto no lugar de <TEXTO PERSONALIZADO>. O Report Scheduler gerou o arquivo ou os arquivos anexados em <data hora>. <TEXTO PERSONALIZADO> Para exibir o(s) relatório(s) gerado(s), clique no(s) seguinte(s) link(s). Obs.: O link não funcionará se o destinatário não tiver acesso ao servidor Web do qual o trabalho foi enviado.
Nome do trabalho agendado	Atribua um nome exclusivo para o trabalho agendado. O nome identifica este trabalho na Fila de trabalhos. Consulte <a href="#">Gerenciando trabalhos programados de relatórios investigativos</a> , página 138.
Formato de saída	Escolha o formato de arquivo para os relatórios agendados. <b>PDF:</b> Portable Document Format: estes arquivos são visualizados no Adobe Reader. <b>Excel:</b> Os arquivos de planilhas Excel são visualizados no Microsoft Excel.
Intervalo de datas	Defina o intervalo de datas para ser coberto por relatórios neste trabalho. <b>Todas as datas:</b> todas as datas disponíveis no banco de dados de log. <b>Relativo:</b> Escolha um período de tempo (Dias, Semanas ou Meses) e o período específico para inclusão (Este, Último, Últimos 2, e assim por diante). <b>Específico:</b> defina datas específicas ou um intervalo de datas para os relatórios neste trabalho.

5. Clique em **Próximo** para exibir a página Confirmação do agendamento.
6. Clique em **Salvar** para salvar suas seleções e ir para a página Fila de trabalhos (consulte [Gerenciando trabalhos programados de relatórios investigativos](#), página 138).

## Gerenciando trabalhos programados de relatórios investigativos

Tópicos relacionados:

- ◆ [Relatórios investigativos](#), página 115
- ◆ [Agendando relatórios de apresentação](#), página 108

Quando você cria um trabalho agendado para relatórios investigativos, a página **Fila de trabalhos** aparece, mostrando o novo trabalho e uma lista de trabalhos agendados existentes. Você também pode acessar a página clicando no link **Fila de trabalhos** na página principal de relatórios investigativos.



**Obs.:**

Se a sua empresa usa administração delegada, esta página não exibe trabalhos agendados por outros administradores.

A seção **Detalhes do relatório agendado** lista cada trabalho agendado na ordem em que foi criado, mostrando uma visão geral do agendamento definido e o status do trabalho. Além disso, as seguintes opções estão disponíveis.

Opção	Descrição
Editar	Exibe o agendamento definido para este trabalho, e permite modificá-lo, conforme necessário.
Excluir	Exclui o trabalho e adiciona uma entrada na seção Log de status, mostrando o trabalho como Excluído.

A seção **Log de status** lista cada trabalho que foi alterado de alguma forma, mostrando a hora inicial agendada para o trabalho, a hora de fim real e o status.

Clique em **Limpar o log de status** para remover todas as entradas na seção Log de status.

## Relatórios de valores atípicos

Tópicos relacionados:

- ◆ [Relatórios investigativos](#), página 115
- ◆ [Relatórios de resumo](#), página 117

Um relatório de Valores atípicos mostra quais usuários têm a atividade de Internet mais incomum no banco de dados. O software Websense calcula a atividade média para todos os usuários por categoria, por dia, por ação (às vezes denominada disposição), e por protocolo. Em seguida, exibe a atividade do usuário que tem a

variância estatisticamente mais significativa em relação à média. A variância é calculada como o desvio padrão da média.

1. Na página principal de relatórios investigativos, gere um relatório de resumo que exibe as informações para as quais você quer ver os valores atípicos. As seleções no relatório sublinhadas e exibidas em azul ao lado do campo **Uso da Internet** por são refletidas no relatório de **Valores atípicos**.

Por exemplo, para exibir valores atípicos por ocorrências para uma categoria específica, selecione **Categoria** na lista **Uso da Internet por** e selecione **Ocorrências** como a **Medida**.



**Obs.:**

Os relatórios de valores atípicos não podem ser gerados por tempo de navegação. Se você começar com um relatório de resumo mostrando o tempo de navegação, o relatório de Valores atípicos relatório baseia-se em ocorrências.

2. Clique em **Exibir valores atípicos**.

As linhas são classificadas em ordem decrescente, com a maior variância mostrada primeiro. Cada linha mostra:

- Total (ocorrências ou largura de banda) para o usuário, categoria, protocolo, dia e ação.
  - Média (ocorrências ou largura de banda) para todos os usuários, para categoria, protocolo, dia e ação.
  - Variância em relação à média para o usuário.
3. Para consultar a atividade de um usuário individual nesta categoria ao longo do tempo, clique no nome do usuário.

Por exemplo, se a atividade de um usuário é visivelmente alta para um determinado dia, clique no nome do usuário para ver um relatório que fornece um entendimento mais aprofundado da atividade geral do usuário.

## Saída para arquivo

Tópicos relacionados:

- ◆ [Relatórios investigativos, página 115](#)
- ◆ [Imprimindo relatórios investigativos, página 140](#)

Depois de gerar um relatório investigativo, você pode usar os botões acima do relatório para salvá-lo como arquivo. O botão em que você clica determina o formato do arquivo.

Opção	Descrição
	<p>Salva o relatório em formato XLS .</p> <p>Se o Microsoft Excel 2003 ou mais recente está instalado no computador em que você está acessando o Websense Manager, você é solicitado a exibir ou salvar o relatório. Caso contrário, você é solicitado a selecionar um diretório e um nome de arquivo para o relatório salvo.</p> <p>Use as opções no Microsoft Excel para imprimir, salvar ou enviar o relatório por e-mail.</p>
	<p>Gera um relatório em formato PDF.</p> <p>Se o Adobe Reader v7.0 ou mais recente está instalado no computador em que você está acessando o Websense Manager, você é solicitado a exibir ou salvar o relatório. Caso contrário, você é solicitado a selecionar um diretório e um nome de arquivo para o relatório salvo.</p> <p>Use as opções no Adobe Reader para imprimir, salvar ou enviar o relatório por e-mail.</p>

## Imprimindo relatórios investigativos

Tópicos relacionados:

- ◆ [Relatórios investigativos, página 115](#)
- ◆ [Saída para arquivo, página 139](#)

Você pode imprimir relatórios investigativos:

- ◆ Usando a função de impressão do navegador de Internet enquanto o relatório está exibido.
- ◆ Criando um arquivo PDF ou XLS, e depois usando a função imprimir no Adobe Reader ou Microsoft Excel (consulte [Saída para arquivo, página 139](#)).

Embora os relatórios tenham sido configurados para impressão a partir do navegador, é recomendado testar a impressão para verificar o resultado.

Os relatórios de detalhes da atividade do usuário por mês são configurados para impressão em modo paisagem. Todos os outros relatórios são configurados para impressão em modo retrato.

Quando você projeta o seu próprio relatório (consulte [Relatórios de detalhes flexíveis, página 122](#)), as larguras das colunas são diferentes, dependendo das informações incluídas. A orientação da página muda para paisagem se a largura do relatório for superior a 20,32 cm.

O conteúdo da página tem 17,78 ou 25,4 cm de largura. No caso de A4, as margens são ligeiramente mais estreitas, mas ainda são impressas no intervalo de impressão. (O

tamanho de papel padrão é Carta ou 20,32 x 27,94 cm. Se você está trabalhando com papel A4, certifique-se de alterar esta configuração no arquivo wse.ini. Consulte [Opções de exibição e saída](#), página 332.)

## Acessando os relatórios próprios

---

Tópicos relacionados:

- ◆ [Relatórios investigativos](#), página 115
- ◆ [Configurando preferências de relatórios](#), página 303
- ◆ [Relatório próprio](#), página 334

Os relatórios próprios do Websense permitem avaliar suas próprias atividades de navegação na Internet e ajustá-las, conforme necessário, para cumprir diretrizes da empresa. Também cumprem normas do governo que exigem que as organizações permitam que os usuários vejam quais tipos de informações estão sendo coletados.

Se os relatórios próprios estão habilitados em sua empresa, acesse-os no navegador:

1. Digite o URL fornecido pelo Administrador do Websense ou clique no link Relatório próprio na página principal de logon do Websense Manager para acessar a página de logon de relatório próprio.
2. Se o **Policy Server** mostrar uma lista suspensa, escolha o IP endereço do Policy Server que registra informações sobre suas atividades na Internet.  
Contate o seu Administrador do Websense para obter orientação.
3. Digite o **Nome de usuário** e a **Senha** que você usa para logon na rede.
4. Clique em **Logon**.

O Websense Manager abre um relatório investigativo que mostra sua atividade de Internet por classe de risco. Clique nos diversos links e elementos na página para acessar outras opções para exibições alternativas das informações armazenadas sobre a sua atividade. Use o sistema de **Ajuda** para obter orientação ao trabalhar com relatórios.



# 7

## Análise de conteúdo com as opções em tempo real

Tópicos relacionados:

- ◆ [Opções de verificação](#), página 145
- ◆ [Classificando conteúdo e verificando para identificar ameaças](#), página 146
- ◆ [Verificação de arquivos](#), página 147
- ◆ [Removendo conteúdo](#), página 148
- ◆ [Relatórios sobre a atividade de verificação em tempo real](#), página 151

O software de filtragem do Websense filtra a atividade de Internet com base em sua política ativa e nas informações armazenadas no Master Database. Se você assina o Websense Content Gateway ou Websense Web Security Gateway, também pode analisar o conteúdo de sites da Web e arquivos em tempo real.

Dependendo de sua assinatura, duas opções de análise em tempo real estão disponíveis: classificação de conteúdo e verificação de Segurança em tempo real.

- ◆ Use a **classificação de conteúdo** para revisar o conteúdo de URLs que ainda não estão bloqueadas (com base em sua política ativa e na classificação de URL do Websense Master Database), e retorne uma categoria para uso em filtragem.
- ◆ Se você assina o Websense Web Security Gateway, três opções de **verificação de segurança em tempo real** estão disponíveis.
  - **Verificação de conteúdo** analisa o conteúdo da Web para localizar ameaças de segurança como phishing, redirecionamento de URL, exploits da Web e proxy avoidance.
  - **Verificação de arquivos** inspeciona o conteúdo de arquivos para determinar uma categoria de ameaças, como vírus, cavalos de Tróia ou worms.
  - **Remoção de conteúdo** remove o conteúdo ativo de páginas Web solicitadas.

Quando qualquer dessas opções são ativadas, apenas os sites ainda **não** bloqueados com base em sua política ativa e na classificação do Websense Master Database são analisados. Para obter mais informações, consulte [Opções de verificação](#), página 145.



### Importante

Os filtros para acesso limitado e os URLs não-filtrados substituem a classificação em tempo real.

Se um usuário solicitar um site em um filtro de acesso limitado ativo (consulte [Restringindo usuários a uma lista definida de sites de Internet](#), página 166) ou na lista de URLs Não-Filtrados (consulte [Redefinindo a filtragem de sites específicos](#), página 180), a solicitação é permitida, mesmo quando a verificação em tempo real é realizada e as ameaças são encontradas.

Para aproveitar esses recursos de segurança em tempo real, digite uma chave de assinatura que inclua suporte para Websense Content Gateway ou Websense Web Security Gateway em dois lugares:

- ◆ No Websense Manager (vá para **Configurações > Conta**).
- ◆ Na interface de gerenciamento do Websense Content Gateway (vá para a guia **Configurar > Meu Proxy > Assinatura > Gestão de assinaturas**).

São necessários diversos minutos para que os dois produtos façam download dos bancos de dados necessários, sincronizem e exibam todos os recursos em tempo real nas duas ferramentas de gerenciamento.

## Opções em tempo real do Websense

---

As opções em tempo real do Websense ajudam a garantir a segurança da rede. Use estas opções para verificar o conteúdo de Internet e designá-lo para uma categoria de filtragem. O resultado em tempo real é enviado ao Filtering Service, que filtra o site com base na ação atribuída à sua classificação em tempo real na política ativa.

## Download do banco de dados

---

As opções em tempo real dependem de pequenos bancos de dados instalados com o Websense Web Security Gateway, que verifica o banco de dados para obter atualizações em intervalos periódicos. As atualizações nesses bancos de dados podem ocorrer de forma independente de todas as atualizações do Master Database (incluindo atualizações do banco de dados em tempo real e Atualizações de segurança em tempo real).

Quando você usa o comando `./WCGAdmin start` para iniciar o Websense Security Gateway, um download do banco de dados é iniciado. Se o download falhar, um novo download é tentado a cada 15 minutos até que um download bem-sucedido ocorra.

O intervalo padrão para verificações de atualização do banco de dados é 15 minutos. Você pode alterar este intervalo editando o valor **PollInterval** no arquivo **/opt/bin/downloadservice.ini** no computador do Websense Content Gateway.

Depois de editar o arquivo **downloadservice.ini**, você deve parar e reiniciar o Websense Content Gateway a partir da linha de comando.

- ◆ Para interromper, digite: **/opt/WCG/WCGAdmin stop**
- ◆ Para reiniciar, digite: **/opt/WCG/WCGAdmin start**

## Opções de verificação

---

Use a página **Configurações > Verificação em tempo real** para habilitar e configurar opções em tempo real. As opções de verificação individuais são detalhadas nas seguintes seções.

- ◆ *Classificando conteúdo e verificando para identificar ameaças*, página 146
- ◆ *Verificação de arquivos*, página 147
- ◆ *Removendo conteúdo*, página 148

Para cada opção, você tem no mínimo duas opções:

- ◆ **Desativada.** Não ocorre verificação em tempo real ou bloqueio. Esta opção não fornece segurança adicional.
- ◆ **Recomendada** ou **Ativada.** Se o seu site está configurado para verificação em tempo real, esta configuração fornece o melhor desempenho. As verificações são realizadas com base em dois fatores:
  - As listas Sempre verificar e Nunca verificar na guia **Configurações > Verificação em tempo real > Exceções** (consulte *Refinando a verificação*, página 149).
  - Se o software Websense identificou o site como incluindo conteúdo dinâmico. Os sites indicados como incluindo conteúdo dinâmico são verificados. O marcador que identifica um site como incluindo conteúdo dinâmico não é configurável pelo usuário.  
  
Os sites com conteúdo dinâmico que aparecem na lista Nunca verificar não são verificados.
- ◆ **Todas.** Todas as páginas Web solicitadas são verificadas. As únicas exceções são as listadas na lista Nunca verificar.

Esta opção fornece a segurança mais elevada, mas pode reduzir o desempenho do sistema de forma significativa.



### Aviso

Os sites na lista Nunca verificar não são analisados em circunstância alguma. Se um site na lista Nunca verificar estiver comprometido, as opções em tempo real não analisam e detectam o código malicioso.

---

## Classificando conteúdo e verificando para identificar ameaças

---

Tópicos relacionados:

- ◆ [Opções de verificação](#), página 145
- ◆ [Verificação de arquivos](#), página 147
- ◆ [Removendo conteúdo](#), página 148
- ◆ [Refinando a verificação](#), página 149
- ◆ [Relatórios sobre a atividade de verificação em tempo real](#), página 151

O conteúdo da Web muda rapidamente. As estatísticas mostraram que uma maioria significativa do conteúdo da Web é dinâmico. Além disso, a Internet está hospedando mais conteúdo gerado pelo usuário; por exemplo, o encontrado em sites de redes sociais. Este material não está sujeito às diretrizes para conteúdo e estilo impostas em sites da Web corporativos.

Quando a classificação de conteúdo está habilitada, os sites selecionados são classificados em tempo real e a categoria resultante é encaminhada ao software de filtragem Websense para ser bloqueada ou permitida com base na política ativa.



### Importante

Habilite o registro de URLs completos (consulte [Configurando o registro de URLs completos](#), página 322) se planeja gerar relatórios da atividade de verificação em tempo real. Caso contrário, os registros incluem apenas o domínio (www.domain.com) do site classificado e as páginas individuais em um site podem recair em diferentes categorias.

Se o seu site usa WebCatcher para reportar URLs não classificados para Websense, Inc. (consulte [Configurando o WebCatcher](#), página 314), os URLs classificados com classificação de conteúdo são encaminhados para inclusão no Master Database.

Se a sua assinatura inclui o Websense Security Gateway, você também pode especificar que os sites sejam verificados para identificar ameaças de segurança.

Use a página **Configurações > Verificação em tempo real > Opções comuns** para especificar quando usar classificação de conteúdo e verificação de conteúdo.

1. Na área Classificação de conteúdo, selecione **Desativada** ou **Ativada** (padrão) para determinar se a verificação é executada. Consulte [Opções de verificação](#), página 145.

Depois que a categoria é determinada, quaisquer outras opções em tempo real que você configurou são aplicadas para fornecer segurança adicional.

2. (*Websense Security Gateway*) Na área Verificação de conteúdo, selecione **Desativado** (padrão), **Recomendado** ou **Tudo** para determinar o nível da verificação.

3. Use um dos seguintes métodos:
  - Para adicionar sites às listas Sempre verificar e Nunca verificar, selecione a guia **Exceções**. Consulte [Refinando a verificação](#), página 149.
  - Para alterar as configurações para outras opções em tempo real, continue na página **Opções comuns**. Consulte [Verificação de arquivos](#), página 147 e [Removendo conteúdo](#), página 148.
4. Quando terminar, clique em **OK** para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Os relatórios de apresentação podem fornecer detalhes sobre tentativas de acessar sites que contêm ameaças. Consulte [Relatórios de apresentação](#), página 96, para obter detalhes sobre a execução de relatórios do Websense.

## Verificação de arquivos

Tópicos relacionados:

- ◆ [Opções de verificação](#), página 145
- ◆ [Classificando conteúdo e verificando para identificar ameaças](#), página 146
- ◆ [Removendo conteúdo](#), página 148
- ◆ [Refinando a verificação](#), página 149
- ◆ [Relatórios sobre a atividade de verificação em tempo real](#), página 151

A verificação de arquivos analisa o conteúdo nos arquivos de aplicativos recebidos que os usuários tentam baixar ou abrir remotamente. Esta opção em tempo real retorna uma categoria para o software de filtragem Websense, de forma que o arquivo seja permitido ou bloqueado, conforme apropriado.

Como prática recomendada, verifique todos os arquivos **executáveis** (por exemplo, **.exe** e **.dll**). Você também pode identificar tipos de arquivos adicionais para verificar e definir um tamanho máximo para verificação.



**Obs.:**

Somente os arquivos de aplicativos portáteis para Windows de 32 bits são verificados.

Use a guia **Configurações > Verificação em tempo real > Opções comuns** para especificar quando usar verificação de arquivos.

1. Na área Verificação de conteúdo, selecione **Desativado**, **Recomendado** (padrão) ou **Tudo** para determinar o nível da verificação. Consulte [Opções de verificação](#), página 145.
2. Clique em **Configurações avançadas**.

3. **A verificação de todos os tipos de arquivos com conteúdo executável** é selecionada por padrão. Marque esta caixa de seleção se preferir listar as extensões de arquivos individuais que serão verificadas.
4. Para especificar tipos de arquivos adicionais para verificação, informe a extensão de arquivo (como **ppt** ou **wmv**) e clique em **Adicionar**. A extensão de arquivo só pode conter caracteres alfanuméricos, uma sublinha ( **\_** ) ou um traço ( **-** ). Não inclua o ponto que precede a extensão.  
  
Para remover uma extensão de arquivo da lista de extensões de arquivos Selecionados, selecione a extensão e clique em **Remover**.
5. Em Opções, digite o tamanho máximo para os arquivos que serão verificados (por padrão, 10 MB). Selecione **Personalizado** para digitar um tamanho até 4096 MB (4 GB). Os arquivos maiores do que o tamanho especificado não são verificados.
6. Use um dos seguintes métodos:
  - Para adicionar sites às listas Sempre verificar e Nunca verificar, selecione a guia **Exceções**. Consulte [Refinando a verificação](#), página 149.
  - Para alterar as configurações para outras opções em tempo real, continue na guia **Opções comuns**. Consulte [Classificando conteúdo e verificando para identificar ameaças](#), página 146, e [Removendo conteúdo](#), página 148.
7. Quando terminar, clique em **OK** para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Diversos relatórios de apresentação fornecem detalhes sobre tentativas de download de arquivos que contêm riscos de segurança. Consulte [Relatórios de apresentação](#), página 96, para obter instruções sobre a execução de relatórios do Websense.

Consulte [Gerenciando o tráfego com base no tipo de arquivo](#), página 191, para obter informações sobre o bloqueio de arquivos com base em tipo e categoria de URL.

## Removendo conteúdo

---

Tópicos relacionados:

- ◆ [Opções de verificação](#), página 145
- ◆ [Classificando conteúdo e verificando para identificar ameaças](#), página 146
- ◆ [Verificação de arquivos](#), página 147
- ◆ [Refinando a verificação](#), página 149
- ◆ [Relatórios sobre a atividade de verificação em tempo real](#), página 151

As ameaças ao seu sistema podem estar ocultas em conteúdo ativo enviado por páginas da Web. Uma forma de preservar a integridade do seu sistema é garantir que esse conteúdo nunca chegue.

As opções em tempo real do Websense tornam possível especificar que o conteúdo em linguagens de script específicas (ActiveX, JavaScript ou VB Script) seja removido das

páginas Web recebidas. Se a remoção de conteúdo for habilitada, todo o conteúdo nas linguagens de script especificadas é removido dos sites marcados como contendo conteúdo dinâmico ou que aparecem na lista Sempre verificar (consulte [Opções de verificação](#), página 145).

O conteúdo só é removido depois que as opções em tempo real classificaram o site e o software de filtragem do Websense determinou qual política é aplicável.



### Importante

As páginas Web que usam conteúdo ativo que foi removido não funcionam conforme esperado. Para permitir o acesso completo a sites que requerem conteúdo ativo, desative a remoção de conteúdo ou adicione os sites à lista Nunca verificar.

O usuário que solicitou uma página com conteúdo ativo não recebe qualquer notificação de que o conteúdo foi removido.

Use a guia **Configurações > Verificação em tempo real > Opções comuns** para especificar quando remover conteúdo de sites com conteúdo dinâmico.

1. Na área Remoção de conteúdo, selecione os tipos de conteúdo ativo que devem ser removidos de páginas Web recebidas.
2. Para alterar as configurações para outras opções em tempo real, consulte:
  - [Classificando conteúdo e verificando para identificar ameaças](#), página 146
  - [Verificação de arquivos](#), página 147.
3. Quando terminar, clique em **OK** para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Para desativar a remoção de conteúdo para qualquer idioma selecionado, desmarque a caixa de seleção associada.

## Refinando a verificação

Tópicos relacionados:

- ◆ [Opções de verificação](#), página 145
- ◆ [Classificando conteúdo e verificando para identificar ameaças](#), página 146
- ◆ [Verificação de arquivos](#), página 147
- ◆ [Removendo conteúdo](#), página 148

Use as listas Sempre verificar e Nunca verificar para personalizar o comportamento as opções de verificação Recomendado e Tudo.

- ◆ Quando uma opção em tempo real é definida como Recomendado ou Ativado, os sites com conteúdo dinâmico e os sites na lista Sempre verificar são verificados (consulte *Opções de verificação*, página 145). Os sites na lista Nunca verificar são ignorados.
- ◆ Quando uma opção em tempo real é configurada como Tudo, os sites na lista Sempre verificar são ignorados. Isso pode melhorar o desempenho.

Use a lista Nunca verificar com cuidado. Se um site nesta lista estiver adulterado, o Websense Security Gateway não verifica o site para identificar o problema de segurança.

Use a página **Configurações > Verificação em tempo real > Exceções** para preencher e editar as listas Sempre verificar e Nunca verificar.

Para adicionar sites às listas Sempre verificar e Nunca verificar:

1. Digite nomes de sites na caixa URLs.

Digite apenas o nome do host (por exemplo, **thissite.com**). Não é necessário digitar o URL completo. Certifique-se de digitar o domínio e a extensão; **thissite.com** e **thissite.net** são entradas diferentes.

Você pode digitar mais de um nome de host de cada vez.

2. Na coluna **Opções**, selecione quais opções em tempo real aplicam-se a todos os sites que você digitou. Você pode selecionar uma ou mais opções. Observe que **Ameaças de segurança** refere-se apenas a verificação de conteúdo e não a verificação de arquivos. A verificação de arquivos não é afetada pelas listas Sempre verificar e Nunca verificar.

Para aplicar diferentes opções a diferentes sites, informe os sites separadamente.

3. Selecione **Adicionar a Sempre verificar** ou **Adicionar a Nunca verificar**.

Um site só pode aparecer em uma das duas listas. Você não pode, por exemplo, especificar que o mesmo site sempre deve ser verificado para ameaças e nunca para remoção de conteúdo.

- Para alterar em que lista um site aparece, primeiro selecione o site e depois use os botões seta para a direita (>) e seta para a esquerda (<) para mover o site para uma nova lista.
  - Para excluir um site de uma das listas, selecione o site e clique em **Remover**.
4. Quando terminar, clique em **OK** para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Para alterar as opções de verificação associadas com um site:

1. Selecione o site na lista Sempre verificar ou Nunca verificar, e clique em **Editar**.
2. Na caixa Editar regras, selecione as novas opções para aquele nome de host:
  - **Sem alteração** mantém a configuração atual.
  - **Ativado** indica que o conteúdo é verificado para a opção especificada, como classificação de conteúdo.
  - **Desativado** indica que não ocorre verificação para a opção especificada. Se uma opção estiver desativada, o desempenho pode melhorar, mas a segurança pode ser comprometida.

- Quando você terminar de fazer alterações, clique em **OK** na caixa Editar regras para voltar à guia Exceções.
- Clique em **OK** novamente para salvar suas alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Relatórios sobre a atividade de verificação em tempo real

Tópicos relacionados:

- ◆ [Opções de verificação, página 145](#)
- ◆ [Classificando conteúdo e verificando para identificar ameaças, página 146](#)
- ◆ [Verificação de arquivos, página 147](#)
- ◆ [Removendo conteúdo, página 148](#)

Se a sua assinatura inclui recursos de verificação em tempo real, você pode analisar os efeitos desses recursos com relatórios de apresentação e relatórios investigativos.

Na página Relatórios de apresentação, um grupo de relatórios denominado Ameaças à segurança em tempo real está disponível. Esses relatórios se concentram especificamente em atividades relacionadas a ameaças. Como ocorre com todos os relatórios de apresentação, você pode copiar um relatório de ameaça de segurança e editar seu filtro de relatórios para refinar as informações incluídas quando você gera um relatório a partir daquela cópia.

Alguns relatórios de ameaças de segurança incluem uma coluna ID da ameaça. Você pode clicar na ID da ameaça individual para abrir uma página do Websense Security Labs que descreve o tipo de ameaça identificada.

Além disso, outros relatórios de apresentação contêm informações sobre atividades de verificação em tempo real e atividades de filtragem padrão. Copie um relatório predefinido e edite seu filtro para criar um relatório específico para as atividades de verificação em tempo real.



### Importante

Habilite o registro de URLs completos (consulte [Configurando o registro de URLs completos, página 322](#)) para garantir que a atividade de verificação em tempo real seja significativa. Caso contrário, os relatórios só podem exibir o domínio (www.domain.com) do site classificado, ainda que as páginas individuais do site recaiam em diferentes categorias ou contenham diferentes ameaças.

Como exemplo, o relatório Detalhe de URLs completos por categoria, localizado no grupo Atividade da Internet do Catálogo de relatórios, fornece uma lista detalhada de cada URL acessado em cada categoria. Para criar um relatório específico para a

verificação em tempo real, copie o relatório Detalhe de URLs completos por categoria e edite seu filtro de relatórios. Na guia Ações, selecione apenas ações permitidas e bloqueadas que se referem à verificação em tempo real. Na guia Opções, altere o título de catálogo do relatório e o nome do relatório para identificá-lo como um relatório de verificação em tempo real. Por exemplo, você pode alterar o nome e o título para Tempo real: Detalhe de URLs completos por categoria.

Os relatórios investigativos também podem ser usados para obter informações sobre as atividades de verificação em tempo real.

1. Na lista suspensa **Uso da Internet por**, selecione Ação.
2. No relatório resultante, clique em uma ação em tempo real, como Categoria bloqueada em tempo real, para exibir uma lista de opções suspensas.
3. Marque a opção suspensa desejada, como Categoria ou Usuário.
4. Clique no valor Ocorrências ou na barra em qualquer linha para ver os detalhes relacionados.
5. Clique em **Modificar relatório**, no alto da página, para adicionar a coluna URL completo ao relatório.

Consulte [Relatórios investigativos](#), página 115, para obter detalhes sobre o uso de todos os recursos de relatórios investigativos.

## Como a verificação em tempo real é registrada

Quando você usa opções de verificação em tempo real, observe que há diferenças na forma como a atividade de filtragem da Web padrão e a atividade de verificação em tempo real são registradas.

Para filtragem da Web padrão, você tem diversas opções para reduzir o tamanho do banco de dados de log.

- ◆ Habilite **visitas** para registrar apenas um registro para cada site da Web visitado. Consulte [Configurando os arquivos de cache de log](#), página 311.
- ◆ Habilite **consolidação** para combinar em um único registro diversas solicitações com determinados elementos em comum. Consulte [Configurando opções de consolidação](#), página 312.
- ◆ Desabilite **Registro dos logs de URLs completos** para registrar apenas o nome do domínio (www.domain.com) para cada solicitação, e não o caminho para a página específica no domínio (/produtos/produtoA). Consulte [Configurando o registro de URLs completos](#), página 322.
- ◆ Habilite **registro seletivo de categorias em log** para limitar o registro a categorias selecionadas que são essenciais para a sua empresa. Consulte [Configurando o Filtering Service para registro em log](#), página 304.

Porém, os recursos de verificação em tempo real são limitados apenas parcialmente por essas configurações. Quando a verificação em tempo real analisa um site, cria dois registros de log separados.

- ◆ **Os registros do Web Filter** são beneficiados por qualquer configuração de redução de tamanho que tenha sido implementada, e estão disponíveis para todos os relatórios do Web Filter.
- ◆ **Os registros em tempo real** ignoram a maioria das configurações de redução de tamanho. Cada ocorrência separada é registrado, as solicitações para todas as categorias são registradas e nenhum registro é consolidado. Um registro em tempo real é gerado, não importa se o site é bloqueado ou permitido como resultado de verificação em tempo real. Somente a configuração de registro de URLs completos é cumprida para registros em tempo real.

Se você habilitou qualquer opção de redução de tamanho do banco de dados de log, os números que aparecem nos relatórios em tempo real podem **não** corresponder aos que aparecem em relatórios de filtragem padrão, mesmo quando os relatórios são configurados para os mesmos usuários, períodos de tempo e categorias. Por exemplo, se você optou por registrar as visitas, e um usuário solicitar que um site seja analisado por recursos de verificação em tempo real, a solicitação do usuário aparece como uma visita em relatórios de filtragem padrão, mas pode aparecer como várias ocorrências nos relatórios em tempo real.

Para ver dados comparáveis para filtragem padrão e em tempo real, **desative** as configurações de redução de tamanho do banco de dados de log. Como isso pode resultar em um banco de dados muito grande e que cresce muito rápido, certifique-se de que o computador do banco de dados de log tenha capacidade adequada de disco rígido, processamento e memória.

Consulte [Administração de relatórios](#), página 299, para obter mais informações sobre as configurações de redução de tamanho. Consulte [Relatórios de apresentação](#), página 96, e [Relatórios investigativos](#), página 115, para obter mais informações sobre a geração de relatórios.



# 8

## Filtrar Clientes Remotos

Tópicos relacionados:

- ◆ [Como o Remote Filtering funciona](#), página 156
- ◆ [Definindo as configurações do Remote Filtering](#), página 162

Muitas empresas têm usuários que às vezes levam seus computadores portáteis para fora da rede. Para usuários remotos que usam um sistema operacional Microsoft Windows, você pode filtrar as solicitações de Internet, implementando o Websense Remote Filtering, um recurso opcional disponível no Websense Web Security e no Websense Web Filter.

O Remote Filtering monitora o tráfego HTTP, SSL e FTP, aplicando a política atribuída ao usuário ou grupo individual, ou a política Padrão, dependendo de como o usuário faz logon no computador remoto. O Remote Filtering não filtra com base em políticas atribuídas a computadores ou intervalos de rede. Consulte [Identificando usuários remotos](#), página 159 para obter mais informações.

A filtragem com base em banda não é suportada para clientes remotos (consulte [Usando o Bandwidth Optimizer para gerenciar a largura de banda](#), página 189). A banda gerada por tráfego remoto não está incluída em medições e relatórios de banda.

A filtragem remota de solicitações FTP e SSL, como HTTPS, só pode ser bloqueada ou permitida. Se um usuário remoto acessar um site de FTP ou HTTPS, por exemplo, de uma categoria à qual foi atribuída a ação cota ou confirmar, o site é bloqueado para clientes do Remote Filtering. Quando esses computadores estão dentro da rede, as ações de filtragem para cota e confirmar são aplicadas normalmente.

Para implementar o Remote Filtering, você deve instalar os seguintes componentes:

- ◆ O Remote Filtering Server deve estar dentro do firewall mais externo e os computadores remotos devem ter permissão para comunicar com ele. Em geral, é instalado na *zona desmilitarizada* da rede, ou DMZ, fora do firewall que protege o resto da rede. Você pode instalar até 3 servidores do Remote Filtering para fornecer recursos de failover.

- ◆ O Remote Filtering Client deve estar em cada computador que executa um sistema operacional Windows e é usado fora da rede.



**Obs.:**

Siga as recomendações no *Guia de Implementação* com cuidado para implementar estes componentes. Consulte o *Guia de Instalação* para obter instruções sobre como instalá-los.

Se você está usando o software Websense em modo independente (stand-alone: sem um produto de integração) configure o Network Agent **para não** monitorar o computador do Remote Filtering Server (consulte [Definindo as configurações globais](#), página 340).

Todas as comunicações entre o cliente do Remote Filtering e o Remote Filtering Server são autenticadas e criptografadas.

## Como o Remote Filtering funciona

---

Tópicos relacionados:

- ◆ [Dentro da rede](#), página 157
- ◆ [Fora da rede](#), página 158
- ◆ [Identificando usuários remotos](#), página 159
- ◆ [Quando a comunicação com o servidor falha](#), página 160
- ◆ [Rede Virtual Privada \(VPN, Virtual Private Network\)](#), página 161
- ◆ [Definindo as configurações do Remote Filtering](#), página 162

Sempre que um computador remoto faz uma solicitação HTTP, SSL ou FTP, seu cliente do Remote Filtering se comunica com o Remote Filtering Server. O Remote Filtering Server comunica-se com o Websense Filtering Service para determinar qual ação é aplicável. Em seguida, o Remote Filtering Server responde ao cliente do Remote Filtering, permitindo o site ou enviando a mensagem de bloqueio apropriada.

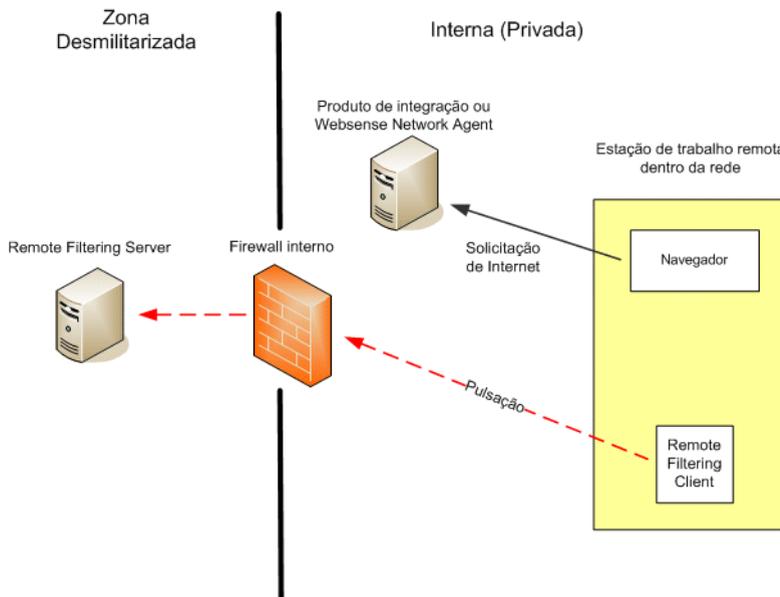
Quando o navegador em um computador que executa o cliente do Remote Filtering faz uma solicitação por HTTP, SSL ou FTP, o cliente do Remote Filtering deve decidir se irá consultar o Remote Filtering Server sobre a solicitação. Esta determinação é controlada pela localização do computador em relação à rede.

## Dentro da rede

Tópicos relacionados:

- ◆ *Como o Remote Filtering funciona*, página 156
- ◆ *Fora da rede*, página 158
- ◆ *Identificando usuários remotos*, página 159
- ◆ *Quando a comunicação com o servidor falha*, página 160
- ◆ *Rede Virtual Privada (VPN, Virtual Private Network)*, página 161
- ◆ *Definindo as configurações do Remote Filtering*, página 162

Quando um computador é inicializado *dentro* da rede, o cliente do Remote Filtering tenta enviar uma **pulsção** ao Remote Filtering Server na DMZ. A pulsção é bem-sucedida porque a porta de pulsção é aberta no firewall interno.



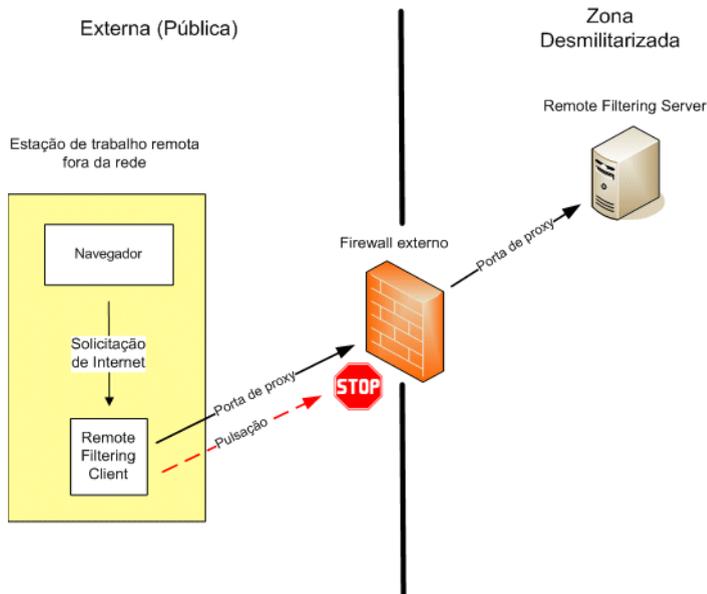
Neste caso, o cliente do Remote Filtering torna-se passivo e não consulta o Remote Filtering Server sobre solicitações de Internet. Em vez disso, essas solicitações são passadas diretamente ao produto de integração (como Cisco Pix, Microsoft ISA Server) ou ao Websense Network Agent. A solicitação é filtrada como qualquer outra solicitação interna.

## Fora da rede

Tópicos relacionados:

- ◆ [Como o Remote Filtering funciona](#), página 156
- ◆ [Dentro da rede](#), página 157
- ◆ [Identificando usuários remotos](#), página 159
- ◆ [Quando a comunicação com o servidor falha](#), página 160
- ◆ [Rede Virtual Privada \(VPN, Virtual Private Network\)](#), página 161
- ◆ [Definindo as configurações do Remote Filtering](#), página 162

Quando um computador é inicializado *dentro* da rede, o cliente do Remote Filtering tenta enviar uma pulsação ao Remote Filtering Server na DMZ. A pulsação não tem êxito porque a porta de pulsação é bloqueada no firewall externo.



Esta falha de pulsação faz com que o cliente do Remote Filtering envie uma consulta sobre cada solicitação HTTP, SSL ou FTP pela porta configurada (padrão 80) para o Remote Filtering Server na DMZ. O Remote Filtering Server encaminha a solicitação de filtragem ao Websense Filtering Service dentro da rede. O Filtering Service avalia a solicitação e envia uma resposta ao Remote Filtering Server. A resposta é encaminhada ao computador remoto. Se o site estiver bloqueado, o cliente do Remote Filtering solicita e recebe a página de bloqueio apropriada, que é exibida para o usuário.

O cliente do Remote Filtering atrasa cada solicitação filtrada até receber uma resposta do Remote Filtering Server. Dependendo da resposta recebida, o Remote Filtering Server permite o site ou exibe a página de bloqueio.

Um arquivo de registro monitora as atividades do Remote Filtering, como entrar e sair da rede, falha em abrir ou fechar, e reinício do cliente. O cliente do Remote Filtering cria o arquivo de log quando é inicializado pela primeira vez. Você controla a presença e o tamanho deste arquivo de log. Consulte [Definindo as configurações do Remote Filtering](#), página 162.

## Identificando usuários remotos

Tópicos relacionados:

- ◆ [Como o Remote Filtering funciona](#), página 156
- ◆ [Dentro da rede](#), página 157
- ◆ [Fora da rede](#), página 158
- ◆ [Quando a comunicação com o servidor falha](#), página 160
- ◆ [Rede Virtual Privada \(VPN, Virtual Private Network\)](#), página 161
- ◆ [Definindo as configurações do Remote Filtering](#), página 162

A forma como um usuário faz logon em um computador remoto determina qual política é aplicada.

Se um usuário faz logon usando credenciais de domínio em cache (informações de logon no diretório de rede), o Websense Filtering Service não pode resolver o nome de usuário, e aplica políticas apropriadas com base em usuários e grupos ao computador remoto. Além disso, a atividade de Internet é registrada em log sob o nome de usuário de rede.

Se o usuário faz logon com uma conta de usuário que é local para o computador, o Filtering Service não pode resolver o nome de usuário e aplica a política Padrão. A atividade de Internet é registrada sob o nome de usuário local. O Remote Filtering não filtra com base em políticas atribuídas a computadores ou intervalos de rede.



---

**Obs.:**

Os usuários remotos são sempre filtrados de acordo com suas credenciais de logon, conforme a descrição aqui. As configurações de autenticação seletiva não se aplicam a esses usuários.

---

## Quando a comunicação com o servidor falha

Tópicos relacionados:

- ◆ [Como o Remote Filtering funciona](#), página 156
- ◆ [Dentro da rede](#), página 157
- ◆ [Fora da rede](#), página 158
- ◆ [Identificando usuários remotos](#), página 159
- ◆ [Rede Virtual Privada \(VPN, Virtual Private Network\)](#), página 161
- ◆ [Definindo as configurações do Remote Filtering](#), página 162

A filtragem ocorre quando o cliente do Remote Filtering, fora da rede, se comunica com êxito com o Remote Filtering Server na DMZ da rede. Porém, pode haver ocasiões em que essa comunicação falha.

A ação que o cliente do Remote Filtering adota se não puder contatar o Remote Filtering Server é configurável. Por padrão, o cliente do Remote Filtering usa a configuração **fail open**, que permite todas as solicitações HTTP, SSL e FTP quando a comunicação entre esses componentes não pode ser estabelecida. O cliente do Remote Filtering continua tentando contatar o Remote Filtering Server. Quando a comunicação é bem-sucedida, a política de filtragem apropriada é aplicada.

Quando o cliente do Remote Filtering está configurado para **fail closed**, um valor de tempo limite é aplicado (o padrão são 15 minutos). O cronômetro começa a funcionar quando o computador remoto é inicializado. O cliente do Remote Filtering tenta a conexão com o Remote Filtering Server imediatamente e continua percorrendo os Remote Filtering Servers disponíveis até ter êxito.

Se o usuário tem acesso à Web na inicialização, não ocorre filtragem (todas as solicitações são permitidas) até que o cliente do Remote Filtering se conecte ao Remote Filtering Server. Quando isso ocorre, a política de filtragem apropriada é aplicada.

Se o cliente do Remote Filtering não pode se conectar com o período de tempo limite configurado, todo o acesso à Internet é bloqueado (fechamento por falha) até que a conexão ao Remote Filtering Server possa ser estabelecida.



**Obs.:**

Se o Remote Filtering Server não puder se conectar ao Websense Filtering Service por qualquer motivo, um erro é retornado ao cliente do Remote Filtering e a filtragem será sempre falha ao abrir.

---

Este período de tempo limite permite que os usuários que pagam por acesso à Internet em viagens inicializem o computador e providenciem a conexão sem serem bloqueados. Se o usuário não estabelecer o acesso à Web antes que o período de tempo limite de 15 minutos termine, o acesso à Web não pode ser estabelecido durante a

sessão. Quando isso ocorre, o usuário deve reinicializar o computador para reiniciar o intervalo de tempo limite.

Para alterar a configuração falha ao abrir/fechamento por falha, e mudar o valor de tempo limite, consulte [Definindo as configurações do Remote Filtering](#), página 162.

## Rede Virtual Privada (VPN, Virtual Private Network)

Tópicos relacionados:

- ◆ [Como o Remote Filtering funciona](#), página 156
- ◆ [Dentro da rede](#), página 157
- ◆ [Fora da rede](#), página 158
- ◆ [Identificando usuários remotos](#), página 159
- ◆ [Quando a comunicação com o servidor falha](#), página 160
- ◆ [Definindo as configurações do Remote Filtering](#), página 162

O Websense Remote Filtering suporta conexões de VPN, incluindo VPN com túnel dividido. Quando um computador remoto se conecta à rede interna via VPN (sem túnel dividido), o cliente do Remote Filtering pode enviar uma pulsação ao Remote Filtering Server. Como resultado, o cliente do Remote Filtering se torna passivo e todas as solicitações HTTP, SSL e FTP do computador remoto são filtradas pelo produto de integração interno ou pelo Network Agent, como os outros computadores na rede.

Se o computador remoto se conecta à rede interna via um cliente VPN com túnel dividido, o cliente do Remote Filtering detecta isso e não envia uma pulsação ao Remote Filtering Server. O cliente do Remote Filtering pressupõe que está operando externamente e envia as solicitações ao Remote Filtering Server para filtragem.

O software Websense suporta tunelamento dividido para os seguintes clientes de VPN:

- ◆ Checkpoint SecureClient
- ◆ Cisco
- ◆ Juniper/Netscreen
- ◆ Microsoft PPTP
- ◆ Nokia
- ◆ Nortel
- ◆ SonicWALL

## Definindo as configurações do Remote Filtering

---

Tópicos relacionados:

- ◆ [Como o Remote Filtering funciona](#), página 156
- ◆ [Dentro da rede](#), página 157
- ◆ [Fora da rede](#), página 158
- ◆ [Identificando usuários remotos](#), página 159
- ◆ [Quando a comunicação com o servidor falha](#), página 160
- ◆ [Rede Virtual Privada \(VPN, Virtual Private Network\)](#), página 161

Os Super administradores incondicionais podem usar a página **Configurações > Gerais > Remote Filtering** para configurar opções que afetam todos os clientes do Remote Filtering associados com esta instalação.

Para obter detalhes sobre como o Remote Filtering opera, consulte [Como o Remote Filtering funciona](#), página 156.

1. Marque a caixa de seleção **Fechamento por falha** para bloquear os clientes do Remote Filtering para todo o acesso à Internet, a não ser que o computador esteja se comunicando com o Remote Filtering Server.

Por padrão, isso não é selecionado, o que significa que os usuários remotos têm acesso não filtrado à Internet quando seus computadores não podem se comunicar com o Remote Filtering Server.

2. Se você marcou a opção **Fechamento por falha**, use o campo **Fechamento por falha timeout** para selecionar um número de minutos até 60 (o padrão é 15), ou escolha **Sem tempo limite**.

Durante o período de tempo limite, todas as solicitações HTTP, SSL e FTP são permitidas.

Se o cliente do Remote Filtering não pode se conectar com o Remote Filtering Server durante o intervalo de tempo limite, todo o acesso à Internet será bloqueado (fechamento por falha).

Escolher **Sem tempo limite** pode bloquear um computador remoto antes que o usuário possa estabelecer uma conexão de Internet a partir de um hotel ou outro provedor pago por uso. Além disso, o cliente do Remote Filtering tenta se comunicar com o Remote Filtering Server continuamente.



### Aviso

A Websense, Inc., não recomenda escolher **Sem tempo limite** ou definir um período de tempo limite muito baixo.

---

3. Selecione um **Tamanho máximo para o cache de registro local** (em megabytes), até 10. Escolha **Sem log** para desativar o registro em log.

Isso controla o tamanho e a existência do arquivo de log que o computador remoto cria quando é desconectado inicialmente do Remote Filtering Server. Este arquivo de log monitora os seguintes eventos:

- O computador sai da rede
- O computador volta à rede
- O cliente do Remote Filtering é reiniciado
- Ocorre uma condição de falha ao abrir
- Ocorre uma condição de fechamento por falha
- O cliente do Remote Filtering recebe uma atualização de política

O computador arquiva os 2 registros mais recentes. Esses registros podem ser usados para solucionar problemas de conexão ou outros problemas com o Remote Filtering.



# 9

## Refinar as diretivas de filtragem

Na configuração mais simples, a filtragem de uso da Internet requer uma única diretiva que aplique um filtro de categoria e um filtro de protocolo 24 horas por dia, 7 dias por semana. Porém, o software Websense oferece ferramentas que vão muito além dessa filtragem básica para atingir precisamente o nível de granularidade que você necessita para gerenciar o uso da Internet. Você pode:

- ◆ Criar **filtros de acesso limitado** para bloquear o acesso a tudo exceto uma lista especificada de sites para determinados usuários (consulte [Restringindo usuários a uma lista definida de sites de Internet](#), página 166).
- ◆ Criar **categorias personalizadas** para redefinir como sites selecionados serão filtrados (consulte [Trabalhando com categorias](#), página 173).
- ◆ **Recategorizar URLs** para mover sites específicos de sua categoria padrão do Master Database para outra categoria personalizada ou definida pelo Websense (consulte [Recategorizando URLs](#), página 182).
- ◆ Definir **URLs não filtrados** para permitir que usuários acessem sites específicos, mesmo se os sites tiverem sido atribuídos a uma categoria bloqueada no filtro de categoria ativo (consulte [Definindo URLs não filtrados](#), página 181).
- ◆ Implementar restrições de **largura de banda**, bloqueando o acesso de usuários a categorias e protocolos de outro modo permitidos quando o uso da largura de banda atingir um limiar especificado.
- ◆ Definir **palavras-chave** usadas para bloquear sites em categorias de outro modo permitidas quando o bloqueio de palavra-chave estiver habilitado e ativado (consulte [Filtrando com base em palavras-chave](#), página 177).
- ◆ Definir os **tipos de arquivo** usados para bloquear o download de tipos de arquivo selecionados de categorias de outro modo permitidas quando esse tipo de bloqueio estiver ativado (consulte [Gerenciando o tráfego com base no tipo de arquivo](#), página 191).

## Restringindo usuários a uma lista definida de sites de Internet

---

Tópicos relacionados:

- ◆ [Filtros de acesso limitado e precedência de filtragem](#), página 166
- ◆ [Criando um filtro de acesso limitado](#), página 168
- ◆ [Editando um filtro de acesso limitado](#), página 168

Os filtros de acesso limitado oferecem um método muito preciso para filtrar o acesso à Internet. Cada filtro de acesso limitado é uma lista de sites da Web individuais. Os filtros de acesso limitado, assim como os de categoria, são adicionados a diretivas e aplicados durante um período especificado. Quando um filtro de acesso limitado estiver ativo em uma diretiva, os usuários que receberem a atribuição dessa diretiva só poderão visitar sites da lista. Todos os outros sites estarão bloqueados.

Por exemplo, se a diretiva Primeira série escolar aplicar um filtro de acesso limitado que inclua somente determinados sites educacionais e de referência, os alunos regidos pela diretiva de primeira série só poderão visitar esses sites e nenhum outro.



### Importante

Quando um filtro de acesso limitado estiver em vigor, o software Websense verificará somente para ver se o site solicitado aparece no filtro. Nenhuma outra verificação será realizada.

Isso significa que, se o site permitido pelo filtro for infectado por códigos maliciosos, as solicitações do usuário para aquele site ainda serão permitidas, independentemente da categorização do Master Database ou da verificação em tempo real do site.

---

Quando um filtro de acesso limitado estiver ativo, uma página de bloqueio será retornada para qualquer URL solicitado não incluído naquele filtro.

O software Websense pode dar suporte a até 2.500 filtros de acesso limitado contendo 25.000 URLs no total.

## Filtros de acesso limitado e precedência de filtragem

Em alguns casos, mais de uma diretiva de filtragem pode aplicar-se a um único usuário. Isso acontece quando o usuário pertence a mais de um grupo e os grupos são regidos por diretivas diferentes. Além disso, o URL pode aparecer tanto como um filtro de acesso limitado quanto ser definido como um URL não filtrado.

Quando várias diretivas de grupo aplicam-se a um usuário, a configuração de **Utilizar bloqueio mais restritivo** (consulte *Ordem de filtragem*, página 78) determinará como o usuário será filtrado. Por padrão, esta configuração está desativada.

O software Websense determina qual configuração de filtragem é menos restritiva no nível de filtro. Em casos onde o usuário possa ser filtrado por várias diretivas, uma delas sendo aplicar um filtro de acesso limitado, a opção de “menos restritivo” poderá ser, às vezes, contrária ao bom senso.

Quando **Utilizar bloqueio mais restritivo** estiver **DESATIVADO**:

- ◆ Se o filtro de categoria **Bloquear tudo** e um filtro de acesso limitado forem aplicados, o filtro de acesso limitado será sempre considerado menos restritivo.
  - ◆ Se qualquer outro filtro de categoria e um filtro de acesso limitado forem aplicados, o filtro de categoria será considerado menos restritivo.
- Isso significa que mesmo que o filtro de acesso limitado permita o site e o filtro de categoria bloqueie o site, o site será bloqueado.

Quando **Utilizar bloqueio mais restritivo** estiver **ATIVADO**, o filtro de acesso limitado será considerado mais restritivo do que qualquer filtro de categoria exceto Bloquear tudo.

A tabela abaixo resume como a configuração **Utilizar bloqueio mais restritivo** afetará a filtragem quando várias diretivas puderem ser aplicadas:

	<i>Utilizar bloqueio mais restritivo</i> <b>DESATIVADO</b>	<i>Utilizar bloqueio mais restritivo</i> <b>ATIVADO</b>
filtro de acesso limitado + filtro de categoria <b>Bloquear tudo</b>	filtro de acesso limitado (solicitação permitida)	<b>Bloquear tudo</b> (solicitação bloqueada)
filtro de acesso limitado + categoria permitida	filtro de categoria (solicitação permitida)	filtro de acesso limitado (solicitação permitida)
filtro de acesso limitado + categoria bloqueada	filtro de categoria (solicitação bloqueada)	filtro de acesso limitado (solicitação permitida)
filtro de acesso limitado + categoria Cota/Confirmar	filtro de categoria (solicitação limitada por cota/confirmar)	filtro de acesso limitado (solicitação permitida)
filtro de acesso limitado + URL não filtrado	URL não filtrado (solicitação permitida)	filtro de acesso limitado (solicitação permitida)

## Criando um filtro de acesso limitado

Tópicos relacionados:

- ◆ [Trabalhando com filtros](#), página 46
- ◆ [Restringindo usuários a uma lista definida de sites de Internet](#), página 166
- ◆ [Editando um filtro de acesso limitado](#), página 168

Use a página **Adicionar filtros de acesso limitado** (acessada pela página **Filtros** ou **Editar diretiva**) para dar um nome exclusivo e uma descrição ao seu novo filtro. Após a criação do filtro, insira uma lista de URLs permitidos, atribua o filtro a uma diretiva e aplique a diretiva aos clientes.

1. Insira um **Nome de filtro** exclusivo. O nome deve ter de 1 a 50 caracteres e não pode incluir nenhum dos seguintes caracteres:

\* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

Os nomes de filtro podem incluir espaços, traços e apóstrofes.

2. Insira uma breve **Descrição** do filtro. Esta descrição é exibida ao lado do nome do filtro na seção Filtros de acesso limitado da página Filtros, e deve explicar o objetivo do filtro para ajudar os administradores a gerenciar diretivas ao longo do tempo.

As restrições de caracteres que se aplicam aos nomes de filtro também se aplicam às descrições, com duas exceções: as descrições podem incluir pontos (.) e vírgulas (,).

3. Para ver e editar o novo filtro, clique em **OK**. Para abandonar suas alterações e voltar à página Filtros, clique em **Cancelar**.

Quando você cria um novo filtro de acesso limitado, ele é adicionado à lista **Gerenciamento de diretivas > Filtros > Filtros de acesso limitado**. Para editar o filtro, clique no nome dele.

Para concluir a personalização do novo filtro, continue com [Editando um filtro de acesso limitado](#).

## Editando um filtro de acesso limitado

Tópicos relacionados:

- ◆ [Restringindo usuários a uma lista definida de sites de Internet](#), página 166
- ◆ [Filtros de acesso limitado e precedência de filtragem](#), página 166
- ◆ [Criando um filtro de acesso limitado](#), página 168
- ◆ [Editando uma diretiva](#), página 75

O filtro de acesso limitado é uma lista de sites da Web (URLs ou endereços IP) e de expressões regulares usada para identificar os sites específicos que os usuários podem acessar. Quando o filtro for aplicado a clientes, esses clientes não poderão visitar um site que não esteja na lista.



### Importante

Quando um filtro de acesso limitado estiver em vigor, o software Websense verificará somente para ver se o site solicitado aparece no filtro. Nenhuma outra verificação será realizada.

Isso significa que, se o site permitido pelo filtro for infectado por códigos maliciosos, as solicitações do usuário para aquele site ainda serão permitidas, independentemente da categorização do Master Database ou da verificação em tempo real do site.

Use a página **Gerenciamento de diretivas > Filtros > Editar filtro de acesso limitado** para alterar um filtro de acesso limitado existente. Você pode alterar o nome e a descrição do filtro, ver a lista de diretivas que aplicam o filtro e gerenciar quais sites serão incluídos no filtro.

Quando você editar um filtro de acesso limitado, as alterações afetarão todas as diretivas que apliquem o filtro.

1. Verifique o nome e a descrição do filtro. Para alterar o nome do filtro, clique em **Renomear** e insira o novo nome. O nome será atualizado em todas as diretivas que apliquem o filtro de acesso limitado selecionado.
2. Use o campo **Diretivas que usam este filtro** para ver quantas diretivas aplicam este filtro atualmente. Se uma ou mais diretivas aplicarem o filtro, clique em **Ver diretivas** para listá-las.
3. Em Adicionar ou remover sites, insira os URLs e endereços IP que você deseja adicionar ao filtro de acesso limitado. Insira um URL ou endereço IP por linha.

Não é necessário incluir o prefixo HTTP://.

Quando um site é filtrado de acordo com sua categoria do Master Database, o software Websense faz a correspondência do URL com o endereço IP equivalente. Esse não é o caso dos filtros de acesso limitado. Para permitir o URL e o endereço IP de um site, adicione-os ao filtro.

4. Clique na seta para a direita (>) para mover os URLs e endereços IP para a lista de sites Permitidos.
5. Além de adicionar sites individuais ao filtro de acesso limitado, você pode adicionar expressões regulares que correspondam a vários sites. Para criar expressões regulares, clique em **Avançado**.
  - Insira uma expressão regular por linha e depois clique na seta para a direita para mover as expressões para a lista de sites Permitidos.
  - Para verificar se uma expressão regular corresponde aos sites planejados, clique em **Testar**.

- Consulte *Usando expressões regulares*, página 194, para obter informações detalhadas sobre o uso de expressões regulares para filtragem.
- 6. Reveja os URLs, endereços IP e expressões regulares na lista **Sites permitidos**.
  - Para alterar um site ou expressão, selecione-o e clique em **Editar**.
  - Para remover um site ou expressão da lista, selecione-o e clique em **Excluir**.
- 7. Depois de editar o filtro, clique em **OK** para colocar suas alterações em cache e voltar à página Filtros. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Adicionando sites pela página Editar diretiva

Tópicos relacionados:

- ◆ *Restringindo usuários a uma lista definida de sites de Internet*, página 166
- ◆ *Filtros de acesso limitado e precedência de filtragem*, página 166
- ◆ *Criando um filtro de acesso limitado*, página 168
- ◆ *Editando uma diretiva*, página 75

Use a página **Diretivas > Editar diretiva > Adicionar sites** para adicionar sites a um filtro de acesso limitado.

Insira um URL ou endereço IP por linha. Se você não especificar um protocolo, o software Websense adicionará automaticamente o prefixo **HTTP://**.

Quando terminar de fazer as alterações, clique em **OK** para voltar à página Editar diretiva. Você também precisa clicar em **OK** na página Editar diretiva para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

As alterações em um filtro de acesso limitado afetarão todas as diretivas que aplicarem o filtro.

## Copiando filtros e diretivas para funções

---

Tópicos relacionados:

- ◆ *Criando um filtro de categoria*, página 47
- ◆ *Criando um filtro de protocolo*, página 49
- ◆ *Criando um filtro de acesso limitado*, página 168
- ◆ *Criando uma diretiva*, página 74

Super administradores podem usar as páginas **Filtros > Copiar Filtros na função e Diretivas > Copiar Diretivas na função** para copiar um ou mais filtros ou diretivas para uma função de administração delegada. Depois que o filtro ou a diretiva for copiado, os administradores delegados poderão usar os filtros ou diretivas para filtrar seus clientes gerenciados.

- ◆ Na função de destino, o tag “(Copied)” é acrescentado ao final do nome do filtro ou da diretiva. Será adicionado um número se o mesmo filtro ou diretiva for copiado várias vezes.
- ◆ Os administradores delegados podem renomear ou editar filtros e diretivas que foram copiados para sua função.
- ◆ Os filtros de categoria copiados para uma função de administração delegada definem a ação de filtragem como Permitir para as categorias personalizadas criadas na função. Os administradores delegados devem atualizar os filtros de categoria copiados para definir a ação desejada para suas categorias personalizadas específicas de função.
- ◆ As alterações feitas por um administrador delegado em um filtro ou diretiva copiado para sua função por um Super administrador não afetam o filtro ou diretiva original do Super administrador ou qualquer outra função que receba uma cópia do filtro ou da diretiva.
- ◆ As restrições de Proteção de filtro não afetam o filtro ou a diretiva original do Super administrador, mas afetam a cópia do filtro ou da diretiva do administrador delegado.
- ◆ Como os administradores delegados são afetados pelas restrições de Proteção de filtro, os filtros de protocolo e da categoria Permitir tudo não podem ser copiados para uma função de administração delegada.

Para copiar um filtro ou uma diretiva:

1. Na página Copiar filtros na função ou Copiar diretivas na função, verifique se as diretivas ou filtros corretos aparecem na lista na parte superior da página.
2. Use a lista suspensa **Selecione uma função** para selecionar uma função de destino.
3. Clique em **OK**.

Uma caixa de diálogo pop-up indica que os filtros ou diretivas selecionados estão sendo copiados. O processo de cópia pode levar alguns instantes.

As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Depois que o processo de cópia terminar, os filtros ou diretivas copiados estarão disponíveis para administradores delegados na função selecionada da próxima vez que eles fizerem logon no Websense Manager. Se um administrador delegado estiver conectado à função com diretiva de acesso quando os filtros ou diretivas forem copiados, ele não verá os novos filtros ou diretivas até que faça logoff e logon novamente.

## Criando componentes de filtro

Use a página **Gerenciamento de diretivas > Componentes do filtro** para acessar as ferramentas usadas para refinar e personalizar o modo como o software Websense aplica as diretivas de acesso de sua empresa à Internet. Os 4 botões na tela estão associados às seguintes tarefas:

<b>Editar categorias</b>	<ul style="list-style-type: none"> <li>• Recategorizar um URL (consulte <a href="#">Redefinindo a filtragem de sites específicos</a>, página 180). Por exemplo, se a categoria Compras estiver bloqueada por suas diretivas de filtragem, mas você deseja permitir acesso a sites de parceiros ou de um fornecedor específico, poderá mover esses sites para uma categoria permitida, como Negócios e economia.</li> <li>• Definir ou editar categorias personalizadas (consulte <a href="#">Criando uma categoria personalizada</a>, página 176). Crie subcategorias adicionais nas categorias pai definidas pelo Websense ou na categoria pai Definida pelo usuário e depois atribua URLs às novas categorias.</li> <li>• Atribuir palavras-chave a uma categoria (consulte <a href="#">Filtrando com base em palavras-chave</a>, página 177). Para recategorizar e bloquear o acesso a sites cujos URLs contenham uma string específica, primeiro defina as palavras-chave e depois habilite o bloqueio de palavras-chave no filtro de categoria.</li> <li>• Criar expressões regulares (consulte <a href="#">Usando expressões regulares</a>, página 194), padrões ou modelos que possam ser usados para corresponder a vários URLs e atribuí-los a uma categoria.</li> </ul>
<b>Editar protocolos</b>	Definir ou editar definições de protocolo personalizadas (consulte <a href="#">Criando um protocolo personalizado</a> , página 187, e <a href="#">Editando protocolos personalizados</a> , página 184). Por exemplo, se membros de sua empresa usarem uma ferramenta de mensagens personalizada, você poderá criar uma definição de protocolo personalizada para permitir o uso dessa ferramenta enquanto bloqueia outros protocolos de mensagens instantâneas/bate-papo.
<b>Tipos de arquivo</b>	Crie ou edite definições de tipos de arquivo usadas para bloquear tipos específicos de arquivos em categorias de outro modo permitidas (consulte <a href="#">Gerenciando o tráfego com base no tipo de arquivo</a> , página 191).
<b>URLs não filtrados</b>	Defina sites específicos para permitir todos os clientes, mesmo se pertencerem a uma categoria bloqueada (consulte <a href="#">Definindo URLs não filtrados</a> , página 181). Observe que a adição de um URL a essa lista não substitui o filtro de categoria Bloquear tudo ou os filtros de acesso limitado.

## Trabalhando com categorias

Tópicos relacionados:

- ◆ [Editando categorias e seus atributos](#), página 173
- ◆ [Criando uma categoria personalizada](#), página 176
- ◆ [Filtrando com base em palavras-chave](#), página 177
- ◆ [Redefinindo a filtragem de sites específicos](#), página 180

O software Websense oferece vários métodos para filtrar sites que não estejam no Master Database e para alterar o modo de filtragem dos sites individuais do Master Database.

- ◆ Crie **categorias personalizadas** para uma filtragem e geração de relatórios mais precisa.
- ◆ Use **URLs recategorizados** para definir as categorias de sites não categorizados ou para alterar a categoria de sites que apareçam no Master Database.
- ◆ Defina **palavras-chave** para recategorizar todos os sites cujo URL contenha uma determinada string.

### Editando categorias e seus atributos

Tópicos relacionados:

- ◆ [Criando uma categoria personalizada](#), página 176
- ◆ [Revisando todos os atributos de categorias personalizadas](#), página 174
- ◆ [Fazendo alterações de filtragem global de categorias](#), página 175
- ◆ [Filtrando com base em palavras-chave](#), página 177
- ◆ [Redefinindo a filtragem de sites específicos](#), página 180

Use a página **Gerenciamento de diretivas > Componentes do filtro > Editar Categorias** para criar e modificar categorias personalizadas, URLs recategorizados e palavras-chave.

As categorias existentes, tanto as definidas pelo Websense quanto as personalizadas, estão listadas na parte esquerda do painel de conteúdo. Para ver configurações personalizadas atuais associadas com uma categoria, ou criar novas definições personalizadas, primeiro selecione uma categoria na lista.

Para ver a lista de todos os URLs, palavras-chave e expressões regulares personalizados associados a todas as categorias, clique em **Ver todos os URLs/palavras-chave personalizados** na barra de ferramentas no alto da página. Consulte

*Revisando todos os atributos de categorias personalizadas*, página 174, para obter mais informações.

- ◆ Para criar uma nova categoria, clique em **Adicionar** e vá para *Criando uma categoria personalizada*, página 176, para obter mais instruções.  
Para remover uma categoria personalizada existente, selecione a categoria e clique em **Excluir**. Categorias definidas pelo Websense não podem ser excluídas.
- ◆ Para alterar o nome ou a descrição de uma categoria personalizada, selecione a categoria e clique em **Renomear** (consulte *Renomeando uma categoria personalizada*, página 176).
- ◆ Para alterar a ação de filtragem associada a uma categoria em todos os filtros de categoria, clique em **Substituir ação** (consulte *Fazendo alterações de filtragem global de categorias*, página 175).
- ◆ A lista **URLs recategorizados** mostra quais sites recategorizados (URLs e endereços IP) foram atribuídos a essa categoria.
  - Para adicionar um site à lista, clique em **Adicionar URLs**. Consulte *Recategorizando URLs*, página 182, para obter mais instruções.
  - Para alterar um site recategorizado existente, selecione o URL ou o endereço IP e clique em **Editar**.
- ◆ A lista de **Palavras-chave** mostra as palavras-chave que foram associadas a essa categoria.
  - Para definir uma palavra-chave associada à categoria selecionada, clique em **Adicionar palavras-chave**. Consulte *Filtrando com base em palavras-chave*, página 177, para obter mais instruções.
  - Para alterar a definição de uma palavra-chave existente, selecione a palavra-chave e clique em **Editar**.
- ◆ Além dos URLs e das palavras-chave, você pode definir **Expressões regulares** para a categoria. Cada expressão regular é um padrão ou modelo usado para associar vários sites à categoria.  
Para ver ou criar expressões regulares para a categoria, clique em **Avançado**.
  - Para definir uma expressão regular, clique em **Adicionar expressões** (consulte *Usando expressões regulares*, página 194).
  - Para alterar uma expressão regular existente, selecione a expressão e clique em **Editar**.
- ◆ Para excluir um URL recategorizado, uma palavra-chave ou uma expressão regular, selecione o item a remover e clique em **Excluir**.

Quando terminar alterar a página **Editar categorias**, clique em **OK** para colocar as alterações em cache e voltar à página **Componentes do filtro**. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Revisando todos os atributos de categorias personalizadas

Use a página **Componentes do filtro > Editar categorias > Ver todos os URLs e palavras-chave personalizados** para revisar as definições de URLs, palavras-chave e

expressões regulares personalizados. Você também pode excluir as definições que não sejam mais necessárias.

A página contém 3 tabelas semelhantes, uma para cada atributo de categoria: URLs, palavras-chave ou expressões regulares personalizados. Em cada tabela, o atributo está listado ao lado do nome da categoria com a qual está associado.

Para excluir um atributo de categoria, marque a caixa de seleção apropriada e clique em **Excluir**.

Para voltar à página Editar categorias, clique em **Fechar**. Se você excluir algum item na página Ver todos os URLs e palavras-chave personalizados, clique em **OK** na página Editar categorias para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Fazendo alterações de filtragem global de categorias

Use a página **Componentes do filtro > Editar categorias > Substituir ação** para alterar a ação aplicada a uma categoria em todos os filtros existentes da categoria. Isso também determinará a ação padrão aplicada à categoria em novos filtros.

Embora essa alteração substitua a ação aplicada à categoria em todos os filtros existentes, os administradores poderão editar posteriormente esses filtros para aplicar outra ação.

Antes de alterar as configurações de filtragem aplicadas à categoria, primeiro verifique se o nome da categoria correta aparece ao lado da **Categoria selecionada**. Em seguida, você poderá:

1. Escolher uma nova **Ação** (Permitir, Bloquear, Confirmar ou Cota). Consulte [Ações de filtragem, página 42](#), para obter mais informações.  
Por padrão, **Não alterar as configurações atuais** está selecionada para todas as opções da página.
2. Especifique se é ou não para **Bloquear palavras-chave**. Consulte [Filtrando com base em palavras-chave, página 177](#), para obter mais informações.
3. Especifique se é ou não para **Bloquear tipos de arquivo** e personalize as configurações de bloqueio. Consulte [Gerenciando o tráfego com base no tipo de arquivo, página 191](#), para obter mais informações.
4. Em **Filtragem avançada**, especifique se é ou não para usar o Bandwidth Optimizer para gerenciar o acesso a sites HTTP, e personalize as configurações de bloqueio. Consulte [Usando o Bandwidth Optimizer para gerenciar a largura de banda, página 189](#), para obter mais informações.



### Importante

As alterações feitas aqui afetarão todos os filtros de categoria existentes, exceto **Bloquear tudo** e **Permitir tudo**.

---

5. Clique em **OK** para voltar à página Editar categorias (consulte [Editando categorias e seus atributos, página 173](#)). As alterações não estarão no cache até que você clique em **OK** na página Editar categorias.

## Renomeando uma categoria personalizada

Use a página **Componentes do filtro > Editar categorias > Renomear categoria** para alterar o nome ou a descrição associada à categoria personalizada.

- ◆ Use o campo **Nome do filtro** para editar o nome da categoria. O novo nome precisa ser exclusivo e não pode exceder 50 caracteres.

O nome não pode incluir os seguintes caracteres:

\* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

- ◆ Use o campo **Descrição** para editar a descrição da categoria. A descrição não pode exceder 255 caracteres.

As restrições de caracteres que se aplicam aos nomes de filtro também se aplicam às descrições, com duas exceções: as descrições podem incluir pontos (.) e vírgulas (,).

Quando terminar de fazer as alterações, clique em **OK** para voltar à página Editar categorias. As alterações não estarão no cache até que você clique em **OK** na página Editar categorias.

## Criando uma categoria personalizada

Tópicos relacionados:

- ◆ [Editando categorias e seus atributos](#), página 173
- ◆ [Filtrando com base em palavras-chave](#), página 177
- ◆ [Redefinindo a filtragem de sites específicos](#), página 180

Além de usar as mais de 90 categorias definidas pelo Websense no Master Database, você pode definir suas próprias **categorias personalizadas** para proporcionar uma filtragem e geração de relatórios mais precisa. Por exemplo, crie categorias personalizadas como:

- ◆ **Viagens de negócios**, para agrupar sites de fornecedores aprovados que os funcionários podem usar para comprar passagens de avião e fazer reservas de hotel e de aluguel de automóveis.
- ◆ **Materiais de referência**, para agrupar sites de dicionários e enciclopédias online considerados apropriados para alunos do primeiro ciclo do ensino fundamental.
- ◆ **Desenvolvimento profissional**, para agrupar sites de treinamento e outros recursos que os funcionários são incentivados a usar para desenvolver suas habilidades.

Use a página **Gerenciamento de diretivas > Componentes do filtro > Editar categorias > Adicionar categoria** para adicionar categorias personalizadas a qualquer categoria pai. Você pode criar até 100 categorias personalizadas.

1. Insira um **Nome de categoria** exclusivo e descritivo. O nome não pode incluir os seguintes caracteres:

\* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

2. Insira uma **Descrição** para a nova categoria.  
As restrições de caracteres que se aplicam aos nomes de filtro também se aplicam às descrições, com duas exceções: as descrições podem incluir pontos (.) e vírgulas (,).
3. Selecione uma categoria pai na lista **Adicionar a**. Por padrão, **Todas as categorias** está selecionada.
4. Insira os sites (URLs ou endereços IP) que você deseja adicionar a esta categoria. Consulte [Recategorizando URLs](#), página 182, para obter mais informações.  
Você também poderá editar essa lista depois de criar a categoria.
5. Insira as palavras-chave que deseja associar a essa categoria. Consulte [Filtrando com base em palavras-chave](#), página 177, para obter mais informações.  
Você também poderá editar essa lista depois de criar a categoria.
6. Defina uma **Ação** de filtragem padrão para aplicar a essa categoria em todos os filtros de categoria existentes. Você poderá editar essa ação em filtros individuais mais tarde.



**Obs.:**

Os filtros de categoria copiados para uma função de administração delegada definem a ação de filtragem como Permitir para as categorias personalizadas criadas na função. Os administradores delegados devem atualizar os filtros de categoria copiados para definir a ação desejada para suas categorias personalizadas específicas de função.

7. Habilite quaisquer ações de **Filtragem avançada** (bloqueio de palavras-chave, bloqueio de tipo de arquivo ou bloqueio de largura de banda) que devam ser aplicadas a essa categoria em todos os filtros de categoria existentes.
8. Quando terminar de definir a nova categoria, clique em **OK** para colocar as alterações em cache e voltar à página Editar categorias. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

A nova categoria será adicionada à lista de Categorias e serão exibidas informações personalizadas de URL e palavra-chave para a categoria.

## Filtrando com base em palavras-chave

Tópicos relacionados:

- ◆ [Recategorizando URLs](#), página 182
- ◆ [Definindo configurações de filtragem do Websense](#), página 54
- ◆ [Criando um filtro de categoria](#), página 47
- ◆ [Editando um filtro de categoria](#), página 48
- ◆ [Trabalhando com categorias](#), página 173

Palavras-chave são associadas com categorias, e depois usadas para oferecer proteção contra sites que não foram explicitamente adicionados ao Master Database ou definidos como URLs personalizados. Três etapas são necessárias para habilitar o bloqueio de palavras-chave:

1. Habilitar o bloqueio de palavras-chave em nível global (consulte [Definindo configurações de filtragem do Websense](#), página 54).
2. Definir as palavras-chave associadas a uma categoria (consulte [Definindo palavras-chave](#), página 179).
3. Habilitar o bloqueio de palavras-chave para a categoria em um filtro de categoria ativo (consulte [Editando um filtro de categoria](#), página 48).

Quando as palavras-chave estiverem definidas e o bloqueio de palavras-chave estiver habilitado para uma categoria específica, o software Websense bloqueará qualquer site cujo URL contenha a palavra-chave e registrará o site como pertencente à categoria especificada. O site será bloqueado mesmo que outros URLs na categoria sejam permitidos.

Por exemplo, se a categoria Esportes for permitida em um filtro de categoria ativo, mas você deseja bloquear o acesso a sites de basquete, poderá associar a palavra-chave “nba” com Esportes e habilitar o bloqueio de palavras-chave. Isso significa que os seguintes URLs serão bloqueados e registrados em log como pertencentes à categoria Esportes:

- ◆ sports.espn.go.com/**nba**/
- ◆ modern**ba**kery.com
- ◆ modern**ba**biesandchildren.com
- ◆ fashion**ba**r.com

Tenha cuidado ao definir as palavras-chave para evitar um excesso de bloqueios não planejados.



#### **Importante**

Se você estiver usando o Websense Web Security, evite associar palavras-chave a uma das subcategorias de Proteção estendida. O bloqueio de palavras-chave não é aplicado para estas categorias.

---

Quando uma solicitação for bloqueada com base em uma palavra-chave, isso será indicado na página de bloqueio do Websense que o usuário receber.

## Definindo palavras-chave

Tópicos relacionados:

- ◆ [Editando um filtro de categoria](#), página 48
- ◆ [Trabalhando com categorias](#), página 173
- ◆ [Filtrando com base em palavras-chave](#), página 177
- ◆ [Usando expressões regulares](#), página 194

Uma palavra-chave é uma string de caracteres (como uma palavra, frase ou acrônimo) que pode ser encontrada em um URL. Atribua palavras-chave a uma categoria e depois habilite o bloqueio de palavras-chave no filtro de categoria.

Use a página **Gerenciamento de diretivas > Componentes do filtro > Editar categorias > Adicionar palavras-chave** para associar palavras-chave a categorias. Se você precisar alterar uma definição de palavra-chave, use a página **Editar palavras-chave**.

Quando definir palavras-chave, tenha cuidado para evitar um excesso de bloqueios não planejados. Você pode, por exemplo, ter a intenção de usar a palavra-chave “sex” para bloquear o acesso a sites adultos, mas acabar bloqueando solicitações de mecanismos de pesquisa para palavras como sêxtuplos ou Cidade de Essex, e sites como [msexchange.org](#) (Informática), [vegasexperience.com](#) (Viagens) e [sci.esa.int/marsexpress](#) (Instituições educacionais).

Insira uma palavra-chave por linha.

- ◆ Não inclua espaços nas palavras-chave. As strings de URL e CGI não incluem espaços entre as palavras.
- ◆ Inclua uma barra invertida (\) antes de caracteres especiais como:  
. , # ? \* +

Se você não incluir a barra invertida, o software Websense ignorará o caractere especial.

- ◆ Se você estiver usando o Websense Web Security, evite associar palavras-chave a uma das subcategorias de Proteção estendida. O bloqueio de palavras-chave não é aplicado para estas categorias.

Quando terminar de adicionar ou editar as palavras-chave, clique em **OK** para colocar as alterações em cache e voltar à página Editar categorias. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Para que o bloqueio de palavras-chave seja aplicado, você precisa também:

1. Habilitar o bloqueio de palavras-chave através da página **Configurações > Filtragem** (consulte [Definindo configurações de filtragem do Websense](#), página 54).
2. Habilitar o bloqueio de palavras-chave em um ou mais dos filtros de categoria ativos (consulte [Editando um filtro de categoria](#), página 48).

## Redefinindo a filtragem de sites específicos

Tópicos relacionados:

- ◆ [Criando uma categoria personalizada](#), página 176
- ◆ [Filtrando com base em palavras-chave](#), página 177
- ◆ [Definindo URLs não filtrados](#), página 181
- ◆ [Recategorizando URLs](#), página 182

Com URLs personalizados, você pode:

- ◆ Aplicar filtragem mais precisa a sites que não estejam no Websense Master Database. Por padrão, a ação aplicada à categoria **Diversos\Não categorizados** é usada para filtrar esses sites.
- ◆ Filtrar sites de modo diferente de suas categorias no Master Database.

O software Websense procura definições do URL personalizado de um site antes de consultar o Master Database, e portanto filtra o site de acordo com a categoria atribuída ao URL personalizado.

Há 2 tipos de URLs personalizados: não filtrado e recategorizado.

- ◆ Os URLs não filtrados são permitidos para todos os usuários não regidos pelo filtro da categoria Bloquear tudo ou por um filtro de acesso limitado (consulte [Definindo URLs não filtrados](#), página 181).
- ◆ Os URLs recategorizados foram movidos de suas categorias no Master Database para outra categoria personalizada ou definida pelo Websense (consulte [Recategorizando URLs](#), página 182).

Um URL recategorizado não é bloqueado por padrão. Ele é filtrado de acordo com a ação aplicada à sua nova categoria em cada filtro de categoria ativo.

Quando o site é filtrado de acordo com sua categoria do Master Database, o software Websense faz a correspondência do URL com o endereço IP equivalente. Esse não é o caso de URLs personalizados. Para alterar o modo como um site é filtrado, defina tanto seu URL quanto seu endereço IP como um URL personalizado.

Se um site puder ser acessado por vários URLs, defina cada URL que possa ser usado para acessar o site como um URL personalizado para garantir que o site seja permitido ou bloqueado de acordo com o planejado.

Se um site foi movido para um novo domínio e for usado um redirecionamento de HTTP para encaminhar usuários para o novo URL, esse novo URL não será automaticamente filtrado do mesmo modo que o site do redirecionamento. Para garantir que o site seja filtrado de forma adequada em seu novo endereço, crie um novo URL personalizado.

## Definindo URLs não filtrados

Tópicos relacionados:

- ◆ [Trabalhando com categorias](#), página 173
- ◆ [Redefinindo a filtragem de sites específicos](#), página 180
- ◆ [Recategorizando URLs](#), página 182

Use a página **Gerenciamento de diretivas > Componentes do filtro > URLs não filtrados** para definir uma lista de sites que qualquer usuário possa acessar, exceto quando regido pelo filtro da categoria Bloquear tudo ou por um filtro de acesso limitado.

A lista **Sites permitidos** na parte esquerda do painel de conteúdo lista os sites não filtrados (URLs e endereços IP) e as expressões regulares que você definiu (consulte [Usando expressões regulares](#), página 194). Cada site é associado a uma categoria.

- ◆ O URL pode ser associado a sua categoria no Master Database ou recategorizado.
- ◆ Quando o usuário solicita acesso ao URL não filtrado, a solicitação é registrada em log como um URL personalizado permitido na categoria à qual foi atribuído.

Para adicionar um URL não filtrado:

1. Em **Definir URLs não filtrados**, insira um único URL ou endereço IP por linha e clique na seta para a direita (>).

O software Websense não faz a correspondência do URL personalizado com seu endereço IP equivalente. Para permitir tanto o URL quanto o endereço IP de um site, adicione ambos à lista de URLs não filtrados.

2. Para adicionar expressões regulares que correspondam a vários sites, clique em **Avançado**. Insira uma única expressão regular por linha e depois clique na seta para a direita para mover as expressões para a lista de URLs não filtrados. Para verificar se um padrão corresponde aos sites planejados, clique em **Testar**.

Consulte [Usando expressões regulares](#), página 194, para obter informações detalhadas.

3. Quando terminar, clique em **OK** para colocar as alterações em cache e voltar à página Editar categorias. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Para remover um site da lista de URLs não filtrados, selecione o URL, o endereço IP ou a expressão regular e clique em **Excluir**.

## Recategorizando URLs

Tópicos relacionados:

- ◆ [Trabalhando com categorias](#), página 173
- ◆ [Redefinindo a filtragem de sites específicos](#), página 180
- ◆ [Definindo URLs não filtrados](#), página 181

Use a página **Gerenciamento de diretivas > Componentes do filtro > Editar categorias > Recategorizar URLs** para adicionar sites individuais a qualquer categoria. Faça alterações nos sites recategorizados existentes na página **Editar URLs**.

Recategorize URLs para mudar o modo como os sites individuais são filtrados e registrados em log. Quando você adicionar sites recategorizados:

- ◆ Insira cada URL ou endereço IP em uma linha separada.
- ◆ Inclua o protocolo de qualquer site não-HTTP. Se o protocolo for omitido, o software Websense filtrará o site como um site HTTP.

Para sites HTTPS, também inclua o número da porta (<https://63.212.171.196:443/>, <https://www.onlinebanking.com:443/>).

- ◆ O software Websense reconhece os URLs personalizados exatamente do modo como são inseridos. Se a categoria Mecanismos de busca e portais estiver bloqueada, mas você recategorizar **www.yahoo.com** em uma categoria permitida, o site só será permitido se os usuários digitarem o endereço completo. Se um usuário digitar [images.search.yahoo.com](https://images.search.yahoo.com) ou apenas [yahoo.com](https://yahoo.com), o site ainda será bloqueado. Se você recategorizar **yahoo.com**, entretanto, todos os sites com [yahoo.com](https://yahoo.com) no endereço serão permitidos.

Quando terminar de adicionar ou editar os sites recategorizados, clique em **OK** para colocar as alterações em cache e voltar à página Editar categorias. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Depois de salvar os URLs recategorizados, use a ferramenta **Categoria de URL** no painel de atalho à direita para verificar se o site está atribuído à categoria correta. Consulte [Usando a Caixa de ferramentas para verificar o comportamento de filtragem](#), página 195.

## Trabalhando com protocolos

---

O Websense Master Database inclui definições de protocolo usadas para filtrar protocolos de Internet diferentes de HTTP, HTTPS e FTP. Essas definições incluem aplicativos de Internet e métodos de transferência de dados como os usados para mensagens instantâneas, streaming media, compartilhamento de arquivos, transferência de arquivos, correio de Internet e outras operações de rede e de bancos de dados.

Essas definições de protocolo podem até ser usadas para filtrar protocolos ou aplicativos que ignorem um firewall fazendo tunelamento por portas normalmente usadas pelo tráfego HTTP. Dados de mensagens instantâneas, por exemplo, podem entrar em uma rede cujo firewall bloqueie protocolos de mensagens instantâneas fazendo tunelamento por portas HTTP. O software Websense identifica de forma precisa esses protocolos e os filtra de acordo com as diretivas configuradas por você.

**Obs.:**

É necessário o Network Agent para habilitar a filtragem com base em protocolos.

Além de usar as definições de protocolo definidas pelo Websense, você pode definir protocolos personalizados para filtragem. As definições de protocolo personalizadas podem ser baseadas nos endereços IP ou nos números de portas e podem ser editadas.

Para bloquear o tráfego por uma porta específica, associe o número dessa porta ao protocolo personalizado e, em seguida, atribua a ação padrão de **Bloquear** a esse protocolo.

Para trabalhar com definições de protocolo personalizadas, vá para **Gerenciamento de diretivas > Componentes do filtro** e clique em **Protocolos**. Consulte [Editando protocolos personalizados](#), página 184, e [Criando um protocolo personalizado](#), página 187, para obter detalhes.

## Filtrando protocolos

Tópicos relacionados:

- ◆ [Trabalhando com protocolos](#), página 182
- ◆ [Editando protocolos personalizados](#), página 184
- ◆ [Criando um protocolo personalizado](#), página 187
- ◆ [Adicionando ou editando identificadores de protocolo](#), página 185
- ◆ [Adicionando a um protocolo definido pelo Websense](#), página 189

Quando o Network Agent está instalado, o software Websense pode bloquear conteúdo de Internet transmitido por determinadas portas, usando endereços IP específicos ou marcado por determinadas assinaturas, independentemente da natureza

dos dados. Por padrão, o bloqueio de uma porta intercepta todo o conteúdo de Internet que entre em sua rede por essa porta, independentemente da fonte.



**Obs.:**

Algumas vezes, o tráfego da rede interna enviado por uma porta específica poderá não ser bloqueado, embora o protocolo que usa essa porta esteja bloqueado. O protocolo pode enviar dados por um servidor interno mais rapidamente do que o Network Agent consegue capturar e processar os dados. Isso não ocorre com dados originados fora da rede.

Quando é feita uma solicitação de protocolo, o software Websense usa as seguintes etapas para determinar se é para bloquear ou permitir a solicitação:

1. Determina o nome do protocolo (ou aplicativo de Internet).
2. Identifica o protocolo com base no endereço de destino da solicitação.
3. Pesquisa por números de portas ou endereços IP relacionados em definições de protocolo personalizadas.
4. Pesquisa por números de porta, endereços IP ou assinaturas relacionados nas definições de protocolo definidas pelo Websense.

Se o software Websense não conseguir determinar nenhuma dessas informações, todo o conteúdo associado ao protocolo será permitido.

## Editando protocolos personalizados

Tópicos relacionados:

- ◆ [Trabalhando com protocolos](#), página 182
- ◆ [Criando um protocolo personalizado](#), página 187
- ◆ [Criando um filtro de protocolo](#)
- ◆ [Editando um filtro de protocolo](#)
- ◆ [Trabalhando com categorias](#)

Use a página **Gerenciamento de diretivas > Componentes do filtro > Editar protocolos** para criar e editar definições de protocolo personalizadas e para rever as definições de protocolo definidas pelo Websense. Os protocolos definidos pelo Websense não podem ser editados.

A lista Protocolos inclui todos os protocolos personalizados e definidos pelo Websense. Clique em um protocolo ou grupo de protocolos para obter informações sobre o item selecionado no lado direito do painel de conteúdo.

Para adicionar um novo protocolo personalizado, clique em **Adicionar protocolo** e, em seguida, continue com [Criando um protocolo personalizado](#), página 187.

Para editar uma definição de protocolo:

1. Selecione o protocolo na lista Protocolos. A definição do protocolo aparece à direita da lista.
2. Clique em **Substituir ação** para alterar a ação de filtragem aplicada a esse protocolo em todos os filtros de protocolo (consulte *Fazendo alterações de filtragem global de protocolos*, página 186).
3. Clique em **Adicionar identificador** para definir identificadores de protocolo adicionais para esse protocolo (consulte *Adicionando ou editando identificadores de protocolo*, página 185).
4. Selecione um identificador na lista e clique em **Editar** para fazer alterações na **Porta, no Intervalo de endereços IP** ou no **Método de transporte** definido por esse identificador.
5. Quando terminar, clique em **OK** para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Para excluir uma definição de protocolo, selecione um item na lista Protocolos e clique em **Excluir**.

## Adicionando ou editando identificadores de protocolo

Use a página **Componentes do filtro > Editar Protocolos > Adicionar identificador de protocolo** para definir identificadores adicionais de protocolo para um protocolo personalizado existente. Use a página **Editar identificador de protocolo** para alterar um identificador definido anteriormente.

Antes de criar ou alterar um identificador, verifique se o nome do protocolo correto aparece ao lado do **Protocolo selecionado**.

Quando trabalhar com identificadores de protocolo, lembre-se de que pelo menos um critério (porta, endereço IP ou tipo de transporte) precisa ser exclusivo para cada protocolo.

1. Especifique quais **Portas** serão incluídas nesse identificador.
  - Quando você seleciona **Todas as portas**, esse critério sobrepõe-se a outros endereços IP ou portas inseridos em outras definições de protocolo.
  - Os intervalos de porta não são considerados exclusivos se estão sobrepostos. Por exemplo, o intervalo de porta 80 - 6000 sobrepõe-se ao intervalo 4000 - 9000.
  - Tenha cuidado ao definir um protocolo na porta 80 ou 8080. O Network Agent ouve solicitações de Internet por essas portas.  
Como protocolos personalizados têm precedência sobre protocolos do Websense, se você definir um protocolo personalizado usando a porta 80, todos os outros protocolos que usarem a porta 80 serão filtrados e registrados em log como o protocolo personalizado.
2. Especifique quais **Endereços IP** serão incluídos nesse identificador.

- Quando você seleciona **Todos os endereços IP externos**, esse critério sobrepõe-se a quaisquer outros endereços IP inseridos em outras definições de protocolo.
  - Os intervalos de porta não são considerados exclusivos se estão sobrepostos.
3. Especifique qual método de **Transporte do protocolo** está incluído nesse identificador.
  4. Clique em **OK** para colocar suas alterações em cache e voltar à página Editar protocolos. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Renomeando um protocolo personalizado

Use a página **Componentes do filtro > Editar protocolos > Renomear protocolo** para alterar o nome de um protocolo personalizado ou movê-lo para outro grupo de protocolos.

- ◆ Use o campo **Nome** para editar o nome do protocolo. O novo nome não pode exceder 50 caracteres.

O nome não pode incluir os seguintes caracteres:

\* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

- ◆ Para mover o protocolo para outro grupo de protocolos, selecione o novo grupo pelo campo **No grupo**.

Quando terminar de fazer as alterações, clique em **OK** para voltar à página Protocolos. Você também precisa clicar em **OK** na página Editar protocolos para colocar as alterações em cache.

## Fazendo alterações de filtragem global de protocolos

Use a página **Componentes do filtro > Editar protocolos > Substituir ação** para alterar como o protocolo é filtrado em todos os filtros de protocolo existentes. Isso também determinará a ação padrão aplicada ao protocolo em novos filtros.

Embora essa alteração substitua a ação de filtragem aplicada em todos os filtros de protocolo existentes, os administradores poderão editar posteriormente esses filtros para aplicar outra ação.

1. Verifique se o nome do protocolo correto aparece ao lado do **Protocolo selecionado**.
2. Selecione uma nova **Ação** (Permitir ou Bloquear) para aplicar a esse protocolo. Por padrão, **Sem alteração** está selecionada. Consulte [Ações de filtragem, página 42](#), para obter mais informações.
3. Especifique novas opções de **Registro em log**. O tráfego de protocolo deve ser registrado em log para aparecer nos relatórios e permitir alertas de uso de protocolo.

- Especifique se o **Bandwidth Optimizer** será ou não usado para gerenciar o acesso a esse protocolo. Consulte [Usando o Bandwidth Optimizer para gerenciar a largura de banda, página 189](#), para obter mais informações.



#### Importante

As alterações feitas aqui afetarão todos os filtros de protocolo existentes, exceto **Bloquear tudo** e **Permitir tudo**.

- Quando terminar, clique em **OK** para voltar à página Editar protocolos (consulte [Editando protocolos personalizados, página 184](#)). Você também precisa clicar em **OK** na página Editar protocolos para colocar as alterações em cache.

## Criando um protocolo personalizado

Tópicos relacionados:

- ◆ [Trabalhando com protocolos, página 182](#)
- ◆ [Filtrando protocolos, página 183](#)
- ◆ [Editando protocolos personalizados, página 184](#)
- ◆ [Adicionando a um protocolo definido pelo Websense, página 189](#)

Use a página **Componentes do filtro > Protocolos > Adicionar protocolo** para definir um novo protocolo personalizado.

- Insira um **Nome** para o protocolo.

O nome não pode incluir os seguintes caracteres:

\* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

É possível atribuir ao protocolo personalizado o mesmo nome de um protocolo definido pelo Websense para estender o número de endereços IP ou de portas associados ao protocolo original. Consulte [Adicionando a um protocolo definido pelo Websense, página 189](#), para obter mais informações.

- Expanda a lista suspensa **Adicionar protocolo a este grupo** e selecione um grupo de protocolos. O novo protocolo aparecerá nesse grupo em todas as listas e filtros de protocolo.
- Defina um **Identificador de protocolo** exclusivo (conjunto de **portas, endereços IP e métodos de transporte**) para esse grupo. Você poderá adicionar outros identificadores depois, pela página Editar protocolos.

Siga essas diretrizes para criar identificadores de protocolo:

- Pelo menos um critério (porta, endereço IP ou tipo de transporte) precisa ser exclusivo para cada definição de protocolo.
- Quando você seleciona **Todas as portas** ou **Todos os endereços IP externos**, esse critério sobrepõe-se a quaisquer outros endereços IP ou portas inseridos em outras definições de protocolo.

- Os intervalos de portas ou intervalos de endereço IP não são considerados exclusivos se estão sobrepostos. Por exemplo, o intervalo de portas 80 - 6000 sobrepõe-se ao intervalo 4000 - 9000.

**Obs.:**

Tenha cuidado ao definir um protocolo na porta 80 ou 8080. O Network Agent ouve solicitações de Internet por essas portas.

Como protocolos personalizados têm precedência sobre protocolos do Websense, se você definir um protocolo personalizado usando a porta 80, todos os outros protocolos que usem a porta 80 serão filtrados e registrados em log como o protocolo personalizado.

As tabelas a seguir fornecem exemplos de definições válidas e inválidas de protocolo:

Porta	Endereço IP	Método de transporte	Combinação aceita?
70	QUALQUER UM	TCP	Sim - o número da porta torna cada identificador de protocolo exclusivo.
90	QUALQUER UM	TCP	

Porta	Endereço IP	Método de transporte	Combinação aceita?
70	QUALQUER UM	TCP	Não - os endereços IP não são exclusivos. 10.2.1.201 está incluído no conjunto "QUALQUER UM".
70	10.2.1.201	TCP	

Porta	Endereço IP	Método de transporte	Combinação aceita?
70	10.2.3.212	TCP	Sim - os endereços IP são exclusivos.
70	10.2.1.201	TCP	

- Em Ação de filtragem padrão, especifique a ação padrão (**Permitir** ou **Bloquear**) que deve ser aplicada a esse protocolo em todos os filtros de protocolo ativos:
  - Indique se o tráfego que usa esse protocolo deve ser **Registrado em log**. O tráfego de protocolo deve ser registrado em log para aparecer nos relatórios e permitir alertas de uso de protocolo.
  - Indique se o acesso a esse protocolo deve ser regulado pelo **Bandwidth Optimizer** (consulte *Usando o Bandwidth Optimizer para gerenciar a largura de banda*, página 189).

5. Quando terminar, clique em **OK** para voltar à página Editar protocolos. A nova definição do protocolo aparecerá na lista Protocolos.
6. Clique em **OK** novamente para salvar suas alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Adicionando a um protocolo definido pelo Websense

Você não pode adicionar um número de porta ou endereço IP diretamente a um protocolo definido pelo Websense. Porém, pode criar um protocolo personalizado com o mesmo nome de um protocolo definido pelo Websense e depois adicionar portas ou endereços IP à definição dele.

Quando um protocolo personalizado e um definido pelo Websense tiverem o mesmo nome, o software Websense pesquisará o tráfego de protocolos nas portas e endereços IP especificados nas duas definições.

Nos relatórios, os nomes de protocolos personalizados têm o prefixo “C\_”. Por exemplo, se você criar um protocolo personalizado para SQL\_NET e especificar números de portas adicionais, os relatórios exibirão C\_SQL\_NET quando o protocolo usar os números de porta no protocolo personalizado.

## Usando o Bandwidth Optimizer para gerenciar a largura de banda

Tópicos relacionados:

- ◆ [Trabalhando com categorias](#), página 173
- ◆ [Trabalhando com protocolos](#), página 182
- ◆ [Configurando os limites padrão do Bandwidth Optimizer](#), página 190

Quando você criar um filtro de categoria ou de protocolo, poderá escolher limitar o acesso à categoria ou ao protocolo com base no uso da largura de banda.

- ◆ Bloquear o acesso a categorias ou protocolos com base no uso total de largura de banda da rede.
- ◆ Bloquear o acesso a categorias com base no uso total de largura de banda pelo tráfego HTTP.
- ◆ Bloquear o acesso a um protocolo específico com base no uso de largura de banda por esse protocolo.

Por exemplo:

- ◆ Bloquear o protocolo AOL Instant Messaging se o uso total da largura de banda da rede exceder 50% da largura de banda disponível ou se o uso atual da largura de banda para AIM exceder 10% da largura de banda total da rede.

- ◆ Bloquear a categoria Esportes quando o uso total da largura de banda da rede atingir 75% ou quando o uso de largura de banda por todo o tráfego HTTP atingir 60% da largura de banda disponível da rede.

O uso de largura de banda por protocolo inclui o tráfego por todas as portas, endereços IP ou assinaturas definidas para o protocolo. Isso significa que se o protocolo ou aplicativo de Internet usar várias portas para transferência de dados, o tráfego em todas as portas incluídas na definição do protocolo será contabilizado em relação ao uso total de largura de banda por esse protocolo. Se o aplicativo de Internet usar uma porta não incluída na definição do protocolo, entretanto, o tráfego naquela porta não será incluído nas medições do uso da largura de banda.

O software Websense registra a largura de banda usada por protocolos filtrados com base em TCP e UDP.

A Websense, Inc., atualiza as definições de protocolos Websense regularmente para garantir a precisão da medição da largura de banda.

O Network Agent envia dados da largura de banda da rede para o Filtering Service em um intervalo predefinido. Isso assegura que o software Websense monitorará com precisão o uso da largura de banda e receberá medições mais próximas da média.

Quando as opções de filtragem com base em largura de banda estiverem ativas, o software Websense começará a filtragem com base em largura de banda 10 minutos após a configuração inicial e 10 minutos após cada reinicialização do Websense Policy Server. Esse atraso garante a medição precisa dos dados da largura de banda e o uso desses dados na filtragem.

Quando uma solicitação for bloqueada com base nas limitações de largura de banda, a página de bloqueio do Websense exibirá essas informações no campo **Motivo**. Para obter mais informações, consulte [Páginas de bloqueio](#), página 83.

## Configurando os limites padrão do Bandwidth Optimizer

Tópicos relacionados:

- ◆ [Editando um filtro de categoria](#), página 48
- ◆ [Editando um filtro de protocolo](#), página 50
- ◆ [Usando o Bandwidth Optimizer para gerenciar a largura de banda](#), página 189

Antes de especificar as configurações de largura de banda em diretivas, verifique os limites de largura de banda que acionam as configurações de filtragem com base em largura de banda. Os valores definidos pelo Websense são:

- ◆ Largura de banda padrão para rede: **50%**
- ◆ Largura de banda padrão por protocolo: **20%**

Os valores de largura de banda padrão são armazenados pelo Policy Server e aplicados por todas as instâncias associadas do Network Agent. Se você tiver vários Policy

Servers, as alterações a valores de largura de banda padrão em um Policy Server não afetarão os outros Policy Servers.

Para alterar os valores de largura de banda padrão:

1. No Websense Manager, vá para **Configurações > Filtragem**.
2. Insira os limites de largura de banda que acionarão a filtragem com base em largura de banda quando a filtragem de largura de banda estiver habilitada.
  - Quando houver bloqueio de uma categoria ou protocolo no tráfego para a rede inteira, a **Largura de banda padrão para rede** definirá o limite de filtragem padrão.
  - Quando houver bloqueio de uma categoria ou protocolo no tráfego para o protocolo, a **Largura de banda padrão por protocolo** definirá o limite de filtragem padrão.

Você poderá substituir os valores de limite padrão para cada categoria ou protocolo em qualquer filtro de categoria ou protocolo.

3. Quando terminar, clique em **OK** para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Quaisquer alterações nos padrões poderão afetar todos os filtros de categoria e protocolo que apliquem as restrições do Bandwidth Optimizer.

- ◆ Para gerenciar o uso de largura de banda associada a um protocolo específico, edite o filtro ou os filtros do protocolo ativo.
- ◆ Para gerenciar o uso de largura de banda associada a uma categoria de URL específica, edite o filtro ou os filtros da categoria apropriada.

Quando você filtrar categorias com base no uso de largura de banda de HTTP, o software Websense medirá o uso total da largura de banda de HTTP em todas as portas especificadas como portas HTTP para o software Websense.

## Gerenciando o tráfego com base no tipo de arquivo

Quando você cria um filtro de categoria, é possível definir a filtragem com base em extensões de arquivo, restringindo o acesso a tipos de arquivo específicos de sites em determinadas categorias. Por exemplo, permitir a categoria Esportes, mas bloquear arquivos de vídeo de sites nessa categoria.

O software Websense fornece vários tipos de arquivo predefinidos ou grupos de extensões de arquivo usados para fins semelhantes. Essas definições de tipo de arquivo são mantidas no Master Database e podem ser alteradas como parte do processo de atualização do Master Database.

Você pode implementar a filtragem usando tipos de arquivo predefinidos, modificar as definições de tipos de arquivo existentes ou criar novos tipos de arquivo. Observe, entretanto, que você não pode excluir tipos de arquivo definidos pelo Websense ou excluir as extensões de arquivo associadas a eles.

Quando um usuário solicitar um site, o software Websense primeiro determinará a categoria do site e, em seguida, verificará as extensões do arquivo filtrado.

**Obs.:**

Para implementar a filtragem completa para mídia de vídeo e áudio de Internet, combine a filtragem baseada em protocolo com a filtragem de tipo de arquivo. Nesse caso, a filtragem de protocolo tratará de streaming media, e a filtragem de tipo de arquivo tratará dos arquivos que podem ser baixados e depois reproduzidos.

Quando um usuário tentar acessar um arquivo cuja extensão estiver bloqueada, o campo **Motivo** da página de bloqueio do Websense indicará que o tipo de arquivo foi bloqueado. Para obter mais informações, consulte [Páginas de bloqueio](#), página 83.

**Obs.:**

A página de bloqueio padrão não será exibida se uma imagem bloqueada GIF ou JPEG abranger apenas uma parte de uma página permitida. Em vez disso, a área da imagem aparecerá em branco. Isso evita a possibilidade de exibir uma pequena parte de uma página bloqueada em vários locais de uma página de outro modo permitida.

As definições de tipo de arquivo podem conter tantas extensões de arquivo quanto sejam úteis para fins de filtragem. Os tipos de arquivo definidos pelo Websense, por exemplo, incluem as seguintes extensões de arquivo:

Áudio	Arquivos compactados		Executáveis	Vídeo	
.aif	.ace	.mim	.bat	.asf	.mpg
.aifc	.arc	.rar	.exe	.asx	.mpv2
.aiff	.arj	.tar		.avi	.qt
.m3u	.b64	.taz		.ivf	.ra
.mid	.bhx	.tgz		.mlv	.ram
.midi	.cab	.tz		.mov	.wm
.mp3	.gz	.uu		.mp2	.wmp
.ogg	.gzip	.uue		.mp2v	.wmv
.rmi	.hqx	.xxe		.mpa	.wmx
.snd	.iso	.z		.mpe	.wxv
.wav	.jar	.zip			
.wax	.lzh				
.wma					

Qualquer extensão de arquivo associada a um tipo de arquivo definido pelo Websense poderá ser adicionada a um tipo de arquivo personalizado. A extensão de arquivo depois será filtrada e registrada em log de acordo com as configurações associadas ao tipo de arquivo personalizado.

Para visualizar as definições de tipo de arquivo existentes, editar tipos de arquivo ou criar tipos de arquivo personalizado, vá para **Gerenciamento de diretivas > Componentes do filtro** e clique em **Tipos de arquivo**. Consulte *Trabalhando com tipos de arquivo*, página 193, para obter mais informações.

## Trabalhando com tipos de arquivo

Tópicos relacionados:

- ◆ *Gerenciando o tráfego com base no tipo de arquivo*, página 191
- ◆ *Editando um filtro de categoria*, página 48
- ◆ *Filtrando um site*, página 79

Use a página **Gerenciamento de diretivas > Componentes do filtro > Editar Tipos de arquivo** para criar e gerenciar até 32 **tipos de arquivo**. Tipos de arquivo são grupos de extensões de arquivo que podem ser explicitamente bloqueados em filtros de categoria (consulte *Gerenciando o tráfego com base no tipo de arquivo*, página 191).

- ◆ Clique em um tipo de arquivo para ver as extensões de arquivo associadas àquele tipo.
- ◆ Para adicionar extensões ao tipo de arquivo selecionado, clique em **Adicionar extensão** e, em seguida, consulte *Adicionando extensões de arquivo a um tipo de arquivo*, página 194, para obter mais instruções.
- ◆ Para criar um novo tipo de arquivo, clique em **Adicionar tipo de arquivo** e, em seguida, consulte *Adicionando tipos de arquivo personalizados*, página 194, para obter mais instruções.
- ◆ Para excluir um tipo de arquivo personalizado ou uma extensão, selecione o item e, em seguida, clique em **Excluir**.

Você não pode excluir tipos de arquivo definidos pelo Websense ou excluir as extensões de arquivo associadas a eles.

Você pode, porém, adicionar extensões de arquivo associadas ao tipo de arquivo definido pelo Websense a um tipo de arquivo personalizado. A extensão de arquivo depois será filtrada e registrada em log de acordo com as configurações associadas ao tipo de arquivo personalizado. Você não pode adicionar a mesma extensão a vários tipos de arquivo personalizados.

Quando terminar de alterar as definições de tipo de arquivo, clique em **OK**. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Adicionando tipos de arquivo personalizados

Use a página **Componentes do filtro > Editar tipos de arquivo > Adicionar tipo de arquivo** para definir tipos de arquivo personalizados.

1. Insira um **Nome de tipo de arquivo** exclusivo.  
Você pode criar um tipo de arquivo personalizado com o mesmo nome do tipo de arquivo definido pelo Websense a fim de adicionar outras extensões de arquivo ao tipo de arquivo existente.
2. Insira extensões de arquivo, uma por linha, na lista **Extensões de arquivo definidas pelo usuário**. Não é necessário incluir o ponto (“.”) antes de cada extensão.
3. Clique em **OK** para voltar à tela Editar tipos de arquivo. O novo tipo de arquivo aparecerá na lista Tipos de arquivo.
4. Quando terminar de trabalhar com as definições de tipo de arquivo, clique em **OK** na página Editar tipos de arquivo. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Adicionando extensões de arquivo a um tipo de arquivo

Use a página **Componentes do filtro > Editar tipos de arquivo > Adicionar extensões de arquivo** para adicionar extensões ao tipo de arquivo selecionado.

1. Verifique se o nome do tipo de arquivo esperado aparece ao lado do **Tipo de arquivo selecionado**.
2. Insira as extensões de arquivo, uma por linha, na lista **Extensões de arquivo**. Não é necessário incluir o ponto (“.”) antes de cada extensão.
3. Clique em **OK** para voltar à tela Editar tipos de arquivo. As novas extensões de arquivo aparecerão na lista de Extensões de arquivos personalizados.
4. Quando terminar de trabalhar com as definições de tipo de arquivo, clique em **OK** na página Editar tipos de arquivo. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Usando expressões regulares

---

Uma **expressão regular** é um modelo ou padrão usado para fazer a correspondência de várias strings ou grupos de caracteres. Você pode usar expressões regulares em filtros de acesso limitado ou para definir URLs personalizados ou palavras-chave. A filtragem do Websense em seguida tentará fazer a correspondência com o padrão geral em vez de com um único URL ou palavra-chave específico.

Considere esta expressão regular simples:

```
domínio.(com|org|net)
```

Esse padrão de expressão corresponde aos URLs:

- ◆ domínio.com
- ◆ domínio.org
- ◆ domínio.net

Use as expressões regulares com cautela. Elas oferecem uma poderosa ferramenta de filtragem, mas podem facilmente resultar no bloqueio ou na permissão de sites inesperados. Além disso, expressões regulares mal construídas podem resultar em trabalho de filtragem excessivo.



### Importante

A utilização de expressões regulares como critérios de filtragem pode aumentar o uso da CPU. Testes mostraram que, com 100 expressões regulares, a média de uso da CPU na máquina do Filtering Service aumentava em 20%.

O software Websense oferece suporte para a maior parte da sintaxe de expressões regulares Perl, com algumas exceções. Algumas das sintaxes sem suporte não são úteis para fazer a correspondência de strings que possam ser encontradas em um URL.

As sintaxes de expressões regulares sem suporte incluem:

<code>(?&lt;=pattern) string</code>	<code>(?&lt;!pattern) string</code>
<code>\N{name}</code>	<code>(?imsx-imsx)</code>
<code>(?(condition) pat1)</code>	<code>\pP</code>
<code>(?(condition) pat1 pat2)</code>	<code>\PP</code>
<code>(?(code))</code>	<code>??{code}</code>

Para obter mais ajuda com expressões regulares, consulte:

[en.wikipedia.org/wiki/Regular\\_expression](http://en.wikipedia.org/wiki/Regular_expression)

[www.regular-expressions.info/](http://www.regular-expressions.info/)

## Usando a Caixa de ferramentas para verificar o comportamento de filtragem

O painel de atalho à direita no Websense Manager inclui uma **Caixa de ferramentas**, que permite fazer verificações rápidas de sua configuração de filtragem.

Clique no nome da ferramenta para acessar a ferramenta. Clique no nome novamente para ver a lista de ferramentas. Para obter mais informações sobre o uso da ferramenta, consulte:

- ◆ [Categoria de URL](#), página 196
- ◆ [Verificar diretiva](#), página 196
- ◆ [Testar filtragem](#), página 196
- ◆ [Acesso ao URL](#), página 197

◆ [Investigar usuário, página 197](#)

Você também pode clicar em **Portal de suporte** para acessar o site Websense Technical Support em uma nova guia ou janela do navegador. Pelo Portal de suporte, você pode usar a Base de conhecimentos para acessar tutoriais, dicas, artigos e documentação.

## Categoria de URL

Para saber como um site está categorizado atualmente:

1. Clique em **Categoria de URL** na Caixa de ferramentas.
2. Insira um URL ou endereço IP.
3. Clique em **Ir**.

A categoria atual do site será exibida em uma janela pop-up. Se sua empresa tiver recategorizado o URL, a nova categoria será exibida.

A categorização do site poderá depender da versão do Master Database que você estiver usando (incluindo atualizações em tempo real).

## Verificar diretiva

Use essa ferramenta para determinar quais diretivas aplicar a um cliente específico. Os resultados são específicos para o dia e a hora atuais.

1. Clique em **Verificar diretiva** na Caixa de ferramentas.
2. Para identificar um diretório ou cliente de computador, insira um dos seguintes:
  - Um nome de usuário totalmente qualificado  
Para procurar ou pesquisar no diretório para identificar o usuário, clique em **Localizar usuário** (consulte [Identificando um usuário para verificar diretiva ou testar filtragem, página 197](#)).
  - Um endereço IP
3. Clique em **Ir**.

O nome de uma ou mais diretivas será exibido em uma janela pop-up. Só serão exibidas várias diretivas quando nenhuma diretiva estiver atribuída ao usuário, mas tiverem sido atribuídas diretivas a vários grupos, domínios ou unidades organizacionais aos quais o usuário pertença.

Mesmo que várias diretivas sejam mostradas, apenas uma diretiva será aplicada a um usuário em qualquer momento específico (consulte [Ordem de filtragem, página 78](#)).

## Testar filtragem

Para saber o que acontece quando um cliente específico solicita um determinado site:

1. Clique em **Testar filtragem** na Caixa de ferramentas.
2. Para identificar um diretório ou cliente de computador, insira um dos seguintes:

- Um nome de usuário totalmente qualificado  
Para procurar ou pesquisar no diretório para identificar o usuário, clique em **Localizar usuário** (consulte *Identificando um usuário para verificar diretiva ou testar filtragem*, página 197).
  - Um endereço IP
3. Insira o URL ou o endereço IP do site que deseja verificar.
  4. Clique em **Ir**.

A categoria do site, a ação aplicada à categoria e o motivo para a ação serão exibidos em uma janela pop-up.

## Acesso ao URL

Para ver se usuários tentaram acessar um site nas últimas 2 semanas, incluindo hoje:

1. Clique em **Acesso ao URL** na Caixa de ferramentas.
2. Insira todo ou parte do URL ou endereço IP do site que deseja verificar.
3. Clique em **Ir**.

Um relatório investigativo mostrará se o site foi acessado e, em caso positivo, quando.

Você pode usar esta ferramenta depois de receber um alerta de segurança para descobrir se a sua empresa foi exposta a phishing ou sites infectados por vírus.

## Investigar usuário

Para rever o histórico de uso da Internet de um cliente para as últimas 2 semanas, excluindo hoje:

1. Clique em **Investigar usuário** na Caixa de ferramentas.
2. Insira todo ou parte do nome do usuário ou endereço IP do computador.
3. Clique em **Ir**.

Um relatório investigativo mostrará o histórico de uso do cliente.

## Identificando um usuário para verificar diretiva ou testar filtragem

Use a página **Localizar usuário** para identificar um cliente de usuário (diretório) para a ferramenta Verificar diretiva ou Testar filtragem.

A página abrirá com a opção **Usuário** selecionada. Expanda a pasta **Entradas de diretório** para procurar no diretório ou clique em **Pesquisar**. O recurso de pesquisa só estará disponível se você estiver usando um serviço de diretório baseado em LDAP.

Para pesquisar no diretório para localizar um usuário:

1. Insira todo ou parte do **Nome** do usuário.
2. Expanda a árvore **Entradas de diretório** e navegue para identificar um contexto de pesquisa.

Você precisará clicar em uma pasta (DC, OU ou CN) na árvore para especificar o contexto. Isso preencherá o campo abaixo da árvore.

3. Clique em **Pesquisar**. As entradas que corresponderem ao seu termo de pesquisa estarão listadas em **Resultados da pesquisa**.
4. Clique em um nome de usuário para selecionar o usuário ou clique em **Pesquisar novamente** para inserir um novo termo ou contexto de pesquisa.  
Para voltar a navegar no diretório, clique em **Cancelar pesquisa**.
5. Quando o nome de usuário totalmente qualificado correto aparecer no campo **Usuário**, clique em **Ir**.

Se você estiver usando a ferramenta Testar filtragem, verifique se o URL ou o endereço IP aparece no campo **URL** antes de clicar em **Ir**.

Para identificar um cliente de computador em vez de um usuário, clique em **Endereço IP**.

# 10

## Identificação do usuário

Para aplicar diretivas a usuários e grupos, o software Websense deve ser capaz de identificar o usuário que está fazendo uma solicitação, considerando o endereço IP originador. Há vários métodos de identificação disponíveis:

- ◆ Um dispositivo ou um aplicativo de integração identifica e autentica usuários e, em seguida, transmite as informações do usuário para o software Websense. Para obter mais informações, consulte o *Guia de Instalação*.
- ◆ Um agente de identificação transparente do Websense é executado em segundo plano para se comunicar com um serviço de diretório e identificar usuários (consulte *Identificação transparente*).
- ◆ O software Websense solicita aos usuários suas credenciais de rede, exigindo que façam logon quando abrirem um navegador da Web (consulte *Autenticação manual*, página 201).

### Identificação transparente

---

Tópicos relacionados:

- ◆ *Autenticação manual*, página 201
- ◆ *Configurando métodos de identificação de usuário*, página 202

Em geral, a **identificação transparente** descreve qualquer método usado pelo software Websense para identificar os usuários em seu serviço de diretório sem solicitar a eles as informações de logon. Isso inclui a integração do software Websense com um dispositivo ou um aplicativo que fornece informações do usuário para uso em filtragem ou o uso de agentes opcionais de identificação transparente do Websense.

- ◆ O Websense *DC Agent*, página 211, é usado com um serviço de diretório baseado no Windows. O agente consulta periodicamente as sessões de logon de usuário nos controladores de domínio e pesquisa as máquinas clientes para verificar o status de logon. Ele é executado em um servidor Windows e pode ser instalado em qualquer domínio da rede.
- ◆ O Websense *Logon Agent*, página 214, identifica os usuários que fazem logon em domínios do Windows. O agente é executado em um servidor Linux ou Windows,

mas seu aplicativo de logon associado é executado apenas em máquinas Windows.

- ◆ O Websense *RADIUS Agent*, página 217, pode ser usado em conjunto com serviços de diretório baseados em Windows ou LDAP. O agente funciona com um servidor e um cliente RADIUS para identificar os usuários que fazem logon de locais remotos.
- ◆ O Websense *eDirectory Agent*, página 222, é usado com o Novell eDirectory. O agente usa a autenticação Novell eDirectory para mapear usuários para endereços IP.

Para obter instruções sobre como instalar cada agente, consulte o *Guia de Instalação*. O agente pode ser usado sozinho ou em determinadas combinações (consulte *Configurando vários agentes*, página 228).



**Obs.:**

Se você estiver usando um appliance NetCache integrado, o NetCache deverá enviar os nomes de usuário ao software Websense no formato WinNT, LDAP ou RADIUS para que a identificação transparente funcione.

Se você tiver um servidor proxy e estiver usando um agente de identificação transparente, é melhor usar a autenticação anônima no servidor proxy.

---

As configurações gerais de identificação do usuário e os agentes específicos de identificação transparente são definidos no Websense Manager. Clique na guia **Configurações** no painel de navegação esquerdo e, em seguida, clique em **Identificação do usuário**.

Consulte *Configurando métodos de identificação de usuário*, página 202, para obter instruções detalhadas de configuração.

Em alguns casos, o software Websense talvez não consiga obter as informações do usuário de um agente de identificação transparente. Isso pode ocorrer quando mais de um usuário está atribuído à mesma máquina ou no caso de um usuário ou convidado anônimo, ou por qualquer outro motivo. Nesses casos, você pode solicitar o logon do usuário através do navegador (consulte *Autenticação manual*, página 201).

## Identificação transparente de usuários remotos

Em determinadas configurações, o software Websense pode identificar transparentemente os usuários conectados à sua rede de locais remotos:

- ◆ Se você tiver implantado o Websense Remote Filtering Server e o Remote Filtering Client, o software Websense poderá identificar qualquer conexão de um usuário remoto em um domínio em cache usando uma conta de domínio. Para obter mais informações, consulte *Filtrar Clientes Remotos*, página 155.
- ◆ Se você tiver implantado o DC Agent e usuários remotos fizerem logon diretamente em domínios do Windows nomeados, o DC Agent poderá identificá-los (consulte *DC Agent*, página 211).

- ◆ Se você estiver usando um servidor RADIUS para autenticar os usuários que fizerem logon de locais remotos, o RADIUS Agent poderá identificar esses usuários transparentemente para que seja possível aplicar diretivas de filtragem com base em usuários ou grupos (consulte *RADIUS Agent*, página 217).

## Autenticação manual

Tópicos relacionados:

- ◆ *Identificação transparente*, página 199
- ◆ *Definindo regras de autenticação para máquinas específicas*, página 204
- ◆ *Autenticação manual segura*, página 207
- ◆ *Configurando métodos de identificação de usuário*, página 202

A identificação transparente nem sempre está disponível ou é desejável em todos os ambientes. Em organizações que não usam identificação transparente ou em situações em que ela não está disponível, ainda será possível filtrar de acordo com diretivas com base em usuários e grupos usando a **autenticação manual**.

A autenticação manual solicita um nome de usuário e uma senha aos usuários no seu primeiro acesso à Internet através de um navegador. O software Websense confirma a senha com um serviço de diretório suportado e, em seguida, recupera as informações de diretiva para esse usuário.

Você pode configurar o software Websense para habilitar a autenticação manual sempre que a identificação transparente não estiver disponível (consulte *Configurando métodos de identificação de usuário*, página 202) ou criar uma lista de máquinas específicas com configurações de autenticação personalizadas solicitadas aos usuários durante o logon ao abrirem um navegador (consulte *Definindo regras de autenticação para máquinas específicas*, página 204).

Quando a autenticação manual estiver habilitada, os usuários poderão receber erros de HTTP e talvez não consigam acessar a Internet se:

- ◆ Fizerem 3 tentativas sem sucesso ao inserir uma senha. Isso ocorre quando o nome de usuário ou a senha é inválida.
- ◆ Clicarem em **Cancelar** para ignorar o prompt de autenticação.

Quando a autenticação manual estiver habilitada, os usuários que não puderem ser identificados serão impedidos de navegar na Internet.

## Configurando métodos de identificação de usuário

---

Tópicos relacionados:

- ◆ [Identificação transparente](#), página 199
- ◆ [Autenticação manual](#), página 201
- ◆ [Trabalhando com usuários e grupos](#), página 60

Use a página **Configurações > Identificação do usuário** para gerenciar quando e como o software Websense tentará identificar usuários na rede para aplicar diretivas com base em usuários e grupos.

- ◆ Configure o Policy Server para se comunicar com agentes de identificação transparente.
- ◆ Examine e atualize as configurações do agente de identificação transparente.
- ◆ Defina uma regra global para determinar como o software Websense responderá quando não for possível identificar os usuários por um agente de identificação transparente ou um dispositivo de integração.
- ◆ Identifique as máquinas na rede às quais as regras globais de identificação de usuário não se aplicam e especifique se e como os usuários dessas máquinas devem ser autenticados.

Se você estiver usando os agentes de identificação transparente do Websense, os agentes estarão listados em **Agentes de identificação transparente**:

- ◆ **Servidor** mostra o endereço IP ou o nome da máquina que hospeda o agente de identificação transparente.
- ◆ **Porta** lista a porta usada pelo software Websense para se comunicar com o agente.
- ◆ **Tipo** indica se a ocorrência especificada é um DC Agent, um Logon Agent, um RADIUS Agent ou um eDirectory Agent. (Consulte [Identificação transparente](#), página 199, para obter uma introdução sobre cada tipo de agente.)

Para adicionar um agente à lista, selecione o tipo de agente na lista suspensa **Adicionar agente**. Clique em um dos links a seguir para obter instruções de configuração:

- ◆ [Configurando o DC Agent](#), página 212
- ◆ [Configurando o Logon Agent](#), página 215
- ◆ [Configurando o RADIUS Agent](#), página 219
- ◆ [Configurando o eDirectory Agent](#), página 224

Para remover uma ocorrência de agente da lista, marque a caixa de seleção ao lado das informações do agente na lista e, em seguida, clique em **Excluir**.

Em **Opções de autenticação adicional**, especifique a resposta padrão do software Websense quando os usuários não forem identificados transparentemente (por um agente ou uma integração):

- ◆ Clique em **Aplicar diretiva do computador ou de rede** para ignorar as diretivas com base em usuários e grupos a favor das diretivas com base no computador e na rede, ou a Diretiva padrão.
- ◆ Clique em **Solicitar informações de logon do usuário** para exigir que os usuários forneçam credenciais de logon ao abrirem um navegador. Em seguida, as diretivas com base em usuários e grupos poderão ser aplicadas (consulte [Autenticação manual](#), página 201).
- ◆ Especifique o domínio padrão **Contexto** a ser usado pelo software Websense sempre que um usuário for solicitado a fornecer as credenciais de logon. Esse é o domínio em que as credenciais dos usuários são válidas.

Se você usar a lista Exceções para especificar todas as máquinas nas quais os usuários serão solicitados a fornecer informações de logon, forneça um contexto de domínio padrão, mesmo que a regra global seja aplicar uma diretiva com base no computador ou na rede.

Após estabelecer a regra geral que determina quando e como os usuários são identificados pelo software Websense, você poderá criar exceções a ela.

Por exemplo, se usar um agente de identificação transparente ou um produto de integração para identificar usuários e tiver habilitado a autenticação manual para solicitar as credenciais aos usuários quando eles não puderem ser identificados transparentemente, você poderá identificar máquinas específicas com base no seguinte:

- ◆ Os usuários que não puderem ser identificados nunca serão solicitados a fornecer suas credenciais. Em outras palavras, quando ocorrer falha da identificação transparente, não será feita tentativa de autenticação manual e a diretiva de computador ou de rede, ou a Diretiva padrão, será aplicada.
- ◆ As informações do usuário são sempre ignoradas, mesmo quando estão disponíveis, e os usuários são sempre solicitados a fornecer suas credenciais.
- ◆ As informações do usuário são sempre ignoradas, mesmo quando estão disponíveis, e os usuários nunca são solicitados a fornecer suas credenciais (a diretiva de computador ou de rede, ou a Diretiva padrão, é sempre aplicada).

Para criar uma exceção, clique em **Exceções** e, em seguida, consulte [Definindo regras de autenticação para máquinas específicas](#), página 204.

Quando terminar de fazer alterações nessa página, clique em **OK** para salvá-las. Para não salvar as alterações, clique em **Cancelar**.

## Definindo regras de autenticação para máquinas específicas

Tópicos relacionados:

- ◆ [Configurando métodos de identificação de usuário](#), página 202
- ◆ [Autenticação manual](#), página 201
- ◆ [Autenticação manual segura](#), página 207

A autenticação seletiva permite que você determine se os usuários que solicitam acesso à Internet de uma máquina cliente específica (identificada pelo endereço IP) são solicitados a fornecer suas credenciais de logon através do navegador. Isso pode ser usado para:

- ◆ Definir regras de autenticação diferentes para um computador em um quiosque público em relação aos funcionários da empresa que fornece o quiosque.
- ◆ Garantir que os usuários de um computador de sala de exame em um consultório médico sempre sejam identificados antes de acessar a Internet.

As máquinas com configurações especiais de identificação de usuário aplicadas são listadas na página **Configurações > Identificação do usuário**. Clique em **Exceções** para estabelecer configurações específicas de identificação de usuário para algumas máquinas da rede ou verifique se foram definidas configurações especiais para uma máquina específica.

Para adicionar uma máquina à lista, clique em **Adicionar** e, em seguida, consulte [Definindo exceções para as configurações de identificação de usuário](#), página 204, para obter instruções adicionais.

Quando terminar de adicionar máquinas ou intervalos de rede à lista, clique em **OK**. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Definindo exceções para as configurações de identificação de usuário

Tópicos relacionados:

- ◆ [Identificação transparente](#), página 199
- ◆ [Autenticação manual](#), página 201
- ◆ [Configurando métodos de identificação de usuário](#), página 202

Use a página **Configurações > Identificação do usuário > Adicionar endereços IP** para identificar as máquinas às quais devem ser aplicadas regras específicas de identificação de usuário.

1. Insira um **Endereço IP** ou um **Intervalo de endereços IP** para identificar as máquinas às quais será aplicado um método de autenticação específico e, em seguida, clique no botão de seta para a direita para adicioná-las à lista **Selecionado**.  
Se for necessário aplicar as mesmas regras a várias máquinas, adicione todas elas à lista.
2. Selecione uma entrada na lista suspensa **Identificação do usuário** para indicar se o software Websense deverá tentar identificar os usuários dessas máquinas de forma transparente.
  - Selecione **Tentar identificar o usuário transparentemente** para solicitar informações do usuário de um agente de identificação transparente ou de um dispositivo de integração.
  - Selecione **Ignorar informações de usuários** para evitar o uso de qualquer método transparente para identificar usuários.
3. Indique se os usuários devem ser solicitados a fornecer credenciais de logon através do navegador. Essa configuração é aplicada quando as informações de usuário não estão disponíveis devido à falha de outra identificação ou porque as informações de usuário foram ignoradas.
  - Selecione **Solicitar informações de logon do usuário** para exigir que os usuários forneçam credenciais de logon.  
Se a opção **Tentar identificar o usuário transparentemente** também estiver selecionada, os usuários só receberão um prompt do navegador se não forem identificados transparentemente.
  - Selecione **Aplicar diretiva do computador ou de rede** para assegurar que os usuários nunca precisem fornecer as credenciais de logon.  
Se a opção **Tentar identificar o usuário transparentemente** também estiver selecionada, os usuários cujas credenciais podem ser verificadas transparentemente são filtradas pela diretiva com base em usuários apropriada.
4. Clique em **OK** para voltar à página Identificação do usuário.
5. Quando terminar de atualizar a lista Exceções, clique em **OK** para armazenar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Revisando exceções para as configurações de identificação de usuário

Tópicos relacionados:

- ◆ [Identificação transparente](#), página 199
- ◆ [Autenticação manual](#), página 201
- ◆ [Configurando métodos de identificação de usuário](#), página 202

Use a página **Configurações > Identificação do usuário > Editar endereços IP** para fazer alterações nas entradas da lista Exceções. As alterações feitas nessa página

afetam todas as máquinas (identificadas pelo endereço IP ou pelo intervalo de endereços IP) exibidas na lista Selecionado.

1. Selecione uma entrada na lista suspensa **Identificação do usuário** para indicar se o software Websense deverá tentar identificar os usuários dessas máquinas de forma transparente.
  - Selecione **Tentar identificar o usuário** para solicitar informações do usuário de um agente de identificação transparente ou de um dispositivo de integração.
  - Selecione **Ignorar informações de usuários** para evitar o uso de qualquer método transparente para identificar usuários.
2. Indique se os usuários devem ser solicitados a fornecer credenciais de logon através do navegador. Essa configuração é aplicada quando as informações de usuário não estão disponíveis devido a uma falha da identificação transparente ou porque essa identificação foi ignorada.
  - Selecione **Solicitar informações de logon do usuário** para exigir que os usuários forneçam credenciais de logon.

Se a opção **Tentar identificar o usuário** também estiver selecionada, os usuários só receberão um prompt do navegador se não forem identificados transparentemente.
  - Selecione **Aplicar diretiva do computador ou de rede** para assegurar que os usuários nunca sejam solicitados a fornecer as credenciais de logon.

Se a opção **Tentar identificar o usuário** também estiver selecionada, os usuários cujas credenciais podem ser verificadas transparentemente são filtrados pela diretiva com base em usuários apropriada.
3. Clique em **OK** para voltar à página Identificação do usuário.
4. Quando terminar de atualizar a lista Exceções, clique em **OK** para armazenar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Autenticação manual segura

Tópicos relacionados:

- ◆ [Configurando métodos de identificação de usuário](#), página 202
- ◆ [Autenticação manual](#), página 201
- ◆ [Definindo regras de autenticação para máquinas específicas](#), página 204
- ◆ [Ativando a autenticação manual segura](#), página 208

A autenticação manual segura do Websense usa a criptografia SSL (Secure Sockets Layer) para proteger os dados de autenticação transmitidos entre as máquinas clientes e o software Websense. Um servidor SSL integrado no Filtering Service fornece criptografia de nomes de usuário e senhas transmitidos entre as máquinas clientes e o Filtering Service. Por padrão, a autenticação manual segura está desabilitada.



**Obs.:**

A autenticação manual segura não pode ser usada com o Remote Filtering. O Remote Filtering Server não pode enviar páginas de bloqueio a clientes se estiver associado a uma ocorrência do Filtering Service que tenha a autenticação manual segura habilitada.

Para habilitar essa funcionalidade, execute as seguintes etapas:

1. Gere certificados e chaves SSL e coloque-os em um local acessível ao software Websense e legível pelo Filtering Service (consulte [Gerando chaves e certificados](#), página 207).
2. Habilite a autenticação manual segura (consulte [Ativando a autenticação manual segura](#), página 208) e a comunicação segura com o serviço de diretório.
3. Importe certificados para o navegador (consulte [Aceitando o certificado no navegador cliente](#), página 209).

## Gerando chaves e certificados

Tópicos relacionados:

- ◆ [Autenticação manual](#), página 201
- ◆ [Definindo regras de autenticação para máquinas específicas](#), página 204
- ◆ [Autenticação manual segura](#), página 207
- ◆ [Ativando a autenticação manual segura](#), página 208
- ◆ [Aceitando o certificado no navegador cliente](#), página 209

Um certificado consiste em uma chave pública, usada para criptografar dados, e uma chave privada, usada para descriptografar dados. Os certificados são emitidos por uma Autoridade de Certificação (AC). Você pode gerar um certificado de um servidor de certificados interno ou obter um certificado cliente de qualquer AC de terceiros, como a VeriSign.

A AC emissora do certificado cliente deve ser de confiança do software Websense. Em geral, isso é determinado por uma configuração do navegador.

- ◆ Para obter respostas para as perguntas comuns sobre chaves privadas, CSRs e certificados, consulte [http://d.apache.org/docs/2.2/ssl/ssl\\_faq.html#aboutcerts](http://d.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts).
- ◆ Para saber mais sobre como gerar sua própria chave privada, CSR e certificado, consulte [www.akadia.com/services/ssh\\_test\\_certificate.html](http://www.akadia.com/services/ssh_test_certificate.html).

Várias ferramentas podem ser usadas para gerar um certificado auto-assinado, incluindo o OpenSSL Toolkit (disponível em [www.openssl.org](http://www.openssl.org)).

Qualquer que seja o método escolhido para gerar o certificado, execute as etapas gerais a seguir.

1. Gere uma chave privada (**server.key**).
2. Gere uma Solicitação de Assinatura de Certificado (CSR) com a chave privada.



#### Importante

Quando for solicitado a inserir o CommonName, digite o endereço IP da máquina do Filtering Server. Se você ignorar essa etapa, os navegadores clientes exibirão um erro de certificado de segurança.

---

3. Use o CSR para criar um certificado auto-assinado (**server.crt**).
4. Salve os arquivos **server.crt** e **server.key** em um local que possa ser acessado pelo software Websense e de onde possam ser lidos pelo Filtering Service.

## Ativando a autenticação manual segura

Tópicos relacionados:

- ◆ [Autenticação manual](#), página 201
- ◆ [Definindo regras de autenticação para máquinas específicas](#), página 204
- ◆ [Autenticação manual segura](#), página 207
- ◆ [Gerando chaves e certificados](#), página 207
- ◆ [Aceitando o certificado no navegador cliente](#), página 209

1. Pare o Websense Filtering Service (consulte [Parando e iniciando os serviços Websense](#), página 283).

2. Navegue até o diretório de instalação do Websense na máquina do Filtering Service (por padrão, **C:\Arquivos de Programas\Websense\bin** ou **/opt/Websense/bin/**).
3. Localize **eimserver.ini** e faça uma cópia de backup do arquivo em outro diretório.
4. Abra o arquivo INI original em um editor de texto.
5. Localize a seção **[WebsenseServer]** e adicione a linha:

```
SSLManualAuth=on
```

6. Abaixo da linha anterior, adicione o seguinte:

```
SSLCertFileLoc=[caminho]
```

Substitua **[caminho]** pelo caminho completo do certificado SSL, incluindo o nome do arquivo de certificado (por exemplo, **C:\secmanauth\server.crt**).

7. Adicione também:

```
SSLCertFileLoc=[caminho]
```

Substitua **[caminho]** pelo caminho completo da chave SSL, incluindo o nome do arquivo de chave (por exemplo, **C:\secmanauth\server.key**).

8. Salve e feche **eimserver.ini**.
9. Inicie o Websense Filtering Service.

Depois de iniciar, o Filtering Service ouvirá as solicitações na porta HTTP segura padrão (**15872**).

As etapas anteriores garantem uma comunicação segura entre a máquina cliente e o software Websense. Para proteger também a comunicação entre o software Websense e o serviço de diretório, verifique se a opção **Usar SSL** está selecionada na página **Configurações > Serviços de diretório**. Consulte [Configurações avançadas de diretório, página 63](#), para obter detalhes.

## Aceitando o certificado no navegador cliente

Tópicos relacionados:

- ◆ [Autenticação manual, página 201](#)
- ◆ [Definindo regras de autenticação para máquinas específicas, página 204](#)
- ◆ [Autenticação manual segura, página 207](#)
- ◆ [Gerando chaves e certificados, página 207](#)
- ◆ [Ativando a autenticação manual segura, página 208](#)

Na primeira vez que você tentar navegar para um site da Web, o navegador exibirá um aviso sobre o certificado de segurança. Para evitar a exibição dessa mensagem no futuro, instale o certificado no armazenamento de certificados.

### Microsoft Internet Explorer (versão 7)

1. Abra o navegador e vá para um site da Web.

Um aviso é exibido, informando que há um problema com o certificado de segurança do site.

2. Clique em **Continuar neste site (não recomendado)**.  
Clique em **Cancelar** se receber um prompt de autenticação.
3. Clique na caixa **Erro do certificado** à direita da barra de endereços (na parte superior da janela do navegador) e, em seguida, clique em **Exibir certificados**.
4. Na guia Geral da caixa de diálogo Certificado, clique em **Instalar certificado**.
5. Selecione **Selecionar automaticamente o armazenamento de certificados conforme o tipo de certificado** e, em seguida, clique em **Avançar**.
6. Clique em **Concluir**.
7. Clique em **Sim** se for exibida uma pergunta para confirmar a instalação do certificado.

Os usuários não receberão mais avisos de segurança de certificado relacionados ao Filtering Service na máquina.

#### Mozilla Firefox (versão 2.x)

1. Abra o navegador e vá para um site da Web.  
Uma mensagem de aviso é exibida.
2. Clique em **Aceitar o certificado permanentemente**.
3. Insira suas credenciais, se for solicitado.
4. Vá para **Ferramentas > Opções** e clique em **Avançado**.
5. Selecione a guia **Criptografia** e, em seguida, clique em **Exibir certificados**.
6. Selecione a guia **Sites** e verifique se o certificado está listado.

Os usuários não receberão mais avisos de segurança de certificado relacionados ao Filtering Service na máquina.

#### Mozilla Firefox (versão 3.x)

1. Abra o navegador e vá para um site da Web.  
Uma mensagem de aviso é exibida.
2. Clique em **Ou você pode adicionar uma exceção**.
3. Clique em **Adicionar exceção**.
4. Verifique se a opção **Armazenar permanentemente esta exceção** está selecionada e clique em **Confirmar exceção de segurança**.

Os usuários não receberão mais avisos de segurança de certificado relacionados ao Filtering Service na máquina.

## DC Agent

Tópicos relacionados:

- ◆ [Identificação transparente](#), página 199
- ◆ [Configurando o DC Agent](#), página 212
- ◆ [Definindo configurações diferentes para uma ocorrência do agente](#), página 230

O Websense DC Agent é executado no Windows e detecta os usuários de uma rede Windows que executam os serviços de rede NetBIOS, WINS ou DNS.

O DC Agent e o User Service reúnem dados do usuário de rede e enviam-nos para o Websense Filtering Service. Várias variáveis determinam a velocidade de transmissão dos dados, incluindo o tamanho da rede e o volume de tráfego de rede existente.

Para habilitar a identificação transparente com o DC Agent:

1. Instale o DC Agent. Para obter mais informações, consulte *Instalando os componentes do Websense separadamente* no *Guia de Instalação*.



**Obs.:**

Execute o DC Agent usando privilégios de administrador de domínio. A conta de administrador de domínio também deve ser membro do grupo Administradores na máquina do DC Agent.

Isso é necessário para que o DC Agent recupere as informações de logon no controlador de domínio. Se não for possível instalar o DC Agent com esses privilégios, configure privilégios de administrador para esses serviços após a instalação. Para obter mais informações, consulte *O software Websense não aplica as diretivas de usuário ou grupo*, página 361.

2. Configure o DC Agent para se comunicar com outros componentes do Websense e com os controladores de domínio de sua rede (consulte *Configurando o DC Agent*).
3. Use o Websense Manager para adicionar usuários e grupos para filtragem (consulte *Adicionando um cliente*, página 66).

O software Websense poderá solicitar a identificação dos usuários se o DC Agent não conseguir identificar os usuários transparentemente. Para obter mais informações, consulte *Autenticação manual*, página 201.

## Configurando o DC Agent

Tópicos relacionados:

- ◆ [Identificação transparente](#)
- ◆ [Autenticação manual](#)
- ◆ [Configurando métodos de identificação de usuário](#)
- ◆ [DC Agent](#)
- ◆ [Configurando vários agentes](#)

Use a página **Configurações > Identificação do usuário > DC Agent** para definir uma nova ocorrência do DC Agent e as configurações globais aplicáveis a todas as ocorrências desse serviço.

Para adicionar uma nova ocorrência do DC Agent, primeiro forneça informações básicas sobre o local de instalação do agente e como o Filtering Service deve ser comunicar com ele. Essas configurações podem ser exclusivas de cada ocorrência do agente.

1. Em Configuração básica do agente, insira o endereço IP ou o nome do **Servidor** no qual o agente está instalado.



**Obs.:**

Os nomes de máquina devem iniciar com um caractere alfabético (a-z), e não com um caractere numérico ou especial.

Os nomes de máquina que contêm determinados caracteres ASCII estendidos talvez não possam ser resolvidos corretamente. Se estiver usando uma versão do software Websense que não esteja em inglês, insira um endereço IP em vez de um nome de máquina.

---

2. Insira a **Porta** a ser usada pelo DC Agent para se comunicar com outros componentes do Websense. O padrão é 30600.
3. Para estabelecer uma conexão autenticada entre o Filtering Service e o DC Agent, marque **Habilitar autenticação** e insira uma **Senha** para a conexão.

Em seguida, personalize as configurações globais de comunicação e solução de problemas, polling do controlador de domínio e polling de computador do DC Agent. Por padrão, as alterações feitas aqui afetam todas as ocorrências do DC Agent. Entretanto, as configurações marcadas com asterisco (\*) podem ser substituídas no arquivo de configuração de um agente para personalizar o comportamento dessa ocorrência de agente (consulte [Definindo configurações diferentes para uma ocorrência do agente](#), página 230).

1. Em Comunicação do DC Agent, insira a **Porta de comunicações** a ser usada para a comunicação entre o DC Agent e outros componentes do Websense. O padrão é 30600.

Não faça alterações na configuração **Porta de diagnóstico**, a menos que receba instruções do Websense Technical Support para isso. O padrão é 30601.

2. Em Polling do controlador de domínio, marque **Habilitar polling do controlador de domínio** para que o DC Agent possa consultar as sessões de logon de usuário nos controladores de domínio.

Você pode especificar quais controladores de domínio serão submetidos a polling por cada ocorrência do DC Agent no arquivo de configuração do agente. Consulte [Configurando vários agentes, página 228](#), para obter detalhes.

3. Use o campo **Intervalo de consulta** para especificar a frequência (em segundos) com que o DC Agent consultará os controladores de domínio.

A diminuição do intervalo de consulta pode resultar em maior exatidão na captura das sessões de logon, mas também aumentar o tráfego geral de rede. O aumento do intervalo de consulta diminui o tráfego de rede, mas também pode atrasar ou impedir a captura de algumas sessões de logon. O padrão é 10 segundos.

4. Use o campo **Tempo limite de entrada do usuário** para especificar a frequência (em horas) com que o DC Agent atualizará as entradas de usuário em seu mapa. O padrão é 24 horas.

5. Em Polling do computador, marque **Habilitar polling do computador** para que o DC Agent possa consultar as sessões de logon de usuário nos computadores. Isso pode incluir os computadores fora dos domínios já consultados pelo agente.

O DC Agent usa WMI (Instrumentação de Gerenciamento do Windows) para o polling do computador. Se você habilitar o polling do computador, configure o Windows Firewall nas máquinas clientes para permitir a comunicação na porta **135**.

6. Insira um **Intervalo de verificação do mapa de usuários** para especificar a frequência com que o DC Agent entrará em contato com as máquinas clientes para verificar quais usuários estão conectados. O padrão é 15 minutos.

O DC Agent compara os resultados da consulta com os pares de nome de usuário/ endereço IP no mapa de usuários que ele enviou para o Filtering Service. A diminuição desse intervalo pode resultar em maior exatidão do mapa de usuários, mas aumentar o tráfego de rede. O aumento do intervalo diminui o tráfego de rede, mas também pode diminuir a exatidão.

7. Insira um período para **Tempo limite de entrada do usuário** para especificar com que frequência o DC Agent atualizará as entradas obtidas através do polling do computador em seu mapa de usuários. O padrão é 1 hora.

O DC Agent remove qualquer entrada de nome de usuário/endereço IP anterior a esse período de tempo limite e que ele não consiga verificar como conectada atualmente. O aumento desse intervalo pode diminuir a exatidão do mapa de

usuários, pois o mapa possivelmente mantém os nomes de usuário antigos por um tempo mais longo.



**Obs.:**

Não defina um intervalo de tempo limite de entrada do usuário menor que o intervalo de verificação do mapa de usuários. Isso poderá causar a remoção dos nomes de usuário do mapa antes de sua verificação.

8. Clique em **OK** para salvar e implementar imediatamente suas alterações.

## Logon Agent

---

Tópicos relacionados:

- ◆ [Identificação transparente, página 199](#)
- ◆ [Configurando o Logon Agent, página 215](#)
- ◆ [Definindo configurações diferentes para uma ocorrência do agente, página 230](#)

O Websense Logon Agent identifica os usuários em tempo real assim que eles fazem logon nos domínios. Isso evita a perda de um logon de usuário devido a um problema de controle de tempo de consulta.

O Logon Agent (também chamado de Authentication Server) pode residir em uma máquina Windows ou Linux. O agente funciona com o Websense Logon Application (LogonApp.exe) em máquinas clientes Windows para identificar os usuários que fazem logon em domínios do Windows.

Na maioria dos casos, basta usar o DC Agent ou o Logon Agent, mas você pode usar os dois agentes juntos. Nesse caso, o Logon Agent terá precedência sobre o DC Agent. O DC Agent somente comunicará uma sessão de logon para o Filtering Service exclusivamente se o Logon Agent tiver perdido essa sessão.

Instale o Logon Agent e, em seguida, implante o Logon Application nas máquinas clientes a partir de um local central. Para obter mais informações, consulte o *Guia de Instalação*.

Após a instalação, configure o agente para se comunicar com as máquinas clientes e com o Websense Filtering Service (consulte [Configurando o Logon Agent](#)).



**Obs.:**

Se estiver usando o Windows Active Directory (Native Mode) e o User Service estiver instalado em uma máquina Linux, consulte [User Service em execução no Linux, página 367](#), para obter as etapas de configuração adicionais.

## Configurando o Logon Agent

Tópicos relacionados:

- ◆ [Identificação transparente](#), página 199
- ◆ [Autenticação manual](#), página 201
- ◆ [Configurando métodos de identificação de usuário](#), página 202
- ◆ [Logon Agent](#), página 214
- ◆ [Configurando vários agentes](#), página 228

Use a página **Configurações > Identificação do usuário > Logon Agent** para definir uma nova ocorrência do Logon Agent e as configurações globais aplicáveis a todas as ocorrências desse serviço.

Para adicionar uma nova ocorrência do Logon Agent:

1. Em Configuração básica do agente, insira o endereço IP ou o nome do **Servidor** no qual o agente está instalado.



**Obs.:**

Os nomes de máquina devem iniciar com um caractere alfabético (a-z), e não com um caractere numérico ou especial.

Os nomes de máquina que contêm determinados caracteres ASCII estendidos talvez não possam ser resolvidos corretamente. Se estiver usando uma versão do software Websense que não esteja em inglês, insira um endereço IP em vez de um nome de máquina.

2. Insira a **Porta** a ser usada pelo Logon Agent para se comunicar com outros componentes do Websense. O padrão é 30602.
3. Para estabelecer uma conexão autenticada entre o Filtering Service e o Logon Agent, marque **Habilitar autenticação** e insira uma **Senha** para a conexão.
4. Clique em **OK** para salvar as alterações ou continue na próxima seção da tela para inserir informações adicionais de configuração.

Em seguida, personalize as configurações globais de comunicação do Logon Agent. Por padrão, as alterações feitas aqui afetam todas as ocorrências do Logon Agent.

1. Em Comunicação do Logon Agent, insira a **Porta de comunicações** a ser usada para a comunicação entre o Logon Agent e outros componentes do Websense. O padrão é 30602.
2. Não faça alterações na configuração **Porta de diagnóstico**, a menos que receba instruções do Websense Technical Support para isso. O padrão é 30603.

3. Em Comunicação do aplicativo de logon, especifique a **Porta de conexão** usada pelo aplicativo de logon para se comunicar com o Logon Agent. O padrão é 15880.
4. Insira o **Número máximo de conexões** permitido por cada ocorrência do Logon Agent. O padrão é 200.  
Se sua rede for grande, talvez seja necessário aumentar esse número. O aumento do número aumenta o tráfego de rede.
5. Clique em **OK** para salvar as alterações ou continue na próxima seção da tela para inserir informações adicionais de configuração.

Para definir as configurações padrão que determinarão como a validade da entrada de usuário será definida, especifique primeiro se o Logon Agent e o aplicativo de logon cliente operarão no **modo persistente** ou no **modo não persistente** (padrão).

O modo não persistente é ativado com a inclusão do parâmetro /NOPERSIST quando **LogonApp.exe** for iniciado. (As informações adicionais estão disponíveis no arquivo **LogonApp\_ReadMe.txt**, incluído na instalação do Logon Agent.)

- ◆ No modo persistente, o aplicativo de logon entra em contato periodicamente com o Logon Agent para comunicar as informações de logon do usuário.  
Se estiver usando o modo persistente, especifique um **Intervalo de consulta** para determinar a frequência com que o aplicativo de logon comunicará as informações de logon.



**Obs.:**

Se você alterar esse valor, a alteração não será implementada até que o período de intervalo anterior tenha transcorrido. Por exemplo, se você alterar o intervalo de 15 para 5 minutos, o intervalo atual de 15 minutos deverá terminar antes que a consulta inicie a cada 5 minutos.

---

- ◆ No modo persistente, o aplicativo de logon envia as informações de logon de usuário para o Logon Agent apenas uma vez para cada logon.  
Se estiver usando o modo não persistente, especifique um período de **Expiração da entrada de usuário**. Quando esse período de tempo de espera for atingido, a entrada de usuário será removida do mapa de usuários.

Quando terminar de fazer alterações de configuração, clique em **OK** para salvar suas configurações.

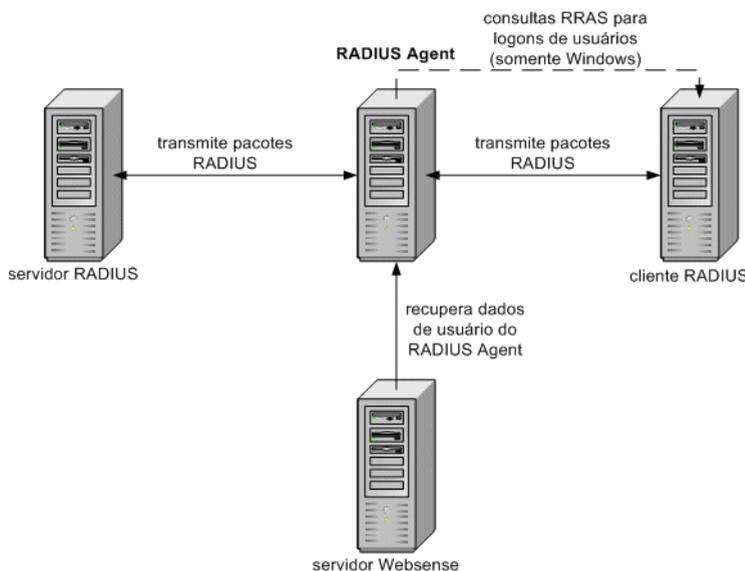
## RADIUS Agent

Tópicos relacionados:

- ◆ [Identificação transparente](#), página 199
- ◆ [Processando o tráfego RADIUS](#), página 218
- ◆ [Configurando o ambiente RADIUS](#), página 218
- ◆ [Configurando o RADIUS Agent](#), página 219
- ◆ [Configurando o cliente RADIUS](#), página 220
- ◆ [Configurando o servidor RADIUS](#), página 221
- ◆ [Definindo configurações diferentes para uma ocorrência do agente](#), página 230

O Websense RADIUS Agent permite que você aplique diretivas com base em usuários e grupos usando a autenticação fornecida por um servidor RADIUS. O RADIUS Agent permite a identificação transparente dos usuários que acessam sua rede usando uma conexão dial-up, VPN (Rede Virtual Privada), DSL (Linha de Assinatura Digital) ou outra conexão remota (dependendo de sua configuração).

O RADIUS Agent funciona junto com o servidor RADIUS e o cliente RADIUS na rede para processar e monitorar o tráfego do protocolo RADIUS (Remote Access Dial-In User Service). Isso permite que você atribua diretivas de filtragem específicas a usuários ou grupos que acessam sua rede remotamente, bem como a usuários locais.



Quando você instala o RADIUS Agent, o Agent é integrado aos componentes existentes do Websense. Entretanto, o RADIUS Agent, seu servidor RADIUS e seu cliente RADIUS devem ser configurados corretamente (consulte [Configurando o RADIUS Agent](#), página 219).

## Processando o tráfego RADIUS

O Websense RADIUS Agent atua como proxy, encaminhando mensagens RADIUS entre um cliente RADIUS e um servidor RADIUS (ou vários clientes e servidores).

O RADIUS Agent não autentica os usuários diretamente. Em vez disso, o agente identifica os usuários remotos e associa-os a endereços IP, de modo que um servidor RADIUS possa autenticá-los. O ideal seria o servidor RADIUS transmitir as solicitações de autenticação para um serviço de diretório baseado em LDAP.

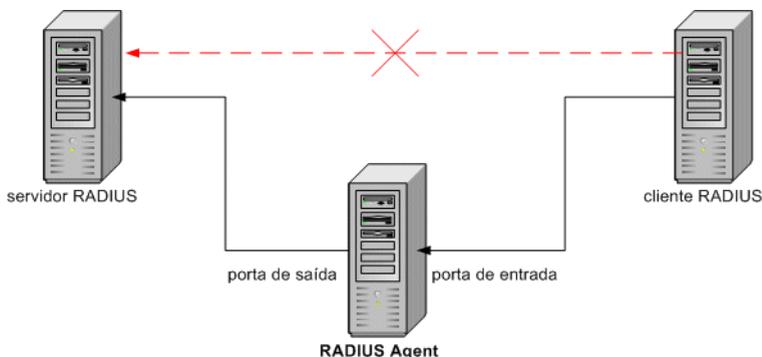
O RADIUS Agent armazena os pares de nome de usuário/endereço IP em um mapa de usuários. Se o seu cliente RADIUS oferecer suporte a contabilidade (ou monitoramento de logon de usuário) e a contabilidade estiver habilitada, o RADIUS Agent coletará mais detalhes sobre as sessões de logon de usuário das mensagens RADIUS que receber.

Quando configurado corretamente, o Websense RADIUS Agent captura e processa todos os pacotes de protocolo RADIUS destes tipos:

- ◆ **Access-Request:** enviado por um cliente RADIUS para solicitar autorização para uma tentativa de conexão de acesso à rede.
- ◆ **Access-Accept:** enviado por um servidor RADIUS em resposta a uma mensagem Access-Request; informa ao cliente RADIUS que a tentativa de conexão foi autorizada e autenticada.
- ◆ **Access-Reject:** enviado por um servidor RADIUS em resposta a uma mensagem Access-Request; informa ao cliente RADIUS que a tentativa de conexão foi rejeitada.
- ◆ **Accounting-Stop-Request:** enviado por um cliente RADIUS para informar ao servidor RADIUS que deve parar o monitoramento da atividade do usuário.

## Configurando o ambiente RADIUS

O Websense RADIUS Agent atua como proxy entre um cliente RADIUS e um servidor RADIUS. Este diagrama mostra uma exibição simplificada de como o uso do RADIUS Agent difere de uma configuração RADIUS padrão.



O RADIUS Agent e o servidor RADIUS devem ser instalados em máquinas separadas. O agente e o servidor não podem ter o mesmo endereço IP e devem usar portas diferentes.

Após instalar o RADIUS Agent, configure-o no Websense Manager (consulte [Configurando o RADIUS Agent](#), página 219). Você também deve:

- ◆ Configurar o cliente RADIUS (em geral, um Servidor de Acesso à Rede [NAS]) para se comunicar com o RADIUS Agent, e não diretamente com seu servidor RADIUS.
- ◆ Configurar o servidor RADIUS para usar o RADIUS Agent como proxy (consulte a documentação do servidor RADIUS). Se tiver vários servidores RADIUS, configure cada um deles separadamente.

**Obs.:**

Se você usar o Lucent RADIUS Server e o RRAS, configure o servidor RADIUS para usar o protocolo PAP (Password Authentication Protocol) e o servidor RRAS para aceitar apenas as solicitações PAP. Para obter mais informações, consulte a documentação do produto.

## Configurando o RADIUS Agent

Tópicos relacionados:

- ◆ [Identificação transparente](#), página 199
- ◆ [Autenticação manual](#), página 201
- ◆ [Configurando métodos de identificação de usuário](#), página 202
- ◆ [RADIUS Agent](#), página 217
- ◆ [Configurando vários agentes](#), página 228

Use a página **Configurações > Identificação do usuário > RADIUS Agent** para definir uma nova ocorrência do RADIUS Agent e as configurações globais aplicáveis a todas as ocorrências desse serviço.

Para adicionar uma nova ocorrência do RADIUS Agent:

1. Em Configuração básica do agente, insira o endereço IP ou o nome do **Servidor** no qual o agente está instalado.

**Obs.:**

Os nomes de máquina devem iniciar com um caractere alfabético (a-z), e não com um caractere numérico ou especial.

Os nomes de máquina que contêm determinados caracteres ASCII estendidos talvez não possam ser resolvidos corretamente. Se estiver usando uma versão do software Websense que não esteja em inglês, insira um endereço IP em vez de um nome de máquina.

2. Insira a **Porta** a ser usada pelo RADIUS Agent para se comunicar com outros componentes do Websense. O padrão é 30800.
3. Para estabelecer uma conexão autenticada entre o Filtering Service e o RADIUS Agent, marque **Habilitar autenticação** e insira uma **Senha** para a conexão.
4. Clique em **OK** para salvar as alterações ou continue na próxima seção da tela para inserir informações adicionais de configuração.

Em seguida, personalize as configurações globais do RADIUS Agent. Por padrão, as alterações feitas aqui afetam todas as ocorrências do RADIUS Agent. Entretanto, as configurações marcadas com asterisco (\*) podem ser substituídas no arquivo de configuração de um agente para personalizar o comportamento dessa ocorrência de agente (consulte [Definindo configurações diferentes para uma ocorrência do agente](#), página 230).

1. Insira a **Porta de comunicações** usada para a comunicação entre o RADIUS Agent e outros componentes do Websense. O padrão é 30800.
2. Não faça alterações na configuração **Porta de diagnóstico**, a menos que receba instruções do Websense Technical Support para isso. O padrão é 30801.
3. Em Servidor RADIUS, digite o **IP ou o nome do servidor RADIUS**. O RADIUS Agent encaminha as solicitações de autenticação para o servidor RADIUS e deve saber a identidade dessa máquina.
4. Se o Microsoft RRAS estiver sendo usado, digite o endereço IP da **máquina do RRAS**. O software Websense consulta as sessões de logon de usuário nessa máquina.
5. Insira o intervalo de **Tempo limite de entrada do usuário**, usado para determinar a frequência com que o RADIUS Agent atualiza o mapa de usuários. Em geral, é recomendável usar o valor de consulta padrão (24 horas).
6. Use as configurações **Portas de autenticação** e **Portas de contabilidade** para especificar as portas usadas pelo RADIUS Agent para enviar e receber solicitações de autenticação e de contabilidade. Para cada tipo de comunicação, é possível especificar a porta usada para a comunicação entre:
  - O RADIUS Agent e o servidor RADIUS
  - O RADIUS Agent e o cliente RADIUS
7. Quando terminar, clique em **OK** para salvar imediatamente suas configurações.

## Configurando o cliente RADIUS

Seu cliente RADIUS deve ser configurado para transmitir as solicitações de autenticação e de contabilidade para o servidor RADIUS através do RADIUS Agent.

Modifique a configuração do cliente RADIUS de modo que:

- ◆ O cliente RADIUS envie as solicitações de autenticação para a máquina e a porta usadas pelo RADIUS Agent para ouvir as solicitações de autenticação. Essa é a **Porta de autenticação** especificada durante a configuração do RADIUS Agent.

- ◆ O cliente RADIUS envie as solicitações de contabilidade para a máquina e a porta usadas pelo RADIUS Agent para ouvir as solicitações de contabilidade. Essa é a **Porta de contabilidade** especificada durante a configuração do RADIUS Agent.

O procedimento exato de configuração de um cliente RADIUS difere conforme o tipo de cliente. Para obter detalhes, consulte a documentação do cliente RADIUS.

**Obs.:**

O cliente RADIUS deve incluir os atributos **User-Name** e **Framed-IP-Address** nas mensagens de autenticação e de contabilidade enviadas. O RADIUS Agent usa os valores desses atributos para interpretar e armazenar os pares de nome/endereço IP. Se, por padrão, o seu cliente RADIUS não gerar essas informações, configure-o para isso (consulte a documentação do cliente RADIUS).

## Configurando o servidor RADIUS

Para permitir a comunicação adequada entre o Websense RADIUS Agent e o seu servidor RADIUS:

- ◆ Adicione o endereço IP da máquina do RADIUS Agent à lista de clientes do servidor RADIUS. Para obter instruções, consulte a documentação do servidor RADIUS.
- ◆ Defina segredos compartilhados entre o servidor RADIUS e todos os clientes RADIUS que usam o agente para se comunicar com esse servidor. Os segredos compartilhados são geralmente especificados como opções de segurança de autenticação.

A configuração de um segredo compartilhado para os clientes RADIUS e o servidor RADIUS permite uma transmissão segura das mensagens RADIUS. Em geral, o segredo compartilhado é uma string de texto comum. Para obter instruções, consulte a documentação do servidor RADIUS.

**Obs.:**

O servidor RADIUS deve incluir os atributos **User-Name** e **Framed-IP-Address** nas mensagens de autenticação e de contabilidade. O RADIUS Agent usa os valores desses atributos para interpretar e armazenar os pares de nome/endereço IP. Se, por padrão, o seu servidor RADIUS não gerar essas informações, configure-o para isso (consulte a documentação do servidor RADIUS).

## eDirectory Agent

---

Tópicos relacionados:

- ◆ [Identificação transparente](#), página 199
- ◆ [Configurando o eDirectory Agent](#), página 224
- ◆ [Definindo configurações diferentes para uma ocorrência do agente](#), página 230

O Websense eDirectory Agent funciona com o Novell eDirectory para identificar os usuários transparentemente, de modo que o software Websense possa filtrá-los de acordo com as diretivas atribuídas a usuários, grupos, domínios ou unidades organizacionais.

O eDirectory Agent reúne as informações de sessão de logon do usuário do Novell eDirectory, que autentica os usuários que fazem logon na rede. Em seguida, o agente associa cada usuário autenticado a um endereço IP e registra os pares de nome de usuário e endereço IP em um mapa de usuários local. Depois disso, o eDirectory Agent comunica essas informações ao Filtering Service.

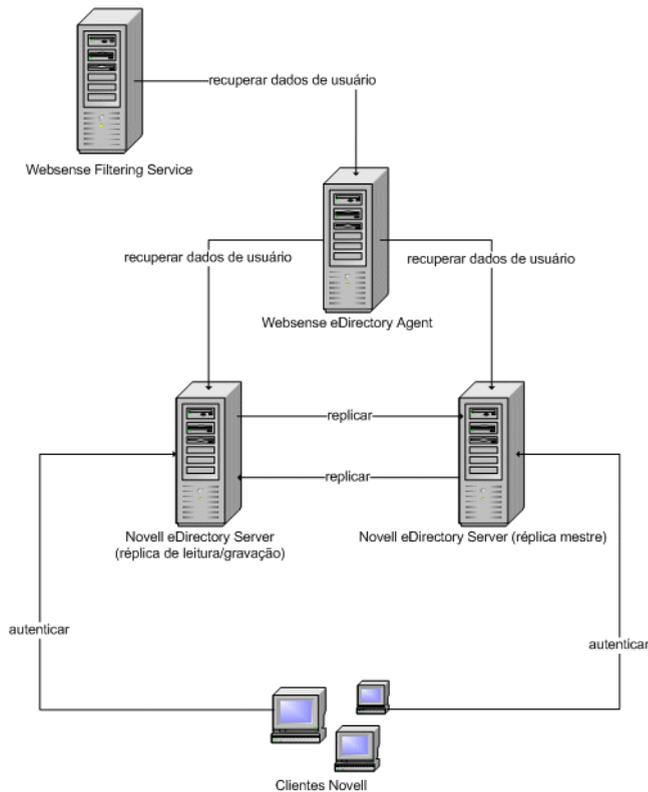


**Obs.:**

Em um cliente Novell que executa o Windows, vários usuários podem fazer logon em um único servidor Novell eDirectory. Isso associa um endereço IP a vários usuários. Neste cenário, o mapa de usuários do eDirectory mantém apenas o par de nome de usuário/endereço IP do último usuário conectado de um endereço IP específico.

---

Uma ocorrência do Websense eDirectory Agent pode aceitar um mestre do Novell eDirectory, mais qualquer número de réplicas do Novell eDirectory.



## Considerações especiais de configuração

- ◆ Se você tiver integrado o Cisco Content Engine v5.3.1.5 ou superior ao software Websense:
  - Execute os seguintes serviços Websense na mesma máquina do Cisco Content Engine:
    - Websense eDirectory Agent
    - Websense User Service
    - Websense Filtering Service
    - Websense Policy Server
  - Certifique-se de que todas as réplicas do Novell eDirectory sejam adicionadas ao arquivo **wsedir.ini** na mesma máquina.
  - Exclua o arquivo **eDirAgent.bak**.

Execute os serviços das Websense Reporting Tools em uma máquina **separada** do Cisco Content Engine e do software Websense.

- ◆ O software Websense aceita o uso de NMAS com o eDirectory Agent. Para usar o eDirectory Agent com o NMAS habilitado, é necessário instalar o eDirectory Agent em uma máquina que também esteja executando o Novell Client.

## Configurando o eDirectory Agent

Tópicos relacionados:

- ◆ [Identificação transparente](#), página 199
- ◆ [Autenticação manual](#), página 201
- ◆ [Configurando métodos de identificação de usuário](#), página 202
- ◆ [eDirectory Agent](#), página 222
- ◆ [Configurando o eDirectory Agent para usar LDAP](#), página 226
- ◆ [Configurando vários agentes](#), página 228

Use a página **Configurações > Identificação do usuário > eDirectory Agent** para definir uma nova ocorrência do eDirectory Agent e as configurações globais aplicáveis a todas as ocorrências desse serviço.

Para adicionar uma nova ocorrência do eDirectory Agent:

1. Em Configuração básica do agente, insira o endereço IP ou o nome do **Servidor** no qual o agente está instalado.



**Obs.:**

Os nomes de máquina devem iniciar com um caractere alfabético (a-z), e não com um caractere numérico ou especial.

Os nomes de máquina que contêm determinados caracteres ASCII estendidos talvez não possam ser resolvidos corretamente. Se estiver usando uma versão do software Websense que não esteja em inglês, insira um endereço IP em vez de um nome de máquina.

2. Insira a **Porta** a ser usada pelo eDirectory Agent para se comunicar com outros componentes do Websense. O padrão é 30700.
3. Para estabelecer uma conexão autenticada entre o Filtering Service e o eDirectory Agent, marque **Habilitar autenticação** e insira uma **Senha** para a conexão.
4. Clique em **OK** para salvar as alterações ou continue na próxima seção da tela para inserir informações adicionais de configuração.

Em seguida, personalize as configurações de comunicação do eDirectory Agent. Por padrão, as alterações feitas aqui afetam todas as ocorrências do eDirectory Agent. Entretanto, as configurações marcadas com asterisco (\*) podem ser substituídas no arquivo de configuração de um agente para personalizar o comportamento dessa ocorrência de agente (consulte [Definindo configurações diferentes para uma ocorrência do agente](#), página 230).

1. Insira a **Porta de comunicações** usada para a comunicação entre o eDirectory Agent e outros componentes do Websense. O padrão é 30700.

2. Não faça alterações na configuração **Porta de diagnóstico**, a menos que receba instruções do Websense Technical Support para isso. O padrão é 30701.
3. Em Servidor eDirectory, especifique uma **Base de pesquisa** (contexto raiz) a ser usada pelo eDirectory Agent como ponto inicial ao procurar informações de usuário no diretório.
4. Forneça as informações de conta de usuário administrativa a serem usadas pelo eDirectory Agent para se comunicar com o diretório:
  - a. Insira o **Nome distinto do administrador** para uma conta de usuário administrativa do Novell eDirectory.
  - b. Insira a **Senha** usada por essa conta.
  - c. Especifique um intervalo de **Tempo limite de entrada do usuário** para indicar quanto tempo as entradas permanecerão no mapa de usuários do agente.

Esse intervalo deve ser aproximadamente 30% maior que uma sessão típica de logon de usuário. Isso ajudará a evitar a remoção das entradas de usuário do mapa antes de os usuários terminarem a pesquisa.

Em geral, é recomendável usar o valor padrão (24 horas).

**Obs.:**

Em alguns ambientes, em vez de usar o intervalo de Tempo limite de entrada do usuário para determinar com que frequência o eDirectory Agent deve atualizar seu mapa de usuários, pode ser apropriado consultar o Servidor eDirectory em intervalos regulares para obter as atualizações de logon de usuário. Consulte [Habilitando consultas completas do Servidor eDirectory](#), página 226.

5. Adicione o mestre do Servidor eDirectory, assim como qualquer réplica, à lista **Réplicas eDirectory**. Para adicionar um mestre ou uma réplica do Servidor eDirectory à lista, clique em **Adicionar** e siga as instruções em [Adicionando uma réplica do servidor eDirectory](#), página 225.

Quando terminar de fazer alterações de configuração, clique em **OK** para salvar suas configurações.

## Adicionando uma réplica do servidor eDirectory

Uma ocorrência do Websense eDirectory Agent pode aceitar um mestre do Novell eDirectory, mais qualquer número de réplicas do Novell eDirectory executadas em máquinas separadas.

O eDirectory Agent deve ser capaz de se comunicar com cada máquina que executa uma réplica do serviço de diretório. Isso garante que o agente obtenha as informações de logon mais recentes e o mais rápido possível sem precisar aguardar a replicação do eDirectory.

O Novell eDirectory replica o atributo que identifica com exclusividade os usuários conectados apenas a cada 5 minutos. Apesar desse atraso no tempo de replicação, o

eDirectory Agent detecta as novas sessões de logon assim que um usuário faz logon em qualquer réplica do eDirectory.

Para configurar a instalação do eDirectory Agent para se comunicar com o eDirectory:

1. Na tela Adicionar réplica do eDirectory, insira o endereço IP ou o nome do **Servidor** eDirectory (mestre ou réplica).
2. Insira a **Porta** usada pelo eDirectory Agent para se comunicar com a outra máquina do eDirectory.
3. Clique em **OK** para voltar à página eDirectory. A nova entrada é exibida na lista Réplicas eDirectory.
4. Repita o processo para qualquer máquina adicional do servidor eDirectory.
5. Clique em **OK** para armazenar as alterações em cache e, em seguida, clique em **Salvar tudo**.
6. Interrompa e inicie o eDirectory Agent para que o agente possa iniciar a comunicação com a nova réplica. Consulte [Parando e iniciando os serviços Websense, página 283](#), para obter instruções.

## Configurando o eDirectory Agent para usar LDAP

O Websense eDirectory Agent pode usar o protocolo NCP (Netware Core Protocol) ou LDAP (Lightweight Directory Access Protocol) para obter informações de logon de usuário do Novell eDirectory. Por padrão, o eDirectory Agent no Windows usa NCP. No Linux, o eDirectory Agent deve usar LDAP.

Se estiver executando o eDirectory Agent no Windows, mas quiser que o agente use LDAP para consultar o Novell eDirectory, defina o agente para usar LDAP em vez de NCP. Em geral, o NCP fornece um mecanismo de consulta mais eficiente.

Para definir o eDirectory Agent no Windows para usar LDAP:

1. Verifique se tem pelo menos uma réplica do Novell eDirectory com todos os objetos de diretório para monitorar e filtrar em sua rede.
2. Interrompa o serviço Websense eDirectory Agent (consulte [Parando e iniciando os serviços Websense, página 283](#)).
3. Navegue até o diretório de instalação do eDirectory Agent (por padrão, **\Arquivos de programas\Websense\bin**) e abra o arquivo **wsedir.ini** em um editor de texto.
4. Modifique a entrada **QueryMethod** da seguinte forma:  

```
QueryMethod=0
```

Isso definirá o Agent a usar LDAP para consultar o Novell eDirectory. (O valor padrão é 1, para NCP.)
5. Salve e feche o arquivo.
6. Reinicie o serviço Websense eDirectory Agent.

## Habilitando consultas completas do Servidor eDirectory

Em redes pequenas, é possível configurar o Websense eDirectory Agent para consultar todos os usuários conectados em intervalos regulares no Servidor

eDirectory. Isso permite que o agente detecte os usuários recém-conectados e os que se desconectaram desde a última consulta, e atualize seu mapa de usuários local de acordo.



### Importante

Em redes grandes, não é recomendado configurar o eDirectory Agent para usar consultas completas, pois a duração necessária para retornar os resultados de consulta depende do número de usuários conectados. Quanto mais usuários conectados, maior será o impacto no desempenho.

Quando você habilita consultas completas para o eDirectory Agent, o intervalo de **Tempo limite de entrada do usuário** não é usado, pois os usuários desconectados são identificados pela consulta. Por padrão, a consulta é realizada a cada 30 segundos.

Quando esse recurso é habilitado, o tempo de processamento do eDirectory Agent aumenta da seguinte forma:

- ◆ Aumenta o tempo necessário para recuperar os nomes dos usuários conectados cada vez que uma consulta é realizada
- ◆ Aumenta o tempo necessário para processar as informações de nome de usuário, remover entradas obsoletas do mapa de usuários local e adicionar novas entradas com base na consulta mais recente

O eDirectory Agent examina todo o mapa de usuários local após cada consulta, em vez de identificar apenas os novos logons. O tempo necessário para esse processo depende do número de usuários retornados por cada consulta. Portanto, o processo de consulta pode afetar os tempos de resposta do eDirectory Agent e do Servidor Novell eDirectory.

Para habilitar consultas completas:

1. Na máquina do eDirectory Agent, navegue até o diretório **bin** do Websense (por padrão, \Arquivos de programas\Websense\bin ou /opt/websense/bin).
2. Localize o arquivo **wsedir.ini** e faça uma cópia de backup em outro diretório.
3. Abra **wsedir.ini** em um editor de texto (como Bloco de notas ou vi).
4. Vá para a seção **[eDirAgent]** do arquivo e localize esta entrada:

```
QueryMethod=<N>
```

Anote o valor de QueryMethod caso queira retornar posteriormente à configuração padrão.

5. Atualize o valor de **QueryMethod** da seguinte forma:
  - Se o valor padrão for 0 (comunicar-se com o diretório via LDAP), altere o valor para **2**.

- Se o valor atual for 1 (comunicar-se com o diretório via NCP), altere o valor para 3.



**Obs.:**

Se depois de alterar esse valor de consulta o desempenho do sistema diminuir, retorne a entrada QueryMethod ao valor anterior.

---

6. Se o intervalo de consulta padrão (30 segundos) não for apropriado ao seu ambiente, edite o valor de **PollInterval** de forma adequada.  
Observe que o intervalo é definido em **milissegundos**.
7. Salve e feche o arquivo.
8. Reinicie o serviço Websense eDirectory Agent (consulte *Parando e iniciando os serviços Websense*, página 283).

## Configurando vários agentes

---

Tópicos relacionados:

- ◆ [DC Agent](#), página 211
- ◆ [Logon Agent](#), página 214
- ◆ [RADIUS Agent](#), página 217
- ◆ [eDirectory Agent](#), página 222

É possível combinar vários agentes de identificação transparente na mesma rede. Se a sua configuração de rede exigir vários agentes, é melhor instalar cada um deles em uma máquina separada. Entretanto, em alguns casos, você pode configurar o software Websense para trabalhar com vários agentes em uma única máquina.

As combinações de agente de identificação transparente a seguir são aceitas:

Combinação	Mesma máquina?	Mesma rede?	Configuração necessária
Vários DC Agents	Não	Sim	Certifique-se de que todas as ocorrências do DC Agent possam se comunicar com o Filtering Service.
Vários RADIUS Agents	Não	Sim	Configure cada ocorrência para se comunicar com o Filtering Service.
Vários eDirectory Agents	Não	Sim	Configure cada ocorrência para se comunicar com o Filtering Service.

Combinação	Mesma máquina?	Mesma rede?	Configuração necessária
Vários Logon Agents	Não	Sim	Configure cada ocorrência para se comunicar com o Filtering Service.
DC Agent + RADIUS Agent	Sim	Sim	Instale esses agentes em diretórios separados. Configure cada agente para se comunicar com o Filtering Service usando uma porta de comunicação diferente.
DC Agent + eDirectory Agent	Não	Não	O software Websense não oferece suporte à comunicação com os serviços de diretório do Windows e da Novell na mesma implantação. Entretanto, você pode ter os dois agentes instalados, com apenas um deles ativo.
DC Agent + Logon Agent	Sim	Sim	Configure os dois agentes para se comunicar com o Filtering Service. Por padrão, cada agente usa uma porta exclusiva, o que não causa conflitos de porta, a menos que essas portas sejam alteradas.
eDirectory Agent + Logon Agent	Não	Não	O software Websense não oferece suporte à comunicação com os serviços de diretório do Windows e da Novell na mesma implantação. Entretanto, você pode ter os dois agentes instalados, com apenas um deles ativo.
RADIUS Agent + eDirectory Agent	Sim	Sim	Configure cada agente para se comunicar com o Filtering Service usando uma porta de comunicação diferente.
DC Agent + Logon Agent + RADIUS Agent	Sim	Sim	Embora esta combinação raramente seja necessária, ela é aceita.  Instale cada agente em um diretório separado. Configure todos os agentes para se comunicar com o Filtering Service usando portas de comunicação diferentes.

## Definindo configurações diferentes para uma ocorrência do agente

As definições de configuração do agente de identificação transparente do Websense Manager são globais e aplicam-se a todas as ocorrências do agente instalado. Entretanto, se tiver várias ocorrências de qualquer agente, você poderá configurar uma ocorrência independentemente das outras.

As configurações exclusivas especificadas para uma ocorrência de agente específica substituem as configurações globais na caixa de diálogo Configurações. As configurações que podem ser substituídas são marcadas com asterisco (\*).

1. Interrompa o serviço do agente de identificação transparente (consulte [Parando e iniciando os serviços Websense](#), página 283).
2. Na máquina que executa a ocorrência do agente, navegue até o diretório de instalação do agente e abra o arquivo apropriado em um editor de texto:
  - para o DC Agent: **transid.ini**
  - para o Logon Agent: **authserver.ini**
  - para o eDirectory Agent: **wsedir.ini**
  - para o RADIUS Agent: **wsradius.ini**
3. Localize o parâmetro a ser alterado para essa ocorrência de agente (consulte [Parâmetros do arquivo INI](#), página 231).

Por exemplo, você pode habilitar uma conexão autenticada entre essa ocorrência de agente e outros serviços Websense. Para isso, insira um valor para o parâmetro **password** no arquivo INI:

```
password=[xxxxxx]
```

4. Modifique qualquer outro valor desejado.
5. Salve e feche o arquivo INI.
6. Se fizer uma alteração nas configurações do **DC Agent**, você deverá remover dois arquivos do diretório **bin** do Websense (C:\Arquivos de programas\Websense\bin, por padrão):
  - a. Interrompa todos os serviços Websense na máquina do DC Agent (consulte [Parando e iniciando os serviços Websense](#), página 283).
  - b. Exclua estes arquivos:

```
Journal.dat
XidDcAgent.bak
```

Esses arquivos serão recriados quando você iniciar o serviço Websense DC Agent.
  - c. Reinicie os serviços Websense (incluindo o DC Agent) e pule para a **etapa 8**.
7. Reinicie o serviço do agente de identificação transparente.
8. Atualize as configurações do agente no Websense Manager:
  - a. Vá para **Configurações** > Identificação do usuário.

- b. Em **Agentes de identificação transparente**, selecione o agente e clique em **Editar**.

**Obs.:**

Se tiver modificado o valor de **porta** para essa ocorrência de agente, remova o agente e adicione-o novamente.

Primeiro, selecione a entrada de agente existente e clique em **Excluir**. Em seguida, clique em **Adicionar agente**.

- c. Verifique o **IP ou nome do servidor** e a **Porta** usados por essa ocorrência do agente. Se tiver especificado um número de porta exclusivo no arquivo INI, certifique-se de que sua entrada corresponda a esse valor.
- d. Se tiver especificado uma senha de autenticação exclusiva no arquivo INI, verifique se a entrada **Senha** mostrada aqui está correta.
- e. Clique em **OK** para armazenar suas alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Parâmetros do arquivo INI

Rótulo do campo do Websense Manager	Nome do parâmetro de .ini	Descrição
Porta de comunicações ( <i>todos os agentes</i> )	port	A porta usada pelo agente para se comunicar com outros serviços Websense.
Porta de diagnóstico ( <i>todos os agentes</i> )	DiagServerPort	A porta usada pela ferramenta de solução de problemas do agente para ouvir dados do agente.
Senha ( <i>todos os agentes</i> )	password	A senha usada pelo agente para autenticar as conexões com outros serviços Websense. Especifique uma senha para habilitar a autenticação.
Intervalo de consulta ( <i>DC Agent</i> )	QueryInterval	O intervalo durante o qual o DC Agent consulta os controladores de domínio.
IP ou nome do servidor Porta ( <i>eDirectory Agent</i> )	Server=IP:port	O endereço IP e o número de porta da máquina que executa o eDirectory Agent.
Base de pesquisa ( <i>eDirectory Agent</i> )	SearchBase	O contexto raiz do servidor Novell eDirectory.
Nome distinto do administrador ( <i>eDirectory Agent</i> )	DN	O nome do usuário administrativo do servidor Novell eDirectory.
Senha ( <i>eDirectory Agent</i> )	PW	A senha do usuário administrativo do servidor Novell eDirectory.
IP ou nome do servidor RADIUS	RADIUSHost	O endereço IP ou o nome da máquina do servidor RADIUS.

IP da máquina RRAS (somente Windows) ( <i>RADIUS Agent</i> )	RRASHost	O endereço IP da máquina que executa o RRAS. O Websense consulta as sessões de logon de usuário nessa máquina.
Portas de autenticação: Entre o RADIUS Agent e o servidor RADIUS	AuthOutPort	A porta usada pelo servidor RADIUS para ouvir as solicitações de autenticação.
Portas de autenticação: Entre clientes RADIUS e o RADIUS Agent	AuthInPort	A porta pela qual o RADIUS Agent aceita as solicitações de autenticação.
Portas de contabilidade: Entre o RADIUS Agent e o servidor RADIUS	AccOutPort	A porta usada pelo servidor RADIUS para ouvir as mensagens de contabilidade RADIUS.
Portas de contabilidade: Entre clientes RADIUS e o RADIUS Agent	AccInPort	A porta pela qual o RADIUS Agent aceita as solicitações de contabilidade.

## Configurando um agente para ignorar determinados nomes de usuário

Você pode configurar um agente de identificação transparente para ignorar os nomes de logon não associados a usuários reais. Esse recurso geralmente é usado para lidar com a maneira como alguns serviços do Windows 200x e do Windows XP entram em contato com os controladores de domínio da rede.

Por exemplo, o usuário **user1** faz logon na rede e é identificado pelo controlador de domínio como **computerA/user1**. Esse usuário é filtrado por uma diretiva do Websense atribuída a **user1**. Se um serviço for iniciado na máquina do usuário que assume a identidade **computerA/ServiceName** para entrar em contato com o controlador de domínio, isso poderá causar problemas de filtragem. O software Websense trata **computerA/ServiceName** como um novo usuário sem diretiva atribuída e filtra-o pela diretiva do computador ou pela diretiva **Padrão**.

Para solucionar esse problema:

1. Interrompa o serviço do agente (consulte [Parando e iniciando os serviços Websense](#), página 283).
2. Navegue até o diretório `\Websense\bin\` e abra o arquivo **ignore.txt** em um editor de texto.
3. Digite cada nome de usuário em uma linha separada. Não inclua curingas, como `“*”`.

```
maran01
WindowsServiceName
```

O software Websense ignora esses nomes de usuário, independentemente da máquina à qual estejam associados.

Para solicitar que o software Websense ignore um nome de usuário em um domínio específico, use o formato **nomedeusuário, domínio**.

`asilva, engenharia1`

4. Quando terminar, salve e feche o arquivo.
5. Reinicie o serviço de agente.

O agente ignorará os nomes de usuário especificados, e o software Websense não considerará esses nomes na filtragem.



# 11

## Administração delegada

Tópicos relacionados:

- ◆ [Introdução às funções administrativas](#), página 236
- ◆ [Introdução aos administradores](#), página 236
- ◆ [Introdução às funções administrativas](#), página 241
- ◆ [Habilitando o acesso ao Websense Manager](#), página 248
- ◆ [Usando a administração delegada](#), página 252
- ◆ [Vários administradores acessando o Websense Manager](#), página 263
- ◆ [Definindo restrições de filtragem para todas as funções](#), página 264

A administração delegada fornece métodos poderosos e flexíveis para gerenciar os relatórios e a filtragem da Internet para determinados grupos de clientes. É uma forma eficiente de distribuir a responsabilidade por geração de relatórios e gerenciamento de acesso à Internet para diversos gerentes quando todos os usuários estão localizados centralmente. É eficaz principalmente em empresas maiores que abrangem vários locais e regiões geográficas, permitindo que os administradores locais gerenciem o acesso à Internet e gerem relatórios sobre a atividade de filtragem para os usuários em seus locais.

A implementação da administração delegada abrange a criação de uma função administrativa para cada grupo de clientes que será gerenciado pelos mesmos administradores. É possível conceder permissões a administradores individuais em cada função para gerenciar diretivas e/ou gerar relatórios para seus clientes. Consulte [Introdução às funções administrativas](#), página 241.

A função Super administrador está pré-instalada e inclui o usuário administrativo padrão: o WebsenseAdministrator. Os Super administradores têm acesso a uma maior variedade de definições de diretivas e configurações do que os administradores em outras funções. Consulte [Super administradores](#), página 237.

## Introdução às funções administrativas

---

Tópicos relacionados:

- ◆ [Introdução aos administradores](#), página 236
- ◆ [Introdução às funções administrativas](#), página 241

Uma função administrativa é uma coleção de clientes — usuários, grupos, domínios, unidades organizacionais, computadores e intervalos de rede — gerenciados por um ou mais administradores. Você concede aos administradores individuais permissões para aplicar diretivas aos clientes da função e/ou para gerar relatórios.

O software Websense vem com uma função Super administrador predefinida. Existe também um usuário padrão, o WebsenseAdministrator, que é automaticamente um membro da função Super administrador. Você pode adicionar administradores a essa função, mas não pode excluir o administrador padrão.



### Importante

Você não pode excluir a função Super administrador predefinida. O usuário padrão, ou WebsenseAdministrator, é um administrador na função Super administrador, mas não aparece listado nessa função. Você não pode excluir ou alterar as permissões do WebsenseAdministrator.

---

Crie quantas funções forem apropriadas à sua organização. Por exemplo, você pode criar uma função para cada departamento, tendo o gerente do departamento como administrador e os membros do departamento como clientes gerenciados. Em uma organização geograficamente distribuída, seria possível criar uma função para cada local e designar todos os usuários do local como clientes gerenciados dessa função. Depois, designe uma ou mais pessoas do local como administrador.

Para obter mais informações sobre as opções disponíveis para definição de administradores, consulte [Introdução aos administradores](#), página 236,.

Para obter instruções sobre como criar funções e configurar permissões, consulte [Usando a administração delegada](#), página 252,.

## Introdução aos administradores

---

Os administradores são as pessoas que podem acessar o Websense Manager para gerenciar diretivas ou gerar relatórios para um grupo de clientes. As permissões específicas disponíveis variam em função do tipo de função.

- ◆ O Super administrador é uma função especial predefinida no Websense Manager e que proporciona a máxima flexibilidade na definição de permissões de acesso. Consulte [Super administradores](#), página 237.
- ◆ As funções de administração delegada devem ser criadas por um Super administrador. Os administradores dessas funções têm permissões de acesso mais limitadas. Consulte [Administradores delegados](#), página 239.

Além disso, você poderia criar algumas funções de administração delegada para relatórios somente, permitindo que várias pessoas gerassem relatórios, mas sem atribuir a responsabilidade de gerenciamento de diretivas.

Você pode designar administradores a funções usando as credenciais que eles já têm para logon na rede, ou criar contas especiais para acessar o Websense Manager. Consulte [Habilitando o acesso ao Websense Manager](#), página 248.

## Super administradores

Tópicos relacionados:

- ◆ [Introdução aos administradores](#), página 236
- ◆ [Administradores delegados](#), página 239
- ◆ [Administradores em várias funções](#), página 240

A função Super administrador é criada durante a instalação. O usuário padrão, o WebsenseAdministrator, é automaticamente designado a essa função. Portanto, na primeira vez em que fizer logon com esse nome de usuário e a senha escolhida durante a instalação, você terá acesso administrativo completo a todas as definições de diretivas, relatórios e configuração no Websense Manager.

Para preservar o acesso completo a essa conta, o WebsenseAdministrator não aparece na lista de administradores da função Super administrador. Ele não pode ser excluído e as permissões não podem ser modificadas.

Você pode adicionar administradores à função Super administrador, conforme necessário. É possível conceder permissões a cada administrador da seguinte maneira:

- ◆ As permissões de **diretiva** permitem que os Super administradores criem e editem funções de administração delegada, e copiem filtros e diretivas para essas funções, conforme apropriado. Eles também podem criar e editar componentes de filtragem, filtros e diretivas, além de aplicar diretivas a clientes que não são gerenciados por outra função.

Além disso, os Super administradores que têm permissões de diretiva podem exibir o log de auditoria e têm acesso a opções de configuração do Websense, bem como a outras opções, como é mostrado a seguir:

- As permissões **incondicionais** dão ao Super administrador acesso a todas as definições de configurações do sistema para a instalação do Websense: por exemplo, conta, Policy Server e Remote Filtering Server, atribuições de classes de risco e opções de registro em log.

Os Super administradores incondicionais têm a opção de criar uma Proteção de filtro que bloqueia determinadas categorias e protocolos para todos os usuários gerenciados pelas funções de administração delegada. Consulte [Definindo restrições de filtragem para todas as funções](#), página 264, para obter mais informações.

Os Super administradores incondicionais podem modificar a função Super administrador, adicionando e excluindo administradores, conforme necessário. Eles também podem excluir funções de administração delegada ou excluir administradores ou clientes dessas funções.

- As permissões **condicionais** concedem ao Super administrador acesso para download de banco de dados, serviços de diretório, identificação de usuários e definições de configuração do Network Agent. Os Super administradores condicionais que também têm permissões de relatório podem acessar definições de configuração das ferramentas de relatório.

Os Super administradores condicionais podem adicionar contas de usuário do Websense, mas não podem excluí-las. Eles podem criar e editar funções de administração delegada, mas não podem excluir funções nem os administradores ou os clientes gerenciados designados a elas. Também não podem excluir administradores da função Super administrador.

- ◆ As permissões de **relatório** permitem que os Super administradores acessem todos os recursos de relatórios e gerem relatórios de todos os usuários. A permissão de relatório é concedida automaticamente aos Super administradores incondicionais.

Se um administrador receber apenas permissões de relatório, as opções Criar diretiva, Recategorizar URL e Desbloquear URL na lista Tarefas comuns não estarão disponíveis. Além disso, a opção Verificar diretiva na Caixa de ferramentas também não estará disponível.

A criação de vários Super administradores incondicionais assegura que, caso o Super administrador não esteja disponível, outro administrador tenha acesso a todas as definições de configuração e de diretiva do Websense.

Lembre-se de que não é possível haver dois administradores conectados ao mesmo tempo para gerenciar a diretiva da mesma função. Consulte [Vários administradores acessando o Websense Manager](#), página 263, para obter informações sobre como evitar conflitos.

Os privilégios exclusivos da função Super administrador concedem a um administrador na função acesso a todas as funções. Para alternar para outra função após o logon, acesse a lista suspensa **Função** no banner e selecione uma função.

Após a alteração de funções, suas permissões de diretiva serão limitadas às que estiverem disponíveis para a função de administração delegada. Os filtros e as diretivas que você cria estão disponíveis somente para administradores nessa função e

só podem ser aplicados a clientes gerenciados nessa função. Consulte [Administradores delegados](#), página 239.

As permissões de relatório são cumulativas, ou seja, você obtém as permissões combinadas de todas as funções em que é administrador. Os Super administradores incondicionais têm permissões completas de relatório, independentemente da função que é acessada.

## Administradores delegados

Tópicos relacionados:

- ◆ [Introdução aos administradores](#), página 236
- ◆ [Super administradores](#), página 237
- ◆ [Administradores em várias funções](#), página 240

Os administradores delegados gerenciam clientes designados a uma função específica. Para cada administrador, designe permissões de diretiva, permissões de relatório ou ambas.

Os administradores delegados que têm permissões de **diretiva** aplicam diretivas aos clientes designados à função deles, determinando, assim, o acesso à Internet disponível a cada cliente. Como parte dessa responsabilidade, os administradores delegados podem criar, editar e excluir diretivas e filtros, que estão sujeitos às limitações da Proteção de filtro estabelecida pelo Super administrador. Consulte [Definindo restrições de filtragem para todas as funções](#), página 264.



### Obs.:

Os administradores delegados têm controle significativo sobre as atividades da Internet de seus clientes gerenciados. Para garantir que esse controle seja tratado de modo responsável e de acordo com as diretivas de uso da sua organização, os Super administradores devem utilizar a página Log de auditoria para monitorar alterações feitas pelos administradores. Consulte [Exibindo e exportando o log de auditoria](#), página 281.

Os administradores delegados não podem excluir a diretiva Padrão.

Os administradores delegados podem editar componentes de filtros, com algumas limitações. Consulte [Criar diretivas e filtros](#), página 246, para obter mais informações.

Os administradores com permissões de diretivas que fizerem logon no Websense Manager com uma conta de usuário do Websense também poderão alterar suas próprias senhas do Websense. (Consulte [Contas de usuário do Websense](#), página 250.)

As opções disponíveis para administradores delegados com permissões de **relatório** variam de acordo com a configuração da função. Eles podem ter permissão para gerar

relatórios apenas dos clientes gerenciados na sua função ou de todos os clientes. Além disso, podem ter acesso a todos os recursos de relatório ou acesso de relatórios mais limitado. Consulte [Editando funções](#), página 254, para obter mais informações.

Um administrador somente com permissões de relatório tem opções limitadas no painel de atalho direito (Tarefas comuns e Caixa de ferramentas).

## Administradores em várias funções

Tópicos relacionados:

- ◆ [Introdução aos administradores](#), página 236
- ◆ [Super administradores](#), página 237
- ◆ [Administradores delegados](#), página 239

Dependendo das necessidades da sua organização, o mesmo administrador pode ser designado a várias funções. Os administradores designados a várias funções devem escolher uma única função para gerenciar no logon.

Após o logon, suas permissões são as seguintes:

- ◆ **Diretiva:** você pode adicionar e editar filtros e diretivas para a função selecionada durante o logon e aplicar diretivas aos clientes gerenciados dessa função. A página Administração delegada lista todas as funções a que você está designado. Assim você pode ver os clientes gerenciados e as permissões de relatório de cada função.
- ◆ **Relatório:** você tem as permissões de relatório combinadas de todas as suas funções. Por exemplo, suponha que você esteja designado a três funções, com permissões de relatório da seguinte maneira:
  - Função 1: sem relatório
  - Função 2: apenas relatórios sobre clientes gerenciados e relatórios investigativos
  - Função 3: relatórios sobre todos os clientes, acesso completo a todos os recursos de relatório

Nessa situação, independentemente da função que escolher durante o logon, você terá permissão para ver relatórios nas páginas Hoje e Histórico, e acessar relatórios sobre todos os clientes usando todos os recursos de relatório.

Se você fez logon apenas para relatório, o campo Função na barra do banner indica se tem permissões Relatório completo (relatório sobre todos os clientes) ou Relatório limitado (relatório apenas sobre clientes gerenciados).

## Introdução às funções administrativas

Tópicos relacionados:

- ◆ [Introdução às funções administrativas](#), página 236
- ◆ [Notificando administradores](#), página 243
- ◆ [Tarefas dos administradores delegados](#), página 244

Para começar a trabalhar com a administração delegada, o Super administrador precisa realizar as seguintes tarefas:

- ◆ Decidir como os administradores farão logon no Websense Manager. Consulte [Habilitando o acesso ao Websense Manager](#), página 248.
- ◆ Adicionar funções e configurá-las. Consulte [Usando a administração delegada](#), página 252.
- ◆ Informar aos administradores sobre suas responsabilidades e opções. Consulte [Notificando administradores](#), página 243.

Além dessas tarefas obrigatórias, existem ainda algumas tarefas opcionais associadas à administração delegada.

### Criando a Proteção de filtro

Os Super administradores incondicionais podem criar uma Proteção de filtro, que define categorias e protocolos específicos como bloqueados para clientes gerenciados em todas as funções de administração delegada. Essas restrições são aplicadas automaticamente a todos os filtros criados em uma função de administração delegada, ou copiados nela, e não podem ser modificados pelo administrador delegado.



**Obs.:**

A Proteção de filtro não se aplica a clientes gerenciados pela função Super administrador.

A Proteção de filtro também pode bloquear e proteger tipos de filtros e palavras-chave associadas a categorias selecionadas, bem como aplicar o registro de protocolos selecionados. Consulte [Criando uma Proteção de filtro](#), página 265.

### Movendo clientes

A inclusão de um cliente na página Clientes enquanto você está conectado como Super administrador designa esse cliente à função Super administrador. Esse cliente não pode ser adicionado a uma função de administração delegada na página Editar função. É melhor você adicionar os clientes diretamente à função, em vez de designar uma diretiva dentro da função Super administrador. No entanto, isso nem sempre é possível.

Para transferir clientes da função Super administrador para outra, utilize a opção **Mover para função** na página Clientes. Consulte [Movendo clientes para funções](#), página 68.

Como parte da transferência, a diretiva aplicada na função Super administrador é copiada para a função de administração delegada. Os filtros aplicados pela diretiva também são copiados. Durante esse processo de cópia, os filtros são atualizados para aplicar as restrições da Proteção de filtro, caso haja alguma.

Na função de destino, o tag “(Copied)” é acrescentado ao final do nome do filtro ou da diretiva. Assim, os administradores dessa função podem identificar de imediato o novo item e atualizá-lo adequadamente.



**Obs.:**

Toda vez que um filtro ou diretiva é copiado para a mesma função, o tag (Copied) recebe um número que aumenta a cada nova cópia: (Copied 1), (Copied 2) e assim por diante. Cada cópia se torna um filtro ou uma diretiva separada na função.

Estimule os administradores na função a renomear as diretivas e os filtros, e também a editá-los se for necessário para tornar as configurações mais claras e minimizar as duplicatas. Essas alterações podem simplificar as tarefas futuras de manutenção.

---

Os filtros Permitir tudo na função Super administrador permitem o acesso a todas as categorias ou protocolos e não podem ser editados. Para preservar a capacidade do Super administrador de implementar uma Proteção de filtro, esses filtros não podem ser copiados para uma função de administração delegada.

Se a diretiva designada ao cliente que estiver sendo movido aplicar um filtro Permitir tudo, ele não poderá ser movido até você aplicar uma diretiva que não utilize um filtro Permitir tudo.

Depois que o cliente for movido para a nova função, somente um administrador dessa função poderá modificar a diretiva do cliente ou os filtros que ela aplica. Alterações nas diretivas ou nos filtros originais na função Super administrador não afetam cópias da diretiva ou dos filtros nas funções de administração delegada.

### Copiando filtros e diretivas

Inicialmente, os filtros e as diretivas criadas por um Super administrador estão disponíveis somente para administradores na função Super administrador. Você pode usar a opção **Copiar para função** para copiar filtros e diretivas para uma função de administração delegada sem mover um cliente para uma função. Consulte [Copiando filtros e diretivas para funções](#), página 170.

Quando se copia filtros e diretivas diretamente, as restrições aplicadas são as mesmas adotadas quando se copia filtros e diretivas como parte de um processo de transferência de cliente.

- ◆ As restrições da Proteção de filtro são implementadas durante a cópia.
- ◆ Os filtros de categoria e protocolo Permitir tudo não podem ser copiados.
- ◆ As diretivas e os filtros copiados são identificados na função pelo tag (Copiado) presente no nome.

Edite as descrições das diretivas antes de começar a cópia; isso garantirá que sejam significativas para os administradores nas funções de destino.

### Aplicando diretivas aos clientes restantes

Os clientes que não são designados especificamente a uma função de administração delegada são gerenciados por Super administradores. Não há uma lista Clientes gerenciados para a função Super administrador.

Para aplicar diretivas a esses clientes, adicione-os à página Gerenciamento de diretivas > Clientes. Consulte [Adicionando um cliente](#), página 66. Os clientes que não foram designados a uma diretiva específica são controlados pela diretiva Padrão para a função deles.

Algumas vezes, não será possível adicionar clientes à página Clientes. Isso pode acontecer quando o cliente for membro de uma rede, grupo, domínio ou unidade organizacional que esteja designado a uma outra função. Nesse caso, se o administrador dessa outra função tiver aplicado uma diretiva a membros específicos da rede ou do grupo, esses clientes não poderão ser adicionados à função Super administrador.

## Notificando administradores

Tópicos relacionados:

- ◆ [Introdução às funções administrativas](#), página 236
- ◆ [Introdução às funções administrativas](#), página 241

Após designar usuários como administradores em qualquer função administrativa, certifique-se de passar as seguintes informações a eles.

- ◆ O URL para fazer logon no Websense Manager. Por padrão:  
`https://<ServerIP>:9443/mng/`  
Em vez de especificar o IP do servidor (<ServerIP>), utilize o endereço IP da máquina em que o Websense Manager está sendo executado.
- ◆ O Policy Server que deverá ser escolhido durante o logon, se aplicável. Em um ambiente com vários Policy Servers, os administradores deverão escolher um Policy Server durante o logon. Eles deverão escolher o Policy Server que está configurado para se comunicar com o serviço de diretório que autentica seus clientes gerenciados.
- ◆ Se é necessário usar a conta de logon na rede ou uma conta de usuário do Websense quando fizerem logon no Websense Manager. Se os administradores

fizerem logon com contas de usuário do Websense, forneça o nome de usuário e a senha.

- ◆ As permissões que terão para criar e aplicar diretivas a clientes na função, para gerar relatórios, ou ambas.

Oriente os administradores com permissões de diretiva e relatório a avaliar quais atividades planejam realizar durante a sessão. Se a intenção deles for apenas gerar relatórios, sugira que acessem o campo **Função** no banner e escolham **Liberar permissões da diretiva**. Isso liberará as permissões de diretiva da função, permitindo que outro administrador acesse o Websense Manager e gerencie a diretiva dessa função.

- ◆ Como encontrar a lista de clientes gerenciados pela função deles. Os administradores podem acessar Gerenciamento de diretivas > Administração delegada e clicar no nome da função deles para exibir a página Editar função, que inclui uma lista de clientes gerenciados.
- ◆ As limitações impostas pela Proteção de filtro, se houver categorias ou protocolos que foram bloqueados e protegidos.
- ◆ As tarefas que normalmente são realizadas pelos administradores. Consulte *Tarefas dos administradores delegados*, página 244.

Não deixe de avisar os administradores delegados quando você adicionar ou alterar protocolos e tipos de arquivos personalizados. Esses componentes aparecem automaticamente nos filtros e nas diretivas de todas as funções. Por isso, é importante que esses administradores saibam quando alterações forem feitas.

## Tarefas dos administradores delegados

Tópicos relacionados:

- ◆ *Introdução às funções administrativas*, página 236
- ◆ *Introdução às funções administrativas*, página 241
- ◆ *Notificando administradores*, página 243

Os administradores delegados que têm permissões de **diretiva** podem executar as seguintes tarefas.

- ◆ *Ver sua conta de usuário*, página 245
- ◆ *Ver a definição da sua função*, página 245
- ◆ *Adicionar clientes à página Clientes*, página 246
- ◆ *Criar diretivas e filtros*, página 246
- ◆ *Aplicar diretivas a clientes*, página 248

As permissões para gerar **relatórios** podem ser concedidas em um nível granular. As permissões de relatório específicas concedidas à sua função determinam quais das seguintes tarefas estão disponíveis para os administradores que têm permissões para gerar relatórios. Consulte *Gerar relatórios*, página 248.

## Ver sua conta de usuário

Tópicos relacionados:

- ◆ [Tarefas dos administradores delegados](#), página 244
- ◆ [Ver a definição da sua função](#), página 245
- ◆ [Adicionar clientes à página Clientes](#), página 246
- ◆ [Criar diretivas e filtros](#), página 246
- ◆ [Aplicar diretivas a clientes](#), página 248

Se você fizer logon no Websense Manager com credenciais de rede, as mudanças de senha serão tratadas por meio do seu serviço de diretório de rede. Entre em contato com o administrador do sistema para obter ajuda.

Se um nome de usuário e uma senha do Websense tiverem sido designados a você, veja informações sobre sua conta e altere sua senha no Websense Manager.

1. Vá para **Gerenciamento de diretivas > Administração delegada**.
2. Clique em **Gerenciar contas de usuário do Websense** no alto da página.
3. Clique em **Alterar senha** caso queira mudar sua senha. Consulte [Alterando a senha de usuário do Websense](#), página 252.
4. Clique em **Exibir** para ver uma lista de funções em que você é administrador.

## Ver a definição da sua função

Tópicos relacionados:

- ◆ [Tarefas dos administradores delegados](#), página 244
- ◆ [Ver sua conta de usuário](#), página 245
- ◆ [Adicionar clientes à página Clientes](#), página 246
- ◆ [Criar diretivas e filtros](#), página 246
- ◆ [Aplicar diretivas a clientes](#), página 248

Abra a página Administração delegada e clique no nome da sua função para exibir a página Editar função, que lista os clientes gerenciados da função. Esta página também mostra os recursos de relatório disponíveis para administradores que têm permissões de relatório nessa função.

Os administradores que têm somente permissões de relatório não conseguem ver essa página. Para eles, só estão disponíveis recursos de relatório específicos.

## Adicionar clientes à página Clientes

Tópicos relacionados:

- ◆ [Tarefas dos administradores delegados](#), página 244
- ◆ [Ver sua conta de usuário](#), página 245
- ◆ [Ver a definição da sua função](#), página 245
- ◆ [Criar diretivas e filtros](#), página 246
- ◆ [Aplicar diretivas a clientes](#), página 248

Embora os Super administradores designem clientes gerenciados a uma função, os administradores delegados devem adicioná-los à página Clientes antes de aplicar diretivas. Consulte [Adicionando um cliente](#), página 66, para obter instruções.

Assim que clientes são adicionados à lista de clientes gerenciados da função, eles são filtrados pela diretiva Padrão dessa função. Os clientes que foram movidos da página Clientes do Super administrador para a função são regidos pela diretiva que o Super administrador aplicou, a qual foi copiada para a função quando o cliente foi movido.

Qualquer cliente listado na página Administração delegada > Editar função da função pode ser adicionado à página Clientes e ser designado a uma diretiva. Você também pode adicionar usuários ou computadores específicos que sejam membros de um grupo, domínio, unidade organizacional ou intervalo de rede designado como um cliente gerenciado na sua função.

Como um usuário pode fazer parte de vários grupos, domínios ou unidades organizacionais, a inclusão de usuários de um agrupamento maior de clientes pode gerar conflitos quando diferentes funções gerenciam grupos, domínios ou unidades organizacionais com membros comuns. Se administradores em funções distintas acessassem o Websense Manager ao mesmo tempo, eles poderiam adicionar o mesmo cliente (por exemplo, um membro individual de um grupo) à página Clientes deles. Em uma situação como essa, a filtragem da Internet para esse cliente é controlada pela prioridade definida para cada função. Consulte [Gerenciando conflitos entre funções](#), página 261.

## Criar diretivas e filtros

Tópicos relacionados:

- ◆ [Tarefas dos administradores delegados](#), página 244
- ◆ [Ver sua conta de usuário](#), página 245
- ◆ [Ver a definição da sua função](#), página 245
- ◆ [Adicionar clientes à página Clientes](#), página 246
- ◆ [Aplicar diretivas a clientes](#), página 248

Quando sua função foi criada, ela herdou automaticamente a diretiva Padrão pré-instalada, o filtro de categoria e o filtro de protocolo, do modo como eles estavam naquele momento. Pode haver também diretivas e filtros que o Super administrador tenha decidido copiar para a função.

Além das diretivas e dos filtros, você também herda os tipos de arquivos personalizados, bem como os protocolos criados pelo Super administrador.

Você tem liberdade para editar as diretivas e os filtros herdados do Super administrador. As alterações que você fizer afetarão apenas a sua função. Qualquer alteração que o Super administrador fizer nas diretivas e nos filtros que você herdou anteriormente não afetarão sua função.

**Obs.:**

As alterações que o Super administrador faz nos protocolos e tipos de arquivos personalizados afetam automaticamente os filtros e as diretivas da sua função.

Quando o Super administrador informar você sobre alterações nesses componentes, avalie seus filtros e diretivas para ter certeza de que sejam tratados apropriadamente.

Você também pode criar quantos filtros novos e diretivas novas precisar. Os filtros e as diretivas criadas por um administrador delegado estão disponíveis somente para administradores conectados na sua função. Para obter instruções sobre como criar diretivas, consulte [Trabalhando com diretivas](#), página 73. Para obter instruções sobre como criar filtros, consulte [Trabalhando com filtros](#), página 46.

Você pode editar componentes de filtro para sua função, com algumas limitações.

- ◆ **Categorias:** adicione categorias personalizadas e edite tanto as categorias do Master Database quanto as personalizadas, definindo palavras-chave e URLs recategorizados para serem usados dentro da respectiva função; mude a ação e a opção de filtragem avançada aplicada por padrão aos filtros de categoria criados. (As mudanças feitas na ação padrão de uma categoria só serão implementadas se a categoria não estiver bloqueada pela Proteção de filtro.)
- ◆ **Protocolos:** muda a ação e as opções de filtragem avançadas que, por padrão, são aplicadas aos filtros de protocolo criados. (As mudanças feitas na ação padrão de um protocolo só serão implementadas se o protocolo não estiver bloqueado pela Proteção de filtro.) Os administradores delegados não podem adicionar nem excluir definições de protocolo.
- ◆ **Tipos de arquivo:** exibe as extensões de arquivo designadas a cada tipo de arquivo. Os administradores delegados não podem adicionar tipos de arquivo nem alterar extensões designadas a um tipo.
- ◆ **URLs não filtrados:** adiciona URLs e expressões regulares que representam sites os quais serão permitidos para todos os clientes gerenciados somente na respectiva função.

Para obter mais informações, consulte [Criando componentes de filtro](#), página 172.

Se um Super administrador tiver implementado restrições de Proteção de filtro, pode haver categorias ou protocolos que serão bloqueados automaticamente e não poderão ser alterados nos filtros que você criar e editar. Consulte [Definindo restrições de filtragem para todas as funções](#), página 264.

## Aplicar diretivas a clientes

Tópicos relacionados:

- ◆ [Tarefas dos administradores delegados](#), página 244
- ◆ [Ver sua conta de usuário](#), página 245
- ◆ [Ver a definição da sua função](#), página 245
- ◆ [Adicionar clientes à página Clientes](#), página 246
- ◆ [Criar diretivas e filtros](#), página 246

Depois de criar uma diretiva, você poderá aplicá-la diretamente aos clientes que já foram adicionados à página Clientes; basta clicar no botão **Aplicar a clientes**. Consulte [Atribuindo uma diretiva aos clientes](#), página 77.

Se preferir, você pode acessar a página Clientes e adicionar os clientes que deverão ser controlados por essa diretiva. Consulte [Trabalhando com clientes](#), página 58.

## Gerar relatórios

Se você tiver permissões de relatório, as opções de relatórios específicas disponíveis serão definidas pelo Super administrador. Para saber quais recursos você pode usar, vá até a página Administração delegada e clique no nome da função. A página Editar função mostra os recursos de relatório para os quais você tem permissões. Consulte [Editando funções](#), página 254, para obter mais informações.

## Habilitando o acesso ao Websense Manager

---

Quando configura funções de administração delegada, você determina quais recursos do Websense Manager os administradores podem acessar. Para garantir que os recursos certos estejam disponíveis para os usuários que fizeram logon no Websense Manager, cada pessoa deverá fazer logon com um nome de usuário e uma senha. Podem ser usados dois tipos de contas:

- ◆ As **Contas de rede** utilizam as credenciais já definidas no seu serviço de diretório de rede (consulte [Contas de diretório](#), página 249).
- ◆ As **contas de usuário do Websense** permitem que você crie um nome de usuário e uma senha especificamente para serem usados no Websense Manager (consulte [Contas de usuário do Websense](#), página 250).

## Contas de diretório

Tópicos relacionados:

- ◆ [Habilitando o acesso ao Websense Manager](#), página 248
- ◆ [Contas de usuário do Websense](#), página 250

Os Super administradores incondicionais podem usar a página **Configurações > Geral > Diretório de logon** para inserir as informações do serviço de diretório necessárias para permitir que administradores façam logon no Websense Manager com suas credenciais de rede.



**Obs.:**

Essas informações são usadas para autenticar apenas usuários do Websense Manager. Elas não se aplicam a clientes de filtragem. As informações do serviço de diretório do cliente são configuradas na página **Configurações > Serviços de diretório** (consulte [Serviços de diretório](#), página 60).

As credenciais de rede dos usuários do Websense Manager devem ser autenticadas em um único serviço de diretório. Se a sua rede inclui vários serviços de diretório, é necessário haver um relacionamento confiável entre o serviço de diretório de logon que você configurar no Websense Manager e os outros.

Se não for possível definir um único diretório de serviço para ser usado com o Websense Manager, considere a criação de contas de usuário do Websense (consulte [Contas de usuário do Websense](#), página 250).

Para definir o serviço de diretório que o Websense Manager deverá usar para autenticar administradores, primeiro verifique se a caixa de seleção com a opção para usar um serviço de diretório para autenticação de administradores está marcada. Depois, selecione um tipo de **serviço de diretório** na lista.

Se você selecionar o padrão, **Windows NT Directory/Active Directory (Mixed Mode)**, não será necessária nenhuma configuração adicional. Clique em **OK** para armazenar suas alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Se você selecionar **Active Directory (Native Mode)** ou **Outro diretório LDAP**, forneça as seguintes informações adicionais:

1. Digite o endereço IP ou o nome da máquina onde o serviço de diretório está instalado.

Se estiver usando o Active Directory (Native Mode) e tiver configurado seus servidores de catálogo globais para failover, você poderá inserir o nome do domínio DNS.

2. Insira a **Porta** usada para comunicação com o serviço de diretório.

3. Para criptografar a comunicação com o serviço de diretório, marque **Usar SSL**.
4. Insira o **Nome distinto do usuário** e a **Senha** que o software Websense usa para se conectar com o serviço de diretório.
5. Insira o **Contexto de domínio padrão** que o software Websense deve usar ao autenticar administradores.
  - Se você estiver usando o Active Directory (Native Mode), a configuração estará concluída. Clique em **OK** para armazenar suas alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.
  - Se você estiver usando outro serviço de diretório baseado em LDAP, continue.
6. Especifique os **Atributos de ID de logon do usuário** e o **Filtro de pesquisa de usuários**, se houver, que o software Websense deverá usar para acelerar a autenticação de usuário.

Essas informações também aparecem na página **Configurações > Serviços de diretório** em **Configurações avançadas de diretório**. Se necessário, você poderá copiar e colar os valores.
7. Em Opções de grupo, especifique se seu esquema LDAP inclui ou não o atributo **memberOf**:
  - Se o atributo memberOf não for usado, especifique o **Filtro de pesquisa de grupos do usuário** que o software Websense deverá aplicar para autenticar administradores.
  - Se memberOf for usado, especifique o **Atributo de grupo** que deverá ser aplicado.
8. Se seu esquema LDAP incluir grupos aninhados, marque **Realizar pesquisa adicional de grupos coletados**.
9. Se o seu serviço de diretório usar referências LDAP, indique se o software Websense deve utilizá-las ou ignorá-las.
10. Clique em **OK** para armazenar suas alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Contas de usuário do Websense

Tópicos relacionados:

- ◆ [Habilitando o acesso ao Websense Manager](#), página 248
- ◆ [Adicionando contas de usuário do Websense](#), página 251

Os Super administradores utilizam a página **Administração delegada > Gerenciar contas de usuário do Websense** para criar contas para os administradores acessarem o Websense Manager sem inserir credenciais de diretório de rede. Essa página também permite que os Super administradores mudem a senha de contas de usuário do Websense e vejam as funções a que um usuário do Websense está designado como administrador.

Os Super administradores incondicionais também podem excluir contas de usuário do Websense dessa página.

Os administradores delegados utilizam essa página para alterar sua senha do Websense e ver as funções a que estão atribuídos como administradores.

Opção	Descrição
Adicionar	Abre a página para criar uma nova conta de usuário do Websense. Consulte <i>Adicionando contas de usuário do Websense</i> , página 251.
Alterar senha	Abre a página para alterar a senha da conta associada. Consulte <i>Alterando a senha de usuário do Websense</i> , página 252.
Ver	Exibe uma lista de funções a que esse usuário está designado como administrador.
Excluir	Marque a caixa de seleção referente a uma ou mais contas de usuário antigas e clique neste botão para excluí-las.
Fechar	Retorna à página Administração delegada.

## Adicionando contas de usuário do Websense

Tópicos relacionados:

- ◆ [Habilitando o acesso ao Websense Manager](#), página 248
- ◆ [Contas de usuário do Websense](#), página 250
- ◆ [Alterando a senha de usuário do Websense](#), página 252

Utilize a página **Administração delegada > Gerenciar contas de usuário do Websense > Adicionar usuário do Websense** para adicionar contas de usuário do Websense.

1. Insira um **Nome de usuário** exclusivo com até 50 caracteres.

O nome deve ter de 1 a 50 caracteres e não pode incluir nenhum destes caracteres:

\* < > ' { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

Os nomes de usuário podem conter espaços e traços.

2. Insira e confirme uma **Senha** (de 4 a 255 caracteres) para este usuário.

Recomenda-se o uso de senhas fortes, com 8 caracteres ou mais, e pelo menos um destes caracteres:

- letra maiúscula
- letra minúscula
- número
- caractere especial (como hífen, sublinhado ou em branco)

3. Quando terminar de fazer as alterações, clique em **OK** para armazená-las em cache e voltar à página Gerenciar contas de usuário do Websense. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Alterando a senha de usuário do Websense

Tópicos relacionados:

- ◆ [Habilitando o acesso ao Websense Manager, página 248](#)
- ◆ [Contas de usuário do Websense, página 250](#)
- ◆ [Adicionando contas de usuário do Websense, página 251](#)

A página **Administração delegada > Gerenciar contas de usuário do Websense > Alterar senha** permite que administradores delegados mudem a senha de suas contas de usuário do Websense. Os Super administradores podem usar esta página para mudar a senha de qualquer conta de usuário do Websense.

1. Verifique se o **Nome de usuário** correto aparece no alto da página.
2. Insira e confirme a nova **Senha** (de 4 a 255 caracteres) para este usuário.  
Recomenda-se o uso de senhas fortes, com 8 caracteres ou mais, e pelo menos um destes caracteres:
  - letra maiúscula
  - letra minúscula
  - número
  - caractere especial (como hífen, sublinhado ou em branco)
3. Quando terminar de fazer as alterações, clique em **OK** para armazená-las em cache e voltar à página Gerenciar contas de usuário do Websense. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Usando a administração delegada

---

Tópicos relacionados:

- ◆ [Introdução às funções administrativas, página 236](#)
- ◆ [Gerenciando conflitos entre funções, página 261](#)

As opções da página **Gerenciamento de diretivas > Administração delegada** variam em função de ela estar sendo acessada por um Super administrador ou um administrador delegado.

Os Super administradores vêem uma lista de todas as funções definidas atualmente e têm as seguintes funções disponíveis.

Opção	Descrição
Adicionar	Clique para adicionar uma nova função. Consulte <a href="#">Adicionando funções, página 254</a> .
Função	Clique para ver ou configurar a função. Consulte <a href="#">Editando funções, página 254</a> .
Excluir	Clique para excluir quaisquer funções que estão marcadas na lista. Essa opção está disponível apenas para Super administradores incondicionais. Consulte <a href="#">Considerações especiais, página 261</a> , para obter informações sobre como os clientes de uma função são gerenciados depois da exclusão da função.
Avançado	Clique para acessar a função Gerenciar prioridades de funções.
Gerenciar prioridades de funções	Clique para especificar quais configurações de diretiva da função são usadas quando o mesmo cliente existe em vários grupos que são gerenciados por diferentes funções. Consulte <a href="#">Gerenciando conflitos entre funções, página 261</a> .
Gerenciar contas de usuário do Websense	Clique para adicionar, editar e excluir nomes de usuário e senhas de contas usadas apenas para acessar o Websense Manager. Consulte <a href="#">Contas de usuário do Websense, página 250</a> .
Gerenciar grupos LDAP personalizados	Clique para adicionar, editar e excluir grupos LDAP personalizados, que podem ser designados como clientes gerenciados em funções de administração delegada. Consulte <a href="#">Trabalhando com grupos LDAP personalizados, página 64</a> . Esta opção não estará disponível se o serviço de diretório configurado for Windows NT/Active Directory (Mixed Mode).

Os administradores delegados vêem apenas as funções em que são administradores e têm acesso a opções mais limitadas.

Opção	Descrição
Função	Clique para ver os clientes designados à função e as permissões de relatório específicas concedidas. Consulte <a href="#">Editando funções, página 254</a> .
Gerenciar contas de usuário do Websense	Clique para acessar opções que permitem alterar sua senha do Websense Manager e exibir as funções designadas. Consulte <a href="#">Contas de usuário do Websense, página 250</a> .

## Adicionando funções

Tópicos relacionados:

- ◆ [Editando funções](#), página 254
- ◆ [Considerações especiais](#), página 261

Utilize a página **Administração delegada** > **Adicionar função** para fornecer um nome e uma descrição para a nova função.

1. Insira um **Nome** para a nova função.

O nome deve ter de 1 a 50 caracteres e não pode incluir nenhum destes caracteres:

\* < > ' { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

Os nomes de função podem conter espaços e traços.

2. Insira uma **Descrição** para a nova função.

A descrição pode ter até 255 caracteres. As restrições de caracteres aplicáveis a nomes de função também são aplicadas a descrições, com 2 exceções: as descrições podem incluir pontos (.) e vírgulas (,).

3. Clique em **OK** para exibir a página **Editar função** e definir as características dessa função. Consulte [Editando funções](#), página 254.

A nova função será adicionada à lista suspensa Função no banner na próxima vez em que você fizer logon no Websense Manager.

## Editando funções

Tópicos relacionados:

- ◆ [Usando a administração delegada](#), página 252
- ◆ [Adicionando funções](#), página 254
- ◆ [Gerenciando conflitos entre funções](#), página 261

Os administradores delegados podem usar a página **Administração delegada** > **Editar função** para ver a lista de clientes gerenciados pela respectiva função, bem como as permissões de relatório específicas concedidas.

Os Super administradores podem usar esta página para selecionar os administradores e clientes para uma função, e definir permissões de administrador, conforme é descrito a seguir. Somente os Super administradores incondicionais podem excluir administradores e clientes de uma função.

1. Altere o **Nome** e a **Descrição** da função, conforme necessário.

**Obs.:**

O nome da função Super administrador não pode ser alterado.

2. Adicione e exclua administradores dessa função. (Por estar disponível somente para Super administradores, esta seção não aparecerá se você tiver feito logon como administrador delegado.)

Item	Descrição
Nome de usuário	Nome de usuário do administrador.
Tipo de conta	Indica se o usuário está definido no serviço de diretório da rede (Diretório) ou como uma conta de usuário do Websense.
Geração de relatórios	Marque esta caixa de seleção para dar ao administrador permissão para usar ferramentas de relatório.
Diretiva	Marque esta caixa de seleção para dar ao administrador permissão para criar filtros e diretivas e aplicar diretivas aos clientes gerenciados da função.  Na função Super administrador, os administradores com permissão de diretiva também pode gerenciar determinadas definições de configuração do Websense. Consulte <a href="#">Super administradores</a> , página 237.
Incondicional	Disponível somente para a função Super administrador; marque esta caixa de seleção para dar ao administrador permissões para gerenciar todas as definições de configuração do Websense e a Proteção de filtro.  Apenas os Super administradores incondicionais podem conceder permissões a um novo administrador.
Adicionar	Abre a página <b>Adicionar administradores</b> . Consulte <a href="#">Adicionando administradores</a> , página 257.
Excluir	Remove da função os administradores que estão marcados na lista Administradores. (Disponível somente para Super administradores incondicionais.)

3. Adicione e exclua **Cientes gerenciados** da função. (As alterações só podem ser feitas por Super administradores. Os administradores delegados podem ver os clientes designados às respectivas funções.)

Item	Descrição
<Nome>	Exibe o nome de cada cliente que está explicitamente designado à função. Os administradores na função deverão adicionar os clientes à página Clientes antes de as diretivas poderem ser aplicadas. Consulte <a href="#">Tarefas dos administradores delegados</a> , página 244.

Item	Descrição
Adicionar	Abre a página <b>Adicionar clientes gerenciados</b> . Consulte <a href="#">Adicionando clientes gerenciados</a> , página 259.
Excluir	Disponível apenas para Super administradores incondicionais, este botão remove da função quaisquer clientes que estejam marcados na lista de clientes gerenciados. Alguns clientes não podem ser excluídos diretamente da lista de clientes gerenciados. Consulte <a href="#">Considerações especiais</a> , página 261, para obter mais informações.

4. Utilize a área **Permissões de relatório** para selecionar os recursos disponíveis a administradores desta função que têm acesso a relatório.
- a. Escolha os vários níveis de permissões de relatório:

Opção	Descrição
Gerar relatório sobre todos os clientes	Selecione esta opção para dar aos administradores permissão para gerar relatórios sobre todos os usuários da rede. Utilize as demais opções da área Permissões de relatório a fim de definir as permissões específicas para administradores nesta função.
Gerar relatório apenas sobre clientes gerenciados	Selecione esta opção a fim de limitar administradores a relatórios de clientes gerenciados designados a esta função. Em seguida, selecione os recursos de relatórios investigativos a que esses administradores terão acesso. Os administradores que só tiverem acesso a relatórios de clientes gerenciados não poderão acessar relatórios de apresentação nem relatórios baseados em usuários na página Hoje e Histórico. Eles também não poderão gerenciar configurações do banco de dados de log.

- b. Marque a caixa de seleção correspondente a cada recurso de relatório que os administradores apropriados na função têm permissão para usar.

Opção	Descrição
Acessar relatórios de apresentação	Habilita o acesso a recursos de relatórios de apresentação. Esta opção está disponível somente quando os administradores podem gerar relatórios sobre todos os clientes. Consulte <a href="#">Relatórios de apresentação</a> , página 96.
Exibir relatórios nas páginas Hoje e Histórico	Habilita a apresentação de gráficos que mostram a atividade da Internet nestas páginas. Consulte <a href="#">Hoje: Saúde, segurança e valor desde a meia-noite</a> , página 19 e <a href="#">Histórico: Últimos 30 dias</a> , página 22. Se esta opção não estiver selecionada, os administradores poderão ver apenas as áreas Alerta de saúde e Valor da página Hoje, bem como a área Estimativas de valor da página Histórico.

Opção	Descrição
Acessar relatórios investigativos	Permite o acesso a recursos de relatórios investigativos básicos. Quando esta opção está marcada, é possível selecionar também recursos adicionais de relatórios investigativos. Consulte <i>Relatórios investigativos</i> , página 115.
Exibir nomes de usuários em relatórios investigativos	Permite que administradores nesta função vejam nomes de usuários, casos eles estejam conectados. Consulte <i>Configurando o Filtering Service para registro em log</i> , página 304. Desmarque esta opção para mostrar somente códigos de identificação gerados pelo sistema, em vez de nomes. Esta opção só está disponível quando é concedido aos administradores acesso a relatórios investigativos.
Salvar relatórios investigativos como favoritos	Permite que os administradores nesta função criem relatórios investigativos favoritos. Consulte <i>Relatórios investigativos favoritos</i> , página 132. Esta opção só está disponível quando é concedido aos administradores acesso a relatórios investigativos.
Agendar relatórios investigativos	Permite que administradores nesta função programem relatórios investigativos para serem executados em um momento futuro ou em um ciclo repetitivo. Consulte <i>Agendando relatórios investigativos</i> , página 135. Esta opção só está disponível quando são concedidas aos administradores permissões para salvar relatórios investigativos como favoritos.
Gerenciar o banco de dados de log	Permite que administradores tenham acesso à página Configurações > banco de dados de log. Consulte <i>Configurações de administração do banco de dados de log</i> , página 320. Esta opção está disponível somente quando os administradores podem gerar relatórios sobre todos os clientes.

- Quando terminar de fazer as alterações, clique em **OK** para armazená-las em cache e voltar à página Administração delegada. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Adicionando administradores

Tópicos relacionados:

- ◆ [Editando funções](#), página 254
- ◆ [Habilitando o acesso ao Websense Manager](#), página 248

Os Super administradores podem usar a página **Administração delegada > Editar função > Adicionar administradores** para especificar quais usuários são administradores de uma função.



**Obs.:**

Os administradores podem ser adicionados a várias funções. Durante o logon, deverão escolher uma função. Nessa situação, o administrador recebe as permissões de relatório combinadas para todas as funções.

---

Os administradores delegados têm controle significativo sobre as atividades da Internet de seus clientes gerenciados. Para garantir que esse controle seja tratado de modo responsável e de acordo com as diretivas de uso da sua organização, os Super administradores devem utilizar a página Log de auditoria para monitorar alterações feitas pelos administradores. Consulte [Exibindo e exportando o log de auditoria, página 281](#).

1. Se você planeja adicionar contas de diretório como administradores delegados, verifique se está conectado ao Policy Server cuja configuração do Serviço de diretório (consulte [Serviços de diretório, página 60](#)) corresponde à do Diretório de logon (consulte [Contas de diretório, página 249](#)).

Se estiver adicionando apenas contas de usuário do Websense como administradores, você poderá estar conectado a qualquer Policy Server.

2. Em **Contas de diretório**, marque a caixa de seleção correspondente a um ou mais usuários e clique no botão de seta para a direita (>) a fim de movê-los para a lista **Selecionado**.



**Obs.:**

Grupos LDAP personalizados não podem ser adicionados como administradores.

---

Se o seu ambiente utiliza o Active Directory (Native Mode) ou outro serviço de diretório baseado em LDAP, você pode pesquisar o diretório para encontrar nomes específicos de usuário, grupo, domínio ou unidade organizacional. Consulte [Pesquisando o serviço de diretório, página 67](#).

3. Em **Contas de usuários do Websense**, marque a caixa de seleção correspondente a um ou mais usuários e clique no botão de seta para a direita a fim de mover os usuários destacados para a lista **Selecionado**.

4. Defina as **permissões** de administradores nesta função.

Opção	Descrição
Diretiva	Marque esta opção para permitir que os administradores nesta função apliquem diretivas a seus clientes gerenciados. Isso também concederá acesso a definições específicas de configuração do Websense.
Incondicional	Marque esta opção para conceder acesso a todas as definições de configuração do Websense. Esta opção só está disponível quando um Super administrador incondicional adiciona administradores à função Super administrador com permissões de diretiva.
Relatório	Marque esta opção para conceder acesso a ferramentas de relatório. Utilize a página Editar função para definir os recursos específicos de relatório permitidos.

5. Quando terminar de fazer alterações, clique em **OK** para voltar à página Editar função.
6. Clique em **OK** na página Editar função para armazenar suas alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Adicionando clientes gerenciados

Tópicos relacionados:

- ◆ [Usando a administração delegada, página 252](#)
- ◆ [Editando funções, página 254](#)

Os clientes gerenciados são os clientes e computadores designados a uma função, cujas diretivas são definidas pelos administradores da função. Os clientes de diretório (usuários, grupos, domínios e unidades organizacionais), computadores e redes podem ser definidos como clientes gerenciados.

Os Super administradores podem usar a página **Administração delegada > Editar função > Adicionar clientes gerenciados** para adicionar quantos clientes forem necessários a uma função. Cada cliente pode ser designado a uma única função.

Se designar um intervalo de rede como cliente gerenciado em uma função, você não poderá designar endereços IP individuais desse intervalo a nenhuma outra função. Além disso, você não poderá designar especificamente um usuário, grupo, domínio ou unidade organizacional a duas funções distintas. No entanto, poderá designar um

usuário a uma função e depois atribuir outra função a um grupo, domínio ou unidade organizacional da qual o usuário seja membro.



**Obs.:**

Se um grupo for um cliente gerenciado em uma função e o administrador dessa função aplicar uma diretiva a cada membro do grupo, mais tarde não será possível designar usuários individuais nesse grupo a outra função.

Ao adicionar clientes gerenciados, considere quais tipos de clientes deseja incluir. Se você adicionar endereços IP a uma função, os administradores dessa função poderão gerar relatórios sobre **toda a** atividade para as máquinas especificadas. Se adicionar usuários a uma função, os administradores poderão gerar relatórios sobre toda a atividade desses usuários, independentemente da máquina em que a atividade ocorreu.

Os administradores não são incluídos automaticamente como clientes gerenciados nas funções que administram porque isso permitiria que eles definissem suas próprias diretivas. Para permitir que administradores vejam o próprio uso da Internet, habilite o relatório próprio (consulte [Relatório próprio](#), página 334).

Se sua organização tiver implantado vários Policy Servers e eles se comunicarem com diferentes diretórios, certifique-se de selecionar o Policy Server conectado ao diretório que contém os clientes a serem adicionados.



**Obs.:**

É aconselhável que todos os clientes gerenciados na mesma função sejam do mesmo serviço de diretório.

1. Selecione clientes para a função:
  - Em **Diretório**, marque a caixa de seleção de um ou mais usuários.  
Se o seu ambiente utiliza o Active Directory (Native Mode) ou outro serviço de diretório baseado em LDAP, você pode pesquisar o diretório para encontrar nomes específicos de usuário, grupo, domínio ou unidade organizacional. Consulte [Pesquisando o serviço de diretório](#), página 67.
  - Em **Computador**, insira o endereço IP de um computador para ser adicionado à função.
  - Em **Rede**, insira o primeiro e o último endereços IP em um intervalo de computadores para serem adicionados como unidade.
2. Clique no botão de seta para a direita (>) ao lado do tipo de cliente a fim de mover os clientes para a lista **Selecionados**.
3. Quando terminar de fazer alterações, clique em **OK** para voltar à página Editar função.
4. Clique em **OK** na página Editar função para armazenar suas alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Gerenciando conflitos entre funções

Tópicos relacionados:

- ◆ [Usando a administração delegada, página 252](#)
- ◆ [Adicionando clientes gerenciados, página 259](#)

Os serviços de diretório permitem que o mesmo usuário pertença a vários grupos. Por isso, um usuário pode pertencer a vários grupos que sejam gerenciados por diferentes funções de administração delegada. O mesmo se aplica a domínios e unidades organizacionais.

Além disso, é possível que um usuário seja gerenciado por uma função e pertença a um grupo, domínio ou unidade organizacional que sejam gerenciados por outra. Se os administradores dessas duas funções estiverem conectados ao mesmo tempo, pode acontecer de o administrador responsável pelo usuário aplicar uma diretiva a ele ao mesmo tempo que o administrador responsável pelo grupo aplica uma diretiva aos membros individuais do grupo.

Utilize a página **Administração delegada > Gerenciar prioridades de funções** para informar ao software Websense o que fazer antes de uma sobreposição se diferentes diretivas se aplicarem ao mesmo usuário. Quando um conflito ocorre, o software Websense aplica a diretiva de filtragem da função que aparece na parte mais alta dessa lista.

1. Selecione qualquer função na lista, exceto Super administrador.



**Obs.:**

A função Super administrador é sempre a primeira da lista. Ela não pode ser movida.

2. Clique em **Mover para cima** ou **Mover para baixo** para mudar a posição na lista.
3. Repita as etapas 1 e 2 até todas as funções terem a prioridade desejada.
4. Quando terminar de fazer as alterações, clique em **OK** para armazená-las em cache e voltar à página Administração delegada. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Considerações especiais

Tópicos relacionados:

- ◆ [Usando a administração delegada, página 252](#)
- ◆ [Editando funções, página 254](#)

Considere as seguintes informações antes de excluir funções de administração delegada ou clientes gerenciados de uma função.

### Excluindo funções

Na página **Administração delegada**, Super administradores incondicionais, você pode excluir quaisquer funções que tenham se tornado obsoletas.

A exclusão de uma função também remove todos os clientes que os administradores da função adicionaram à página Clientes. Após a função ser excluída, se esses clientes pertencerem a quaisquer redes, grupos ou domínios gerenciados por outras funções, serão regidos pela diretiva apropriada aplicada nessas funções (consulte [Ordem de filtragem, página 78](#)). Caso contrário, serão regidos pela diretiva Padrão do Super administrador.

1. Na página **Administração delegada**, marque a caixa de seleção ao lado de cada função que deseja excluir.



**Obs.:**

Você não pode excluir a função Super administrador.

---

2. Clique em **Excluir**.
3. Confirme a solicitação de exclusão para remover as funções selecionadas da página Administração delegada. As alterações só se tornarão permanentes quando você clicar em **Salvar tudo**.

A função excluída será apagada da lista suspensa Função no banner na próxima vez em que você fizer logon no Websense Manager.

### Excluindo clientes gerenciados

Os clientes não poderão ser excluídos diretamente da lista de clientes gerenciados (Administração delegada > Editar função) se:

- ◆ O administrador tiver aplicado uma diretiva ao cliente.
- ◆ O administrador tiver aplicado uma diretiva a um ou mais membros de uma rede, grupo, domínio ou unidade organizacional.

Também podem ocorrer problemas se, durante o logon do Websense Manager, o Super administrador escolher um Policy Server que não seja o que se comunica com o serviço de diretório que contém os clientes a serem excluídos. Nessa situação, o atual Policy Server e o serviço de diretório não reconhecem os clientes.

Um Super administrador incondicional pode garantir que os clientes apropriados sejam excluídos, conforme é descrito a seguir.

1. Faça logon no Websense Manager selecionando o Policy Server cujo serviço de diretório contém os clientes gerenciados a serem excluídos. Você precisa fazer logon com permissões de Super administrador incondicional.
2. Abra a lista **Função** no banner e selecione a função de onde os clientes gerenciados serão excluídos.

3. Vá para **Gerenciamento de diretivas > Clientes** para ver uma lista de todos os clientes a que o administrador delegado designou explicitamente uma diretiva. Isso pode incluir clientes que estão especificamente identificados na lista de clientes gerenciados para a função e clientes que são membros de redes, grupos, domínios ou unidades organizacionais na lista de clientes gerenciados.
4. Exclua os clientes apropriados.
5. Clique em **OK** para armazenar as alterações em cache.
6. Abra a lista **Função** no banner e selecione a função **Super administrador**.
7. Vá para **Gerenciamento de diretivas > Administração delegada > Editar função**.
8. Exclua os clientes apropriados da lista de clientes gerenciados e clique em **OK** para confirmar a solicitação de exclusão.
9. Clique em **OK** na página Editar função para armazenar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Vários administradores acessando o Websense Manager

Tópicos relacionados:

- ◆ [Introdução aos administradores](#), página 236
- ◆ [Habilitando o acesso ao Websense Manager](#), página 248

Administradores de diferentes funções podem acessar o Websense Manager ao mesmo tempo para realizar as atividades que as permissões de sua função permitam. Por exemplo, os administradores nas Funções A e B com permissões de diretiva podem fazer logon no Websense Manager ao mesmo tempo. Como gerenciam diferentes clientes, eles podem criar e aplicar diretivas sem conflito.

A situação é diferente quando administradores que têm permissões de diretiva na mesma função fazem logon ao mesmo tempo. Para preservar a integridade da estrutura de diretivas e atribuições, apenas um administrador de uma função pode acessar o Websense Manager com permissões de diretiva por vez. Se um segundo administrador com permissões de diretiva para a mesma função tentar fazer logon enquanto o primeiro administrador ainda estiver conectado, o segundo receberá uma opção.

- ◆ Fazer logon apenas para relatórios, caso tenha permissões de relatório.
- ◆ Fazer logon em outra função, caso esteja designado a outras funções.
- ◆ Tentar novamente mais tarde, depois que o primeiro administrador fizer logoff.

Quando administradores com permissões de diretiva e de relatório fazem logon para gerar relatórios, devem liberar imediatamente as permissões de diretiva para que outros administradores na função possam realizar atividades de gerenciamento de diretiva.

- ▶ Vá até a lista suspensa **Função** no banner e escolha **Liberar permissões da diretiva**.

Um método alternativo é criar uma conta de usuário do Websense (consulte [Contas de usuário do Websense, página 250](#)) para cada função e conceder a esse usuário somente permissões de relatório. Forneça essas credenciais de logon (nome de usuário e senha) a administradores na função que possuem tanto permissões de diretiva quanto de relatório. Quando os administradores precisam executar relatórios, podem fazer logon como administrador desse relatório, deixando o acesso à diretiva aberto para outro administrador.

## Definindo restrições de filtragem para todas as funções

---

Tópicos relacionados:

- ◆ [Introdução aos administradores, página 236](#)
- ◆ [Criando uma Proteção de filtro, página 265](#)

O software Websense permite que Super administradores incondicionais estabeleçam uma Proteção de filtro que bloqueie categorias e protocolos para todos os clientes gerenciados pelas funções de administração delegada. Consulte [Criando uma Proteção de filtro, página 265](#), para obter mais informações.

Os administradores dessas funções têm liberdade para aplicar qualquer ação de filtragem a outras categorias e protocolos em suas diretivas, mas categorias e protocolos bloqueados na Proteção de filtro não podem ser permitidos.

Assim que são salvas, as alterações feitas na Proteção de filtro são implementadas para todos os clientes gerenciados. Os administradores delegados que já estiverem trabalhando no Websense Manager quando as alterações entrarem em efeito só verão essas alterações na próxima vez em que fizerem logon.



**Obs.:**

Quando um filtro é copiado da função Super administrador para outra função, a cópia leva as restrições de Proteção de filtro.

---

Os Super administradores não são limitados pela Proteção de filtro. Eles podem definir diretivas que permitam acesso a categorias e protocolos bloqueados e protegidos para funções de administração delegada. Portanto, os usuários que precisarem de direitos de acesso especiais deverão ser gerenciados pela função Super administrador.

## Criando uma Proteção de filtro

Tópicos relacionados:

- ◆ [Definindo restrições de filtragem para todas as funções](#), página 264
- ◆ [Protegendo categorias](#), página 265
- ◆ [Protegendo protocolos](#), página 266

A página **Gerenciamento de diretivas > Proteção de filtro** dá a opção de editar categorias ou protocolos para protegê-los em todos os clientes gerenciados em funções de administração delegada. Qualquer recurso de uma categoria ou protocolo bloqueado na Proteção de filtro é considerado **protegido e bloqueado**.

- ◆ Clique no botão **Categorias** para bloquear e proteger categorias específicas ou elementos de categorias (palavras-chave e tipos de arquivos). Consulte [Protegendo categorias](#), página 265.
- ◆ Clique no botão **Protocolos** para bloquear e proteger protocolos ou um registro em log de protocolos. Consulte [Protegendo protocolos](#), página 266.

## Protegendo categorias

Tópicos relacionados:

- ◆ [Definindo restrições de filtragem para todas as funções](#), página 264
- ◆ [Criando uma Proteção de filtro](#), página 265
- ◆ [Protegendo protocolos](#), página 266

Utilize a página **Gerenciamento de diretivas > Proteção de filtro > Categorias** para selecionar as categorias a serem bloqueadas e protegidas para todos os membros de funções de administração delegada. Você também pode bloquear e proteger palavras-chave e tipos de arquivos de uma categoria.

1. Selecione uma categoria na árvore.

As funções de administração delegada não têm acesso a categorias personalizadas criadas pelos Super administradores. Por isso, as categorias personalizadas não aparecem nesta árvore.

2. Defina as restrições para essa categoria na caixa que aparece ao lado da árvore de categorias.

Opção	Descrição
Proteger categoria	Protege e bloqueia o acesso a sites dessa categoria.
Proteger palavras-chave	Protege e bloqueia o acesso com base nas palavras-chave definidas para essa categoria em cada função.

Opção	Descrição
Proteger tipos de arquivo	<p>Protege e bloqueia os tipos de arquivo selecionados para sites desta categoria.</p> <p>Certifique-se de marcar a caixa de seleção para cada tipo de arquivo a ser bloqueado e protegido.</p> <p>Os tipos de arquivo personalizados criados pelo Super administrador são incluídos nesta lista porque estão disponíveis para funções de administração delegada.</p>
Aplicar a subcategorias	Aplica as mesmas configurações a todas as subcategorias dessa categoria.

Você pode bloquear e proteger elementos selecionados para todas as categorias de uma vez, caso isso seja apropriado. Selecione **Todas as categorias** na árvore e escolha os elementos que deverão ser bloqueados para todas as categorias. Em seguida, clique em **Aplicar a subcategorias**.

- Quando terminar de fazer as alterações, clique em **OK** para armazená-las em cache e voltar à página Proteção de filtro. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Protegendo protocolos

Tópicos relacionados:

- ◆ [Definindo restrições de filtragem para todas as funções](#), página 264
- ◆ [Criando uma Proteção de filtro](#), página 265
- ◆ [Protegendo categorias](#), página 265

Utilize a página **Gerenciamento de diretivas > Proteção de filtro > Protocolos** para bloquear e proteger o acesso ou proteger o registro em log de protocolos selecionados para clientes gerenciados por funções de administração delegada.



### Obs.:

O registro em log de protocolo está associado a alertas de uso de protocolo. Você só pode gerar alertas de uso para um protocolo se ele estiver definido para registro em no mínimo um filtro de protocolo. A habilitação da opção **Proteger registro em log de protocolo** através da Proteção de filtro assegura que alertas de uso sejam gerados para o protocolo. Consulte [Configurando alertas de uso de protocolo](#), página 289.

- Selecione um protocolo na árvore.

As funções de administração delegada não têm acesso a protocolos personalizados criados pelos Super administradores. Por isso, os protocolos personalizados não aparecem nesta árvore.

2. Defina as restrições para esse protocolo na caixa que aparece ao lado da árvore de protocolos.

<b>Opção</b>	<b>Descrição</b>
Proteger protocolo	Bloqueia e protege o acesso a aplicativos e websites usando esse protocolo.
Proteger registro em log de protocolo	Registra informações sobre acesso a esse protocolo e impede que administradores delegados desabilitem o registro em log.
Aplicar ao grupo	Aplica as mesmas configurações a todos os protocolos no grupo.

3. Quando terminar de fazer as alterações, clique em **OK** para armazená-las em cache e voltar à página Proteção de filtro. As alterações só serão implementadas quando você clicar em **Salvar tudo**.



# 12

## Administração do Websense Server

Tópicos relacionados:

- ◆ *Componentes de produtos Websense*, página 270
- ◆ *Trabalhando com o Policy Server*, página 275
- ◆ *Exibindo e exportando o log de auditoria*, página 281
- ◆ *Parando e iniciando os serviços Websense*, página 283
- ◆ *Alertas*, página 284
- ◆ *Fazendo backup e restaurando dados do Websense*, página 292

A filtragem de uso da Internet requer interação entre vários componentes do software Websense:

- ◆ Solicitações do usuário para acesso à Internet são recebidas pelo Network Agent ou um produto de integração de terceiros.
- ◆ As solicitações são enviadas ao Websense Filtering Service para processamento.
- ◆ O Filtering Service comunica-se com o Policy Server e o Policy Broker para aplicar a diretiva apropriada em resposta à solicitação.

Na maioria dos ambientes, um único Policy Database armazena informações de clientes, filtros, diretivas e configurações gerais, não importa se há um Policy Server ou vários.

Cada instância do Websense Manager é associada a um único Policy Database e pode ser usada para configurar cada Policy Server associado a esse banco de dados.

Como a configuração de diretiva realizada no Websense Manager é armazenada no banco de dados central, as informações de diretivas são disponibilizadas automaticamente para todos os Policy Servers associados a esse Policy Database.

## Componentes de produtos Websense

---

Tópicos relacionados:

- ◆ [Componentes de filtragem](#), página 271
- ◆ [Componentes de relatório](#), página 273
- ◆ [Componentes de identificação de usuário](#), página 274
- ◆ [Trabalhando com o Policy Server](#), página 275
- ◆ [Parando e iniciando os serviços Websense](#), página 283
- ◆ [Verificando o status atual do sistema](#), página 291

O software Websense tem vários componentes que trabalham juntos para fornecer identificação de usuário, filtragem da Internet e recursos de geração de relatórios. Esta seção apresenta uma visão geral de cada componente para ajudar a entender e gerenciar o ambiente de filtragem.

Os principais componentes do Websense incluem:

- ◆ Policy Database
- ◆ Policy Broker
- ◆ Policy Server
- ◆ Filtering Service
- ◆ Network Agent
- ◆ Master Database
- ◆ Websense Manager
- ◆ Usage Monitor
- ◆ User Service
- ◆ Log Server
- ◆ banco de dados de log

O Websense também inclui agentes de identificação transparente que são opcionais:

- ◆ DC Agent
- ◆ RADIUS Agent
- ◆ eDirectory Agent
- ◆ Logon Agent

Os componentes adicionais opcionais incluem:

- ◆ Remote Filtering Server
- ◆ Remote Filtering Client
- ◆ Websense Content Gateway

## Componentes de filtragem

Componente	Descrição
<b>Policy Database</b>	Armazena informações de diretiva e configurações do software Websense.
<b>Policy Broker</b>	Gerencia as solicitações de informações de configurações gerais e diretivas dos componentes do Websense.
<b>Policy Server</b>	<ul style="list-style-type: none"> <li>• Identifica e monitora o local e o status de outros componentes do Websense.</li> <li>• Armazena informações de configuração específicas a uma instância do Policy Server.</li> <li>• Comunica os dados de configuração ao Filtering Service para que sejam usados na filtragem de solicitações da Internet.</li> </ul> <p>Defina as configurações do Policy Server no Websense Manager (consulte <a href="#">Trabalhando com o Policy Server</a>, página 275).</p> <p>A maioria do que é definido, inclusive para as diretivas, é compartilhado entre Policy Servers que têm um Policy Database comum (consulte <a href="#">Trabalhando em um ambiente com vários Policy Servers</a>, página 276).</p>
<b>Filtering Service</b>	<p>Oferece filtragem da Internet junto com o Network Agent ou um produto de integração de terceiros. Quando um usuário solicita um site, o Filtering Service recebe a solicitação e determina qual diretiva será aplicada.</p> <ul style="list-style-type: none"> <li>• O Filtering Service deve estar em execução para que as solicitações da Internet sejam filtradas e registradas em log.</li> <li>• Cada instância do Filtering Service faz download de sua própria cópia do Websense Master Database.</li> </ul> <p>Configure a filtragem e o comportamento do Filtering Service no Websense Manager (consulte <a href="#">Filtros de uso da Internet</a>, página 35, e <a href="#">Definindo configurações de filtragem do Websense</a>, página 54).</p>
<b>Network Agent</b>	<ul style="list-style-type: none"> <li>• Aprimora as funções de filtragem e registro em log</li> <li>• Permite o gerenciamento de protocolos</li> <li>• Permite a filtragem em um ambiente autônomo</li> </ul> <p>Para obter mais informações, consulte <a href="#">Configuração da rede</a>, página 337.</p>
<b>Master Database</b>	<ul style="list-style-type: none"> <li>• Inclui mais de 36 milhões de sites, classificados em mais de 90 categorias e subcategorias</li> <li>• Contém mais de 100 definições de protocolo para uso em protocolos de filtragem</li> </ul> <p>Faça download do Websense Master Database para ativar a filtragem da Internet e verificar se o banco de dados está atualizado. Se o Master Database tiver mais de duas semanas, não haverá filtragem. Consulte <a href="#">O Websense Master Database</a>, página 29, para obter mais informações.</p>

<b>Componente</b>	<b>Descrição</b>
<b>Websense Manager</b>	<p>Atua como a interface de configuração e gerenciamento para o software Websense.</p> <p>Use o Websense Manager para definir e personalizar as diretivas de acesso à Internet, adicionar ou remover clientes de filtragem, configurar componentes do software Websense e mais.</p> <p>Consulte <i>Trabalhando no Websense Manager</i>, página 14, para obter mais informações.</p>
<b>Usage Monitor</b>	<p>Ativa o sistema de alertas com base no uso da Internet.</p> <p>O Usage Monitor monitora o acesso a protocolos e categorias de URL, e gera mensagens de alerta de acordo com o comportamento de alerta configurado.</p> <p>Consulte <i>Alertas</i>, página 284, para obter mais informações.</p>
<b>Remote Filtering Client</b>	<ul style="list-style-type: none"><li>• Reside em máquinas clientes fora do firewall da rede.</li><li>• Identifica as máquinas como clientes a serem filtrados e comunica-se com o Remote Filtering Server.</li></ul> <p>Consulte <i>Filtrar Clientes Remotos</i>, página 155, para obter mais informações.</p>
<b>Remote Filtering Server</b>	<ul style="list-style-type: none"><li>• Permite a filtragem de clientes fora de um firewall de rede.</li><li>• Comunica-se com o Filtering Service para permitir o gerenciamento do acesso à Internet das máquinas remotas.</li></ul> <p>Consulte <i>Filtrar Clientes Remotos</i>, página 155, para obter mais informações.</p>
<b>Websense Content Gateway</b>	<ul style="list-style-type: none"><li>• Oferece uma plataforma robusta com cache e proxy.</li><li>• É capaz de analisar o conteúdo de arquivos e sites da Web em tempo real para categorizar sites ainda não categorizados.</li></ul> <p>Consulte <i>Análise de conteúdo com as opções em tempo real</i>, página 143.</p>
<b>Websense Security Gateway</b>	<p>Além da funcionalidade padrão do Websense Content Gateway:</p> <ul style="list-style-type: none"><li>• Analisa código HTML para detectar ameaças à segurança (por exemplo, phishing, redirecionamento de URLs, exploits na Web e proxy avoidance).</li><li>• Inspecciona o conteúdo dos arquivos para atribuir uma categoria de ameaça (por exemplo, vírus, cavalos de Tróia ou worms).</li><li>• Remove o conteúdo ativo de determinadas páginas da Web.</li></ul> <p>Consulte <i>Análise de conteúdo com as opções em tempo real</i>, página 143.</p>

## Componentes de relatório

Componente	Descrição
<b>Log Server</b>	<p>Registra dados de solicitações da Internet, inclusive:</p> <ul style="list-style-type: none"><li>• A origem da solicitação</li><li>• A categoria ou o protocolo associado à solicitação</li><li>• Se a solicitação foi permitida ou bloqueada</li><li>• Se o bloqueio de palavras-chave, o bloqueio de tipos de arquivo, as alocações de cota, os níveis de largura de banda ou a proteção por senha foram aplicados</li></ul> <p>Com o Network Agent e alguns produtos de integração, o Log Server também armazena informações sobre o volume de largura de banda utilizado.</p> <p>O Log Server deve ser instalado em uma máquina com Windows para ativar relatórios investigativos e de apresentação, e os gráficos das páginas Hoje e Histórico no Websense Manager.</p> <p>Após a instalação do Log Server, configure o Filtering Service para que passe dados de registro em log para o local correto (consulte <a href="#">Configurando o Filtering Service para registro em log</a>, página 304).</p>
<b>Log Database</b>	<p>Armazena dados de solicitações da Internet coletados pelo Log Server para uso pelas ferramentas de relatório do Websense.</p>

## Componentes de identificação de usuário

Componente	Descrição
<b>User Service</b>	<ul style="list-style-type: none"> <li>• Comunica-se com o serviço de diretório.</li> <li>• Transmite informações relacionadas ao usuário, incluindo relacionamentos do usuário com o grupo e do usuário com o domínio, para o Policy Server e o Filtering Service, para serem usadas na aplicação das diretivas de filtragem.</li> </ul> <p>Se você instalou e configurou um agente de identificação transparente do Websense (consulte <a href="#">Identificação transparente</a>, página 199), o User Service ajudará a interpretar as informações da sessão de logon do usuário e usará essas informações para fornecer associações entre nomes de usuário e endereços IP ao Filtering Service.</p> <p>Quando você adiciona usuários e grupos como clientes Websense (consulte <a href="#">Adicionando um cliente</a>, página 66), o User Service fornece informações de nome e caminho do serviço de diretório ao Websense Manager.</p> <p>Para obter informações sobre como configurar o acesso ao serviço de diretório, consulte <a href="#">Serviços de diretório</a>, página 60.</p>
<b>DC Agent</b>	<ul style="list-style-type: none"> <li>• Oferece identificação transparente para os usuários em um serviço de diretório do Windows.</li> <li>• Comunica-se com o User Service para fornecer informações atualizadas sobre a sessão de logon do usuário ao software Websense para filtragem.</li> </ul> <p>Para obter mais informações, consulte <a href="#">DC Agent</a>, página 211.</p>
<b>Logon Agent</b>	<ul style="list-style-type: none"> <li>• Garante precisão incomparável na identificação transparente do usuário em redes Linux e Windows.</li> <li>• Não precisa de um serviço de diretório ou outro intermediário ao capturar sessões de logon do usuário.</li> <li>• Detecta as sessões de logon do usuário quando elas ocorrem.</li> </ul> <p>O Logon Agent comunica-se com o aplicativo de logon em máquinas clientes para garantir que sessões de logon do usuário específicas sejam capturadas e processadas diretamente pelo Websense.</p> <p>Para obter mais informações, consulte <a href="#">Logon Agent</a>, página 214.</p>
<b>eDirectory Agent</b>	<ul style="list-style-type: none"> <li>• Trabalha com o Novell eDirectory para identificar os usuários com transparência.</li> <li>• Coleta informações de sessão de logon do usuário do Novell eDirectory, que autentica os usuários que se conectam à rede.</li> <li>• Associa cada usuário autenticado a um endereço IP e, em seguida, trabalha com o User Service para fornecer as informações ao Filtering Service.</li> </ul> <p>Para obter mais informações, consulte <a href="#">eDirectory Agent</a>, página 222.</p>
<b>RADIUS Agent</b>	<p>Permite a identificação transparente dos usuários que usam uma linha discada, rede virtual privada (VPN), conexão DSL ou outra conexão remota para acesso à rede.</p> <p>Para obter mais informações, consulte <a href="#">RADIUS Agent</a>, página 217.</p>

## Entendendo o Policy Database

---

O Websense Policy Database armazena dados de diretiva (incluindo configurações de clientes, filtros, componentes de filtro e administração delegada) e configurações globais especificadas no Websense Manager. As configurações específicas a uma única instância do Policy Server são armazenadas separadamente.

Em quase todos os ambientes com vários Policy Servers, um único Policy Database contém os dados de configurações gerais e de diretivas para os vários Policy Servers.

1. Na inicialização, cada componente do Websense solicita informações de configuração aplicáveis ao Policy Database através do Policy Broker.
2. Os componentes em execução buscam com frequência alterações no Policy Database.
3. O Policy Database é atualizado toda vez que os administradores fazem alterações no Websense Manager e clicam em Salvar tudo.
4. Após uma alteração no Policy Database, cada componente solicita e recebe as alterações que afetam seu funcionamento.

Faça backup do Policy Database com regularidade para proteger informações importantes sobre configurações e diretivas. Consulte [Fazendo backup e restaurando dados do Websense, página 292](#), para obter mais informações.

## Trabalhando com o Policy Server

---

O Policy Server é o componente do software Websense que gerencia informações de diretiva e se comunica com o Filtering Service para ajudar na aplicação de diretivas. O Policy Server também é responsável por identificar outros componentes e monitorar sua localização e seu status.

Ao fazer logon no Websense Manager, você se conecta a uma interface gráfica com o Policy Server.

- ◆ Não é possível fazer logon no Websense Manager até ele estar configurado para se comunicar com o Policy Server.
- ◆ Se a instalação do seu software Websense incluir vários Policy Servers, você poderá escolher a instância do Policy Server no momento do logon.
- ◆ Você pode adicionar e remover instâncias do Policy Server no Websense Manager.

Por padrão, a comunicação entre o Websense Manager e uma instância central do Policy Server é estabelecida durante a instalação do Websense Manager.

A maioria dos ambientes requer somente um Policy Server. Um único Policy Server pode se comunicar com várias instâncias do Filtering Service e do Network Agent para balanceamento de carga. Entretanto, em organizações de grande porte (mais de 10.000 usuários), pode ser útil instalar várias instâncias do Policy Server. Se você

instalar Policy Servers extras, adicione cada instância ao Websense Manager (consulte [Adicionando e editando instâncias do Policy Server](#), página 276).

## Adicionando e editando instâncias do Policy Server

Use a página **Configurações > Policy Server** para adicionar as instâncias do Policy Server ao Websense Manager ou para configurar ou remover Policy Servers existentes.

Para adicionar uma instância do Policy Server:

1. Clique em **Adicionar**. A página Adicionar Policy Server será exibida.
2. Insira o endereço IP ou o nome de host da máquina com o Policy Server no campo **Nome ou IP do servidor**.
3. Especifique a **Porta** que o Websense Manager deve usar para se comunicar com essa instância do Policy Server. O padrão é **55806**.
4. Clique em **OK** para voltar à página do Policy Server. A nova instância do Policy Server aparece na lista.
5. Clique em **OK** para salvar todas as alterações em cache na página dos Policy Servers. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Para editar uma instância do Policy Server (por exemplo, se o nome ou o endereço IP da máquina com o Policy Server for alterado), selecione um endereço IP ou um nome de host na lista de Policy Servers e clique em **Editar**.

Para excluir uma instância do Policy Server, selecione um endereço IP ou um nome de host na lista de Policy Servers e clique em **Excluir**. Quando clica em Excluir, você remove a instância do Policy Server do Websense Manager, mas não desinstala ou pára o serviço Websense Policy Server. Se houver apenas uma instância do Policy Server listada, não será possível excluí-la.

## Trabalhando em um ambiente com vários Policy Servers

Em alguns ambientes distribuídos com um grande número de usuários, pode ser aconselhável instalar vários Policy Servers. Essa situação requer algumas considerações especiais.

- ◆ Se você implementar uma configuração que permita que o mesmo cliente seja gerenciado por diversos Policy Servers, dependendo da carga atual, **não** implemente ações de diretivas baseadas em tempo:
  - Acesso com senha
  - Confirmar
  - Cota

As informações de tempo associadas a esses recursos não são compartilhadas entre os Policy Servers e é possível que seja concedido aos clientes mais ou menos acesso à Internet do que você pretendia.

Lembre-se de que a diretiva Padrão é aplicada sempre que nenhuma outra diretiva se aplica ao cliente. Se os clientes podem ser regidos por mais de um Policy Server, convém verificar se a diretiva Padrão não utiliza filtros de categoria que aplicam ações baseadas em tempo.

- ◆ Como as informações de diretiva são armazenadas no Policy Database, as alterações realizadas nas diretivas são compartilhadas automaticamente entre todos os Policy Servers quando você clica em **Salvar tudo**.
- ◆ Muitas configurações globais (como definições de classe de risco e opções de alerta) também são compartilhadas entre os Policy Servers.
- ◆ As configurações que são específicas a um único Policy Server (como as respectivas conexões do Filtering Service e Network Agent) são armazenadas localmente por cada Policy Server, e não distribuídas.

Para alternar entre Policy Servers no Websense Manager a fim de verificar ou definir configurações aplicáveis a uma única instância do Policy Server:

1. No banner do Websense, expanda a lista **Policy Server** e selecione um endereço IP.
2. Se houver alguma alteração não salva na instância atual do Policy Server, será exibida uma lista de alterações. Use um dos seguintes métodos:
  - Clique em **Salvar tudo e fazer logout** para salvar as alterações e fazer logout no Policy Server atual.
  - Clique em **Cancelar alterações e fazer logout** para abandonar as alterações e fazer logout no Policy Server atual.
  - Clique em **Voltar** para continuar a configurar o Policy Server atual.

Se houver alterações que não foram salvas, você será direcionado para a tela de logon.
3. Na tela de logon, insira um nome de usuário e uma senha para se conectar ao Policy Server selecionado e clique em **Logon**.

## Alterando o endereço IP do Policy Server

Antes de alterar o endereço IP da máquina com o Policy Server, **pare todos os serviços Websense** na máquina. Se o Websense Manager também estiver instalado na máquina, isso inclui os serviços Apache2Websense e ApacheTomcatWebsense.

Após a alteração do endereço IP, você deve atualizar manualmente os arquivos de configuração do Websense usados por Websense Manager, Policy Server e outros serviços Websense antes de prosseguir a filtragem.

### Etapa 1: Atualizar a configuração do Websense Manager

Atualize o Websense Manager para usar o novo endereço IP para se conectar ao Policy Server.

1. Na máquina com Websense Manager, pare os serviços **Apache2Websense** e **ApacheTomcatWebsense** (se necessário).

Se o Websense Manager e o Policy Server estiverem instalados na mesma máquina, os serviços Apache já devem estar interrompidos.

2. Navegue até o seguinte diretório:
  - Windows:  
C:\Arquivos de Programas\Websense\tomcat\conf\Catalina\localhost\
  - Linux:  
/opt/Websense/tomcat/conf/Catalina/localhost/
3. Localize o arquivo **mng.xml** e faça backup desse arquivo em outro diretório.
4. Abra **mng.xml** em um editor de texto (como Bloco de notas ou vi) e substitua cada instância do antigo endereço IP do Policy Server pelo novo.  
O endereço IP do Policy Server aparece duas vezes: como o valor **ps/default/host** e o valor **psHosts**.
5. Quando terminar, salve e feche o arquivo.

Não reinicie os serviços Apache até ter concluído as demais atualizações de configuração nesta seção.

## Etapa 2: Atualizar a configuração do Policy Server

Atualize o arquivo de configuração do Policy Server e o arquivo de inicialização usado para configurar a comunicação entre os componentes do Websense.

1. Se você ainda não fez isso, pare todos os serviços Websense na máquina com o Policy Server (consulte [Parando e iniciando os serviços Websense](#), página 283).
2. Navegue até o diretório **bin** do Websense.
  - Windows:  
C:\Arquivos de Programas\Websense\bin
  - Linux  
/opt/Websense/bin
3. Localize o arquivo **config.xml** e faça backup desse arquivo em outro diretório.
4. Abra **config.xml** em um editor de texto e substitua cada instância do antigo endereço IP do Policy Server pelo novo.
5. Quando terminar, salve e feche o arquivo.
6. No diretório **bin**, localize o arquivo **websense.ini** e faça backup em outro diretório.
7. Abra **websense.ini** em um editor de texto e substitua cada instância do antigo endereço IP do Policy Server pelo novo.
8. Quando terminar, salve e feche o arquivo.

## Etapa 3: Verificar a conexão do banco de dados de log

Use o administrador da fonte de dados ODBC do Windows na máquina com o Policy Server para verificar a conexão do ODBC com o banco de dados de log.

1. Vá para **Iniciar > Configurações > Painel de controle > Ferramentas administrativas > Fontes de dados (ODBC)**.

2. Na guia **DSN de sistema**, selecione o nome da fonte de dados apropriada (por padrão, **wslogdb70**) e clique em **Configurar**.
3. Verifique se a máquina com o servidor de banco de dados correta está selecionada e clique em **Avançar**.
4. Insira as credenciais usadas para conexão com o banco de dados e clique em **Avançar**.
5. Aceite os padrões nas duas telas seguintes e clique em **Testar fonte de dados**.

**Obs.:**

Se o teste falhar, verifique o nome da máquina do servidor de banco de dados e tente novamente.

Se o nome da máquina estiver correto e o teste falhar, verifique se a porta de conexão correta está sendo usada e se o firewall permite comunicação na porta selecionada.

#### Etapa 4: Reiniciar os serviços Websense

1. Reinicie a máquina com o Policy Server. Verifique se todos os serviços Websense da máquina são reiniciados normalmente.
2. Se o Websense Manager usado para configurar esse Policy Server estiver instalado em outra máquina, reinicie os serviços **Apache2Websense** e **ApacheTomcatWebsense** nessa máquina.

**Obs.:**

Se o Websense Manager estiver instalado na mesma máquina do Policy Server, os administradores deverão usar o novo endereço IP para logon.

## Trabalhando com o Filtering Service

O Filtering Service é o componente do Websense que trabalha com o Network Agent ou um produto de integração de terceiros para filtrar atividades na Internet. Quando um usuário solicita um site, o Filtering Service recebe a solicitação, determina qual diretiva aplicar e usa a diretiva aplicável para determinar como o site será filtrado.

Cada instância do Filtering Service faz download de sua própria cópia do Websense Master Database para determinar como filtrar as solicitações da Internet.

O Filtering Service também envia informações sobre atividades da Internet para o Log Server, para que possam ser registradas e usadas em relatórios.

Quando você faz logon no Websense Manager, um **Resumo do Filtering Service** na página Status > Hoje indica o endereço IP e o status atual de cada instância do Filtering Service associada ao Policy Server em questão. Clique no endereço IP de um Filtering Service para obter informações mais detalhadas sobre o Filtering Service selecionado.

## Verificar detalhes do Filtering Service

Use a página **Status > Hoje > Detalhes do Filtering Service** para verificar o status de uma instância específica do Filtering Service.

A página informa:

- ◆ O endereço IP do Filtering Service
- ◆ Se a instância selecionada está em execução
- ◆ A versão do Filtering Service  
Essa informação deve corresponder à versão do software Websense, incluindo os hotfixes aplicados.
- ◆ O sistema operacional em execução na máquina com o Filtering Service
- ◆ A plataforma do software Websense  
Isso indica se o software Websense está em execução em modo autônomo ou integrado com um produto de terceiros.
- ◆ O endereço IP e o status de qualquer instância do Network Agent com que o Filtering Service se comunica.

Clique em **Fechar** para voltar à página Hoje.

## Verificar o status de download do Master Database

Cada instância do Filtering Service na rede faz download de sua própria cópia do Master Database. Quando você trabalha no Websense Manager, o Resumo do alerta de saúde, na página **Status > Hoje**, exibe uma mensagem de status quando há algum download do Master Database em andamento ou se alguma tentativa de download falhar.

Para obter informações detalhadas sobre downloads de banco de dados recentes ou em andamento, clique em **Download do banco de dados** na barra de ferramentas da página Hoje. A página Download do banco de dados inclui uma entrada para cada instância do Filtering Service associada ao atual Policy Server.

Inicialmente, a página Download do banco de dados exibe um resumo do download, indicando onde ocorreu o download do banco de dados, de qual versão do banco de dados foi feito download e se o download foi bem-sucedido. Nessa exibição resumida, é possível:

- ◆ Iniciar um download de banco de dados para um único Filtering Service (clique em **Atualizar**).
- ◆ Iniciar downloads de banco de dados para todas as instâncias do Filtering Service listadas (clique em **Atualizar tudo**).
- ◆ Cancelar uma ou mais atualizações em andamento.

Clique em um endereço IP na lista à direita para verificar o status mais detalhado do download do banco de dados do Filtering Service selecionado.

- ◆ Se o Filtering Service teve problemas de download, poderá ser exibida uma recomendação para solucionar o problema.
- ◆ Para iniciar manualmente um download de banco de dados para o Filtering Service selecionado (clique em **Atualizar**).

Durante o download do banco de dados, a tela de status mostra informações detalhadas do progresso de cada etapa do processo de download. Clique em **Fechar** para ocultar as informações de progresso e continuar a trabalhar no Websense Manager.

## Downloads do Master Database que podem ser retomados

Se um download do Master Database for interrompido, o Websense tentará continuar o download automaticamente. Se o Filtering Service puder se reconectar ao servidor de download, o download continuará de onde foi interrompido.

Você pode reiniciar manualmente um download que tenha falhado ou que tenha sido interrompido. Com isso, o download não continua do ponto de interrupção; o processo recomeça desde o início.

1. No Websense Manager, vá para **Status >Hoje** e clique em **Downloads do banco de dados**.
2. Clique em **Parar todas as atualizações** para parar o processo interrompido.
3. Selecione uma instância do Filtering Service e clique em **Atualizar** ou em **Atualizar tudo** para reiniciar o processo de download desde o início.

## Exibindo e exportando o log de auditoria

---

O Websense fornece uma trilha de auditoria que mostra os administradores que acessaram o Websense Manager, bem como todas as alterações feitas nas diretivas e configurações. Essas informações estão disponíveis somente para os Super administradores que têm permissões de diretivas (consulte [Super administradores, página 237](#)).

Os administradores delegados têm controle significativo sobre as atividades da Internet de seus clientes gerenciados. O monitoramento das alterações pelo log de auditoria permite garantir que esse controle seja utilizado com responsabilidade e de acordo com as diretivas de uso aceitável da organização.

Use a página **Status > Log de auditoria** para exibir o log de auditoria e exportar os trechos selecionados para uma planilha do Excel (XLS), se desejado.

Os registros de auditoria são salvos por 60 dias. Para manter os registros de auditoria por mais de 60 dias, use a opção de exportação para exportar o log regularmente. A exportação não remove os registros do log de auditoria.

Quando a página Log de auditoria é aberta, os registros mais recentes são exibidos. Use a barra de rolagem e os botões de paginação acima do log para exibir registros mais antigos.

O log exibe as informações a seguir. Se um item estiver truncado, clique na entrada parcial para exibir o registro inteiro na caixa de diálogo pop-up.

Coluna	Descrição
Data	Data e hora da alteração, ajustada para os fusos horários. Para garantir a consistência dos dados no log de auditoria, todas as máquinas que executam componentes do Websense devem ter as configurações de data e hora sincronizadas.
Usuário	Nome de usuário do administrador que fez a alteração.
Servidor	Endereço IP ou nome da máquina que executa o Policy Server afetado pela alteração. Aparece somente para as alterações que afetam o Policy Server, como as realizadas na guia Configurações.
Função	Função de administração delegada afetada pela alteração. Quando uma alteração afeta um cliente explicitamente atribuído como um cliente gerenciado na função do administrador delegado, essa alteração parece afetar a função de Super administrador. Se a alteração afeta um cliente que é membro de um intervalo de rede, um grupo, um domínio ou uma unidade organizacional que foram atribuídos à função, a alteração afeta a função do administrador delegado.
Tipo	Elemento de configuração que foi alterado, como diretiva, filtro de categoria ou logon/logoff.
Elemento	Identificador do objeto específico alterado, como nome da função ou nome do filtro de categoria.
Ação	Tipo de alteração feita, como adicionar, excluir, alterar, fazer logon e assim por diante.
Anterior	Valor antes da alteração.
Atual	Novo valor após a alteração.

Nem todos os itens são exibidos para todos os registros. Por exemplo, a função não é exibida para os registros de logon e logoff.

Para exportar registros do log de auditoria:

1. Selecione um período de tempo na lista **Exportar intervalo**.  
Escolha **Últimos 60 dias** para exportar o arquivo de log de auditoria inteiro.
2. Clique em **Ir**.  
Se o Microsoft Excel estiver instalado na máquina que executa o Websense Manager, o arquivo exportado será aberto. Use as opções do Excel para salvar ou imprimir o arquivo.  
Se o Microsoft Excel não estiver instalado na máquina que executa o Websense Manager, siga as instruções na tela para localizar o software ou salvar o arquivo.

## Parando e iniciando os serviços Websense

Os serviços Websense são configurados para iniciar toda vez que a máquina reinicia. Entretanto, em alguns casos, é preciso parar ou iniciar um ou mais componentes do produto separadamente de um reinício da máquina.

**Obs.:**

Se o Filtering Service estiver no processo de fazer download do Master Database, só pára quando o download estiver concluído.

Quando você pára todos os serviços Websense, sempre termina com os seguintes serviços (na ordem exibida):

1. Websense Policy Server
2. Websense Policy Broker
3. Websense Policy Database

Lembre-se de que é raramente necessário reiniciar o Policy Broker ou o Policy Database, a não ser que haja um problema específico nesses serviços. Sempre que possível, evite reiniciar esses serviços.

Quando você inicia todos os serviços Websense, os seguintes serviços são iniciados (na ordem exibida):

1. Websense Policy Database
2. Websense Policy Broker
3. Websense Policy Server

### Windows

1. Abra a caixa de diálogo Serviços do Windows (**Iniciar > Configurações > Painel de controle > Ferramentas administrativas > Serviços**).
2. Clique com o botão direito no nome do serviço Websense e selecione **Parar** ou **Iniciar**.

### Linux

Nas máquinas com Linux, todos os serviços param e iniciam juntos quando você adota esse procedimento.

1. Vá para o diretório **/opt/Websense**.
2. Verifique o status dos serviços Websense com o comando:
  - `./WebsenseAdmin status`
3. Pare, inicie ou reinicie todos os serviços Websense com os comandos:
  - `./WebsenseAdmin stop`
  - `./WebsenseAdmin start`

- `./WebsenseAdmin restart`



**Aviso**

Não use o comando **kill** para parar um serviço Websense, pois ele pode corromper o serviço.

---

## Alertas

---

Tópicos relacionados:

- ◆ [Controle de inundação, página 285](#)
- ◆ [Configurando opções de alertas gerais, página 285](#)
- ◆ [Configurando alertas do sistema, página 287](#)
- ◆ [Configurando alertas de uso de categoria, página 288](#)
- ◆ [Configurando alertas de uso de protocolo, página 289](#)

Para facilitar o monitoramento e o gerenciamento do software Websense e das atividades do cliente na Internet, os Super administradores podem configurar alertas para serem enviados quando eventos selecionados ocorrerem.

- ◆ **Alertas do sistema:** Notificação sobre o status da assinatura e atividade do Master Database.
- ◆ **Alertas de uso:** Notificação quando a atividade da Internet para determinadas categorias ou protocolos atinge limites configurados.

Os alertas podem ser enviados para destinatários selecionados por e-mail, mensagens pop-up na tela (mensagens **net send** do Windows) ou mensagens SNMP.



**Obs.:**

Alertas pop-up na tela não podem ser enviados para máquinas com Linux. Contudo, podem ser enviados de uma máquina com Linux que execute o Policy Server para máquinas com Windows, desde que o cliente Samba esteja instalado na máquina com Linux. Consulte o *Guia de Implantação*.

---

Os alertas de uso podem ser gerados para protocolos ou categorias definidos pelo Websense ou personalizados.

## Controle de inundação

Tópicos relacionados:

- ◆ [Alertas, página 284](#)
- ◆ [Configurando opções de alertas gerais, página 285](#)
- ◆ [Configurando alertas de uso de categoria, página 288](#)
- ◆ [Configurando alertas de uso de protocolo, página 289](#)

Existem controles incorporados para os alertas de uso para evitar que eles gerem mensagens em excesso. Use a configuração **Máximo de alertas diários por tipo de uso** para especificar um limite para o número de alertas enviados em resposta a solicitações de determinados protocolos e categorias pelo usuário. Consulte [Configurando opções de alertas gerais, página 285](#), para obter mais informações.

Você também pode definir limites para cada alerta de uso de categoria e protocolo. Por exemplo, se você definir um limite de 10 para uma categoria, será gerado um alerta após 10 solicitações para essa categoria (por qualquer combinação de clientes). Consulte [Configurando alertas de uso de categoria, página 288](#), e [Configurando alertas de uso de protocolo, página 289](#), para obter mais informações.

Suponha que a configuração máxima para os alertas diários seja 20 e que o limite do alerta da categoria seja 10. Os administradores só receberão alertas sobre as primeiras 20 solicitações de categoria que excederem o limite. Isso significa que somente as primeiras 200 instâncias resultam em mensagens de alerta (o limite de 10 multiplicado pelo limite de 20 para os alertas).

## Configurando opções de alertas gerais

Tópicos relacionados:

- ◆ [Alertas, página 284](#)
- ◆ [Configurando alertas do sistema, página 287](#)
- ◆ [Configurando alertas de uso de categoria, página 288](#)
- ◆ [Configurando alertas de uso de protocolo, página 289](#)

O software Websense pode notificar os administradores sobre vários tipos de eventos do sistema, como atualizações de categorias do Master Database e problemas de assinatura, bem como o uso da Internet que exceda os limites definidos.

Use a página **Configurações > Alertas e notificações > Alertas** para selecionar e configurar os métodos de notificação desejados, como descrito abaixo. Use então as outras páginas na seção Configurações > Alertas e notificações para ativar os alertas que você deseja receber.

1. Insira um número no campo **Máximo de alertas diários por tipo de uso** para limitar o número total de alertas gerados diariamente para cada alerta de uso de categoria e protocolo.

Por exemplo, você pode configurar os alertas de uso para que sejam enviados a cada cinco solicitações (limite) de um site da categoria Esportes. Dependendo do número de usuários e respectivos padrões de uso da Internet, poderão ser gerados centenas de alertas todos os dias.

Se você inserir 10 como o máximo de alertas diários por tipo de uso, somente dez mensagens de alerta serão geradas a cada dia para a categoria Esportes. No exemplo, essas mensagens alertam sobre as primeiras 50 solicitações de sites de Esportes (5 solicitações de alerta multiplicadas por 10 alertas).

2. Marque a caixa de seleção **Habilitar alertas por e-mail** para enviar alertas e notificações por e-mail. Em seguida, defina essas configurações de e-mail.

IP ou nome do servidor SMTP	Endereço IP ou nome do servidor SMTP pelo qual os alertas de e-mail devem ser roteados.
Do endereço de e-mail	Endereço de e-mail a ser usado como o remetente dos alertas.
Endereço de e-mail do administrador (Para)	Endereço de e-mail do destinatário principal dos alertas de e-mail.
Endereços de e-mail dos destinatários (Cc)	Endereço de e-mail para até 50 destinatários adicionais. Cada endereço deve estar em uma linha separada.

3. Marque a caixa de seleção **Ativar alertas pop-up** para exibir mensagens pop-up em computadores específicos. Em seguida, insira o endereço IP ou o nome da máquina para até 50 **Destinatários**, cada um em uma linha separada.



**Obs.:**

Alertas pop-up não podem ser enviados a máquinas com Linux. Contudo, podem ser enviados de uma máquina com Linux que execute o Policy Server para máquinas com Windows, desde que o cliente Samba esteja instalado na máquina com Linux. Consulte o *Guia de Implantação*.

4. Marque a caixa de seleção **Habilitar alertas SNMP** para que as mensagens de alerta sejam enviadas por um sistema de interceptação SNMP instalado na rede. Em seguida, forneça informações sobre o seu sistema de interceptação SNMP.

Nome da comunidade	Nome da comunidade de interceptação no servidor de interceptação SNMP.
IP ou nome do servidor	Endereço IP ou nome do servidor de interceptação SNMP.
Porta	Número da porta que as mensagens SNMP usam.

5. Quando terminar, clique em **OK** para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Configurando alertas do sistema

Tópicos relacionados:

- ◆ [Alertas](#), página 284
- ◆ [Configurando opções de alertas gerais](#), página 285
- ◆ [Verificando o status atual do sistema](#), página 291

O Websense Manager exibe informações detalhadas de status e saúde do sistema na página **Status > Alertas** (informações detalhadas), descrita em [Verificando o status atual do sistema](#), página 291.

Para garantir que os administradores sejam notificados sobre eventos do sistema significativos, como uma falha de download de um banco de dados ou uma assinatura que está prestes a expirar, quando eles não estiverem conectados ao Websense Manager, configure os alertas do sistema Websense para que sejam distribuídos por e-mail, mensagem pop-up ou sistema de interceptação SNMP.

Na guia Configurações, use a página **Alertas e notificações > Sistema** para selecionar o método usado para enviar esses alertas aos administradores do Websense, bem como quais alertas serão enviados.

1. Para cada alerta, marque os métodos de entrega a serem usados. Dependendo dos métodos que forem ativados na página Alertas, você poderá escolher **E-mail**, **Pop-up** e **SNMP**.



**Obs.:**

Além de gerar um alerta, as informações sobre falhas de download do Master Database e níveis de assinatura excedidos são registradas no Windows Event Viewer (Windows somente) e no arquivo Websense.log (Windows e Linux).

Os alertas estão disponíveis para eventos como:

- Sua assinatura expira em uma semana.
  - Os mecanismos de pesquisa suportados pelo Search Filtering foram alterados.
  - Falha em um download do Websense Master Database.
  - Uma categoria ou um protocolo foi adicionado ao Master Database ou removido do Master Database.
  - O número atual de usuários excedeu o seu nível de assinatura.
  - O número de usuários alcançou 90% do seu nível de assinatura.
  - Sua assinatura expira em um mês.
  - O Websense Master Database foi atualizado.
2. Quando terminar, clique em **OK** para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Configurando alertas de uso de categoria

Tópicos relacionados:

- ◆ [Alertas, página 284](#)
- ◆ [Controle de inundação, página 285](#)
- ◆ [Configurando opções de alertas gerais, página 285](#)
- ◆ [Adicionando alertas de uso de categoria, página 288](#)

O software Websense pode notificar você quando a atividade da Internet para determinadas categorias de URL atingir um limite definido. Você pode definir alertas para solicitações permitidas ou bloqueadas da categoria.

Por exemplo, você pode ser alertado toda vez que houver permissão para 50 solicitações de sites na categoria Compras, para poder decidir se serão aplicadas restrições a essa categoria. Ou você pode definir que receberá um alerta toda vez que 100 solicitações de sites na categoria Entretenimento forem bloqueadas, para verificar se os usuários estão se adaptando a uma nova diretiva de uso da Internet.

Na guia Configurações, use a página **Alertas e notificações > Uso de categorias** para ver os alertas que já foram estabelecidos e adicionar ou excluir categorias de alertas de uso.

1. Exiba as listas **Alertas de uso de categorias permitidas** e **Alertas de uso de categorias bloqueadas** para saber quais categorias estão configuradas para alertas, o limite de cada uma e os métodos de alerta selecionados.
2. Clique em **Adicionar** abaixo da lista apropriada para abrir a página Adicionar alertas de uso de categorias (consulte [Adicionando alertas de uso de categoria, página 288](#)) e configurar categorias de URL adicionais para alertas.
3. Marque a caixa de seleção de todas as categorias que você deseja excluir da lista e clique em **Excluir** na lista apropriada.
4. Quando terminar, clique em **OK** para salvar as alterações em cache e voltar à página Alertas de uso de categorias. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Adicionando alertas de uso de categoria

Tópicos relacionados:

- ◆ [Alertas, página 284](#)
- ◆ [Configurando opções de alertas gerais, página 285](#)
- ◆ [Configurando alertas de uso de categoria, página 288](#)

A página **Adicionar alertas de uso de categorias** aparece quando você clica em Adicionar na página Alertas de uso de categorias. Aqui, você pode selecionar novas

categorias para alertas de uso, estabelecer o limite desses alertas e selecionar os métodos de alerta.

1. Marque a caixa de seleção ao lado de cada categoria a ser adicionada com o mesmo limite e métodos de alerta.



**Obs.:**

Não é possível adicionar alertas de uso para qualquer categoria que esteja excluída do registro em log. Consulte [Configurando o Filtering Service para registro em log](#), página 304.

2. Para definir o **Limite**, selecione o número de solicitações que geram um alerta.
3. Marque a caixa de seleção para cada método de alerta desejado (**E-mail, Pop-up, SNMP**) para essas categorias.  
Somente os métodos de alerta que foram ativados na página Alertas (consulte [Configurando opções de alertas gerais](#), página 285) estarão disponíveis para seleção.
4. Clique em **OK** para salvar suas alterações em cache e voltar à página Alertas de uso de categorias (consulte [Configurando alertas de uso de categoria](#), página 288). As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Configurando alertas de uso de protocolo

Tópicos relacionados:

- ◆ [Alertas](#), página 284
- ◆ [Controle de inundação](#), página 285
- ◆ [Configurando opções de alertas gerais](#), página 285
- ◆ [Adicionando alertas de uso de protocolo](#), página 290

O software Websense pode notificar você quando a atividade da Internet de determinado protocolo atingir um limite definido. Você pode definir alertas para solicitações permitidas ou bloqueadas do protocolo selecionado.

Por exemplo, você pode ser alertado toda vez que forem permitidas 50 solicitações de determinado protocolo de mensagens instantâneas, para decidir se serão aplicadas restrições a esse protocolo. Ou você pode definir que receberá um alerta toda vez que 100 solicitações de determinado protocolo de compartilhamento de arquivos P2P forem bloqueadas, para verificar se os usuários estão se adaptando a uma nova diretiva de uso da Internet.

Na guia Configurações, use a página **Alertas e notificações > Alertas de uso de protocolos** para ver os alertas que já foram definidos, e adicionar ou excluir protocolos de alertas de uso.

1. Exiba as listas **Alertas de uso de protocolos permitidos** e **Alertas de uso de protocolos bloqueados** para saber quais protocolos estão configurados para alertas, o limite de cada um e os métodos de alerta selecionados.
2. Clique em **Adicionar** abaixo da lista apropriada para abrir a página Adicionar alertas de uso de protocolos (consulte [Adicionando alertas de uso de protocolo, página 290](#)) e configurar protocolos adicionais para alertas.
3. Marque a caixa de seleção de todos os protocolos que deseja excluir e clique em **Excluir** na lista apropriada.
4. Quando terminar, clique em **OK** para salvar as alterações em cache e voltar à página Alertas de uso de protocolos. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Adicionando alertas de uso de protocolo

Tópicos relacionados:

- ◆ [Alertas, página 284](#)
- ◆ [Configurando opções de alertas gerais, página 285](#)
- ◆ [Configurando alertas de uso de protocolo, página 289](#)

Use a página **Alertas de uso de protocolos > Adicionar protocolo Alertas de uso** para selecionar novos protocolos para alertas de uso, definir o limite desses alertas e selecionar os métodos de alerta.

1. Marque a caixa de seleção ao lado de cada protocolo a ser adicionado com o mesmo limite e métodos de alerta.



**Obs.:**

Não é possível selecionar um protocolo para alerta se não estiver configurado para registrar em log um ou mais filtros de protocolo.

Os alertas de protocolo refletem apenas o uso pelos clientes regidos por um filtro que registra o protocolo.

2. Para definir o **Limite**, selecione o número de solicitações que geram um alerta.
3. Selecione cada método de alerta desejado (**E-mail, Pop-up, SNMP**) para esses protocolos.  
Somente os métodos de alerta que foram ativados na página Alertas (consulte [Configurando opções de alertas gerais, página 285](#)) estarão disponíveis para seleção.
4. Clique em **OK** para salvar suas alterações em cache e voltar à página Alertas de uso de protocolos (consulte [Configurando alertas de uso de protocolo, página 289](#)). As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Verificando o status atual do sistema

Use a página **Status > Alertas** para localizar informações sobre os problemas que afetam a saúde do Websense, obter ajuda com a solução de problemas e verificar os detalhes de atualizações recentes em tempo real para o Websense Master Database.

A lista **Alertas ativos** mostra o status de componentes do software Websense monitorados.

- ◆ Para obter informações detalhadas sobre quais componentes são monitorados, clique em **O que é monitorado?** acima da lista de mensagens de alerta.
- ◆ Para solucionar um problema, clique no botão **Soluções** ao lado da mensagem de erro ou de aviso.
- ◆ Para ocultar uma mensagem de alerta, clique em **Avançado**. Se a sua organização não usa o Log Server, o Network Agent ou o User Service, ou se você não pretende ativar o WebCatcher, marque uma caixa de seleção para ocultar o alerta associado. Quando terminar, clique em **OK** para implementar a alteração.

Clique em **Avançado** novamente para ocultar as opções avançadas.

A lista **Atualizações do banco de dados em tempo real** fornece informações sobre atualizações de emergência para o Websense Master Database, indicando:

- ◆ Quando a atualização ocorreu
- ◆ O tipo de atualização
- ◆ O número da versão do novo banco de dados
- ◆ O motivo da atualização
- ◆ O endereço IP da instância do Filtering Service que recebeu a atualização

Essas atualizações complementares ocorrem além das atualizações regulares e programadas do Master Database, e podem ser usadas, por exemplo, para recategorizar um site que tenha tido uma categorização temporária incorreta. O Websense procura atualizações do banco de dados a cada hora.

Para os usuários do Websense Web Security, a página Alertas inclui uma terceira lista: **Atualizações de segurança em tempo real**. Esta lista tem o mesmo formato da lista Atualizações do banco de dados em tempo real, mas mostra especificamente atualizações do banco de dados relacionadas à segurança.

A instalação de atualizações de segurança assim que elas são criadas elimina a vulnerabilidade a ameaças como novos golpes de phishing (fraude de identidade), aplicativos falsos ou códigos maliciosos que infectam aplicativos ou sites comuns.

Para obter mais informações sobre Atualizações de segurança em tempo real, consulte [Atualizações de segurança em tempo real™](#), página 30.

Use o botão **Imprimir**, acima da página, para abrir uma janela secundária com uma versão imprimível da área Alertas. Use as opções do navegador para imprimir esta página, que omite todas as opções de navegação encontradas na janela principal do Websense Manager.

## Fazendo backup e restaurando dados do Websense

---

Tópicos relacionados:

- ◆ [Programando backups](#), página 294
- ◆ [Executando backups imediatos](#), página 295
- ◆ [Mantendo os arquivos de backup](#), página 296
- ◆ [Restaurando os dados do Websense](#), página 296
- ◆ [Suspendendo backups programados](#), página 297
- ◆ [Referência de comando](#), página 298

O Websense Backup Utility facilita o backup das configurações e dos dados de diretivas do Websense e o retorno a uma configuração anterior. Os dados salvos pelo utilitário também podem ser usados para importar informações de configuração do Websense após um upgrade.

O Backup Utility salva:

- ◆ Informações de configuração global, incluindo dados de clientes e diretivas, armazenados no Policy Database.
- ◆ Informações de configuração local, como configurações do Filtering Service e do Log Server, armazenadas por cada Policy Server.
- ◆ Arquivos de inicialização e configuração de componentes do Websense.

O processo de backup funciona da seguinte maneira:

1. Você inicia um backup imediato (consulte [Executando backups imediatos](#), página 295) ou define uma programação de backup (consulte [Programando backups](#), página 294).
  - Inicie um backup manualmente quando quiser.
  - Os arquivos de backup são armazenados em um diretório que você especifica ao executar ou programar o backup.
2. O Backup Utility verifica todos os componentes do Websense na máquina, coleta os dados qualificados para backup e cria um arquivo de backup. O nome do arquivo tem o formato:

```
wbackup_aaaa-mm-dd_hhmmss.tar.gz
```

*aaaa-mm-dd\_hhmmss* representa a data e a hora do backup. **tar.gz** é um formato de arquivo compactado portátil.

Somente o raiz (Linux) e os membros do grupo Administradores (Windows) podem acessar os arquivos de backup.

Execute o Websense Backup Utility em cada máquina que inclua componentes do Websense. A ferramenta identifica e salva qualquer um dos seguintes arquivos que encontrar na máquina:

<b>Caminho</b>	<b>Nome do arquivo</b>
<b>\Arquivos de Programas\Websense\bin ou /opt/Websense/bin</b>	authserver.ini BrokerService.cfg config.xml eimsrver.ini LogServer.ini netcache.conf securewisproxy.ini transid.ini upf.conf websense.ini WebUI.ini wsauthserver.ini wscitrix.ini WSE.ini wsedir.ini wsradius.ini wsufpserver.ini
<b>bin/i18n</b>	i18n.ini
<b>bin/postgres/data</b>	postgresql.conf pg_hba.conf
<b>BlockPages/*/Custom</b>	Todas as configurações de página de bloqueio personalizadas
<b>tomcat/conf/Catalina/Localhost</b>	mng.xml
<b>Windows\system32</b>	isa_ignore.txt
<b>Windows\system32\bin</b>	ignore.txt
<b>/etc/wsLib</b>	wsSquid.ini

Armazene os arquivos de backup do Websense em local seguro. Esses arquivos devem integrar os procedimentos de backup normais da organização.

Para voltar a uma configuração anterior:

1. Recupere os arquivos de backup no respectivo site de armazenamento.
2. Copie cada arquivo de backup para a máquina com Websense em que foi criado.

3. Execute o Backup Utility no modo de restauração.



### Importante

Sempre use o Backup Utility para restaurar a configuração do software Websense. Não extraia os arquivos do arquivamento usando outros utilitários de extração.

Se o arquivo de backup estiver corrompido, você não poderá restaurar suas configurações.

Durante o processo de restauração, os avisos ou as mensagens de erro são exibidos na máquina em que a restauração está sendo executada.

## Programando backups

Tópicos relacionados:

- ◆ [Executando backups imediatos](#), página 295
- ◆ [Mantendo os arquivos de backup](#), página 296
- ◆ [Restaurando os dados do Websense](#), página 296
- ◆ [Suspendendo backups programados](#), página 297
- ◆ [Referência de comando](#), página 298

Para programar backups, abra um shell de comando e navegue até o diretório bin do Websense (**C:\Arquivos de Programas\Websense\bin** ou **opt/Websense/bin**, por padrão). Especifique o comando a seguir.

```
wsbackup -s -t "<m> <h> <dia do mês> <mês>
<dia da semana>" -d <diretório>
```

Observe que as informações de tempo usam o formato **crontab**, e as aspas e os espaços são obrigatórios.

Em vez das variáveis do exemplo, forneça as seguintes informações:

Variável	Informações
<m>	0 - 59 Especifique o minuto exato para o início do backup.
<h>	0 - 23 Especifique a hora geral do dia para o início do backup.
<day_of_month>	1 - 31 Especifique a data para a execução do backup. Se você programar um backup para os dias 29 - 31, o utilitário usará o procedimento de substituição padrão para o sistema operacional em meses que não incluem essa data.

Variável	Informações
<month>	1 - 12 Especifique o mês para a execução do backup.
<day_of_week>	0 - 6 Especifique o dia da semana. 0 representa domingo.

Cada campo pode aceitar um número, um asterisco ou uma lista de parâmetros. Consulte alguma referência a **crontab** para obter detalhes.

## Executando backups imediatos

Tópicos relacionados:

- ◆ [Programando backups](#), página 294
- ◆ [Mantendo os arquivos de backup](#), página 296
- ◆ [Restaurando os dados do Websense](#), página 296
- ◆ [Suspendendo backups programados](#), página 297
- ◆ [Referência de comando](#), página 298

Para iniciar um backup imediato, abra um shell de comando e navegue até o diretório bin do Websense (**C:\Arquivos de Programas\Websense\bin** ou **opt/Websense/bin**, por padrão). Especifique o comando a seguir.

```
wbackup -b -d <diretório>
```

Aqui, *diretório* indica o diretório de destino para o arquivamento de backup.



### Aviso

Não armazene arquivos de backup no diretório **bin** do Websense. Esse diretório é excluído quando você desinstala o software Websense.

Quando você inicia um backup imediato, todas as mensagens de erro e notificações são exibidas no console da máquina que executa o backup.

## Mantendo os arquivos de backup

Tópicos relacionados:

- ◆ [Programando backups](#), página 294
- ◆ [Executando backups imediatos](#), página 295
- ◆ [Restaurando os dados do Websense](#), página 296
- ◆ [Suspendendo backups programados](#), página 297
- ◆ [Referência de comando](#), página 298

Quando você executa um backup, um arquivo de configuração (**WebsenseBackup.cfg**) é criado e armazenado com o arquivamento de backup. Esse arquivo de configuração especifica:

- ◆ O tempo que o arquivamento de backup será mantido no diretório de backup
- ◆ O volume máximo de espaço em disco que pode ser consumido por todos os arquivos de backup do diretório

Edite o arquivo **WebsenseBackup.cfg** em qualquer editor de texto para alterar qualquer desses parâmetros:

Parâmetro	Valor
KeepDays	Número de dias que os arquivos de arquivamento devem permanecer no diretório de backup. O padrão é 365.
KeepSize	Número de bytes destinados aos arquivos de backup. O padrão é 10857600.

Todos os arquivos mais antigos que o valor de **KeepDays** são excluídos do diretório de backup. Se o volume de espaço em disco definido for ultrapassado, os arquivos mais antigos serão excluídos do diretório de backup para dar espaço aos arquivos mais recentes.

## Restaurando os dados do Websense

Tópicos relacionados:

- ◆ [Programando backups](#), página 294
- ◆ [Executando backups imediatos](#), página 295
- ◆ [Mantendo os arquivos de backup](#), página 296
- ◆ [Suspendendo backups programados](#), página 297
- ◆ [Referência de comando](#), página 298

Ao restaurar dados de configuração do Websense, verifique se está restaurando os dados dos componentes que existem na máquina atual.

Para iniciar o processo de restauração, abra um shell de comando e navegue até o diretório bin do Websense (**C:\Arquivos de Programas\Websense\bin** ou **opt/Websense/bin**, por padrão). Especifique o comando a seguir.

```
wsbackup -r -f arquivo de backup.tar.gz
```



### Importante

O processo de restauração pode levar vários minutos. Não interrompa o processo enquanto a restauração está em andamento.

Durante o processo de restauração, o Backup Utility pára todos os serviços Websense. Se o utilitário não conseguir parar os serviços, ele enviará uma mensagem pedindo que o usuário o faça manualmente. Os serviços devem ser parados na ordem descrita em [Parando e iniciando os serviços Websense](#), página 283.

O Backup Utility salva alguns arquivos usados para a comunicação com produtos de integração de terceiros. Como esses arquivos residem fora da estrutura de diretório do Websense, você deve restaurá-los manualmente, copiando cada arquivo para o diretório correto.

Estes são arquivos que devem ser restaurados manualmente:

Nome do arquivo	Restaurar para
isa_ignore.txt	Windows\system32
ignore.txt	Windows\system32\bin
wsSquid.ini	/etc/wsLib

## Suspendendo backups programados

Tópicos relacionados:

- ◆ [Programando backups](#), página 294
- ◆ [Executando backups imediatos](#), página 295
- ◆ [Mantendo os arquivos de backup](#), página 296
- ◆ [Restaurando os dados do Websense](#), página 296
- ◆ [Referência de comando](#), página 298

Para desfazer uma programação de backup e suspender a execução dos backups programados, abra um shell de comando e navegue até o diretório bin do Websense (**C:\Arquivos de Programas\Websense\bin** ou **opt/Websense/bin**, por padrão). Especifique o comando a seguir:

wbackup -u

## Referência de comando

Tópicos relacionados:

- ◆ *Programando backups*, página 294
- ◆ *Executando backups imediatos*, página 295
- ◆ *Mantendo os arquivos de backup*, página 296
- ◆ *Restaurando os dados do Websense*, página 296
- ◆ *Suspendendo backups programados*, página 297

Somente o raiz (Linux) e os membros do grupo Administradores (Windows) podem executar o Backup Utility.

Para ver uma lista completa de opções de comando do Backup Utility a qualquer momento, insira:

```
wbackup -h  
ou  
wbackup --help
```

O comando **wbackup** aceita as seguintes opções:

- ◆ *-b ou --backup*
- ◆ *-d caminho do diretório ou --dir caminho do diretório*
- ◆ *-f nome completo do arquivo ou --file nome completo do arquivo*
- ◆ *-h ou --help ou -?*
- ◆ *-r ou --restore*
- ◆ *-s ou --schedule*
- ◆ *-t ou --time*
- ◆ *-u ou --unschedule*
- ◆ *-v ou --verbose [0...3]*

# 13

## Administração de relatórios

Tópicos relacionados:

- ◆ *Planejando a sua configuração*, página 300
- ◆ *Gerenciando o acesso às ferramentas de relatórios*, página 300
- ◆ *Configuração básica*, página 301
- ◆ *Utilitário Configuração do Log Server*, página 306
- ◆ *Administrando o banco de dados de log*, página 319
- ◆ *Configurando relatórios investigativos*, página 330
- ◆ *Relatório próprio*, página 334

Para usar os relatórios de apresentação e os relatórios investigativos do Websense, você deve instalar o Websense Manager e os componentes de relatórios em um servidor Windows. Você também deve configurar o software Websense para registrar em log a atividade de filtragem da Internet.

O registro em log envia registros para o Websense Log Server, que os processa em um banco de dados de log que deve ser instalado em um mecanismo de banco de dados suportado: Microsoft SQL Server Desktop Engine (também denominado MSDE neste documento) ou Microsoft SQL Server Enterprise ou Standard (ambos denominados como Microsoft SQL Server). Consulte o *Guia de Instalação* do Websense para obter mais informações sobre como instalar esses componentes de relatórios.

Quando você gera um relatório, o Websense Manager exibe informações do banco de dados de log de acordo com o filtro que você define para o relatório.

As organizações que instalam o Websense Manager em um servidor Linux, ou preferem usar o Linux para suas necessidades de relatórios, podem instalar o produto Websense Explorer for Linux para gerar relatórios. Este produto opera de forma independente do Websense Manager. Consulte o *Websense Explorer for Linux Administrator's Guide* para obter informações sobre como instalar e usar o programa.

## Planejando a sua configuração

---

Dependendo do volume de tráfego de Internet em sua rede, o banco de dados de log pode ficar muito grande. Para ajudar a determinar uma estratégia eficaz para registro em log e relatórios para a sua organização, considere estas questões:

- ◆ Quando o tráfego de rede é mais intenso?  
Considere o agendamento de trabalhos de banco de dados e relatórios com uso intensivo de recursos para horários em que o volume de tráfego é menor. Isso melhora o desempenho de registro em log e relatórios em horários de pico. Consulte [Configurando as opções de tempo de navegação na Internet, página 324](#), e [Configurando opções de manutenção do banco de dados de log, página 325](#).
- ◆ Durante quanto tempo os dados de registro em log devem ser mantidos para apoiar os relatórios históricos?  
Considere a exclusão automática de partições depois que alcançam esse tempo. Isso reduz a quantidade de espaço em disco necessário para o banco de dados de log. Consulte [Configurando opções de manutenção do banco de dados de log, página 325](#).
- ◆ Quantos detalhes realmente são necessários?  
Considere quais opções de registro em log devem ser ativadas: registrar ocorrências e URLs completos aumenta o tamanho do banco de dados de log. Para reduzir o tamanho do banco de dados de log, considere:
  - desativar o registro de URLs completos (consulte [Configurando o registro de URLs completos, página 322](#))
  - registrar em log as visitas em vez das ocorrências (consulte [Configurando os arquivos de cache de log, página 311](#))
  - habilitar a consolidação (consulte [Configurando opções de consolidação, página 312](#))
  - habilitar o registro seletivo de categorias em log (consulte [Configurando o Filtering Service para registro em log, página 304](#))

As implementações bem-sucedidas de relatórios são implementadas em hardware que cumpre ou supera os requisitos de carga esperada e retenção de dados históricos.

## Gerenciando o acesso às ferramentas de relatórios

---

Quando o Websense Manager e os componentes de relatórios são instalados em servidores Windows, as opções de relatórios aparecem no Websense Manager e no utilitário Configuração do Log Server.

Quando você instala os componentes de relatórios, o Log Server é conectado a um Policy Server específico. Você deve selecionar esse Policy Server durante o logon no Websense Manager para acessar os recursos de relatórios. Se você fizer logon em outro Policy Server, não poderá acessar Relatórios de apresentação ou Relatórios

investigativos na guia Principal, ou a seção completa de Geração de relatórios na guia Configurações.

Em organizações que usam apenas a conta de logon WebsenseAdministrator, todos que usam o Websense Manager têm acesso a todas as opções de relatórios no Websense Manager, incluindo relatórios de apresentação, relatórios investigativos e configurações para as ferramentas de relatórios.

Em organizações que usam administração delegada, o acesso às ferramentas de relatórios no Websense Manager é controlado pelo WebsenseAdministrator e por membros da função Super administrador. Ao criar uma função, o Super administrador designa se a função tem acesso a opções de relatório específicas.

Consulte [Editando funções, página 254](#), para obter informações sobre as configurações de acesso a ferramentas de relatórios.

O utilitário Configuração do Log Server é acessado no menu Iniciar do Windows. Somente as pessoas com acesso à máquina da instalação podem abrir este utilitário e modificar as configurações do Log Server. Consulte [Utilitário Configuração do Log Server, página 306](#).

Se a sua empresa instalou o Websense Manager em um servidor Linux ou escolher o programa de relatórios Websense Explorer for Linux em vez dos componentes de relatório para Windows, as opções de relatórios não aparecem no Websense Manager. Nenhum gráfico de filtragem de Internet aparecerá nas páginas Hoje e Histórico. Consulte o *Explorer for Linux Administrator's Guide* para obter informações sobre como instalar o programa e gerar relatórios.

## Configuração básica

Tópicos relacionados:

- ◆ [Configurando o Filtering Service para registro em log, página 304](#)
- ◆ [Atribuindo categorias a classes de risco, página 302](#)
- ◆ [Configurando preferências de relatórios, página 303](#)
- ◆ [Utilitário Configuração do Log Server, página 306](#)
- ◆ [Administrando o banco de dados de log, página 319](#)

Você pode usar diversas opções de configuração para personalizar os relatórios para o seu ambiente.

O Websense Master Database organiza as categorias em **classes de risco**. As classes de risco sugerem tipos ou níveis possíveis de vulnerabilidades geradas pelos sites que estão nas categorias. Use a página Geral > Classes de risco, acessada na guia Configurações, para personalizar as classes de risco para a sua organização. Consulte [Atribuindo categorias a classes de risco, página 302](#).

Use a página Geração de relatórios > Preferências, acessada na guia Configurações, para configurar o servidor de e-mail usado para distribuir relatórios, e para ativar o recurso de relatório próprio. Consulte [Configurando preferências de relatórios](#), página 303.

O registro em log é o processo de armazenar informações sobre as atividades de filtragem do Websense em um banco de dados de log para poder gerar relatórios.

Use a página Geral > Registro em log, acessada na guia Configurações, para habilitar o registro em log, selecionar as categorias que serão registradas e determinar quais informações do usuário serão registradas. Consulte [Configurando o Filtering Service para registro em log](#), página 304, para obter mais informações.

Use o utilitário Configuração do Log Server para administrar como os registros em log são processados e as conexões com o banco de dados de log. Consulte [Utilitário Configuração do Log Server](#), página 306, para obter mais informações.

Use a página Geração de relatórios > Banco de dados de log, acessada na guia Configurações, para administrar o banco de dados de log, incluindo controles de tempo de navegação na Internet, opções de partição de banco de dados, e registros de erros. Consulte [Administando o banco de dados de log](#), página 319, para obter mais informações.

## Atribuindo categorias a classes de risco

Tópicos relacionados:

- ◆ [Classes de risco](#), página 39
- ◆ [Páginas de bloqueio](#), página 83
- ◆ [Usando relatórios para avaliar diretivas de filtragem](#), página 93

O Websense Master Database organiza as categorias em **classes de risco**. As classes de risco sugerem tipos ou níveis possíveis de vulnerabilidades geradas pelos sites que estão nas categorias.

As classes de risco são usadas principalmente na geração de relatórios. As páginas Hoje e Histórico contêm gráficos que exibem a atividade na Internet por classe de risco. É possível gerar relatórios de apresentação ou relatórios investigativos organizados por classe de risco.

Os Super administradores incondicionais podem exibir ou alterar as categorias designadas a cada classe de risco na página **Configurações > Classes de risco**. Por exemplo, algumas empresas podem considerar que sites com vídeos publicados pelos usuários recaem nas classes de risco de responsabilidade legal, perda de banda de rede e perda de produtividade. Porém, se a sua empresa faz pesquisa de mercado sobre uma

determinada faixa demográfica, você poderia considerar como parte da classe de risco Uso empresarial.



**Obs.:**

A página de bloqueio de segurança aparece para sites bloqueados nas categorias padrão da classe Risco de segurança. As alterações nas categorias da classe Risco de segurança afetam os relatórios, mas não afetam as páginas de bloqueio. Consulte [Páginas de bloqueio](#), página 83.

As informações sobre classes de risco em relatórios do Websense são refletidas nas atribuições que você faz nesta página.

1. Selecione uma entrada na lista **Classes de risco**.
2. Revise a lista **Categorias** para ver quais categorias estão incluídas atualmente na classe de risco.

Uma marca de seleção mostra que a categoria está atribuída à classe de risco selecionada. O ícone W azul indica categorias que estão incluídas na classe de risco por padrão.

3. Marque ou desmarque entradas na árvore de categorias para incluir ou excluir uma categoria da classe de risco selecionada. As categorias podem pertencer a mais de uma classe de risco.

Outras opções incluem:

Opção	Descrição
<b>Selecionar tudo</b>	Seleciona todas as categorias na árvore.
<b>Limpar tudo</b>	Desmarca todas as categorias na árvore.
<b>Restaurar padrões</b>	Redefine os padrões da categoria para a classe de risco selecionada aos fornecidos pelo software Websense. Um ícone W azul indica uma categoria padrão.

4. Repita este processo para cada classe de risco.
5. Clique em **OK** para armazenar suas alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Configurando preferências de relatórios

Tópicos relacionados:

- ◆ [Relatório próprio](#), página 334
- ◆ [Agendando relatórios de apresentação](#), página 108
- ◆ [Agendando relatórios investigativos](#), página 135

Quando você programa a execução de relatórios investigativos ou de apresentação posteriormente ou em um ciclo repetitivo, os relatórios são distribuídos por e-mail para destinatários especificados. Use a página **Geração de relatórios > Preferências**, acessada na guia Configurações, para fornecer as informações essenciais para essas mensagens de e-mail.

Esta página também é usada para habilitar relatórios próprios, em que os indivíduos podem gerar relatórios investigativos sobre suas próprias atividades de Internet.

1. Digite o **Endereço de e-mail** para aparecer no campo De quando relatórios agendados são distribuídos por e-mail.
2. Insira o **IP ou nome do servidor SMTP** para o servidor de e-mail usado para distribuir relatórios programados por e-mail.
3. Marque a caixa de seleção **Permitir relatório próprio** para permitir que os usuários finais em sua organização acessem o Websense Manager e executem relatórios investigativos sobre sua atividade de Internet pessoal. Consulte [Relatório próprio](#), página 334.
4. Clique em **Salvar agora** para implementar as alterações

## Configurando o Filtering Service para registro em log

Tópicos relacionados:

- ◆ [Apresentando o banco de dados de log](#), página 317
- ◆ [Utilitário Configuração do Log Server](#), página 306

Use a página **Geral > Registro em log** na guia Configurações para fornecer o endereço IP e a porta para envio dos registros em log ao Log Server. Esta página também permite selecionar quais categorias de informações do usuário e URL o Websense Filtering Service deve enviar ao Log Server e disponibilizar para relatórios e alertas de uso de categorias (consulte [Configurando alertas de uso de categoria](#), página 288).

Em um ambiente com vários Policy Servers, configure a página Geral > Registro em log separadamente para cada um. Todos os Filtering Services associados com o Policy Server ativo enviam seus registros em log para o Log Server identificado nesta página.

Lembre-se dos seguintes fatos ao trabalhar com vários Policy Servers:

- ◆ Se o endereço IP e a porta do Log Server estiverem em branco para qualquer Policy Server, os Filtering Services associados com o Policy Server não podem registrar em log qualquer tráfego para relatórios ou eventos.
- ◆ Cada Filtering Service registra o tráfego de acordo com as configurações do Policy Server ao qual está conectado. Se você alterar as seleções de registro de informações do usuário ou categorias para diferentes Policy Servers, os relatórios gerados para usuários associados com diferentes Policy Servers podem parecer inconsistentes.

Se o seu ambiente inclui vários Policy Servers e vários Log Servers, certifique-se de fazer logon em cada Policy Server separadamente e verifique se está se comunicando com o Log Server correto.

1. Para registrar em log as informações de identificação das máquinas que acessam a Internet, marque **Log de endereços IP**.
2. Para registrar em log as informações de identificação dos usuários que acessam a Internet, marque **Log de nomes de usuários**.

**Obs.:**

Se você não registrar em log os endereços IP ou nomes de usuários, não será possível incluir dados de usuários em seus relatórios. Isso às vezes é denominado **registro em log anônimo**.

3. Insira o endereço IP ou o nome da máquina onde o Log Server está instalado no campo **Endereço IP ou nome do Log Server**.

**Importante**

Se o Log Server está instalado em uma máquina separada do Policy Server, esta entrada poderá ser localhost por padrão. Se isso ocorrer, insira o endereço IP correto da máquina do Log Server para habilitar a exibição de gráficos nas páginas Hoje e Histórico, e também outros recursos de relatórios.

4. Insira o número da **Porta** para envio de registros de log ao Log Server.
5. Clique em **Verificar status** para determinar se o Websense Manager é capaz de se comunicar com o Log Server especificado.

Uma mensagem indica se o teste de conexão foi aprovado. Atualize o endereço IP ou o nome da máquina e a porta, se necessário, até o teste ser bem-sucedido.

6. Clique no botão **Registro seletivo de categorias em log** para abrir a área para indicar quais categorias de URL devem ser registradas em log.

As seleções que você fizer aqui aplicam-se a todos os filtros de categorias em todas as diretivas ativas.

**Obs.:**

Se você desativar o registro em log para as categorias com alertas de uso (consulte [Configurando alertas de uso de categoria](#), página 288), não será possível enviar alertas de uso.

Os relatórios não podem incluir informações sobre categorias que não são registradas em log.

- a. Expanda ou contraia as categorias pai conforme necessário para ver as categorias de interesse.
- b. Selecione cada categoria que será registrada em log marcando sua caixa de seleção.

Você deve selecionar ou cancelar a seleção de cada categoria separadamente. Selecionar uma categoria pai não seleciona automaticamente as suas subcategorias. Use **Selecionar tudo** e **Limpar tudo** para ajudar nas seleções.

7. Clique em **OK** para armazenar suas alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Utilitário Configuração do Log Server

---

Tópicos relacionados:

- ◆ [Gerenciando o acesso às ferramentas de relatórios](#), página 300
- ◆ [Configuração básica](#), página 301
- ◆ [Interrompendo e iniciando o Log Server](#), página 317

Durante a instalação, você configura determinados aspectos da operação do Log Server, incluindo como o Log Server interage com os componentes de filtragem do Websense.

O utilitário Configuração do Log Server permite alterar essas configurações quando necessário, e configurar outros detalhes sobre a operação do Log Server. Este utilitário é instalado no mesmo computador do Log Server.

1. No menu Iniciar do Windows, selecione **Programas > Websense > Utilitários > Configuração do Log Server**.

O utilitário Configuração do Log Server é aberto.

2. Selecione uma guia para exibir suas opções e fazer alterações. Para obter instruções detalhadas, consulte:
  - [Configurando conexões do Log Server](#), página 307
  - [Configurando opções do servidor do banco de dados de log](#), página 308
  - [Configurando os arquivos de cache de log](#), página 311
  - [Configurando opções de consolidação](#), página 312
  - [Configurando o WebCatcher](#), página 314
3. Clique em **Aplicar** para salvar as alterações

- Use a guia **Conexão** para desativar e reiniciar o Log Server, para que as alterações sejam implementadas.

---

**IMPORTANTE**

Depois de fazer alterações em uma guia do utilitário Configuração do Log Server, clique em **Aplicar**. Em seguida, você **deve** interromper e reiniciar o Log Server para que as alterações sejam implementadas. Para não reiniciar o Log Server várias vezes, faça todas as alterações no utilitário Configuração do Log Server antes de reiniciar o Log Server.

---

## Configurando conexões do Log Server

Tópicos relacionados:

- ◆ [Utilitário Configuração do Log Server](#), página 306
- ◆ [Configurando opções do servidor do banco de dados de log](#), página 308
- ◆ [Configurando os arquivos de cache de log](#), página 311
- ◆ [Configurando opções de consolidação](#), página 312
- ◆ [Configurando o WebCatcher](#), página 314
- ◆ [Interrompendo e iniciando o Log Server](#), página 317

A guia **Conexão** do utilitário Configuração do Log Server contém opções para criar e manter uma conexão entre o Log Server e os componentes de filtragem do Websense.

- Aceite o padrão para **porta de entrada do Log Server** (55805) ou informe outra porta disponível.

Esta é a porta pela qual o Log Server se comunica com o Filtering Service. A porta informada aqui deve corresponder à porta informada na página Geral > Registro em log, da guia Configurações no Websense Manager.
- Informe um número de horas como o **Intervalo de atualização do Usuário/Grupo** para especificar com que frequência o Log Server deve contatar o serviço de diretório para obter atualizações.

O Log Server contata o serviço de diretório para obter informações atualizadas, como nome de usuário completo e atribuições de grupos, sobre os usuários com registros no banco de dados de log.

A atividade para um usuário cujo grupo mudou continua a ser reportada com o grupo anterior até que a atualização seguinte ocorra. As empresas que atualizam o serviço de diretório com frequência ou têm um grande número de usuários devem considerar a atualização das informações de usuários/grupos com frequência superior ao padrão de 12 horas.
- Clique em **Aplicar** para salvar as alterações

- Use o botão na área Status do serviço para **Iniciar** ou **Parar** o Log Server. A etiqueta no botão muda para refletir a ação que ocorrerá quando você clicar nele.



**Obs.:**

Nenhuma atividade de acesso à Internet pode ser registrada quando o Log Server está desativado.

As alterações realizadas no utilitário Configuração do Log Server só serão implementadas depois que você interromper e reiniciar o Log Server.

## Configurando opções do servidor do banco de dados de log

Tópicos relacionados:

- ◆ [Utilitário Configuração do Log Server](#), página 306
- ◆ [Configurando conexões do Log Server](#), página 307
- ◆ [Configurando a conexão do banco de dados](#), página 310
- ◆ [Configurando os arquivos de cache de log](#), página 311
- ◆ [Configurando opções de consolidação](#), página 312
- ◆ [Configurando o WebCatcher](#), página 314
- ◆ [Interrompendo e iniciando o Log Server](#), página 317

Abra a guia **Banco de dados** do utilitário Configuração do Log Server para configurar como o Log Server funciona com o banco de dados de log.

- Escolha um **Método de inserção de log** entre as seguintes opções.
  - Open Database Connectivity (ODBC): Insere os registros no banco de dados individualmente, usando um driver de banco de dados para administrar os dados entre o Log Server e o banco de dados de log.
  - Bulk Copy Program (BCP) (*recomendado*): Insere os registros no banco de dados de log em grupos denominados lotes. Esta opção é recomendada porque oferece melhor eficiência do que a inserção com ODBC.



**Obs.:**

A opção BCP só está disponível se você instalar as ferramentas de cliente do SQL Server no computador do Log Server.

- Clique no botão **Conexão** para selecionar o banco de dados de log para armazenamento de novas informações de acesso à Internet do Websense. Consulte [Configurando a conexão do banco de dados](#), página 310.

**DSN (nome da fonte de dados do ODBC)** e **Nome de logon do DBC** exigem as configurações definidas para a conexão com o banco de dados.

3. Se você escolheu BCP como o método de inserção de log na etapa 1, defina as seguintes opções. Se você escolheu ODBC como o método de inserção de log, ignore esta etapa.

Opção	Descrição
Local de caminho de arquivo BCP	Caminho de diretório para armazenar arquivos BCP. Deve ser um caminho onde o Log Server tem acesso para leitura e gravação. Esta opção só está disponível se o Log Server estiver instalado no computador do banco de dados de log ou se as ferramentas de cliente do SQL Server estiverem instaladas no computador do Log Server.
Data de criação do arquivo BCP	Número máximo de minutos que o Log Server dedica a colocar registros em um arquivo de lote antes de fechar o arquivo de lote e criar um novo arquivo. Esta configuração funciona em combinação com a configuração de tamanho do lote: O Log Server cria um novo arquivo de lote assim que um limite é alcançado.
Tamanho de lote máximo do BCP	Número máximo de registros de log antes que um novo arquivo de lote seja criado. Esta configuração funciona em combinação com a configuração de intervalo de criação: O Log Server cria um novo arquivo de lote assim que um limite é alcançado.

4. Defina o **Máximo de conexões permitidas** para indicar quantas conexões internas podem ocorrer entre o Log Server e o mecanismo do banco de dados. As opções disponíveis dependem do mecanismo de banco de dados que está sendo usado.
- **MSDE:** Este valor é predefinido como 4 e não pode ser alterado.
  - **SQL Server:** Defina um número de 4 a 50, conforme apropriado para a sua licença do SQL Server. O número mínimo de conexões depende do método de inserção de log selecionado.



**Obs.:**

Aumentar o número de conexões pode aumentar a velocidade de processamento para registros, mas pode ter impacto sobre outros processos na rede que usam o mesmo SQL Server. Na maioria dos casos, você deve definir o número de conexões como inferior a 20. Contate o seu Administrador do Banco de Dados para obter orientação.

5. Marque ou desmarque **Registro de log aprimorado** para habilitar ou desabilitar esta opção, que controla como o Log Server continua os registros de log depois de ter sido desativado.

Quando esta opção está desmarcada (o padrão), o Log Server começa o processamento no início do arquivo de cache de log mais antigo após uma parada. Isso poderia resultar em entradas duplicadas no banco de dados de log, mas acelera o processamento do Log Server.

Quando esta opção está marcada, o Log Server monitora sua localização no arquivo de cache de log ativo. Após um reinício, o Log Server continua o processamento onde foi interrompido. O registro de log aprimorado pode reduzir a velocidade de processamento do Log Server.

6. Clique em **Aplicar** para salvar as alterações, depois interrompa e reinicie o Log Server (consulte [Interrompendo e iniciando o Log Server](#), página 317).

## Configurando a conexão do banco de dados

Tópicos relacionados:

- ◆ [Configurando conexões do Log Server](#), página 307
- ◆ [Configurando opções do servidor do banco de dados de log](#), página 308

O botão **Conexão** na guia Banco de dados do utilitário Configuração do Log Server permite selecionar o banco de dados de log para armazenamento de informações de acesso à Internet recebidas do Websense. Isso é configurado automaticamente durante a instalação, mas pode ser alterado sempre que você quiser alterar o banco de dados para registros. (O banco de dados já deve existir para estabelecer uma conexão.)

1. Na caixa de diálogo Fonte de dados, selecione a guia **Fonte de dados na máquina**.
2. Selecione a conexão ODBC para o banco de dados no qual novas informações serão registradas.
3. Clique em **OK** para exibir a caixa de diálogo Logon no SQL Server.
4. Se a opção **Usar conexão confiável** estiver disponível, verifique se está configurada corretamente para o seu ambiente.

**Usuários de MSDE:** Desmarque a opção Conexão confiável.

**Usuários de SQL Server:** Contate o seu Administrador do Banco de Dados para obter orientação.



### Obs.:

Se você usa uma conexão confiável para comunicações com o SQL Server, poderá ser necessário configurar diversos serviços Websense com o nome de usuário e a senha confiáveis. Consulte o *Guia de Instalação* do Websense para obter detalhes.

5. Digite a **ID de logon** e a **Senha** definidas quando o banco de dados foi criado. Em geral, são a ID de logon e a senha digitadas durante a instalação do Log Server e a criação do banco de dados.
6. Interrompa e reinicie o Log Server na guia **Conexão** depois de fazer esta e outras alterações no utilitário Configuração do Log Server.

## Configurando os arquivos de cache de log

Tópicos relacionados:

- ◆ [Utilitário Configuração do Log Server](#), página 306
- ◆ [Configurando conexões do Log Server](#), página 307
- ◆ [Configurando opções do servidor do banco de dados de log](#), página 308
- ◆ [Configurando opções de consolidação](#), página 312
- ◆ [Configurando o WebCatcher](#), página 314
- ◆ [Interrompendo e iniciando o Log Server](#), página 317

A guia **Configurações** do utilitário Configuração do Log Server permite administrar as opções de criação de arquivo de cache de log e especificar se o Log Server monitora os arquivos individuais que compõem cada site da Web solicitado, ou apenas o site da Web.

1. Digite o caminho para armazenar arquivos de cache de log no campo **Localização do caminho do arquivo de log**. O caminho padrão é **<diretório de instalação>\bin\Cache**. (O diretório de instalação padrão é C:\Arquivos de Programas\WebSense\).

2. Para **Intervalo de criação do arquivo de cache**, indique o número máximo de minutos que o Log Server deve dedicar a enviar informações de acesso à Internet para um arquivo de cache de log (**logn.tmp**) antes de fechá-lo e criar um novo arquivo.

Esta configuração funciona em combinação com a configuração de tamanho: O Log Server cria um novo arquivo de cache de log assim que um limite é alcançado.

3. Para **Tamanho de criação de arquivo de cache**, especifique qual tamanho um arquivo de cache de log deve ter para o Log Server fechá-lo e criar um novo arquivo.

Esta configuração funciona em combinação com a configuração de intervalo de criação: O Log Server cria um novo arquivo de cache de log assim que um limite é alcançado.

4. Marque **Habilitar visitas** para criar um registro para cada site da Web visitado.



**Obs.:**

Administrar o tamanho do banco de dados de log é uma preocupação importante em redes de alto volume.

Habilitar o registro de visitas é uma forma de controlar o tamanho e o crescimento do banco de dados.

Quando esta opção está desmarcada, um registro de log separado é criado para cada solicitação HTTP gerada para exibir os diferentes elementos da página, como imagens e anúncios. Também conhecida como ocorrências de registro, esta opção cria um banco de dados de log muito maior, que cresce rapidamente.

Quando esta opção está selecionada, o Log Server combina os elementos individuais que criam a página da Web (como gráficos e anúncios) em um único registro de log.

Se você instalou o Websense Web Security Gateway, a atividade de verificação em tempo real é sempre reportada em ocorrências nos relatórios que são específicas da verificação em tempo real, mesmo quando o registro das visitas em log está habilitado. Nesta situação, os números mostrados nos relatórios de filtragem da Web que incluem tráfego bloqueado por verificação em tempo real serão menores do que os números que aparecem em relatórios de verificação em tempo real.

**Obs.:**

É melhor criar uma nova partição de banco de dados antes de alterar o método de registro entre visitas e ocorrências. Consulte a página Reporting > Banco de dados de log no Websense Manager para criar uma nova partição do banco de dados.

---

5. Clique em **Aplicar** para salvar as alterações, depois interrompa e reinicie o Log Server (consulte [Interrompendo e iniciando o Log Server](#), página 317).

## Configurando opções de consolidação

Tópicos relacionados:

- ◆ [Utilitário Configuração do Log Server](#), página 306
- ◆ [Configurando conexões do Log Server](#), página 307
- ◆ [Configurando opções do servidor do banco de dados de log](#), página 308
- ◆ [Configurando os arquivos de cache de log](#), página 311
- ◆ [Configurando o WebCatcher](#), página 314
- ◆ [Interrompendo e iniciando o Log Server](#), página 317

Abra a guia **Consolidação** do utilitário Configuração do Log Server para habilitar a consolidação e definir preferências de consolidação.

**Obs.:**

Administrar o tamanho do banco de dados de log é uma preocupação importante em redes de alto volume. Habilitar a consolidação é uma forma de controlar o tamanho e o crescimento do banco de dados.

---

A consolidação reduz o tamanho do seu banco de dados de log, combinando solicitações de Internet que compartilham os seguintes elementos:

- ◆ Nome de domínio (por exemplo: www.websense.com)

- ◆ Categoria
- ◆ Palavra-chave
- ◆ Ação (por exemplo: Categoria Bloqueada)
- ◆ Usuário/estação de trabalho

Os relatórios são executados mais rápido quando o banco de dados de log é menor. Porém, a consolidação de dados de log pode reduzir a precisão de alguns relatórios de detalhes, porque registros separados para o mesmo nome de domínio podem ser perdidos.



### Importante

Habilitar a consolidação pode distorcer a precisão de alguns dados de relatórios, como os cálculos de Tempo de navegação na Internet.

---

1. Marque **Consolidar registros de log** para habilitar a consolidação, que combina várias solicitações de Internet semelhantes em um único registro de log.

Quando esta opção está desmarcada (padrão), o banco de dados de log arquiva ocorrências completas ou detalhes de visitas para cada solicitação de Internet (dependendo de sua seleção na guia Configurações, consulte [Configurando os arquivos de cache de log, página 311](#)). Isso fornece mais detalhes nos relatórios, mas gera um banco de dados de log maior.

Selecionar esta opção cria um banco de dados de log menor, com relatórios menos detalhados.



### Importante

Para garantir relatórios consistentes, considere a criação de uma nova partição de banco de dados sempre que você habilitar ou desabilitar a consolidação. Além disso, certifique-se de gerar relatórios de partições com a mesma configuração de consolidação.

---

Se você instalou o Websense Web Security Gateway, a atividade de verificação em tempo real é sempre reportada como ocorrências separadas nos relatórios que são específicos da verificação em tempo real, mesmo quando a consolidação está habilitada. Nesta situação, os números mostrados nos relatórios de filtragem da Web que incluem tráfego bloqueado por verificação em tempo real serão menores do que os números que aparecem em relatórios de verificação em tempo real.

2. Para o **Intervalo da consolidação**, especifique o tempo máximo entre o primeiro e o último registro que serão combinados.

Isso representa a maior diferença de tempo entre o registro mais antigo e o mais recente que são combinados para criar um registro de consolidação.

Reduza o intervalo para aumentar a granularidade dos relatórios. Aumente o intervalo para maximizar a consolidação. Esteja ciente de que um intervalo maior também pode aumentar o uso de recursos do sistema, como memória, CPU e espaço em disco.

Se você habilitou a opção URL completo na página Reporting > Banco de dados de log, na guia Configurações do Websense Manager, o registro de log consolidado conterá o caminho completo (até 255 caracteres) do primeiro site correspondente que o Log Server encontrar.

Por exemplo, suponha que um usuário visitou os seguintes sites e todos foram classificados na categoria Compras.

- www.domain.com/shoeshopping
- www.domain.com/purseshopping
- www.domain.com/jewelrshopping

Com o registro de URLs completos ativo, a consolidação criaria uma única entrada de registro de log sob o URL www.domain.com/shoeshopping.

3. Clique em **Aplicar** para salvar as alterações, depois interrompa e reinicie o Log Server (consulte [Interrompendo e iniciando o Log Server](#), página 317).

## Configurando o WebCatcher

Tópicos relacionados:

- ◆ [Utilitário Configuração do Log Server](#), página 306
- ◆ [Configurando conexões do Log Server](#), página 307
- ◆ [Configurando opções do servidor do banco de dados de log](#), página 308
- ◆ [Configurando os arquivos de cache de log](#), página 311
- ◆ [Configurando opções de consolidação](#), página 312
- ◆ [Configurando o WebCatcher](#), página 314
- ◆ [Autenticação do WebCatcher](#), página 316
- ◆ [Interrompendo e iniciando o Log Server](#), página 317

O WebCatcher é um recurso opcional que coleta URLs não reconhecidos e URLs de segurança, e os envia para Websense, Inc., onde são analisados para identificar riscos potenciais de segurança e responsabilidade, e para classificação. (O registro de URLs completos não é necessário para processamento pelo WebCatcher.) A Websense, Inc., analisa as informações e atualiza o Master Database com URLs recém-classificadas, resultando em melhoria da filtragem.

Escolha os tipos de URLs que serão encaminhados e defina o tamanho de arquivo e o tempo de processamento na guia **WebCatcher** do utilitário Configuração do Log Server.



### Obs.:

Em um ambiente com vários Log Servers, o WebCatcher é habilitado para apenas um Log Server. Depois da habilitação, esta guia estará indisponível ao executar a ferramenta Configuração do Log Server para outras instâncias do Log Server.

As informações encaminhadas para a Websense, Inc., contêm apenas URLs e não incluem informações do usuário.

O seguinte exemplo ilustra as informações que seriam encaminhadas se você ativar o WebCatcher. O endereço IP neste exemplo reflete o endereço do computador que hospeda o URL, e não o endereço IP do solicitante.

```
<URL HREF="http://www.ack.com/uncategorized/" CATEGORY="153"  
IP_ADDR="200.102.53.105" NUM_HITS="1" />
```

Os dados do WebCatcher são encaminhados para Websense, Inc., via HTTP Post. Pode ser necessário criar funções ou fazer outras alterações em seu servidor proxy ou firewall para permitir a saída de tráfego HTTP. Consulte a documentação do servidor proxy ou firewall para obter instruções.

1. Selecione uma das seguintes opções:
  - **Sim, envie somente os URLs especificados à Websense** ativa o processamento do WebCatcher. Você deve indicar quais URLs serão encaminhados. Continue para a etapa 2.
  - **Não, não envie informações à Websense** desativa o processamento do WebCatcher. Não são necessárias entradas adicionais se você escolher esta opção.
2. Marque **Enviar URLs não categorizados** para enviar uma lista de todos os URLs não categorizados encontrados em seu banco de dados de log.

A Websense, Inc., analisa os URLs não categorizados que recebe e os acrescenta às categorias do Master Database, conforme apropriado. Isso melhora a precisão da filtragem para todas as empresas.



---

**Obs.:**

Os sites de Intranet não são encaminhados pelo WebCatcher. Isso inclui todos os sites com endereços IP nos intervalos 10.xxx.xxx.xxx, 172.16.xxx.xxx e 192.168.xxx.xxx.

---

3. Marque **Enviar URLs de segurança** para enviar uma lista de URLs de segurança encontrados em seu banco de dados de log.

Os URLs de segurança recebidos são analisados pela Websense, Inc., para determinar a atividade de sites nas categorias Keyloggers, Websites nocivos, Phishing e outras fraudes, e Spyware.
4. Em **Selecione o país que melhor corresponde à sua localização**, selecione o país onde a maioria das atividades estão sendo registradas.
5. Marque a opção **Salvar uma cópia dos dados enviados à Websense** para salvar uma cópia dos dados que estão sendo enviados à Websense, Inc.

Quando esta opção está habilitada, o WebCatcher salva os dados como arquivos XML não criptografados no diretório Websense\Reporter. Esses arquivos têm carimbo de data e hora.
6. Em **Tamanho de arquivo de upload máximo**, indique até que tamanho o arquivo pode crescer (de 4096 KB até 8192 KB) antes do envio à Websense.

Certifique-se de que o seu sistema pode postar um arquivo desse tamanho por HTTP Post.

7. Para **Hora inicial diária mínima**, defina a hora de início para que o WebCatcher envie o arquivo se o limite de tamanho não tiver sido alcançado no dia.  
Isso garante que as informações são encaminhadas e apagadas de seu sistema pelo menos uma vez ao dia.
8. Clique no botão **Autenticação** se o computador do Log Server deve autenticar para acessar a Internet.  
Consulte [Autenticação do WebCatcher](#), página 316, para obter informações sobre a caixa de diálogo **Autenticação** que aparece.
9. Clique em **Aplicar** para salvar as alterações, depois interrompa e reinicie o Log Server (consulte [Interrompendo e iniciando o Log Server](#), página 317).

## Autenticação do WebCatcher

Tópicos relacionados:

- ◆ [Utilitário Configuração do Log Server](#), página 306
- ◆ [Configurando o WebCatcher](#), página 314
- ◆ [Interrompendo e iniciando o Log Server](#), página 317

A caixa de diálogo Autenticação aparece depois que você clica em **Autenticação** na guia WebCatcher.

1. Marque a opção **Usar servidor proxy** se o computador do Log Server acessa a Internet por um servidor proxy, e depois forneça as informações solicitadas.

Campo	Descrição
<b>Nome do servidor proxy</b>	Digite o endereço IP ou nome do computador do servidor proxy pelo qual o Log Server acessa a Internet.
<b>Porta do servidor proxy</b>	Digite o número da porta pela qual o servidor proxy se comunica.

2. Marque a opção **Usar autenticação básica** se o computador do Log Server deve autenticar para acessar a Internet, e depois digite o nome de usuário e a senha para autenticação.
3. Clique em **OK** para salvar as alterações e voltar à guia WebCatcher.

---

## Interrompendo e iniciando o Log Server

---

Tópicos relacionados:

- ◆ [Utilitário Configuração do Log Server, página 306](#)
- ◆ [Configurando conexões do Log Server, página 307](#)

O Log Server recebe informações do Filtering Service e as salva no banco de dados de log para uso ao gerar relatórios. É executado como um serviço do Windows, inicializado durante a instalação, e é inicializado sempre que você reinicia um computador.

As alterações no utilitário Configuração do Log Server só serão implementadas depois que você interromper e reiniciar o Log Server. Isso pode ser feito facilmente, na guia Conexão do utilitário Configuração do Log Server.

1. No menu Iniciar do Windows, selecione **Programas > Websense > Utilitários > Configuração do Log Server**.
2. Na guia **Conexões**, clique em **Parar**.
3. Espere alguns minutos e clique em **Iniciar** para reiniciar o serviço Log Server.
4. Clique em **OK** para fechar o utilitário Configuração do Log Server.



**Obs.:**

O Websense não pode registrar em log os acessos à Internet que ocorrem quando o Log Server está desativado.

---

---

## Apresentando o banco de dados de log

---

Tópicos relacionados:

- ◆ [Trabalhos de banco de dados, página 318](#)
- ◆ [Administrando o banco de dados de log, página 319](#)

O Log Database armazena os registros da atividade de Internet e as ações de filtragem do Websense associadas. A instalação cria o banco de dados de log com um banco de dados de catálogo e uma partição de banco de dados.

O **banco de dados de catálogo** fornece um único ponto de conexão para os vários componentes do Websense que precisam acessar o banco de dados de log: páginas de Status, Log Server, relatórios de apresentação e relatórios investigativos. Contém informações de apoio para as partições do banco de dados, incluindo a lista de nomes de categorias, definições de classes de risco, mapeamento de usuários para grupos,

trabalhos de banco de dados e assim por diante. O banco de dados de catálogo também mantém uma lista de todas as partições de banco de dados disponíveis.

**As partições do banco de dados** armazenam os registros individuais da atividade de Internet. Para usuários do MSDE, novas partições são criadas com base em regras de substituição por tamanho estabelecidas pelo software Websense. Os usuários de Microsoft SQL Server podem configurar o banco de dados de log para iniciar uma nova partição com base no tamanho da partição ou um intervalo de datas (consulte *Configurando opções de substituição*, página 321, para obter mais informações).



**Obs.:**

As partições baseadas em data estão disponíveis apenas quando o software Websense usa o Microsoft SQL Server como o mecanismo de banco de dados.

---

Quando as partições são baseadas em tamanho, todos os registros em log recebidos são inseridos na partição ativa mais recente que cumpre a regra de tamanho. Quando a partição alcança o tamanho máximo designado, uma nova partição é criada para inserção de novos registros em log.

Quando as partições são baseadas em data, novas partições são criadas de acordo com o ciclo estabelecido. Por exemplo, se a opção de substituição é mensal, uma nova partição é criada assim que registros são recebidos para o novo mês. Os registros em log recebidos são inseridos na partição apropriada com base em data.

As partições de banco de dados fornecem vantagens de flexibilidade e desempenho. Por exemplo, você pode gerar relatórios a partir de uma única partição para limitar o escopo dos dados que devem ser analisados a fim de localizar as informações solicitadas.

## Trabalhos de banco de dados

Os seguintes trabalhos de banco de dados são instalados junto com o banco de dados de log. O SQL Server Agent deve estar em execução na máquina que executa o mecanismo de banco de dados (MSDE ou Microsoft SQL Server).

- ◆ O trabalho Extract, Transform, and Load (ETL) é executado continuamente, recebendo dados do Log Server, processando e inserindo no banco de dados de partição. O trabalho ETL deve estar em execução para processar registros de log no banco de dados de log.
- ◆ O trabalho de manutenção do banco de dados executa tarefas de manutenção do banco de dados e preserva o desempenho ótimo. É executado todas as noites, por padrão.
- ◆ O trabalho Internet Browse Time (IBT) analisa os dados recebidos e calcula o tempo de navegação para cada cliente. O trabalho de banco de dados IBT tem uso intensivo de recursos e afeta a maioria dos recursos do banco de dados. É executado todas as noites, por padrão.

Determinados aspectos desses trabalhos de banco de dados podem ser configurados na página Configurações > Banco de dados de log. Consulte [Configurações de administração do banco de dados de log](#), página 320, para obter mais informações.

Ao configurar a hora de início para o trabalho de manutenção e o trabalho de tempo de navegação na Internet, considere os recursos de sistema e o tráfego de rede. Esses trabalhos têm uso intensivo de recursos e podem reduzir o desempenho de registros em log e relatórios.

## Administrando o banco de dados de log

Tópicos relacionados:

- ◆ [Configurações de administração do banco de dados de log](#), página 320
- ◆ [Configurando opções de substituição](#), página 321
- ◆ [Configurando as opções de tempo de navegação na Internet](#), página 324
- ◆ [Configurando o registro de URLs completos](#), página 322
- ◆ [Configurando opções de manutenção do banco de dados de log](#), página 325
- ◆ [Configurando opções de partição do banco de dados de log](#), página 327
- ◆ [Configurando as partições disponíveis](#), página 328
- ◆ [Visualizando logs de erros](#), página 329

Administrar o banco de dados de log envolve controlar muitos aspectos das operações de bancos de dados, incluindo:

- ◆ Quais operações os trabalhos de banco de dados executam, e quando são executadas.
- ◆ As condições para criar novas partições de banco de dados.
- ◆ Quais partições estão disponíveis para relatórios.

Estas e outras opções fornecem um controle significativo à pessoa que administra o banco de dados de log. Consulte [Configurações de administração do banco de dados de log](#), página 320.

O Super administrador designa quem pode administrar o banco de dados de log ao criar funções. Consulte [Editando funções](#), página 254.



**Obs.:**

É recomendável limitar o número de administradores que têm a permissão para alterar as configurações do banco de dados de log.

## Configurações de administração do banco de dados de log

Tópicos relacionados:

- ◆ [Administrando o banco de dados de log](#), página 319

A página **Geração de relatórios > Log Database**, acessada na guia Configurações, permite administrar diversos aspectos das operações do banco de dados de log. As opções são agrupadas em seções lógicas que são descritas separadamente.

Você deve clicar no botão **Salvar agora** em uma seção para ativar as alterações na seção. Clicar em **Salvar agora** registra as alterações na seção imediatamente. (Não é necessário clicar em **Salvar tudo**.)

O alto da página mostra o nome do banco de dados de log ativo e um link **Atualizar**. Este link **Atualizar** exibe novamente as informações na página banco de dados de log. Quaisquer alterações que não foram aplicadas com o botão **Salvar agora** apropriado são perdidas.

Para obter instruções detalhadas sobre o uso de cada seção, clique no link apropriado, abaixo.

- ◆ Opções de substituição do banco de dados: [Configurando opções de substituição](#), página 321.
- ◆ Registro de URLs completos: [Configurando o registro de URLs completos](#), página 322.
- ◆ Configuração de tempo de navegação na Internet: [Configurando as opções de tempo de navegação na Internet](#), página 324.
- ◆ Configuração de manutenção: [Configurando opções de manutenção do banco de dados de log](#), página 325.
- ◆ Criação de partição do banco de dados: [Configurando opções de partição do banco de dados de log](#), página 327.
- ◆ Partições disponíveis: [Configurando as partições disponíveis](#), página 328.
- ◆ Atividade do log de erros: [Visualizando logs de erros](#), página 329.

## Configurando opções de substituição

Tópicos relacionados:

- ◆ [Configurações de administração do banco de dados de log](#), página 320
- ◆ [Configurando as opções de tempo de navegação na Internet](#), página 324
- ◆ [Configurando o registro de URLs completos](#), página 322
- ◆ [Configurando opções de manutenção do banco de dados de log](#), página 325
- ◆ [Configurando opções de partição do banco de dados de log](#), página 327
- ◆ [Configurando as partições disponíveis](#), página 328
- ◆ [Visualizando logs de erros](#), página 329

Use a seção **Opções de substituição do banco de dados** da página Geração de relatórios > Banco de dados de log (guia Configurações) para especificar quando o Log Database deve criar uma nova partição de banco de dados (substituição).

1. Use as opções **Substituição a cada** para indicar se as partições do banco de dados devem ser substituídas com base em tamanho (MB) ou data (semanas ou meses), dependendo do mecanismo de banco de dados que está sendo usado.

Os usuários de MSDE devem usar a opção de substituição por tamanho. Os usuários de Microsoft SQL Server podem escolher tamanho ou data.

- Para substituições com base em data, selecione **semanas** ou **meses** como a unidade de medida, e especifique durante quantas semanas ou meses de calendário uma partição deve ser mantida antes da criação de uma nova.
- Para substituições baseadas em tamanho, selecione **MB** e especifique o número de megabytes que o banco de dados deve alcançar para que a substituição comece.

Os usuários de **Microsoft SQL Server** podem usar um tamanho até 204800 MB.

Os usuários de **MSDE** devem usar um tamanho entre 100 MB e 1536 MB.



**Obs.:**

Se a substituição começar usando uma parte do dia com muito movimento, o desempenho pode ficar mais lento durante o processo de substituição.

Para evitar essa possibilidade, alguns ambientes optam por definir a substituição automática para um período de tempo longo ou um tamanho máximo grande. Então, fazem substituições manuais periódicas para evitar que a substituição automática ocorra. Consulte [Configurando opções de partição do banco de dados de log](#), página 327, para obter informações sobre substituições manuais.

Lembre-se de que partições individuais extremamente grandes não são recomendadas. O desempenho de relatórios pode ficar lento se os dados não forem divididos em várias partições menores.

Quando uma nova partição de banco de dados é criada, os relatórios são habilitados automaticamente para a partição (consulte [Configurando as partições disponíveis](#), página 328).

2. Clique em **Salvar agora** para ativar as alterações para as opções de substituição do banco de dados.

## Configurando o registro de URLs completos

Tópicos relacionados:

- ◆ [Configurações de administração do banco de dados de log](#), página 320
- ◆ [Configurando opções de substituição](#), página 321
- ◆ [Configurando as opções de tempo de navegação na Internet](#), página 324
- ◆ [Configurando opções de manutenção do banco de dados de log](#), página 325
- ◆ [Configurando opções de partição do banco de dados de log](#), página 327
- ◆ [Configurando as partições disponíveis](#), página 328
- ◆ [Visualizando logs de erros](#), página 329

A seção **Registro de URLs completos** da página Geração de relatórios > Banco de dados de log (guia Configurações) permite que você decida qual parte do URL é registrada em log para cada solicitação de Internet.

**Obs.:**

Administrar o tamanho do banco de dados de log é uma preocupação importante em redes de alto volume. Desabilitar a opção Registro de URLs completos é uma forma de controlar o tamanho e o crescimento do banco de dados.

1. Marque **Registro dos logs de URLs completos de cada site solicitado** para registrar o URL completo, incluindo o domínio (www.domain.com) e o caminho para a página específica (/products/productA.html).

**Importante**

Habilite o registro de URLs completos se planeja gerar relatórios da atividade de verificação em tempo real (consulte *Relatórios sobre a atividade de verificação em tempo real*, página 151). Caso contrário, os relatórios só podem exibir o domínio (www.domain.com) do site classificado, ainda que as páginas individuais do site recaiam em diferentes categorias ou contenham diferentes ameaças.

Se esta opção não estiver marcada, somente os nomes de domínios são registrados em log. Esta opção resulta em um banco de dados menor, mas fornece menos detalhes.

Registrar os URLs completos produz um banco de dados do registro maior, mas oferece mais detalhes.

Se você ativar o registro de URLs completos quando a consolidação estiver ativa, o registro consolidado contém o URL completo do primeiro registro no grupo de consolidação. Consulte *Configurando opções de consolidação*, página 312, para obter mais informações.

2. Clique em **Salvar agora** para ativar as alterações para as opções de registro de URLs completos.

## Configurando as opções de tempo de navegação na Internet

Tópicos relacionados:

- ◆ [Configurações de administração do banco de dados de log](#), página 320
- ◆ [Configurando opções de substituição](#), página 321
- ◆ [Configurando o registro de URLs completos](#), página 322
- ◆ [Configurando opções de manutenção do banco de dados de log](#), página 325
- ◆ [Configurando opções de partição do banco de dados de log](#), página 327
- ◆ [Configurando as partições disponíveis](#), página 328
- ◆ [Visualizando logs de erros](#), página 329

Os relatórios de tempo de navegação na Internet fornecem uma visão da quantidade de tempo que os usuários gastaram na Internet. Um trabalho de banco de dados noturno calcula o tempo de navegação para cada cliente com base nos novos registros recebidos naquele dia. Defina as opções de tempo de navegação na seção **Configuração de tempo de navegação na Internet** da página Geração de relatórios > Banco de dados de log.

1. Escolha uma **Hora inicial do trabalho** para o trabalho de banco de dados de IBT.

Os recursos de tempo e sistema requeridos por este trabalho variam dependendo do volume de dados registrados por dia. É melhor executar este trabalho em um horário diferente do trabalho de manutenção noturno (consulte [Configurando opções de manutenção do banco de dados de log](#), página 325), e selecionar um horário de pouco movimento na rede para minimizar qualquer impacto sobre a geração de relatórios.

O trabalho de banco de dados IBT tem uso intensivo de recursos e afeta a maioria dos recursos do banco de dados. Se você habilitar este trabalho, defina a hora de início para que não interfira com a capacidade do sistema de banco de dados de processar relatórios programados e outras operações importantes. Além disso, monitore o trabalho para determinar se um hardware mais robusto é necessário para acomodar todas as necessidades de processamento.

2. Para **Limite de tempo de leitura**, defina um número médio de minutos para ler um site da Web específico.

O limite de tempo de leitura define as sessões do navegador para o objetivo de relatórios de tempo de navegação na Internet. Abrir um navegador gera tráfego HTTP. Isso representa o início de uma sessão de navegação. A sessão fica aberta enquanto o tráfego HTTP é gerado continuamente no intervalo de tempo definido

aqui. A sessão de navegação é considerada fechada quando essa quantidade de tempo passa sem tráfego HTTP. Uma nova sessão de navegação começa assim que o tráfego HTTP é gerado novamente.

**Obs.:**

É melhor alterar o Limite de tempo de leitura o mais raramente possível e iniciar uma nova partição do banco de dados sempre que você fizer uma alteração.

Para evitar dados inconsistentes nos relatórios, gere os relatórios IBT a partir de partições do banco de dados que usam o mesmo valor de Limite de tempo de leitura.

Lembre-se de que alguns sites da Web usam uma técnica de atualização automática para atualizar as informações com frequência. Um exemplo é um site de notícias que alterna a exibição das reportagens mais recentes. Essa atualização gera novo tráfego HTTP. Portanto, quando esse tipo de site é deixado aberto, novos registros em log são gerados cada vez que o site é atualizado. Não há intervalo no tráfego HTTP e a sessão do navegador não é fechada.

3. Defina um valor de **Último tempo de leitura** para contabilizar o tempo dedicado à leitura do último site da Web antes do fim de uma sessão de navegação.  
Quando o intervalo de tempo de tráfego HTTP é mais longo do que o limite de tempo de leitura, a sessão é encerrada e o valor do Último tempo de leitura é adicionado ao tempo da sessão.
4. Clique em **Salvar agora** para ativar as alterações na configuração de tempo de navegação na Internet.

## Configurando opções de manutenção do banco de dados de log

Tópicos relacionados:

- ◆ [Configurações de administração do banco de dados de log, página 320](#)
- ◆ [Configurando opções de substituição, página 321](#)
- ◆ [Configurando as opções de tempo de navegação na Internet, página 324](#)
- ◆ [Configurando o registro de URLs completos, página 322](#)
- ◆ [Configurando opções de partição do banco de dados de log, página 327](#)
- ◆ [Configurando as partições disponíveis, página 328](#)
- ◆ [Visualizando logs de erros, página 329](#)

Use a seção **Configuração de manutenção** da página Geração de relatórios > Banco de dados de log (guia Configurações) para controlar determinados aspectos do processamento do banco de dados, como a hora para execução do trabalho de manutenção do banco de dados, algumas das tarefas que executa, e exclusão das partições do banco de dados e dos registros em log dos erros.

1. Para **Hora inicial da manutenção**, selecione a hora do dia para execução do trabalho de manutenção do banco de dados.

Os recursos de tempo e sistema requeridos por este trabalho variam dependendo das tarefas que você seleciona nesta área. Para minimizar qualquer impacto sobre outras atividades e sistemas, é melhor executar este trabalho durante um horário de pouco movimento na rede, diferente do horário definido para o trabalho de IBT (consulte [Configurando as opções de tempo de navegação na Internet](#), página 324).

2. Marque **Excluir partições automaticamente**, e especifique o número de dias (de 2 a 365) após os quais as partições devem ser excluídas.



#### **Aviso**

Depois que uma partição foi excluída, os dados não podem ser recuperados. Consulte [Configurando as partições disponíveis](#), página 328, para uma forma alternativa de excluir partições.

---

3. Marque **Ativar a reindexação automática**, e selecione um dia da semana para que esse processamento seja executado automaticamente a cada semana.

Reindexar o banco de dados é importante para manter a integridade do banco de dados e otimizar a velocidade dos relatórios.



#### **Importante**

É melhor executar este processamento durante um período de pouco uso da rede. Reindexar as partições do banco de dados exige muitos recursos e tempo. Os relatórios não devem ser executados durante o processo.

---

4. Marque **Número de dias antes de excluir os batches com falha** e digite um número de dias (de 0 a 90) após os quais os batches com falha devem ser excluídos.

Se esta opção não for marcada, os batches com falha são retidos indefinidamente para processamento futuro.

Se houver espaço em disco insuficiente ou permissões de banco de dados inadequadas para inserir registros em log no banco de dados, os registros são marcados como um **batch com falha**. Em geral, esses batches são reprocessados com êxito e inseridos no banco de dados durante o trabalho de de manutenção do banco de dados noturno.

Porém, este reprocessamento não pode ser bem-sucedido se o problema de espaço em disco ou permissão não foi solucionado. Além disso, se a opção **Processar os batches não processados** não estiver selecionada, os batches com falha nunca são reprocessados. Eles são excluídos após o tempo especificado aqui.

5. Marque **Processar os batches não processados** para que o trabalho de manutenção do banco de dados noturno reprocessasse quaisquer batches com falha.

Se esta opção estiver desmarcada, os batches com falha nunca são reprocessados. Eles são excluídos após o tempo especificado acima, se houver.

6. Marque **Número de dias antes de excluir o log de erros**, e digite um número de dias (0 a 90) após o qual os registros de erro no banco de dados devem ser excluídos do banco de dados de catálogo.  
Se esta opção não estiver marcada, os logs de erros são mantidos indefinidamente.
7. Clique em **Salvar agora** para ativar as alterações nas opções de configuração de manutenção.

## Configurando opções de partição do banco de dados de log

Tópicos relacionados:

- ◆ [Configurações de administração do banco de dados de log](#), página 320
- ◆ [Configurando opções de substituição](#), página 321
- ◆ [Configurando as opções de tempo de navegação na Internet](#), página 324
- ◆ [Configurando o registro de URLs completos](#), página 322
- ◆ [Configurando opções de manutenção do banco de dados de log](#), página 325
- ◆ [Configurando as partições disponíveis](#), página 328
- ◆ [Visualizando logs de erros](#), página 329

Use a seção **Criação de partição do banco de dados** da página Geração de relatórios > Banco de dados de log (guia Configurações) para definir características para novas partições do banco de dados, como local e tamanho. Esta área também permite criar uma nova partição imediatamente, em vez de esperar a substituição planejada (consulte [Configurando opções de substituição](#), página 321).

1. Insira o **Caminho de arquivo** para criar os arquivos de **Dados** e **Log** para novas partições do banco de dados.
2. Em **Tamanho inicial**, defina o tamanho de arquivo inicial (de 100 a 204800 MB) para os arquivos de **Dados** e **Log** para novas partições do banco de dados.

**Usuários de Microsoft SQL Server:** O intervalo aceitável é 100 - 204800

**Usuários de MSDE:** O intervalo aceitável é 100 - 1500



### Obs.:

A prática recomendada é calcular o tamanho médio da partição em um período de tempo. Em seguida, atualizar o tamanho inicial para aquele valor. Essa abordagem minimiza o número de vezes em que a partição deve ser expandida e libera recursos para processar dados nas partições.

3. Em **Crescimento**, defina o incremento pelo qual deve ser aumentado o tamanho, em megabytes (MB), dos arquivos de **Dados** e **Log** de uma partição quando espaço adicional é necessário.

**Usuários de Microsoft SQL Server:** O intervalo aceitável é 1 - 999999

**Usuários de MSDE:** O intervalo aceitável é 1 - 450

4. Clique em **Salvar agora** para implementar as alterações em caminho, tamanho e crescimento informadas.

As partições do banco de dados criadas após essas alterações usam as novas configurações.

5. Clique em **Criar agora** para criar uma nova partição na próxima vez que o trabalho ETL for executado (consulte *Trabalhos de banco de dados*, página 318), não importa quais sejam as configurações de substituição automática. Este processo em geral leva poucos minutos.

Para que a nova partição use as alterações realizadas nesta seção, clique em **Salvar agora** antes de clicar em **Criar agora**.

Clique no link Atualizar no painel de conteúdo periodicamente. A área Partições disponíveis mostrará a nova partição quando o processo de criação estiver concluído.

## Configurando as partições disponíveis

Tópicos relacionados:

- ◆ [Configurações de administração do banco de dados de log](#), página 320
- ◆ [Configurando opções de substituição](#), página 321
- ◆ [Configurando as opções de tempo de navegação na Internet](#), página 324
- ◆ [Configurando o registro de URLs completos](#), página 322
- ◆ [Configurando opções de manutenção do banco de dados de log](#), página 325
- ◆ [Configurando opções de partição do banco de dados de log](#), página 327
- ◆ [Visualizando logs de erros](#), página 329

A seção **Partições disponíveis** da página Geração de relatórios > Banco de dados de log (guia Configurações) lista todas as partições de banco de dados disponíveis para relatórios. A lista mostra as datas cobertas, e também o tamanho e o nome de cada partição.

Use esta lista para controlar quais partições do banco de dados estão incluídas em relatórios, e para selecionar partições individuais para exclusão.

1. Marque **Habilitar** ao lado de cada partição que será incluída em relatórios.

Use as opções **Todas** e **Nenhuma** acima da lista, conforme apropriado.

Você deve ativar pelo menos uma partição para relatórios. Use a opção **Nenhuma** para desativar todas as partições simultaneamente, de forma a poder ativar apenas algumas.

Use estas opções para administrar quantos dados devem ser analisados ao gerar relatórios e acelerar o processamento dos relatórios. Por exemplo, se você planeja gerar uma série de relatórios para junho, desmarque todas as partições exceto as que têm datas em junho.



#### Importante

Esta seleção afeta os relatórios agendados e também relatórios executados de forma interativa. Para evitar a geração de relatórios sem data, certifique-se de que as partições relevantes estejam habilitadas quando os relatórios são agendados para execução.

2. Clique na opção **Excluir** ao lado de um nome de partição se a partição não é mais necessária. A partição é excluída na próxima execução do trabalho noturno de manutenção do banco de dados.



#### Aviso

Use esta opção com cuidado. Não é possível recuperar partições excluídas.

Excluir as partições obsoletas minimiza o número de partições no banco de dados de log, o que melhora o desempenho do banco de dados e de relatórios. Use esta opção Excluir para excluir partições individuais, conforme necessário. Consulte [Configurando opções de manutenção do banco de dados de log](#), página 325, se prefere excluir as partições mais antigas de acordo com uma programação.

3. Clique em **Salvar agora** para ativar as alterações para as opções de partições disponíveis.

## Visualizando logs de erros

Tópicos relacionados:

- ◆ [Configurações de administração do banco de dados de log](#), página 320
- ◆ [Configurando opções de substituição](#), página 321
- ◆ [Configurando as opções de tempo de navegação na Internet](#), página 324
- ◆ [Configurando o registro de URLs completos](#), página 322
- ◆ [Configurando opções de manutenção do banco de dados de log](#), página 325
- ◆ [Configurando opções de partição do banco de dados de log](#), página 327
- ◆ [Configurando as partições disponíveis](#), página 328

Use a seção **Atividade do log de erros** da página Geração de relatórios > Banco de dados de log (guia Configurações) para exibir registros de erros que ocorreram durante os trabalhos executados no banco de dados do Websense (consulte [Trabalhos de banco de dados](#), página 318). Estas informações podem ser úteis para solucionar problemas.

Escolha uma das seguintes opções.

- ◆ Escolha um número na lista suspensa para exibir essa quantidade de entradas no log de erros.
- ◆ Escolha **Visualizar todos** para exibir todas as entradas no log de erros.
- ◆ Escolha **Visualizar nenhum** para ocultar todas as entradas no log de erros.

## Configurando relatórios investigativos

---

Tópicos relacionados:

- ◆ [Conexão de banco de dados e padrões de relatórios](#), página 330
- ◆ [Opções de exibição e saída](#), página 332

Os relatórios investigativos permitem aprofundar interativamente as informações sobre o uso de Internet de sua empresa. Consulte [Relatórios investigativos](#), página 115.

O link Opções na página principal de relatórios investigativos permite modificar qual banco de dados de log é usado para relatórios. Também permite modificar a exibição padrão para relatórios de detalhes. Consulte [Conexão de banco de dados e padrões de relatórios](#), página 330.

O arquivo **wse.ini** permite configurar determinados padrões para exibição de relatórios de resumo e em vários níveis. Também fornece controle sobre o tamanho de página padrão usado quando um relatório é exportado como PDF. Consulte [Opções de exibição e saída](#), página 332.

## Conexão de banco de dados e padrões de relatórios

Tópicos relacionados:

- ◆ [Configurando relatórios investigativos](#), página 330
- ◆ [Opções de exibição e saída](#), página 332
- ◆ [Relatórios de resumo](#), página 117
- ◆ [Relatórios de resumo em vários níveis](#), página 121

Use a página **Relatórios investigativos > Opções** para conectar-se com o banco de dados de log desejado, e controlar padrões para a exibição de dados de relatórios investigativos.

As alterações realizadas nesta página afetam os seus relatórios. Outros administradores, ou mesmo usuários que fazem logon para relatórios próprios, podem alterar esses valores para suas próprias atividades de relatórios.

1. Escolha o banco de dados de log para uso para relatórios investigativos.
  - Marque **Visualizar o banco de dados do catálogo** para se conectar com o banco de dados de log onde o Log Server está fazendo registros. Continue para a etapa 2.
  - Para acessar outro banco de dados de log:
    - a. Desmarque a opção **Visualizar o banco de dados do catálogo**.
    - b. Digite as seguintes informações para identificar o banco de dados de log desejado. (Os relatórios investigativos podem ser gerados a partir de um banco de dados da versão v6.3.x ou v7.0.)

Campo	Descrição
Servidor	Insira o nome da máquina ou o endereço IP onde o banco de dados de log está localizado.
Banco de dados	Insira o nome do banco de dados de log.
ID de usuário	Insira o ID de usuário de uma conta que tem permissão para acessar o banco de dados. Deixe em branco se o Log Server foi instalado para usar uma conexão confiável para acessar o banco de dados de log. Se não tiver certeza, insira <b>sa</b> . É o ID de usuário padrão para MSDE e o ID de administrador padrão para o Microsoft SQL Server.
Senha	Insira a senha para o ID de usuário especificado. Deixe em branco para uma conexão confiável.

2. Selecione os seguintes padrões para relatórios de detalhes.

Campo	Descrição
Selecione o intervalo de datas padrão para Relatórios investigativos.	Escolha o intervalo de datas para a exibição do relatório de resumo inicial.
Selecione o formato de relatório de detalhes padrão	Escolha <b>Seleção inteligente de colunas</b> para exibir relatórios de detalhes com o conjunto de colunas padrão para as informações que estão sendo reportadas. Escolha <b>Seleção personalizada de colunas</b> para especificar as colunas exatas para exibição inicial em todos os relatórios de detalhes. Use a lista Colunas disponíveis para fazer as suas seleções. Os usuários podem modificar as colunas exibidas após a geração do relatório.

Campo	Descrição
Selecione o tipo de relatório	<p>Escolha se deseja abrir os relatórios de detalhes mostrando inicialmente:</p> <ul style="list-style-type: none"> <li>• <b>Detalhe:</b> cada registro aparece em uma linha separada; o tempo pode ser exibido.</li> <li>• <b>Resumo:</b> agrupa em uma única entrada todos os registros que compartilham um elemento comum. O elemento especificado varia, de acordo com as informações no relatório. Tipicamente, a coluna mais à direita antes da medida mostra o elemento resumido. O tempo não pode ser exibido.</li> </ul>
Colunas disponíveis / Relatório atual	<p>Selecione um nome de coluna na lista Colunas disponíveis e clique na seta apropriada para movê-la para a lista Relatório atual. Até 7 colunas podem estar na lista Relatório atual.</p> <p>Depois que a lista Relatório atual contém todas as colunas para relatórios de detalhes iniciais, defina a ordem das colunas. Selecione uma entrada na lista e use os botões de seta para cima e para baixo para alterar sua posição.</p>

3. Clique em **Salvar opções** para salvar todas as alterações imediatamente.

## Opções de exibição e saída

Tópicos relacionados:

- ◆ [Configurando relatórios investigativos](#), página 330
- ◆ [Conexão de banco de dados e padrões de relatórios](#), página 330
- ◆ [Saída para arquivo](#), página 139

Você pode fazer ajustes na forma como determinadas opções de relatórios e resultados de relatórios são exibidos em relatórios investigativos de resumo e em vários níveis, e especificar o tamanho de página padrão quando os relatórios são exportados para o formato PDF.

Essas opções de configuração de relatórios investigativos são definidas no arquivo **wse.ini**. O local padrão é:

C:\Program Files\WebSense\webroot\Explorer\wse.ini

A tabela a seguir lista os parâmetros que afetam a exibição e a saída de relatórios investigativos, o que cada um controla e seu valor padrão. (Não modifique quaisquer outras configurações no arquivo wse.ini.)

Parâmetro	Descrição
maxUsersMenu	O banco de dados deve ter menos usuários do que este valor (por padrão, 5000) para exibir Usuário como uma opção de relatório na lista Uso da Internet por.
maxGroupsMenu	O banco de dados deve ter menos grupos do que este valor (por padrão, 3000) para exibir Grupo como uma opção de relatório na lista Uso da Internet por. <b>Obs.:</b> Deve haver 2 ou mais grupos para que Grupo apareça na lista Uso da Internet por. Também deve haver 2 ou mais domínios para que Domínio apareça na lista Uso da Internet por. Não há um valor máximo para domínios.
maxUsersDrilldown	Isso funciona com o parâmetro warnTooManyHits para controlar quando a opção Usuário é exibida em vermelho. As letras vermelhas indicam que selecionar Usuário produzirá um relatório muito grande, cuja geração poderá demorar muito. Se houver mais usuários do que este valor (por padrão, 5000), e mais ocorrências do que o valor warnTooManyHits, a opção Usuário é exibida em vermelho em várias listas suspensas e listas de valores. Se houver mais usuários do que este valor, mas menos ocorrências do que o valor warnTooManyHits, a opção Usuário é exibida em cor normal e o relatório resultante terá um tamanho mais razoável.
maxGroupsDrilldown	A opção Grupo é exibida em vermelho durante o aprofundamento se o relatório proposto inclui mais grupos do que este número (por padrão, 2000). As letras vermelhas indicam que selecionar Grupo produzirá um relatório muito grande, cuja geração poderá demorar muito.
warnTooManyHits	Isso funciona com o parâmetro maxUsersDrilldown para controlar quando a opção Usuário é exibida em vermelho. Se houver mais usuários do que o valor maxUsersDrilldown, mas menos ocorrências do que este valor (por padrão, 10000), a opção Usuário <i>não</i> é exibida em vermelho. Se houver mais usuários do que o valor maxUsersDrilldown, e mais ocorrências do que este valor, a opção Usuário é exibida em vermelho. As letras vermelhas indicam que selecionar Usuário produzirá um relatório muito grande, cuja geração poderá demorar muito.
hitsPerPage	Isso determina o número máximo de itens (por padrão, 100) exibidos por página. (Não afeta os relatórios impressos.)

Parâmetro	Descrição
maxOutputBufferSize	É a quantidade máxima de dados (em bytes) que podem ser exibidos na página principal de relatórios investigativos. Se os dados solicitados excederem este limite (por padrão, 4000000, ou 4 milhões de bytes), uma mensagem declarando que alguns resultados não são mostrados aparece em vermelho no fim do relatório.  Valores maiores permitem que você exiba quantidades maiores de dados em um relatório, se isso for uma questão. Porém, se ocorrerem erros de memória, considere a redução deste valor.
sendMulti	Esta opção é desabilitada (0) por padrão. Defina como 1 (habilitada) para dividir relatórios de detalhes programados muito grandes em vários arquivos com 10.000 linhas cada. Os arquivos que representam um relatório são compactados e encaminhados aos destinatários de e-mail. Os arquivos de relatórios podem ser extraídos com os utilitários de compactação de arquivos mais comuns.
maxSlices	É o número máximo de fatias distintas (por padrão, 6) em um gráfico de pizza, incluindo uma fatia Outro, que combina todos os valores que não têm fatias individuais.
timelineCompressionThreshold	Esta opção é usada apenas para Atividade do usuário por dia ou Atividade do usuário por mês, quando a opção Agrupar ocorrências similares/Exibir todas as ocorrências está disponível. O relatório contrai todas as ocorrências com a mesma categoria que ocorrem no número de segundos definido aqui (por padrão, 10).
PageSize	Os resultados de relatórios investigativos podem ser exportados para o formato PDF para facilitar a distribuição ou a impressão. O tamanho de página (por padrão, Carta) pode ser: <ul style="list-style-type: none"> <li>♦ A4 (8,27 X 11,69 polegadas)</li> <li>♦ Carta (8,5 X 11 polegadas)</li> </ul>

## Relatório próprio

Tópicos relacionados:

- ♦ [Configurando preferências de relatórios, página 303](#)
- ♦ [Acessando os relatórios próprios, página 141](#)
- ♦ [Relatórios investigativos, página 115](#)

Relatório próprio é um recurso que você pode habilitar para permitir que os usuários exibam relatórios investigativos sobre sua atividade de Internet pessoal. Isso permite que vejam qual tipo de informações está sendo coletada e monitorada sobre eles, o que

cumpra as normas governamentais em muitos países. Além disso, visualizar sua própria atividade pode estimular outros usuários a alterar seus hábitos de navegação a fim de cumprir a política de Internet da empresa.

**Obs.:**

O relatório próprio está disponível apenas quando o Websense Manager e os componentes de relatórios estão instalados em um sistema operacional Windows. Consulte o *Guia de Implantação* para obter informações adicionais.

Para habilitar o relatório próprio:

1. Vá para **Configurações > Gerais > Serviços de diretório**, e configure o serviço de diretório usado para autenticar usuários que acessam o Websense Manager com suas credenciais de rede. Isso pode ter sido feito anteriormente para habilitar a filtragem por nomes de usuário e grupo. Consulte *Serviços de diretório*, página 60.  
Se a sua instalação inclui vários Policy Servers, você deve fazer logon em cada um deles e configurar a página Serviços de diretório com informações para o serviço de diretório apropriado.
2. Vá para **Configurações > Geração de relatórios > Preferências**, e marque a caixa de seleção **Permitir relatório próprio**. Consulte *Configurando preferências de relatórios*, página 303.

Depois de habilitar a opção, forneça aos usuários as informações que precisam para executar os relatórios:

- ◆ O URL para acessar a interface de relatório próprio. Lembre aos usuários que eles podem salvar o URL como um favorito ou marcar para uso futuro.  
Leia mais para obter informações detalhadas sobre o URL.
- ◆ Qual Policy Server deve ser escolhido durante o logon.  
Em redes com apenas um Policy Server, isso não é necessário. Se a sua rede inclui vários Policy Servers, forneça aos usuários o endereço IP do Policy Server configurado para comunicação com o serviço de diretório que autentica o logon de rede. Este também é o Policy Server especificado quando você instalou o Log Server.
- ◆ Qual nome de usuário e senha devem ser usados durante o logon.  
Os usuários de relatórios próprios devem informar o nome de usuário de rede e a senha durante o logon.

O URL para acessar a interface de relatório próprio é:

```
https://<IPdoServidor>:9443/mng/login/pages/  
selfReportingLogin.jsf
```

Em lugar de <IPdoServidor>), utilize o endereço IP da máquina em que o Websense Manager está sendo executado.

Os administradores e usuários também podem acessar a página de logon de relatório próprio abrindo a página de logon no Websense Manager e clicando no link Relatório próprio.

Se a sua rede inclui **vários Policy Servers**, você deve informar aos usuários qual deve ser escolhido durante o logon de relatório próprio.

# 14

## Configuração da rede

Tópicos relacionados:

- ◆ [Configuração de hardware](#), página 338
- ◆ [Configuração do Network Agent](#), página 339
- ◆ [Verificando a configuração do Network Agent](#), página 346

Quando você executa o software Websense em modo independente (stand-alone: não integrado com um proxy ou firewall), o Websense Network Agent habilita:

- ◆ Filtragem de conteúdo de Internet
- ◆ Gerenciamento de protocolos de rede e aplicativos de Internet
- ◆ Gerenciamento de largura de banda
- ◆ Registro dos bytes transferidos

Em uma implementação integrada do software Websense, um produto de terceiros pode cuidar da tarefa de rotear solicitações de usuários para o software Websense para filtragem, e rotear as páginas de bloqueio de volta para o cliente. Neste ambiente, o Network Agent pode ser usado para filtrar solicitações não-HTTP, fornecer detalhes de registro ou ambos.

O Network Agent monitora continuamente o uso geral da rede, incluindo bytes transferidos pela rede. O agente envia resumos de uso para o software Websense em intervalos predefinidos. Cada resumo inclui hora de início e fim, bytes usados no total e bytes usados por protocolo.

Por padrão, o Network Agent também fornece dados de uso de banda para o Policy Server e dados de registro de filtragem para o Filtering Service.

O Network Agent em geral é configurado para ver todo o tráfego em sua rede. O agente diferencia entre:

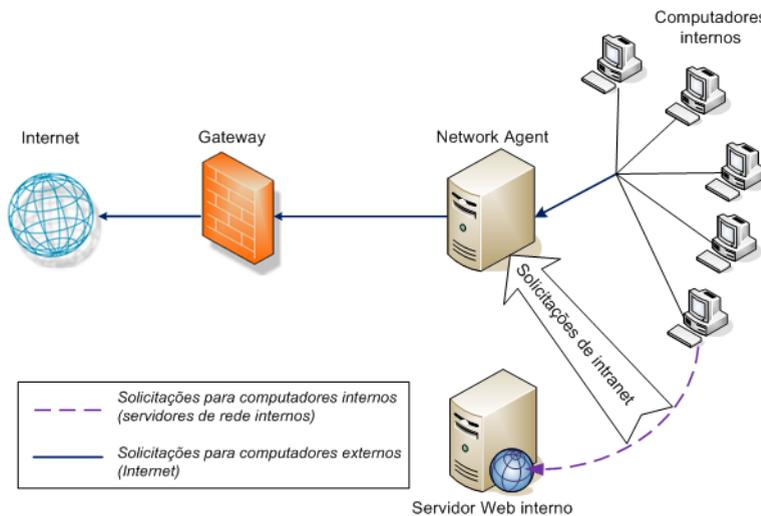
- ◆ Solicitações enviadas de computadores internos para computadores internos (acessos em um servidor de intranet, por exemplo)
- ◆ Solicitações enviadas de computadores internos para computadores externos, como servidores Web (solicitações de Internet de usuários, por exemplo)

Esta última é a preocupação primária no monitoramento do uso da Internet por funcionários.

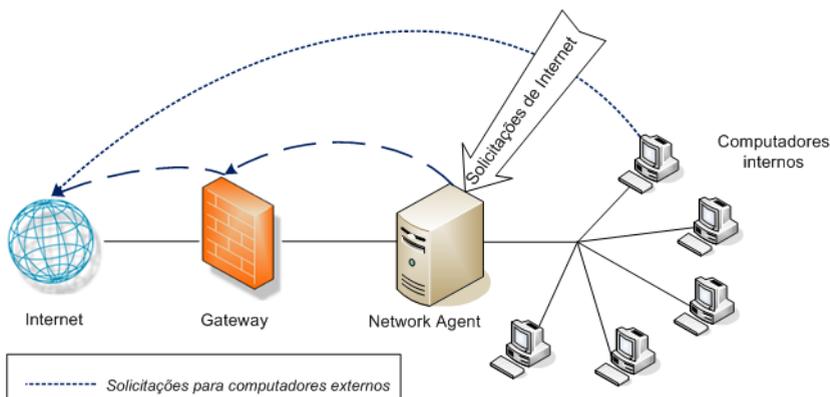
## Configuração de hardware

Cada instância do Network Agent monitora o tráfego **com origem** nos computadores que você identificar como pertencentes à sua rede. Por padrão, monitora o tráfego **de destino** apenas para os computadores internos que você especificar (por exemplo, servidores Web internos).

Você pode personalizar quais computadores internos (segmentos de rede) são monitorados por cada instância do Network Agent, ou mesmo por cada placa de rede em um computador com Network Agent.



Monitorando solicitações para computadores internos



Monitorando solicitações para computadores externos

Cada instância do Network Agent deve:

- ◆ Estar posicionada de forma apropriada na rede para detectar tráfego de/para todos os computadores monitorados.
- ◆ Ter no mínimo 1 placa de rede dedicada ao monitoramento do tráfego.

O Network Agent pode ser instalado em um computador com várias placas de rede, e pode usar várias placas de rede para monitorar solicitações e enviar páginas de bloqueio. Se você acrescentar uma nova placa de rede ao computador do Network Agent, reinicialize o serviço Network Agent e depois configure a nova placa de rede (consulte [Definindo as configurações de placa de rede](#), página 343).

**Obs.:**

Para determinar se o Network Agent pode ver o tráfego em um segmento de rede, use o utilitário Network Traffic Detector. Consulte [Verificando a configuração do Network Agent](#), página 346.

Mais informações sobre o posicionamento do Network Agent e os requisitos de placas de rede estão disponíveis no *Guia de Implantação*.

Para obter informações sobre como configurar o Network Agent para monitorar solicitações de rede interna, usar placas de rede específicas e o registro de log aprimorado, consulte [Configuração do Network Agent](#), página 339.

## Configuração do Network Agent

**Tópicos relacionados:**

- ◆ [Configuração de hardware](#), página 338
- ◆ [Definindo as configurações globais](#), página 340
- ◆ [Definindo as configurações locais](#), página 341
- ◆ [Definindo as configurações de placa de rede](#), página 343
- ◆ [Adicionando ou editando endereços IP](#), página 345

Depois de instalar o Network Agent, use o Websense Manager para configurar seu comportamento de monitoramento de rede. As configurações do Network Agent são divididas em duas áreas principais:

- ◆ **Configurações globais** afetam todas as instâncias do Network Agent. Use essas configurações para:
  - Identificar os computadores em sua rede.
  - Listar os computadores em sua rede que devem ser monitorados pelo Network Agent para solicitações **recebidas** (por exemplo, servidores Web internos).
  - Especificar o comportamento de registro de protocolos e cálculo de banda.

- ◆ **Configurações locais** aplicam-se apenas à instância selecionada do Network Agent. Use essas configurações para:
  - Identificar qual instância do Filtering Service está associada com cada Network Agent.
  - Identificar os proxies e caches usados pelos computadores que este Network Agent monitora.
  - Configurar como cada placa de rede no computador do Network Agent é usada (para monitorar solicitações, enviar páginas de bloqueio ou ambos).  
As configurações de placa de rede também determinam qual segmento da rede cada instância do Network Agent monitora.

## Definindo as configurações globais

Tópicos relacionados:

- ◆ [Configuração de hardware](#), página 338
- ◆ [Definindo as configurações locais](#), página 341
- ◆ [Definindo as configurações de placa de rede](#), página 343
- ◆ [Adicionando ou editando endereços IP](#), página 345

Use a página **Configurações > Network Agent > Global** para definir o comportamento básico de monitoramento e registro para todas as instâncias do Network Agent.

A lista **Definição de rede interna** identifica os computadores que são parte de sua rede. Por padrão, o Network Agent não monitora o tráfego (comunicações da rede interna) enviado entre esses computadores.

Um conjunto inicial de entradas é fornecido por padrão. Você pode adicionar outras entradas, ou editar ou excluir entradas existentes.

A lista **Tráfego interno a ser monitorado** inclui quaisquer computadores incluídos com a Definição de rede interna para a qual você **quer** que o Network Agent monitore o tráfego. Isso pode incluir servidores Web internos, por exemplo, para ajudar você a monitorar conexões internas.

Quaisquer solicitações enviadas de qualquer lugar da rede para os computadores internos especificados são monitoradas. Por padrão, esta lista está em branco.

- ◆ Clique em **Adicionar** para adicionar um endereço IP ou um intervalo de endereços na lista apropriada. Consulte [Adicionando ou editando endereços IP](#), página 345, para obter mais informações.
- ◆ Para editar uma entrada na lista, clique no endereço IP ou no intervalo. Consulte [Adicionando ou editando endereços IP](#), página 345, para obter mais informações.
- ◆ Para remover uma entrada da lista, marque a caixa de seleção ao lado de um endereço IP ou intervalo, e depois clique em **Excluir**.

As opções **Configurações adicionais** permitem que você determine com que frequência o Network Agent calcula o uso de banda, e se e com que frequência o tráfego de protocolo é registrado:

<b>Campo</b>	<b>O que fazer</b>
Intervalo de cálculo da largura de banda	Digite um número entre 1 e 300 para especificar com que frequência, em segundos, o Network Agent deve calcular o uso de largura de banda. Uma entrada de 300, por exemplo, indica que o Network Agent calculará a largura de banda a cada 5 minutos. O padrão é 10 segundos.
Registrar tráfego de protocolos em log periodicamente	Marque esta opção para habilitar o campo Intervalo de registro em log.
Intervalo de registro em log	Digite um número entre 1 e 300 para especificar com que frequência, em minutos, o Network Agent registra protocolos. Uma entrada de 60, por exemplo, indica que o Network Agent gravará no arquivo de registro a cada hora. O padrão é 1 minuto.

Quando você terminar de fazer alterações, clique em **OK** para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Definindo as configurações locais

Tópicos relacionados:

- ◆ [Configuração de hardware, página 338](#)
- ◆ [Definindo as configurações globais, página 340](#)
- ◆ [Definindo as configurações de placa de rede, página 343](#)

Use a página **Configurações > Network Agent > Configurações locais** para configurar o comportamento de filtragem, as informações de proxy e outras configurações para a instância selecionada do Network Agent. O endereço IP da instância selecionada do Network Agent aparece na barra de título do painel de conteúdo e é destacado no painel de navegação da esquerda.

Use as configurações de **Definição do Filtering Service** para especificar qual Filtering Service está associado com a instância selecionada do Network Agent, e como responder a solicitações da Internet se o Filtering Service não estiver disponível.

<b>Campo</b>	<b>O que fazer</b>
Endereço IP do Filtering Service	Selecione o Filtering Service que está associado com este Network Agent.
Se o Filtering Service não estiver disponível	Selecione <b>Permitir</b> para permitir todas as solicitações ou selecione <b>Bloquear</b> para bloquear todas as solicitações até que o Filtering Service esteja disponível novamente. O padrão é Permitir.

Para garantir que as solicitações de usuário sejam monitoradas, filtradas e registradas corretamente, use a lista **Proxies e caches** para especificar o endereço IP de qualquer servidor proxy ou cache que se comunique com o Network Agent.

- ◆ Clique em **Adicionar** para adicionar um endereço IP ou um intervalo à lista. Consulte [Adicionando ou editando endereços IP](#), página 345, para obter mais informações.
- ◆ Para editar uma entrada na lista, clique no endereço IP ou no intervalo.
- ◆ Para remover uma entrada da lista, marque a caixa de seleção ao lado de um endereço IP ou intervalo, e depois clique em **Excluir**.

Use a lista **Placas de interface de rede** para configurar placas de rede individuais. Clique em uma placa de rede na coluna **Nome** e consulte [Definindo as configurações de placa de rede](#), página 343, para obter instruções adicionais.

Se as solicitações HTTP em sua rede forem passadas por uma porta não-padrão, clique em **Configurações avançadas do Network Agent** para fornecer as portas corretas para que o Network Agent monitore. Por padrão, as **Portas usadas para tráfego HTTP** são **8080, 80**.

As outras configurações nesta seção não devem ser alteradas, a não ser que você seja orientado pelo Suporte Técnico da Websense.

<b>Campo</b>	<b>Descrição</b>
Modo	<ul style="list-style-type: none"> <li>◆ Nenhum (padrão)</li> <li>◆ Geral</li> <li>◆ Erro</li> <li>◆ Detalhe</li> <li>◆ Largura de banda de rede</li> </ul>
Saída	<ul style="list-style-type: none"> <li>◆ Arquivo (padrão)</li> <li>◆ Janela</li> </ul>
Porta	55870 (padrão)

Quando terminar de alterar as configurações do Network Agent, clique em **OK** para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Definindo as configurações de placa de rede

Tópicos relacionados:

- ◆ [Configuração de hardware](#), página 338
- ◆ [Configuração do Network Agent](#), página 339
- ◆ [Definindo as configurações de monitoramento para uma placa de rede](#), página 344
- ◆ [Adicionando ou editando endereços IP](#), página 345

Use a página **Network Agent > Configurações locais > Configuração de NIC** para especificar como o Network Agent usa cada placa de rede disponível para monitorar e administrar o uso da rede.

A área **Informações NIC** fornece o contexto para as alterações que você faz, mostrando **endereço IP**, **descrição breve da placa de rede** e **nome da placa**. Use essas informações para garantir que está configurando a placa de rede certa.

### Monitoramento

Em uma configuração com várias placas de rede, você pode identificar uma placa de rede para monitorar o tráfego da rede e outra para servir páginas de bloqueio. Pelo menos uma placa de rede deve ser usada para monitoramento e mais de uma placa de rede pode monitorar o tráfego.

Use a seção **Monitoramento** para indicar se vai **Usar esta NIC para monitorar o tráfego**.

- ◆ Se esta placa de rede não for usada para monitoramento, desmarque a caixa de seleção e continue com a próxima seção.
- ◆ Se a placa de rede for usada para monitoramento, marque a caixa de seleção e clique em **Configurar**. Você é levado à página Configurar comportamento de monitoramento. Consulte [Definindo as configurações de monitoramento para uma placa de rede](#), página 344, para obter instruções.

### Outras opções de placa de rede

Além de configurar opções de monitoramento, você também pode determinar outros comportamentos de placa de rede:

1. Em Bloqueio, certifique-se de que a placa de rede apropriada esteja listada no campo **NIC de bloqueio**. Se você está configurando várias placas de rede, as configurações para cada placa de rede devem ter o mesmo valor neste campo. Em outras palavras, apenas uma placa de rede é usada para bloqueio.

2. Se você está usando software Websense em modo **Stand-Alone**, **Filtrar e registrar solicitações HTTP em log** está selecionada e não pode ser alterada.
3. Se você tem o software Websense integrado com um dispositivo ou aplicativo de terceiros, use as opções **Integrações** para indicar como este Network Agent deve filtrar e registrar solicitações HTTP. As opções que não se aplicam ao seu ambiente são desativadas.
  - Selecione **Log de solicitações HTTP** para aumentar a precisão em relatórios do Websense.
  - Selecione **Filtrar todas as solicitações não enviadas via portas HTTP** para usar o Network Agent para filtrar apenas as solicitações HTTP não enviadas pelo produto de integração.
4. Em Gerenciamento de protocolos, indique se o Network Agent deve usar esta placa de rede para filtrar protocolos não-HTTP:
  - Marque **Filtrar solicitações de protocolo que não sejam protocolos HTTP** para ativar o recurso de gerenciamento de protocolos. Isso permite que o software Websense filtre aplicativos de Internet e métodos de transferência de dados, como os usados para mensagens instantâneas, streaming media, compartilhamento de arquivos, correio pela Internet e assim por diante. Consulte [Filtragem de categorias e protocolos](#), página 36, e [Trabalhando com protocolos](#), página 182, para obter mais informações.
  - Marque **Medir o uso de largura de banda por protocolo** para ativar o recurso Bandwidth Optimizer. O Network Agent usa esta placa de rede para monitorar o uso de banda de rede por protocolo ou aplicativo. Consulte [Usando o Bandwidth Optimizer para gerenciar a largura de banda](#), página 189, para obter mais informações.

## Definindo as configurações de monitoramento para uma placa de rede

Use a página **Configurações locais > Configuração de NIC > Monitorar lista** para especificar quais computadores o Network Agent monitora com a placa de rede selecionada.

1. Em Monitorar lista, especifique quais solicitações o Network Agent monitora:
  - **Todos:** O Network Agent monitora as solicitações de todos os computadores que vê usando a placa de rede selecionada. Em geral, isto inclui todos os computadores no mesmo segmento de rede do computador atual do Network Agent ou placa de rede.
  - **Nenhum:** O Network Agent não monitora solicitações.
  - **Específico:** O Network Agent só monitora os segmentos de rede incluídos em Monitorar lista.

- Se você selecionou **Específico**, clique em **Adicionar** e especifique os endereços IP dos computadores que o Network Agent deve monitorar. Consulte [Adicionando ou editando endereços IP](#), página 345, para obter mais informações.

**Obs.:**

Você não pode digitar intervalos de endereços IP sobrepostos. Se os intervalos se sobrepõem, as medições de banda de rede podem não ser exatas e a filtragem baseada em banda pode não ser aplicada corretamente.

Para remover um endereço IP ou intervalo de rede da lista, marque o item de lista apropriado e clique em **Excluir**.

- Em **Monitorar exceções** da lista, identifique quaisquer computadores internos que o Network Agent deve excluir do monitoramento.  
Por exemplo, o Network Agent poderia ignorar solicitações do CPM Server. Assim, as solicitações do CPM Server não se acumularão nos dados de registro do Websense ou na saída de qualquer dos monitores de status.
  - Para identificar um computador, clique em **Adicionar** e digite seu endereço IP.
  - Repita o processo para identificar computadores adicionais.
- Clique em **OK** para colocar suas alterações em cache e voltar à página **Configuração de NIC**. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Adicionando ou editando endereços IP

Tópicos relacionados:

- ◆ [Definindo as configurações globais](#), página 340
- ◆ [Definindo as configurações locais](#), página 341
- ◆ [Definindo as configurações de placa de rede](#), página 343

Use a página **Adicionar endereços IP** ou **Editar endereços IP** para alterar qualquer das listas do Network Agent: Definição de rede interna, Tráfego interno a ser monitorado, Proxies e caches, Monitorar lista ou Monitorar exceções da lista.

- ◆ Ao adicionar ou editar um intervalo de endereços IP, certifique-se de que não sobrepõe qualquer entrada existente (endereço IP único ou intervalo) na lista.
- ◆ Ao adicionar ou editar um endereço IP único, certifique-se de que não recai em um intervalo que já aparece na lista.

Para adicionar um novo endereço IP ou intervalo:

- Selecione o botão de seleção **Endereço IP** ou **Intervalo de endereços IP**.
- Informe um endereço IP ou intervalo válido.

3. Clique em **OK** para voltar à página anterior de Configurações do Network Agent. O novo endereço IP ou intervalo aparece na tabela apropriada.

Para voltar à página anterior sem salvar as alterações em cache, clique em **Cancelar**.

4. Repita este processo para endereços IP adicionais, conforme necessário.

Ao editar um endereço IP ou intervalo existente, a página Editar endereços IP exibe o item selecionado com o botão de seleção correto já selecionado. Faça as alterações necessárias e clique em **OK** para voltar à página anterior.

Quando terminar de adicionar ou alterar endereços IP, clique em **OK** na página Configurações do Network Agent. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Verificando a configuração do Network Agent

---

Depois de configurar o Network Agent no Websense Manager, use o Network Traffic Detector para garantir que os computadores em sua rede estejam visíveis para o software Websense.

1. Vá para **Iniciar > Programas > Websense > Utilitários > Network Traffic Detector** para iniciar a ferramenta.
2. Selecione uma placa de rede na lista suspensa **Adaptador de rede**.
3. Marque os endereços que aparecem na lista **Intervalos de rede monitorados** para verificar se todas as sub-redes apropriadas estão listadas.
4. Use os botões **Adicionar sub-rede** e **Remover sub-rede** para alterar quais partes da rede são testadas.
5. Clique em **Iniciar monitoramento**.

O Network Traffic Detector detecta os computadores na rede, monitorando as informações que enviam pela rede. A lista **Número de computadores detectados** exibe uma contagem dos computadores detectados.

6. Para ver informações específicas sobre os computadores detectados pela ferramenta, selecione uma sub-rede na lista Intervalos de rede monitorados e clique em **Exibir computadores detectados**.

Se um computador específico não estiver listado, verifique se está gerando tráfego de rede. Para fazer isso, vá para o computador, inicialize um navegador e acesse um website. Em seguida, volte ao Network Traffic Detector e veja se o computador aparece na caixa de diálogo **Computadores detectados**.

7. Ao terminar de testar a visibilidade do tráfego de rede, clique em **Parar monitoramento**.

Se alguns computadores não estiverem visíveis:

- ◆ Revise a configuração de rede e os requisitos de posicionamento de placa de rede (consulte [Configuração de hardware](#), página 338).

- ◆ Revise as informações mais detalhadas para configuração de rede no *Guia de Instalação* do seu software Websense.
- ◆ Verifique se configurou adequadamente a placa de rede de monitoramento (*Definindo as configurações de placa de rede*, página 343).



# 15

## Solução de problemas

Antes de entrar em contato com o Suporte técnico, consulte esta seção para encontrar soluções para problemas comuns.

O site da Websense apresenta uma extensa base de conhecimentos, disponível em [www.websense.com/global/en/SupportAndKB/](http://www.websense.com/global/en/SupportAndKB/). Procure os tópicos por palavra-chave ou número de referência, ou consulte os artigos mais conhecidos.

As instruções sobre solução de problemas estão agrupadas nas seguintes seções:

- ◆ *Problemas de instalação e assinatura*
- ◆ *Problemas do Master Database*, página 351
- ◆ *Problemas de filtragem*, página 357
- ◆ *Problemas do Network Agent*, página 361
- ◆ *Problemas de identificação do usuário*, página 364
- ◆ *Problemas com mensagens de bloqueio*, página 374
- ◆ *Problemas de registro, mensagem de status e alerta*, página 377
- ◆ *Problemas do Policy Server e do Policy Database*, página 378
- ◆ *Problemas de administração delegada*, página 380
- ◆ *Problemas de relatório*, página 381
- ◆ *Ferramentas de solução de problemas*, página 392

### Problemas de instalação e assinatura

---

- ◆ *O status do Websense indica um problema de assinatura*, página 349
- ◆ *Há usuários ausentes no Websense Manager após a atualização*, página 350

### O status do Websense indica um problema de assinatura

É necessária uma chave de assinatura válida para o download do Websense Master Database e para a filtragem na Internet. Se a sua assinatura expirar ou for inválida, e se o Master Database não foi baixado há mais de duas semanas, o monitor de saúde do Websense exibirá um aviso.

- ◆ Verifique se você especificou a chave de assinatura exatamente da forma como a recebeu. A chave diferencia maiúsculas e minúsculas.
- ◆ Verifique se a assinatura ainda não expirou. Consulte [Chave de assinatura, página 352](#).
- ◆ Certifique-se de que o download do Master Database foi realizado corretamente nas últimas duas semanas. Você pode verificar o status do download no Websense Manager: clique em **Download do banco de dados** na página Status > Hoje.  
Consulte [Não é feito o download do Master Database, página 352](#), para obter ajuda sobre como solucionar problemas de download de banco de dados.

Se você inseriu a chave corretamente, mas continua a receber um erro de status, ou se a sua assinatura expirou, entre em contato com a Websense, Inc. ou com o revendedor autorizado.

Quando a sua assinatura expira, as configurações do Websense Manager determinam se todos os usuários têm acesso à Internet sem filtro ou se todas as solicitações de Internet são bloqueadas. Consulte [Sua assinatura, página 26](#), para obter mais informações.

## Há usuários ausentes no Websense Manager após a atualização

Se você definiu o Active Directory como seu serviço de diretório, pode acontecer de, após uma atualização para o software Websense, os nomes de usuário não aparecerem no Websense Manager. Isso ocorre quando os nomes de usuário incluem caracteres que não fazem parte do conjunto de caracteres UTF-8.

Para utilizar o protocolo LDAP 3.0, o programa de instalação do Websense altera o conjunto de caracteres de MBCS para UTF-8 durante a atualização. Como resultado, os nomes de usuário que incluem caracteres que não são UTF-9 não são reconhecidos corretamente.

Para solucionar o problema, altere manualmente o conjunto de caracteres para MBCS:

1. No Websense Manager, vá para **Configurações > Serviços de diretório**.
2. Certifique-se de que **Active Directory (Native Mode)** esteja selecionado em Diretórios, na parte superior da página.
3. Clique em **Configurações avançadas de diretório**.
4. Em Conjunto de caracteres, clique em **MBCS**. Você talvez tenha que rolar a página para baixo para ver essa opção.
5. Clique em **OK** para salvar a alteração em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

---

## Problemas do Master Database

---

- ◆ [O banco de dados de filtragem inicial está em uso](#), página 351
- ◆ [O Master Database tem mais de 1 semana de idade](#), página 351
- ◆ [Não é feito o download do Master Database](#), página 352
- ◆ [O download do Master Database não ocorre no horário correto](#), página 356
- ◆ [Entrando em contato com o suporte técnico para solucionar problemas de download do banco de dados](#), página 356

### O banco de dados de filtragem inicial está em uso

O Websense Master Database armazena as definições de protocolo e categoria que fornecem a base para a filtragem de conteúdo na Internet.

Uma versão parcial do Master Database é instalada com o software Websense em cada máquina com o Filtering Service. Esse banco de dados parcial é usado para ativar a função de filtragem básica no momento em que você insere sua chave de assinatura.

É necessário baixar o banco de dados integral para que a filtragem completa possa ocorrer. Consulte [O Websense Master Database](#), página 29, para obter mais informações.

O processo de download do banco de dados completo pode levar alguns minutos ou mais de uma hora, dependendo de fatores como velocidade da conexão com a Internet, largura de banda, memória disponível e espaço livre em disco.

### O Master Database tem mais de 1 semana de idade

O Websense Master Database armazena as definições de protocolo e categoria que fornecem a base para a filtragem de conteúdo na Internet. O software Websense baixa as alterações para o Master Database de acordo com a programação definida no Websense Manager. Por padrão, o download é programado para ocorrer uma vez ao dia.

Para iniciar o download de um banco de dados manualmente:

1. No Websense Manager, vá para a página **Status > Hoje** e clique em **Download do banco de dados**.
2. Clique em **Atualizar** ao lado da instância apropriada do Filtering Service para iniciar o download do banco de dados ou clique em **Atualizar tudo** para iniciar o download em todas as máquinas com o Filtering Service.

**Obs.:**

Após o download de atualizações para o Master Database, a utilização da CPU pode chegar a 90% ou mais durante o breve período em que o banco de dados é carregado na memória local. É recomendável baixar fora dos horários de pico.

---

3. Para continuar a trabalhar durante o download do banco de dados, clique em **Fechar**.

Clique no botão **Download do banco de dados** quando quiser verificar o status do download.

Se uma nova versão do Master Database adicionar ou remover categorias ou protocolos, os administradores que executam tarefas de gerenciamento de diretivas relacionadas a categorias ou protocolos (como a edição de um conjunto de categorias) durante o download poderão receber mensagens de erro. Embora essas atualizações sejam de certa forma raras, é recomendável tentar evitar alterações relacionadas a categorias e protocolos enquanto o banco de dados é atualizado.

## Não é feito o download do Master Database

Se você não consegue fazer download do Websense Master Database com êxito:

- ◆ Certifique-se de inserir a chave de assinatura corretamente no Websense Manager e de verificar se a chave ainda não expirou (*Chave de assinatura*, página 352).
- ◆ Verifique se a máquina com o Filtering Service pode acessar a Internet (*Acesso à Internet*, página 353).
- ◆ Verifique se as configurações de firewall ou servidor proxy permitem que o Filtering Service se conecte ao servidor de download da Websense (*Verificar as configurações de firewall e servidor proxy*, página 353).
- ◆ Verifique se há espaço em disco (*Espaço em disco insuficiente*, página 354) e memória (*Memória insuficiente*, página 355) suficientes na máquina usada para o download.
- ◆ Procure na rede por aplicativos, como software antivírus, que possam impedir a conexão de download (*Aplicativos com restrições*, página 356).

## Chave de assinatura

Para verificar se a chave de assinatura foi inserida corretamente e não expirou:

1. No Websense Manager, vá para **Configurações > Conta**.
2. Compare a chave que você recebeu da Websense, Inc., ou do revendedor com o campo **Chave de assinatura**. A chave deve usar o mesmo padrão de letras maiúsculas e minúsculas encontrado no documento da chave.
3. Verifique a data em **Chave expira em**. Se for uma data passada, entre em contato com o revendedor ou com a Websense, Inc., para renovar a assinatura.
4. Se você alterou a chave na caixa de diálogo Configurações, clique em **OK** para ativar a chave e permitir o download do banco de dados.

Para começar a baixar um banco de dados manualmente ou para verificar o status do download de banco de dados mais recente, clique em **Download do banco de dados** na barra de ferramentas na parte superior da página Status > Hoje.

## Acesso à Internet

Para baixar o Master Database, a máquina com o Filtering Service envia um comando **HTTP post** para os servidores de download nos seguintes URLs:

download.websense.com  
ddsdm.websense.com  
ddsint.websense.com  
portal.websense.com  
my.websense.com

Para verificar se o Filtering Service tem o acesso à Internet necessário para se comunicar com o servidor de download:

1. Abra um navegador na máquina que executa o Filtering Service.
2. Informe o seguinte URL:

<http://download.websense.com/>

Se a máquina conseguir estabelecer uma conexão HTTP com o site, uma página de redirecionamento será exibida e o navegador apresentará a página inicial da Websense.

Se isso não acontecer, verifique se a máquina:

- Pode se comunicar através da porta 80 ou da porta designada em sua rede para o tráfego HTTP
- Está configurada para fazer pesquisas DNS corretamente
- Está configurada para usar qualquer servidor proxy necessário (consulte *Verificar as configurações de firewall e servidor proxy*, página 353)

Verifique também se o gateway não inclui regras que bloqueiem o tráfego HTTP da máquina com o Filtering Service.

3. Use um dos seguintes métodos para confirmar se a máquina pode se comunicar com o site de download:
  - No prompt de comando, insira o seguinte comando:  

```
ping download.websense.com
```

Verifique se o ping recebe uma resposta do servidor de download.
  - Use telnet para se conectar a **download.websense.com 80**. Se nenhuma mensagem de erro for exibida e aparecer um cursor, você poderá se conectar ao servidor de download.

## Verificar as configurações de firewall e servidor proxy

Se o download do Master Database ocorreu por meio de um firewall ou servidor proxy que requer autenticação, verifique se o navegador na máquina com o Filtering Service carrega as páginas da Web corretamente. Se as páginas abrirem normalmente, mas o Master Database não baixar, verifique as configurações do servidor proxy no navegador da Web.

Microsoft Internet Explorer:

1. Selecione **Ferramentas > Opções da Internet**.
2. Abra a guia **Conexões**.
3. Clique em **Configurações da LAN**. As informações sobre configuração do servidor proxy aparecem em **Servidor proxy**.  
Anote as configurações de proxy.

Mozilla Firefox:

1. Selecione **Tools > Options > Advanced**.
2. Selecione a guia **Network (Rede)**.
3. Clique em **Settings (Configurações)**. A caixa de diálogo Connection Settings (Configurações de conexão) mostra se o navegador está configurado para se conectar a um servidor proxy.  
Anote as configurações de proxy.

Em seguida, verifique se o software Websense está configurado para usar o mesmo servidor proxy para o download.

1. No Websense Manager, vá para **Configurações > Download do banco de dados**.
2. Verifique se a opção **Usar servidor proxy ou firewall** está selecionada e se o servidor e a porta corretos estão na lista.
3. Verifique se as configurações de **Autenticação** estão corretas. Verifique o nome de usuário e a senha, a grafia e o uso de maiúsculas e minúsculas.

Se o software Websense fornecer informações sobre autenticação, o firewall ou o servidor proxy devem ser configurados para aceitar autenticação básica ou texto simples. Há informações sobre como ativar a autenticação básica disponíveis na [Base de conhecimentos](#) Websense.

Se algum firewall restringir o acesso à Internet no momento em que o software Websense normalmente baixa o banco de dados ou limitar o tamanho de um arquivo que pode ser transferido por HTTP, o software Websense não poderá baixar o banco de dados. Para determinar se o firewall é a causa da falha de download, procure uma regra no firewall que possa estar bloqueando o download e altere os horários de download no Websense Manager ([Configurando downloads do banco de dados, página 31](#)), caso necessário.

## Espaço em disco insuficiente

O Websense Master Database está armazenado no diretório **bin** do Websense (`/opt/Websense/bin` ou `C:\Arquivos de Programas\Websense\bin`, por padrão). A unidade que contém esse diretório deve ter espaço suficiente para baixar o banco de dados compactado, e espaço suficiente para a sua descompactação.

A máquina deve ter pelo menos o dobro do tamanho do Master Database em espaço livre em disco. À medida que aumentam as entradas no Master Database, também aumenta o tamanho necessário para um download bem-sucedido. Como regra geral, a Websense, Inc. recomenda no mínimo 3 GB de espaço em disco na unidade de download.

No Windows, use o Windows Explorer para verificar o espaço em disco disponível:

1. Abra **Meu computador** no Windows Explorer (e não no Internet Explorer).
2. Selecione a unidade em que o software Websense está instalado. Por padrão, o software Websense está localizado na unidade C.
3. Clique com o botão direito e selecione **Propriedades** no menu pop-up.
4. Na guia Geral, verifique se há pelo menos 3 GB de espaço livre disponível. Se não houver espaço livre suficiente na unidade, exclua os arquivos desnecessários para liberar o espaço requerido.

Nos sistemas Linux, use o comando **df** para verificar o volume de espaço disponível no sistema de arquivos em que o software Websense está instalado:

1. Abra uma sessão de terminal.
2. No prompt, especifique:

```
df -h /opt
```

Em geral, o software Websense é instalado no diretório /opt/Websense/bin. Se for instalado em outro local, use esse caminho.

3. Verifique se há ao menos 3 GB de espaço livre. Se não houver espaço livre suficiente na unidade, exclua os arquivos desnecessários para liberar o espaço requerido.

Se você perceber que há espaço em disco suficiente e mesmo assim ocorrem problemas de download, tente parar todos os serviços Websense (consulte [Parando e iniciando os serviços Websense](#), página 283), excluindo os arquivos **Websense.xfr** e **Websense** (sem extensão), iniciando os serviços e baixando manualmente um novo banco de dados.

## Memória insuficiente

A memória necessária para executar o software Websense e baixar o Master Database varia de acordo com o porte da rede. Por exemplo, em uma rede pequena, são recomendáveis 2 GB de memória para todas as plataformas.

Consulte o *Guia de Implantação* para se informar sobre as recomendações de sistema.

Para verificar a memória em um sistema Windows:

1. Abra o Gerenciador de tarefas.
2. Selecione a guia **Desempenho**.
3. Verifique a **memória física** total disponível.
4. Se houver menos de 2 GB instalados, aumente a memória RAM na máquina.

Você também pode selecionar **Painel de controle > Ferramentas administrativas > Desempenho** para obter informações.

Para verificar a memória em um sistema Linux:

1. Abra uma sessão de terminal.

2. No prompt, especifique:  
top
3. Para calcular a memória total disponível, adicione **Mem: av** e **Swap: av**.
4. Se houver menos de 2 GB instalados, aumente a memória RAM na máquina.

## Aplicativos com restrições

Alguns aplicativos com restrições (como verificadores de vírus, aplicativos com limitação de tamanho ou sistemas de detecção de intrusão) podem interferir nos downloads do banco de dados. O ideal é configurar o software Websense para acessar diretamente o último gateway para não se conectar a esses aplicativos. Como alternativa:

1. Desative as restrições relacionadas à máquina com o Filtering Service e ao local do download do Master Database.  
Consulte a documentação do aplicativo ou do software para obter instruções sobre como alterar a configuração do dispositivo.
2. Tente baixar o Master Database.

Se essa alteração não produzir qualquer efeito, reconfigure o aplicativo para incluir a máquina que executa o Filtering Service.

## O download do Master Database não ocorre no horário correto

A data e a hora do sistema podem não estar definidas corretamente na máquina com o Filtering Service. O software Websense utiliza o relógio do sistema para determinar a hora correta para baixar o Master Database.

Se o download não estiver ocorrendo, consulte [Não é feito o download do Master Database, página 352](#).

## Entrando em contato com o suporte técnico para solucionar problemas de download do banco de dados

Se após as etapas de solução de problemas desta seção da Ajuda ainda ocorrerem problemas de download do Master Database, envie as seguintes informações ao Suporte técnico da Websense:

1. A mensagem de erro exata que é exibida na caixa de diálogo Download do banco de dados
2. Os endereços IP externos das máquinas que estão tentando baixar o banco de dados
3. Sua chave de assinatura do Websense
4. A data e a hora da última tentativa
5. O número de bytes transferidos, se houver algum

6. Abra um prompt de comando e execute **nslookup** em **download.websense.com**. Se for estabelecida conexão com o servidor de download, envie os endereços IP retornados ao suporte técnico.
7. Abra um prompt de comando e execute **tracert** em **download.websense.com**. Se for estabelecida conexão com o servidor de download, envie o rastreamento de rota ao suporte técnico.
8. Um rastreamento de pacote ou uma captura de pacote realizados no servidor de download Websense durante uma tentativa de download.
9. Um rastreamento de pacote ou uma captura de pacote realizados no gateway de rede durante a mesma tentativa de download.
10. Os seguintes arquivos do diretório **bin** do Websense: **websense.ini**, **eimserver.ini** e **config.xml**.

Vá para [www.websense.com/SupportPortal/default.aspx](http://www.websense.com/SupportPortal/default.aspx) para obter informações de contato do suporte técnico.

## Problemas de filtragem

- ◆ *O Filtering Service não está em execução*, página 357
- ◆ *O User Service não está disponível*, página 358
- ◆ *Os sites são categorizados incorretamente como Informática*, página 359
- ◆ *Palavras-chave não estão sendo bloqueadas*, página 359
- ◆ *URLs de filtro de acesso personalizado ou limitado não são filtrados como esperado*, página 360
- ◆ *O usuário não pode acessar um protocolo ou um aplicativo como esperado*, página 360
- ◆ *Uma solicitação FTP não é bloqueada como esperado*, página 360
- ◆ *O software Websense não aplica as diretivas de usuário ou grupo*, página 361
- ◆ *Os usuários remotos não são filtrados pela diretiva correta*, página 361

## O Filtering Service não está em execução

Quando o Filtering Service não está em execução, as solicitações da Internet não podem ser filtradas nem registradas em log.

A execução do Filtering Service pode ser interrompida se:

- ◆ Não houver espaço em disco suficiente na máquina com o Filtering Service.
- ◆ Ocorrer falha de download de um Master Database devido a falta de espaço de disco (consulte *Não é feito o download do Master Database*, página 352).
- ◆ O arquivo **websense.ini** está ausente ou corrompido.
- ◆ Você pára o serviço (após criar páginas de bloqueio personalizadas, por exemplo) e não o reinicia.

O Filtering Service também pode dar a impressão de ter parado quando você reinicia vários serviços Websense e eles não se iniciam na ordem correta. Ao reiniciar vários serviços, lembre-se de iniciar o Policy Database, o Policy Broker e o Policy Server antes de outros serviços Websense.

Para solucionar esses problemas:

- ◆ Verifique se há ao menos 3 GB de espaço livre em disco na máquina com o Filtering Service. Talvez seja necessário remover arquivos não utilizados ou aumentar a capacidade.
- ◆ Navegue até o diretório **bin** do Websense (C:\Arquivos de Programas\Websense\bin ou /opt/Websense/bin, por padrão) e confirme se consegue abrir o arquivo **websense.ini** em um editor de texto. Se o arquivo estiver corrompido, substitua-o por um arquivo de backup.
- ◆ Verifique no Windows Event Viewer ou no arquivo **websense.log** se há mensagens de erro do Filtering Service (consulte [Ferramentas de solução de problemas](#), página 392).
- ◆ Faça logoff no Websense Manager, reinicie o Websense Policy Server e reinicie o Websense Filtering Service (consulte [Parando e iniciando os serviços Websense](#), página 283).

Aguarde um minuto antes de se reconectar ao Websense Manager.

## O User Service não está disponível

Quando o User Service não é executado ou quando o Policy Server não consegue se comunicar com o User Service, o software Websense não pode aplicar as diretivas de filtragem do usuário corretamente.

Pode parecer que o User Service parou se você reiniciar o Policy Server após reiniciar outros serviços do Websense. Para corrigir esse problema:

1. Reinicie o serviço Websense Policy Server (consulte [Parando e iniciando os serviços Websense](#), página 283).
2. Inicie ou reinicie o Websense User Service.
3. Feche o Websense Manager.

Aguarde um minuto antes de se reconectar ao Websense Manager.

Se as etapas anteriores não corrigirem o problema:

- ◆ Verifique no Windows Event Viewer ou no arquivo **websense.log** se há mensagens de erro do User Service (consulte [Ferramentas de solução de problemas](#), página 392).
- ◆ Navegue até o diretório **bin** do Websense (C:\Arquivos de Programas\Websense\bin ou /opt/Websense/bin, por padrão) e confirme se você pode abrir **websense.ini** em um editor de texto. Se o arquivo estiver corrompido, substitua-o por um arquivo de backup.

## Os sites são categorizados incorretamente como Informática

As versões 4.0 e posteriores do Internet Explorer aceitam pesquisas na barra de endereços. Quando essa opção está ativada, se um usuário insere somente um nome de domínio na barra de endereços (**websense** em vez de **http://www.websense.com**, por exemplo), o Internet Explorer considera a entrada uma solicitação de pesquisa, e não uma solicitação de site. Ele exibe o site que muito provavelmente o usuário está procurando, além de uma lista de outros sites que apresentem alguma correspondência com a pesquisa.

Como resultado, o software Websense permite, bloqueia ou limita a solicitação com base no status da categoria Informática/Mecanismos de pesquisa e Portais na diretiva ativa, e não na categoria do site solicitado. Para que o software Websense filtre pela categoria do site solicitado, desative o mecanismo de pesquisa na barra de endereços:

1. Vá para **Ferramentas > Opções da Internet**.
2. Vá para a guia **Avançadas**.
3. Em Pesquisar na barra de endereços, selecione **Não fazer pesquisas na barra de endereços**.
4. Clique em **OK**.

**Obs.:**

Essas etapas são válidas para o Internet Explorer versões 5, 6 e 7.

## Palavras-chave não estão sendo bloqueadas

Há dois motivos possíveis para esse problema: A opção **Desabilitar bloqueio de palavras-chave** está selecionada ou o site cujo URL contém a palavra-chave usa **post** para enviar dados para seu servidor Web.

Para garantir que o bloqueio de palavras-chave seja ativado:

1. No Websense Manager, vá para **Configurações > Filtragem**.
2. Em Filtragem geral, verifique a lista **Opções de pesquisa por palavra-chave**. Se a opção **Desabilitar bloqueio de palavras-chave** aparecer, selecione outra opção na lista. Consulte *Definindo configurações de filtragem do Websense*, página 54, para obter mais informações sobre as opções disponíveis.
3. Clique em **OK** para salvar a alteração em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Se um site usar **post** para enviar dados para o servidor Web, o software Websense não reconhecerá as configurações de filtragem de palavras-chave para esse URL. A não ser que seu produto de integração reconheça os dados enviados por post, os usuários ainda poderão acessar os URLs que contêm palavras-chave bloqueadas.

Para ver se um site usa um comando post, verifique a origem do site em seu navegador. Se o código-fonte contiver uma string como **<method=post>**, o comando post será usado para carregar esse site.

## URLs de filtro de acesso personalizado ou limitado não são filtrados como esperado

Se um URL HTTPS em uma lista de URLs personalizados ou com filtro de acesso limitado (recategorizado ou não filtrado) não for filtrado da forma esperada, um produto de integração pode estar transformando o URL em um formato que o Filtering Service não reconhece.

Produtos de integração que não sejam proxy convertem os URLs do formato do domínio para o formato IP. Por exemplo, o URL **https://<domínio>** é lido como **https://<endereço IP>:443**. Quando isso ocorre, o Filtering Service não consegue estabelecer uma correspondência entre o URL recebido do produto de integração com um URL personalizado ou um filtro de acesso limitado, e assim não filtra o site corretamente.

Para solucionar esse problema, adicione os endereços IP e os URLs dos sites a serem filtrados usando URLs personalizados ou filtros de acesso limitado.

## O usuário não pode acessar um protocolo ou um aplicativo como esperado

Se a sua rede inclui o Microsoft ISA Server, determinadas configurações de método de autenticação podem causar a falha de conexões com aplicativos de mensagens.

Se houver algum método ativo que não seja o de autenticação anônima, o servidor proxy tentará identificar os pacotes de dados recebidos quando os usuários solicitarem conexões de aplicativos. O servidor proxy não consegue identificar o pacote de dados e a conexão cai. Isso pode prejudicar a atividade de filtragem de protocolo do Websense.

O acesso a algum protocolo ou aplicativo da Internet pode se tornar impossível se a porta usada pelo aplicativo estiver bloqueada. Isso pode ocorrer se:

- ◆ A porta estiver bloqueada por um firewall.
- ◆ Um protocolo personalizado bloqueado incluir a porta (como uma porta única ou como parte de um intervalo de portas) em qualquer um de seus identificadores.

## Uma solicitação FTP não é bloqueada como esperado

Quando integrado a firewalls Check Point<sup>®</sup>, o software Websense requer que a **exibição de pasta** seja ativada no navegador do cliente para o reconhecimento e a filtragem de solicitações FTP.

Quando a exibição de pasta não está ativada, as solicitações FTP enviadas ao proxy FireWall-1 são enviadas ao software Websense com um prefixo "http://". Como resultado, o software Websense filtra essas solicitações como solicitações HTTP, e não como solicitações FTP.

## O software Websense não aplica as diretivas de usuário ou grupo

Se o software Websense estiver aplicando diretivas de rede ou de computador, ou a diretiva **Padrão**, mesmo depois que as diretivas de usuário ou de grupo estiverem designadas, consulte [Problemas de identificação do usuário](#), página 364. Você pode encontrar informações adicionais através da [Base de conhecimentos](#).

## Os usuários remotos não são filtrados pela diretiva correta

Se um usuário remoto faz login na rede usando credenciais de domínio salvas em cache (informações de logon da rede), o software Websense aplica a diretiva atribuída a esse usuário, ao grupo do usuário ou ao domínio, conforme apropriado. Se nenhuma diretiva estiver atribuída ao usuário, grupo ou domínio, ou se o usuário se conectar ao computador com uma conta de usuário local, o software Websense aplicará a diretiva padrão.

Ocasionalmente, um usuário não é filtrado por uma diretiva de usuário ou de grupo ou pela diretiva padrão. Isso ocorre quando o usuário se conecta ao computador remoto com uma conta de usuário local, e a última parte do endereço MAC (Media Access Control) do computador remoto é sobreposta por um endereço IP da rede ao qual uma diretiva foi atribuída. Nesse caso, a diretiva atribuída a esse endereço IP específico será aplicada ao usuário remoto.

## Problemas do Network Agent

---

- ◆ [O Network Agent não está instalado](#), página 361
- ◆ [O Network Agent não está em execução](#), página 362
- ◆ [O Network Agent não está monitorando NICs](#), página 362
- ◆ [O Network Agent não pode se comunicar com o Filtering Service](#), página 362

## O Network Agent não está instalado

O Network Agent é necessário para ativar a filtragem de protocolo. Com algumas integrações, o Network Agent também é usado para fornecer registros mais precisos.

Se você estiver executando com um produto de integração e não precisar do registro nem da filtragem de protocolos do Network Agent, poderá ocultar a mensagem de status “Nenhum Network Agent está instalado”. Consulte [Verificando o status atual do sistema](#), página 291, para obter instruções.

Para instalações autônomas, o Network Agent deve ser instalado para que o tráfego de rede seja monitorado e filtrado. Consulte o [Guia de Instalação](#) para obter instruções sobre instalação e, em seguida, consulte [Configuração do Network Agent](#), página 339.

## O Network Agent não está em execução

O Network Agent é necessário para ativar a filtragem de protocolo. Com algumas integrações, o Network Agent também é usado para fornecer registros mais precisos.

Para instalações autônomas, o Network Agent deve estar em execução para monitorar e filtrar o tráfego de rede.

Para solucionar esse problema:

1. Marque a caixa de diálogo Serviços do Windows (consulte [A caixa de diálogo Serviços do Windows, página 392](#)) para ver se o serviço **Websense Network Agent** já foi iniciado.
2. Reinicie os serviços **Websense Policy Broker** e **Websense Policy Server** (consulte [Parando e iniciando os serviços Websense, página 283](#)).
3. Inicie ou reinicie o serviço **Websense Network Agent**.
4. Feche o Websense Manager.
5. Aguarde um minuto e reconecte-se ao Websense Manager.

Se esse procedimento não corrigir o problema:

- ◆ Verifique se há mensagens de erro do Network Agent no **Windows Event Viewer** (consulte [O Windows Event Viewer, página 393](#)).
- ◆ Consulte o arquivo **Websense.log** para verificar se há mensagens de erro do Network Agent (consulte [O arquivo de log do Websense, página 393](#)).

## O Network Agent não está monitorando NICs

O Network Agent deve ser associado a pelo menos uma NIC (placa de rede) para monitorar o tráfego de rede.

Se você adicionar ou remover as placas de rede da máquina com o Network Agent, terá que atualizar a configuração do Network Agent.

1. No Websense Manager, vá para **Configurações**.
2. No painel de navegação à esquerda, em Network Agent, selecione o endereço IP da máquina com o Network Agent.
3. Verifique se todas as NICs para a máquina selecionada estão listadas.
4. Verifique se ao menos uma NIC está definida para monitorar o tráfego de rede.

Consulte [Configuração do Network Agent, página 339](#), para obter mais informações.

## O Network Agent não pode se comunicar com o Filtering Service

O Network Agent deve ser capaz de se comunicar com o Filtering Service para aplicar suas diretivas de uso da Internet.

- ◆ Você alterou o endereço IP da máquina com o Filtering Service ou reinstalou o Filtering Service?

Se isso aconteceu, consulte [Atualizar informações de UID ou endereço IP do Filtering Service](#), página 363.

- ◆ Você tem mais de 2 NICs (placas de rede) na máquina com o Network Agent?  
Caso tenha, consulte [Configuração da rede](#), página 337, para verificar as configurações do software Websense.
- ◆ Você reconfigurou o switch conectado ao Network Agent?  
Se reconfigurou, consulte o *Guia de Instalação* para verificar a instalação do hardware e consulte [Configuração do Network Agent](#), página 339, para verificar as configurações do Websense.

Se nada disso é aplicável, consulte [Definindo as configurações locais](#), página 341, para obter informações sobre como associar o Network Agent e o Filtering Service.

## Atualizar informações de UID ou endereço IP do Filtering Service

Depois que o Filtering Service é desinstalado e reinstalado, o Network Agent não atualiza automaticamente o UID (identificador interno) do Filtering Service. O Websense Manager tenta consultar o Filtering Service usando o UID antigo, que não existe mais.

Da mesma forma, quando você altera o endereço IP da máquina com o Filtering Service, essa alteração não é registrada automaticamente.

Para restabelecer a conexão com o Filtering Service:

1. Abra o Websense Manager.  
Uma mensagem de status indica que uma instância do Network Agent não pode se conectar ao Filtering Service.
2. Clique em **Configurações** na parte superior do painel de navegação à esquerda.
3. No painel de navegação à esquerda, em Network Agent, selecione o endereço IP da máquina com o Network Agent.
4. Na parte superior da página, em Definição do Filtering Service, expanda a lista **Endereço IP do servidor** e selecione o endereço IP da máquina com o Filtering Service.
5. Clique em **OK** na parte inferior da página para salvar a atualização em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

## Problemas de identificação do usuário

---

Tópicos relacionados:

- ◆ [Problemas de filtragem](#), página 357
- ◆ [Os usuários remotos não são solicitados a fazer autenticação manual](#), página 373
- ◆ [Os usuários remotos não estão sendo filtrados corretamente](#), página 373

Se o software Websense está usando diretivas de rede ou de computador ou a diretiva **Padrão** para filtrar solicitações da Internet, mesmo depois de você ter atribuído diretivas com base em usuário ou grupo, ou se a diretiva baseada em usuário ou grupo incorreta está sendo aplicada, siga as seguintes etapas para detectar o problema:

- ◆ Se você estiver usando o Microsoft ISA Server e alterou seu método de autenticação, verifique se o Web Proxy Service foi reiniciado.
- ◆ Se você está usando grupos aninhados no Windows Active Directory, as diretivas atribuídas a um grupo pai são aplicadas aos usuários pertencentes a um subgrupo, e não diretamente ao grupo pai. Para obter informações sobre hierarquias de usuários e grupos, consulte a documentação de seu serviço de diretório.
- ◆ O cache do User Service pode estar desatualizado. O User Service salva em cache o nome de usuário para mapeamentos de endereço IP por três horas. Você pode forçar a atualização do cache do User Service salvando todas as alterações em cache no Websense Manager e clicando em **Salvar tudo**.
- ◆ Se o usuário que está sendo filtrado incorretamente estiver em uma máquina que executa o Windows XP SP2, o problema pode ser devido ao ICF (firewall de conexão com a Internet) do Windows, incluído e ativado por padrão no Windows XP SP2. Para obter mais informações sobre o Windows ICF, consulte o artigo 320855 da Microsoft Knowledge Base.

Para que o DC Agent ou o Logon Agent obtenha informações de logon do usuário em uma máquina que executa o Windows XP SP2:

1. No menu **Iniciar** do Windows na máquina cliente, selecione **Configurações > Painel de controle > Central de segurança > Firewall do Windows**.
2. Vá para a guia **Exceções**.
3. Marque **Compartilhamento de arquivos e impressoras**.
4. Clique em **OK** para fechar a caixa de diálogo do firewall do Windows e feche todas as outras janelas abertas.

Se você está usando um agente de identificação transparente Websense, consulte a seção apropriada de solução de problemas.

- ◆ [Solução de problemas do DC Agent](#), página 365.
- ◆ [Solucionando problemas do Logon Agent](#), página 366.
- ◆ [Solucionando problemas do eDirectory Agent](#), página 369.

- ◆ [Solucionando problemas do RADIUS Agent, página 372.](#)

## Solução de problemas do DC Agent

Para solucionar problemas de identificação de usuário com o DC Agent:

1. Verifique todas as conexões de rede.
2. Verifique se há mensagens de erro no Windows Event Viewer (consulte [O Windows Event Viewer, página 393](#)).
3. Verifique o arquivo de registro do Websense (Websense.log) para obter informações detalhadas sobre o erro (consulte [O arquivo de log do Websense, página 393](#)).

As causas comuns para os problemas de identificação de usuário do DC Agent incluem:

- ◆ Os serviços de rede ou do Windows estão se comunicando com o controlador de domínio de uma forma que faz com que o DC Agent identifique o serviço como um novo usuário para quem nenhuma diretiva foi definida. Consulte [Os usuários são filtrados incorretamente pela diretiva Padrão, página 365](#).
- ◆ O DC Agent ou o User Service podem ter sido instalados como um serviço que utiliza a conta de convidado, o que equivale a um usuário anônimo para o controlador de domínio. Se o controlador de domínio foi definido para não oferecer a lista de usuários e grupos a um usuário anônimo, o DC Agent não poderá baixar a lista. Consulte [Alterando as permissões do DC Agent e do User Service manualmente, página 366](#).
- ◆ O cache do User Service está desatualizado. O User Service salva em cache mapeamentos de nome de usuário para endereço IP por três horas, por padrão. O cache também é atualizado toda vez que você faz alterações e clica em **Salvar tudo** no Websense Manager.

## Os usuários são filtrados incorretamente pela diretiva Padrão

Quando alguma rede ou o Microsoft Windows 200x entra em contato com o controlador de domínio, o nome da conta utilizada pode fazer com que o software Websense entenda que um usuário não identificado está acessando a Internet pela máquina filtrada. Como nenhuma diretiva com base em usuário ou grupo foi atribuída a esse usuário, a diretiva do computador ou da rede ou a diretiva Padrão é aplicada.

- ◆ Os serviços de rede podem exigir privilégios de domínio para acessar dados na rede, e usar o nome de usuário do domínio em que são executados para entrar em contato com o controlador de domínio.

Para solucionar esse problema, consulte [Configurando um agente para ignorar determinados nomes de usuário, página 232](#).

- ◆ Os serviços do Windows 200x entram em contato com o controlador de domínio periodicamente com um nome de usuário que consiste no nome do computador seguido de um cifrão (jsilva-computador\$). O DC Agent interpreta o serviço como um novo usuário a quem nenhuma diretiva foi atribuída.

Para solucionar esse problema, configure o DC Agent para ignorar qualquer logon de **computador\$**.

1. Na máquina com o DC Agent, navegue até o diretório **bin** do Websense (por padrão, **C:\Arquivos de Programas\WebSense\bin**).
2. Abra o arquivo **transid.ini** em um editor de texto.
3. Adicione a seguinte entrada ao arquivo:  

```
IgnoreDollarSign=true
```
4. Salve e feche o arquivo.
5. Reinicie o DC Agent (consulte [Parando e iniciando os serviços Websense](#), página 283).

## Alterando as permissões do DC Agent e do User Service manualmente

Na máquina que executa o controlador de domínio:

1. Crie uma conta de usuário como **Websense**. Você pode usar uma conta já existente, mas a conta Websense será a preferencial para definir que a senha não expire. Não há necessidade de privilégios especiais.  
Defina a senha para nunca expirar. Essa conta oferece apenas um contexto de segurança para o acesso aos objetos de diretório.  
Anoto o nome de usuário e a senha definidos para esta conta, porque serão solicitados nas etapas 6 e 7.
2. Abra a caixa de diálogo Serviços do Windows em cada máquina com o Websense DC Agent (vá para **Iniciar > Programas > Ferramentas administrativas > Serviços**).
3. Selecione a entrada **Websense DC Agent** e clique em **Parar**.
4. Clique duas vezes na entrada **Websense DC Agent**.
5. Na guia **Logon**, selecione a opção **Esta conta**.
6. Insira o nome de usuário da conta do Websense DC Agent criado na etapa 1. Por exemplo: **NomedoDomínio\websense**.
7. Insira e confirme a senha do Windows para essa conta.
8. Clique em **OK** para fechar a caixa de diálogo.
9. Selecione a entrada **Websense DC Agent** na caixa de diálogo Serviços e clique em **Iniciar**.
10. Repita esse procedimento para cada instância do Websense User Service.

## Solucionando problemas do Logon Agent

Se alguns usuários de sua rede forem filtrados pela diretiva **Padrão** porque o Logon Agent não consegue identificá-los:

- ◆ Verifique se os GPOs (objetos de diretiva de grupo) do Windows estão sendo aplicados corretamente às máquinas desses usuários (consulte [Objetos de diretiva de grupo](#), página 367).

- ◆ Se o User Service estiver instalado em uma máquina com Linux e você estiver usando o Windows Active Directory (Modo nativo), verifique a configuração do seu serviço de diretório (consulte [User Service em execução no Linux](#), página 367).
- ◆ Verifique se a máquina cliente pode se comunicar com o controlador de domínio onde o script de logon está sendo executado (consulte [Visibilidade do controlador de domínio](#), página 368).
- ◆ Garanta que o NetBIOS esteja ativado na máquina cliente (consulte [NetBIOS](#), página 368).
- ◆ Verifique se o perfil do usuário na máquina cliente não está danificado (consulte [Problemas de perfil de usuário](#), página 369).

## Objetos de diretiva de grupo

Após verificar se o ambiente atende aos pré-requisitos descritos no *Guia de Instalação* do software Websense, verifique se os GPOs estão sendo aplicados corretamente:

1. Na máquina com o Active Directory, abra o Painel de controle do Windows e vá para **Ferramentas administrativas > Usuários e computadores do Active Directory**.
2. Clique com o botão direito na entrada de domínio e selecione **Propriedades**.
3. Clique na guia **Diretiva de grupo** e selecione a diretiva de domínio na lista de links de objetos de diretivas de domínios de grupo.
4. Clique em **Editar** e expanda o nó Configuração do usuário na árvore de diretórios.
5. Expandir o nó Configurações do Windows e selecione **Scripts**.
6. No painel direito, clique duas vezes em **Logon** e verifique se **logon.bat** aparece na caixa de diálogo Propriedades de logon.

Esse script é exigido pelo aplicativo de logon do cliente.

- Se **logon.bat** não estiver no script, consulte o capítulo *Configuração inicial* do *Guia de Instalação* do software Websense.
- Se **logon.bat** não aparecer no script, e o Logon Agent não estiver funcionando, use as etapas adicionais de solução de problemas desta seção para verificar se há algum problema de conectividade de rede, ou consulte a [Base de conhecimentos](#) do Websense.

## User Service em execução no Linux

Quando você usa o Logon Agent para identificação transparente de usuários, e o User Service está instalado em uma máquina com Linux, configure temporariamente o software Websense para se comunicar com o Active Directory no modo misto.

1. No Websense Manager, vá para **Configurações > Serviços de diretório**.
2. Anote as suas configurações de diretório atuais.
3. Em Diretórios, selecione **Windows NT Directory/Active Directory (Mixed Mode)**.

4. Clique em **OK** para salvar as alterações em cache e clique em **Salvar tudo**.
5. Em Diretórios, selecione **Active Directory (Native Mode)**. Se a sua configuração original não aparecer, use as notas da etapa 2 para recriar as configurações de diretório. Consulte *Windows Active Directory (Native Mode)*, página 61, para obter instruções detalhadas.
6. Depois de alterar a configuração, clique em **OK** e em **Salvar tudo**.

## Visibilidade do controlador de domínio

Para verificar se a máquina cliente pode se comunicar com o controlador de domínio:

1. Tente mapear uma unidade na máquina cliente para a unidade raiz compartilhada do controlador de domínio. É aí que o script de logon costuma ser executado e onde está localizado o arquivo **LogonApp.exe**.
2. Na máquina cliente, abra um prompt de comando do Windows e execute o seguinte comando:

```
net view /domain:<nome de domínio>
```

Se um desses testes falhar, consulte a documentação do sistema operacional Windows sobre as possíveis soluções. Existe um problema de conectividade de rede não relacionado ao software Websense.

## NetBIOS

O NetBIOS para TCP/IP deve ser ativado e o serviço Auxiliar NetBIOS TCP/IP deve estar em execução para que o script de logon do Websense seja executado na máquina do cliente.

Para verificar se o NetBIOS para TCP/IP está ativado na máquina cliente:

1. Clique com o botão direito em **Meus locais de rede** e selecione **Propriedades**.
2. Clique com o botão direito em **Conexão local** e selecione **Propriedades**.
3. Selecione **Protocolo TCP/IP** e clique em **Propriedades**.
4. Clique em **Avançadas**.
5. Selecione a guia **WINS** e verifique se a opção NetBIOS correta está definida.
6. Se fizer alguma alteração, clique em **OK** e depois mais duas vezes em **OK** para fechar as diversas caixas de diálogo Propriedades e salvar as alterações.

Se nenhuma alteração for necessária, clique em **Cancelar** para fechar cada caixa de diálogo sem fazer alterações.

Use a caixa de diálogo Serviços do Windows para verificar se o serviço **Auxiliar NetBIOS TCP/IP** está em execução na máquina cliente (consulte *A caixa de diálogo Serviços do Windows*, página 392). O serviço Auxiliar NetBIOS TCP/IP é executado em Windows 2000, Windows XP, Windows Server 2003 e Windows NT.

## Problemas de perfil de usuário

Se o perfil de usuário na máquina cliente estiver corrompido, o script de logon do Websense (e as configurações de GPO do Windows) não será executado. Para resolver esse problema, é preciso recriar o perfil de usuário.

Quando você recria um perfil de usuário, a pasta Meus documentos do usuário, os Favoritos e outros dados e configurações personalizadas não são transferidos automaticamente para o novo perfil. Não exclua o perfil existente e corrompido antes de verificar se o novo perfil solucionou o problema e copiou os dados existentes do usuário para o novo perfil.

Para recriar o perfil de usuário:

1. Faça logon na máquina cliente como administrador local.
2. Renomeie o diretório que contém o perfil de usuário.  
`C:\Documents and Settings\`
3. Reinicie a máquina.
4. Faça logon na máquina como o usuário filtrado. Um novo perfil de usuário será criado automaticamente.
5. Verifique se o usuário é filtrado como esperado.
6. Copie os dados personalizados (como o conteúdo da pasta Meus documentos) do antigo perfil para o novo. Não use o Assistente para transferência de arquivos e configurações, pois ele pode transferir os dados corrompidos para o novo perfil.

## Solucionando problemas do eDirectory Agent

Tópicos relacionados:

- ◆ [Ativando o diagnóstico do eDirectory Agent, página 370](#)
- ◆ [O eDirectory Agent erra na contagem de conexões do eDirectory Server, página 371](#)
- ◆ [Executando o eDirectory Agent em modo de console, página 371](#)

Um usuário não pode ser filtrado corretamente se o nome de usuário não for passado para o eDirectory Agent. Se um usuário não fizer logon no servidor Novell eDirectory, o eDirectory Agent não poderá detectar o logon. Isso ocorre porque:

- ◆ Um usuário faz logon em um domínio que não está incluído no contexto raiz padrão para as sessões de logon do usuário do eDirectory. Esse contexto raiz é especificado durante a instalação e deve corresponder ao contexto raiz especificado para o Novell eDirectory na página **Configurações > Serviços de diretório**.
- ◆ Um usuário tenta ignorar o prompt de logon para burlar a filtragem do Websense.
- ◆ Um usuário não tem uma conta configurada no servidor eDirectory.

Se um usuário não fizer logon no servidor eDirectory, as diretivas específicas do usuário não poderão ser aplicadas a esse usuário. A diretiva **Padrão** será habilitada. Se houver estações de trabalho compartilhadas em sua rede onde os usuários fazem logon anonimamente, configure uma diretiva de filtragem para essas máquinas específicas.

Para determinar se o eDirectory Agent está recebendo um nome de usuário e identificando esse usuário:

1. Ative o registro em log do eDirectory Agent, como descrito em [Ativando o diagnóstico do eDirectory Agent](#), página 370.
2. Abra o arquivo de registro especificado em um editor de texto.
3. Procure uma entrada que corresponda ao usuário que não está sendo filtrado corretamente.
4. Uma entrada como a seguinte indica que o eDirectory Agent identificou um usuário:

```
WsUserData::WsUserData()  
User: cn=Admin,o=novell (10.202.4.78)  
WsUserData::~~WsUserData()
```

No exemplo acima, o usuário **Admin** se conectou ao servidor eDirectory e foi identificado com êxito.

5. Se um usuário está sendo identificado, mas ainda não está sendo filtrado como esperado, verifique a configuração de diretiva para ver se a diretiva apropriada é aplicada ao usuário e se o nome de usuário no Websense Manager corresponde ao nome de usuário no Novell eDirectory.

Se o usuário *não* estiver sendo identificado, verifique se:

- O usuário tem uma conta do Novell eDirectory.
- O usuário está fazendo logon em um domínio que está incluído no contexto raiz padrão para os logons do usuário do eDirectory.
- O usuário não está ignorando um prompt de comando.

## Ativando o diagnóstico do eDirectory Agent

O eDirectory Agent tem recursos de diagnóstico incorporados, mas eles não são ativados por padrão. Você pode ativar o registro em log e a depuração durante a instalação, ou em qualquer outro momento.

1. Pare o eDirectory Agent (consulte [Parando e iniciando os serviços Websense](#), página 283).
2. Na máquina com o eDirectory Agent, vá para o diretório de instalação do eDirectory Agent.
3. Abra o arquivo **wseDir.ini** em um editor de texto.
4. Localize a seção **[eDirAgent]**.
5. Para ativar o registro e a depuração, altere o valor de **DebugMode** para **On**:  
DebugMode=On
6. Para especificar o nível de detalhes do registro, modifique a seguinte linha:

```
DebugLevel=<N>
```

**N** pode ser um valor de 0 a 3, onde 3 indica o maior nível de detalhes.

7. Modifique a linha **LogFile** para especificar o nome do arquivo de saída de registro:

```
LogFile=nomedearquivo.txt
```

Por padrão, a saída do registro é enviada para o console do eDirectory Agent. Se você está executando o agente no modo de console (consulte [Executando o eDirectory Agent em modo de console](#), página 371), pode manter o valor padrão.

8. Salve e feche o arquivo **wsedir.ini**.
9. Inicie o serviço eDirectory Agent (consulte [Parando e iniciando os serviços Websense](#), página 283).

## O eDirectory Agent erra na contagem de conexões do eDirectory Server

Se o eDirectory Agent estiver monitorando mais de 1000 usuários em sua rede, mas mostrar somente 1000 conexões com o servidor Novell eDirectory, pode haver alguma limitação da API do Windows que transmite informações do servidor eDirectory para o Websense eDirectory Agent. Isso ocorre raramente.

Para solucionar essa limitação, adicione um parâmetro ao arquivo **wsedir.ini** que conta as conexões do servidor com precisão (somente o Windows):

1. Pare o serviço Websense eDirectory Agent (consulte [Parando e iniciando os serviços Websense](#), página 283).
2. Vá para o diretório **bin** do Websense (por padrão, **C:\Arquivos de Programas\Websense\bin**).
3. Abra o arquivo **wsedir.ini** em um editor de texto.
4. Insira uma linha em branco e pressione Enter.

```
MaxConnNumber = <NNNN>
```

Aqui, **<NNNN>** é o número máximo de conexões possíveis com o servidor Novell eDirectory. Por exemplo, se a sua rede tem 1950 usuários, você pode inserir 2000 como o número máximo.

5. Salve o arquivo.
6. Reinicie o eDirectory Agent.

## Executando o eDirectory Agent em modo de console

1. Use um dos seguintes métodos:
  - No prompt de comando do Windows, (**Iniciar > Executar > cmd**), insira o comando:
 

```
eDirectoryAgent.exe -c
```
  - No shell de comando do Linux, insira o comando:
 

```
eDirectoryAgent -c
```

- Quando estiver pronto para parar o agente, pressione **Enter**. O agente pode levar alguns segundos até parar.

## Solucionando problemas do RADIUS Agent

O RADIUS Agent tem recursos de diagnóstico incorporados, mas eles não são ativados por padrão. Para ativar o registro e a depuração do RADIUS Agent:

- Pare o serviço RADIUS Agent (consulte [Parando e iniciando os serviços Websense](#), página 283).
- Na máquina com o RADIUS Agent, vá para o diretório de instalação do agente (por padrão, **Websense\bin**).
- Abra o arquivo **wradius.ini** em um editor de texto.
- Localize a seção **[RADIUSAgent]**.
- Para ativar o registro e a depuração, altere o valor de **DebugMode** para **On**:

```
DebugMode=On
```

- Para especificar o nível de detalhes do registro, modifique a seguinte linha:

```
DebugLevel=<N>
```

**N** pode ser um valor de 0 a 3, onde 3 indica o maior nível de detalhes.

- Modifique a linha **LogFile** para indicar o nome do arquivo de saída:

```
LogFile=nomedearquivo.txt
```

Por padrão, a saída do registro é enviada para o console do RADIUS Agent. Se você está executando o agente no modo de console (consulte [Executando o RADIUS Agent em modo de console](#), página 372), tem a opção de manter o valor padrão.

- Salve e feche o arquivo **wradius.ini**.
- Inicie o serviço RADIUS Agent (consulte [Parando e iniciando os serviços Websense](#), página 283).

Se os usuários remotos não estiverem sendo identificados e filtrados da maneira esperada, a causa provável é que estejam ocorrendo problemas de comunicação entre o RADIUS Agent e seu servidor RADIUS. Verifique se há erros nos registros em log do RADIUS Agent para determinar a causa.

## Executando o RADIUS Agent em modo de console

Para iniciar o RADIUS Agent em modo de console (como um aplicativo), insira o seguinte:

- No prompt de comando do Windows:

```
RadiusAgent.exe -c
```

- No prompt de shell do Linux:

```
./RadiusAgent -c
```

Quando quiser parar o agente, pressione **Enter** novamente. O agente pode levar alguns segundos até parar.

O RADIUS Agent aceita os seguintes parâmetros de linha de comando:



**Obs.:**

Em Linux, a Websense, Inc., recomenda o uso do script fornecido para iniciar ou parar o Websense RADIUS Agent (**WsRADIUSAgent start|stop**), em vez dos parâmetros **-r** e **-s**.

Parâmetro	Descrição
-i	Instala o serviço/daemon RADIUS Agent.
-r	Executa o serviço/daemon RADIUS Agent.
-s	Pára o serviço/daemon RADIUS Agent.
-c	Executa o RADIUS Agent como um processo de aplicativo, e não como um serviço ou daemon. Quando está no modo de console, o RADIUS Agent pode ser configurado para enviar saída de registro em log para o console ou para um arquivo de texto.
-v	Exibe o número da versão do RADIUS Agent.
-? -h -ajuda <nenhuma opção>	Exibe informações de uso na linha de comando. Lista e descreve todos os parâmetros possíveis da linha de comando.

## Os usuários remotos não são solicitados a fazer autenticação manual

Se você configurou usuários remotos para a autenticação manual ao acessarem a Internet, pode haver algumas ocasiões em que determinados usuários não recebem a solicitação de autenticação. Isso pode ocorrer quando alguns endereços IP na rede são configurados para ignorar a autenticação manual.

Quando um usuário remoto acessa a rede, o software Websense lê a última parte do endereço MAC (Media Access Control) do computador. Se ela corresponder a um endereço IP na rede que tenha sido configurado para ignorar a autenticação manual, o usuário remoto não será solicitado a autenticar manualmente ao acessar a Internet.

Uma solução é reconfigurar o endereço IP na rede para usar a autenticação manual. Uma solução alternativa é desativar a solicitação de autenticação manual para o usuário remoto afetado.

## Os usuários remotos não estão sendo filtrados corretamente

Se os usuários remotos não estão sendo filtrados ou não estão sendo filtrados por diretivas específicas atribuídas a eles, verifique se nos registros do RADIUS Agent você encontra a mensagem de erro de recepção do servidor: **Error receiving from server: 10060** (Windows) ou **Error receiving from server: 0** (Linux).

Geralmente isso ocorre quando o servidor RADIUS não reconhece o RADIUS Agent como um cliente (fonte das solicitações RADIUS). Verifique se o servidor RADIUS está configurado corretamente (consulte *Configurando o ambiente RADIUS*, página 218).

Você pode usar a ferramenta de diagnóstico incorporada do RADIUS Agent para solucionar problemas de filtragem (consulte *Solucionando problemas do RADIUS Agent*, página 372).

Se você implementou o recurso de filtragem remota (consulte *Filtrar Clientes Remotos*, página 155), os usuários remotos não poderão ser filtrados se o Remote Filtering Client não puder se comunicar com o Remote Filtering Server na rede.

Para obter instruções sobre como configurar o Remote Filtering, consulte o documento técnico *Remote Filtering*.

## Problemas com mensagens de bloqueio

---

- ◆ *Nenhuma página de bloqueio aparece para um tipo de arquivo bloqueado*, página 374
- ◆ *Os usuários recebem um erro do navegador, e não uma página de bloqueio*, página 374
- ◆ *Uma página branca vazia aparece em vez de uma página de bloqueio*, página 375
- ◆ *Mensagens de bloqueio de protocolo não são exibidas como esperado*, página 376
- ◆ *Uma mensagem de bloqueio de protocolo é exibida em vez de uma página de bloqueio*, página 376

### Nenhuma página de bloqueio aparece para um tipo de arquivo bloqueado

Quando o bloqueio de tipo de arquivo é usado, a mensagem de bloqueio pode nem sempre estar visível ao usuário. Por exemplo, quando um arquivo para download estiver contido em um quadro interno (IFRAME) em um site permitido, a mensagem de bloqueio enviada a esse quadro não estará visível porque o tamanho do quadro é zero.

Esse é apenas um problema de exibição; os usuários não podem acessar nem baixar o arquivo bloqueado.

### Os usuários recebem um erro do navegador, e não uma página de bloqueio

Se os usuários receberem uma mensagem de erro, e não uma página de bloqueio, as duas causas mais prováveis são:

- ◆ O navegador do usuário está configurado para usar um proxy externo. Na maioria dos navegadores, há uma configuração que permite o uso de um proxy externo. Verifique se o navegador não está definido para usar um proxy externo.
- ◆ Existe um problema na identificação ou comunicação com a máquina do Filtering Service.

Se as configurações do navegador do usuário estiverem corretas, verifique se o endereço IP da máquina com o Filtering Service está indicado corretamente no arquivo **eimserver.ini**.

1. Pare o **Websense Filtering Service** (consulte [Parando e iniciando os serviços Websense](#), página 283).
2. Navegue até o diretório **bin** do Websense (por padrão, C:\Arquivos de Programas\Websense\bin ou /opt/Websense/bin).
3. Abra o arquivo **eimserver.ini** em um editor de texto.
4. Em [WebsenseServer], adicione uma linha em branco e insira o seguinte:
 

```
BlockMsgServerName = <endereço IP do Filtering Service>
```

 Por exemplo, se o endereço IP do Filtering Service for 10.201.72.15, insira:
 

```
BlockMsgServerName = 10.201.72.15
```
5. Salve e feche o arquivo.
6. Reinicie o Filtering Service.

Se a máquina com o Filtering Service tiver mais de uma NIC, e a página de bloqueio ainda não aparecer corretamente após a edição do arquivo **eimserver.ini**, experimente os endereços IP das outras NICs no parâmetro **BlockMsgServerName**.

Se a página de bloqueio ainda não aparecer, verifique se esses usuários têm acesso de leitura aos arquivos nos diretórios da página de bloqueio do Websense.

- ◆ Websense\BlockPages\en\Default
- ◆ Websense\BlockPages\en\Custom

Se o problema da página de bloqueio persistir, consulte a [Base de conhecimentos](#) do Websense para obter dicas adicionais sobre solução de problemas.

## Uma página branca vazia aparece em vez de uma página de bloqueio

Quando anúncios são bloqueados ou quando um navegador não detecta corretamente a codificação associada a uma página de bloqueio, os usuários talvez recebam uma página branca vazia em vez de uma página de bloqueio. Os motivos para isso são os seguintes:

- ◆ Quando a categoria Anúncios é bloqueada, o software Websense algumas vezes interpreta uma solicitação de arquivo de imagem como uma solicitação de anúncio e exibe uma página vazia em vez de uma mensagem de bloqueio (o método normal de bloquear anúncios). Se o URL solicitado terminar em .gif ou

algo semelhante, peça que o usuário reinsira o URL, deixando de fora o trecho \*.gif.

- ◆ Alguns navegadores antigos podem não detectar a codificação das páginas de bloqueio. Para ativar a detecção de caracteres apropriada, configure o navegador para exibir o conjunto de caracteres adequado (UTF-8 para francês, alemão, italiano, espanhol, português do Brasil, chinês simplificado, chinês tradicional ou coreano, e Shift\_JIS para japonês). Consulte as instruções na documentação do navegador ou atualize a versão do navegador.

## Mensagens de bloqueio de protocolo não são exibidas como esperado

As mensagens de bloqueio de protocolo podem não ser exibidas ou aparecem somente com atraso por um dos seguintes motivos:

- ◆ O User Service deve ser instalado em uma máquina com o Windows para que as mensagens de bloqueio de protocolo sejam exibidas corretamente. Para obter mais informações, consulte o *Guia de Instalação*.
- ◆ As mensagens de bloqueio de protocolo podem não chegar às máquinas clientes se o Network Agent estiver instalado em uma máquina com várias placas de rede (NICs), e uma NIC estiver monitorando um segmento de rede diferente do Filtering Service. Verifique se a máquina com o Filtering Service tem NetBIOS e o protocolo SMB (Server Message Block) tem acesso às máquinas clientes, e se a porta 15871 não está bloqueada.
- ◆ Uma mensagem de bloqueio de protocolo pode estar um pouco atrasada ou aparecer em uma máquina interna onde os dados do protocolo solicitado foram originados (e não na máquina cliente), quando o Network Agent é configurado para monitorar solicitações **enviadas a** máquinas internas.
- ◆ Se a máquina com o cliente filtrado ou a filtragem do Websense estiver executando o Windows 200x, o serviço Windows **Messenger** deverá estar em execução para que a mensagem de bloqueio de protocolo seja exibida. Use a caixa de diálogo Serviços do Windows no cliente ou no servidor para ver se o Messenger está em execução (consulte [A caixa de diálogo Serviços do Windows, página 392](#)). Mesmo que a mensagem de bloqueio não seja exibida, as solicitações de protocolo são bloqueadas.

## Uma mensagem de bloqueio de protocolo é exibida em vez de uma página de bloqueio

Se o seu produto de integração não enviar informações HTTPS ao software Websense ou se o software Websense estiver em execução no modo autônomo, o Network Agent poderá interpretar uma solicitação por site HTTPS que esteja bloqueado via configurações de categoria como uma solicitação de protocolo. Como resultado, uma mensagem de bloqueio de protocolo será exibida. A solicitação HTTPS também é registrada como uma solicitação de protocolo.

---

## Problemas de registro, mensagem de status e alerta

---

- ◆ [Onde encontro as mensagens de erro dos componentes do Websense?](#), página 377
- ◆ [Alertas de saúde do Websense](#), página 377
- ◆ [Dois registros em log são gerados para uma única solicitação](#), página 378

### Onde encontro as mensagens de erro dos componentes do Websense?

Quando há erros ou avisos relacionados aos principais componentes do Websense, são exibidas mensagens de alerta rápidas na lista **Resumo do alerta de saúde** na parte superior da página **Status > Hoje** do Websense Manager (consulte [Alertas de saúde do Websense](#), página 377).

- ◆ Clique em uma mensagem de alerta para ver informações mais detalhadas na página **Status > Alertas**.
- ◆ Clique em **Soluções** ao lado de uma mensagem na página **Status > Alertas** para obter ajuda na solução de problemas.

Erros, avisos e mensagens de componentes do software Websense, bem como mensagens de status de download de banco de dados, são registrados no arquivo **websense.log** no diretório **bin** do Websense (C:\Arquivos de Programas\WebSense\bin ou /opt/WebSense/bin, por padrão). Consulte [O arquivo de log do Websense](#), página 393.

Para os componentes do software Websense instalados em máquinas com Windows, você também pode verificar o Windows Event Viewer. Consulte [O Windows Event Viewer](#), página 393.

### Alertas de saúde do Websense

O Resumo do alerta de saúde do Websense inclui os possíveis problemas encontrados por componentes monitorados do software Websense. Estão incluídos:

- ◆ O Filtering Service não está em execução
- ◆ O User Service não está disponível
- ◆ O Log Server não está em execução
- ◆ Nenhum Log Server está instalado para um Policy Server
- ◆ O banco de dados de log não está disponível
- ◆ O Network Agent não está em execução
- ◆ Nenhum Network Agent está instalado para um Policy Server
- ◆ Nenhuma NIC de monitoramento foi configurada para um Network Agent
- ◆ Nenhum Filtering Service foi configurado para um Network Agent
- ◆ O banco de dados de filtragem inicial está em uso
- ◆ O Master Database está em andamento pela primeira vez

- ◆ O Master Database está sendo atualizado
- ◆ O Master Database tem mais de 1 semana de idade
- ◆ O download do Master Database não teve êxito
- ◆ WebCatcher não está ativado
- ◆ Problema de assinatura
- ◆ A chave de assinatura está prestes a expirar
- ◆ Nenhuma chave de assinatura foi inserida

A página **Alertas** fornece informações básicas sobre qualquer condição de erro ou aviso. Clique em **Soluções** para obter informações sobre como solucionar o problema.

Em alguns casos, se estiver recebendo mensagens de erro ou de status sobre um componente que não está em uso ou que foi desativado, você poderá ocultar as mensagens de alerta. Consulte [Verificando o status atual do sistema](#), página 291, para obter mais informações.

## Dois registros em log são gerados para uma única solicitação

Quando o Agendador de pacotes QoS do Windows é instalado na mesma máquina do Network Agent, duas solicitações são registradas para cada solicitação HTTP ou de protocolo emitida pela máquina com o Network Agent. (Essa duplicação não ocorre com solicitações com origem em máquinas clientes em sua rede.)

Para corrigir o problema, desative o Agendador de pacotes QoS do Windows na máquina com o Network Agent.

Esse problema não ocorre quando você usa o Network Agent para todos os registros em log. Consulte [Definindo as configurações de placa de rede](#), página 343, para obter detalhes.

## Problemas do Policy Server e do Policy Database

---

- ◆ [Esqueci minha senha](#), página 378
- ◆ [Não consigo fazer logon no Policy Server](#), página 379
- ◆ [Falha do serviço Websense Policy Database ao iniciar](#), página 379

### Esqueci minha senha

Se você é um Super administrador ou administrador delegado que usa uma conta de usuário do Websense para fazer logon no Policy Server via Websense Manager, qualquer Super administrador incondicional pode redefinir a senha.

- ◆ A senha do WebsenseAdministrator é definida na página **Configurações > Conta**.
- ◆ As outras senhas da conta de administrador são definidas na página **Administração delegada > Gerenciar contas de usuário do Websense**.

Se você não está usando administração delegada e esqueceu a senha do WebsenseAdministrator, faça logon em MyWebsense para redefinir a senha.

- ◆ A chave de assinatura associada à conta no MyWebsense deve corresponder à chave de assinatura do Websense Web Security ou do Websense Web Filter.
- ◆ Se você tem várias chaves de assinatura, deve selecionar a chave apropriada do Websense Web Security ou do Websense Web Filter para que o processo de redefinição seja correto.
- ◆ É preciso ter acesso à máquina com o Websense Manager para a conclusão do processo de redefinição.

## Não consigo fazer logon no Policy Server

Verifique se o endereço IP do Policy Server está correto. Se o endereço da máquina com o Policy Server mudou desde que o Policy Server foi adicionado ao Websense Manager, você terá que fazer logon em outro Policy Server, remover o antigo endereço IP do Websense Manager e adicionar o novo endereço IP do Policy Server. Consulte [Adicionando e editando instâncias do Policy Server](#), página 276.

Se o Websense Manager tiver parado repentinamente ou parado com os comandos kill (Linux) ou Finalizar tarefa (Windows), aguarde alguns minutos antes de se conectar novamente. O software Websense detecta e fecha a sessão encerrada no prazo de três minutos.

## Falha do serviço Websense Policy Database ao iniciar

O Websense Policy Database é executado como uma conta especial: **WebsenseDBUser**. Se ocorrerem problemas de logon nessa conta, o Policy Database não consegue iniciar.

Para solucionar o problema, altere a senha do WebsenseDBUser.

1. Faça logon na máquina com o Policy Database como administrador local.
2. Vá para **Iniciar > Programas > Ferramentas administrativas > Gerenciamento do computador**.
3. No painel de navegação, em Ferramentas do sistema, expanda **Usuários e grupos locais** e selecione **Usuários**. As informações do usuário são exibidas no painel de conteúdo.
4. Clique com o botão direito em **WebsenseDBUser** e selecione **Definir senha**.
5. Insira e confirme a nova senha para esta conta de usuário e clique em **OK**.
6. Feche a caixa de diálogo Gerenciamento do computador.
7. Vá para **Iniciar > Programas > Ferramentas administrativas > Serviços**.
8. Clique com o botão direito em **Websense Policy Database** e selecione **Propriedades**.
9. Na guia Logon da caixa de diálogo Propriedades, insira informações da nova senha do WebsenseDBUser e clique em **OK**.

10. Clique com o botão direito no Websense Policy Database novamente e selecione **Iniciar**.

Depois que o serviço iniciar, feche a caixa de diálogo Serviços.

## Problemas de administração delegada

---

- ◆ *Os clientes gerenciados não podem ser excluídos da função*, página 380
- ◆ *Mensagem de erro de logon informa que outra pessoa se conectou em minha máquina*, página 380
- ◆ *Alguns usuários não conseguem acessar um site na lista de URLs não filtrados*, página 381
- ◆ *Os sites recategorizados são filtrados de acordo com a categoria incorreta*, página 381
- ◆ *Não consigo criar um protocolo personalizado*, página 381

## Os clientes gerenciados não podem ser excluídos da função

Os clientes não podem ser excluídos diretamente da lista de clientes gerenciados na página Administração delegada >Editar função se:

- ◆ o administrador aplicou uma diretiva ao cliente
- ◆ o administrador aplicou uma diretiva a um ou mais membros de uma rede, grupo, domínio ou unidade organizacional

Também podem ocorrer problemas se, durante o logon do Websense Manager, o Super administrador escolher um Policy Server que não seja o que se comunica com o serviço de diretório que contém os clientes a serem excluídos. Nessa situação, o atual Policy Server e o serviço de diretório não reconhecem os clientes.

Para obter ajuda sobre como excluir clientes gerenciados, consulte [Excluindo clientes gerenciados](#), página 262.

## Mensagem de erro de logon informa que outra pessoa se conectou em minha máquina

Quando você tenta fazer logon no Websense Manager, pode receber a mensagem de erro “Falha de logon. A função <nome da função> está em uso por <nome de usuário>, desde <data, hora>, no computador 127.0.0.1.” O endereço IP 127.0.0.1 também é chamado de endereço de loopback e, normalmente, indica a máquina local.

Essa mensagem indica que alguém se conectou na máquina de instalação do Websense Manager, na mesma função que você está solicitando. Você pode selecionar outra função (se você administra várias funções), fazer logon apenas para criar relatórios ou esperar até o administrador se desconectar.

## Alguns usuários não conseguem acessar um site na lista de URLs não filtrados

Os URLs não filtrados afetam somente os clientes gerenciados por função em que os URLs são adicionados. Por exemplo, se um Super administrador adiciona URLs não filtrados, os clientes gerenciados por funções de administração delegada não têm acesso a esses sites.

Para que o site fique disponível aos clientes em outras funções, o Super administrador pode alternar para cada função e adicionar sites relevantes a essa lista de URLs não filtrados da função.

## Os sites recategorizados são filtrados de acordo com a categoria incorreta

Os URLs recategorizados afetam somente os clientes gerenciados pela função em que os URLs são adicionados. Por exemplo, quando um Super administrador recategoriza URLs, os clientes gerenciados por funções de administração delegada continuam a ser filtrados de acordo com a categoria do Master Database para esses sites.

Para aplicar a recategorização aos clientes em outras funções, o Super administrador pode alternar para cada função e recategorizar os sites para essa função.

## Não consigo criar um protocolo personalizado

Somente os Super administradores são capazes de criar protocolos personalizados. Entretanto, os administradores delegados podem definir ações de filtragem para protocolos personalizados.

Ao criar protocolos personalizados, os Super administradores devem definir a ação padrão apropriada para a maioria dos clientes. Em seguida, informam os administradores delegados sobre o novo protocolo para que estes possam atualizar os filtros para suas funções, conforme apropriado.

## Problemas de relatório

---

- ◆ *O Log Server não está em execução, página 382*
- ◆ *Nenhum Log Server está instalado para um Policy Server, página 383*
- ◆ *O banco de dados de log não foi criado, página 383*
- ◆ *O banco de dados de log não está disponível, página 384*
- ◆ *Tamanho do banco de dados de log, página 385*
- ◆ *O Log Server não está registrando dados no banco de dados de log, página 385*
- ◆ *Atualizando a senha de conexão do Log Server, página 386*

- ◆ [Configurando permissões de usuário para o Microsoft SQL Server 2005](#), página 386
- ◆ [O Log Server não pode se conectar ao serviço de diretório](#), página 387
- ◆ [Os dados sobre o tempo de navegação na Internet estão distorcidos](#), página 388
- ◆ [A largura de banda é maior que o esperado](#), página 388
- ◆ [Algumas solicitações de protocolo não estão sendo registradas](#), página 388
- ◆ [Todos os relatórios estão vazios](#), página 388
- ◆ [Nenhum gráfico é exibido nas páginas Hoje ou Histórico](#), página 390
- ◆ [Não é possível acessar determinados recursos de relatório](#), página 390
- ◆ [A saída do Microsoft Excel não contém alguns dados de relatório](#), página 390
- ◆ [Salvando a saída de relatórios de apresentação como HTML](#), página 391
- ◆ [Problemas de pesquisa de relatórios investigativos](#), página 391
- ◆ [Problemas gerais de relatórios investigativos](#), página 392

## O Log Server não está em execução

Se o Log Server não estiver em execução ou se outros componentes do Websense não puderem se comunicar com o Log Server, as informações de uso da Internet não serão armazenadas e você não poderá gerar relatórios de uso da Internet.

O Log Server pode não estar disponível se:

- ◆ Não houver espaço em disco suficiente na máquina com o Log Server.
- ◆ Você alterou a senha do Microsoft SQL Server ou do MSDE sem atualizar a configuração do ODBC ou do Log Server.
- ◆ Já se passaram mais de 14 dias desde o último download do Master Database.
- ◆ O arquivo logserver.ini está ausente ou corrompido.
- ◆ Você parou o Log Server para evitar o registro em log das informações de uso da Internet.

Para solucionar o problema:

- ◆ Verifique o volume de espaço livre em disco e remova os arquivos irrelevantes, se necessário.
- ◆ Se você acreditar que a alteração de senha é a fonte do problema, consulte [Atualizando a senha de conexão do Log Server](#), página 386.
- ◆ Navegue até o diretório **bin** do Websense (C:\Arquivos de Programas\Websense\bin, por padrão) e confirme se você pode abrir **logserver.ini** em um editor de texto. Se o arquivo estiver corrompido, substitua-o por um arquivo de backup.
- ◆ Verifique na caixa de diálogo Serviços do Windows se o Log Server iniciou e reinicie o serviço se necessário (consulte [Parando e iniciando os serviços Websense](#), página 283).
- ◆ Verifique no Windows Event Viewer e no arquivo **websense.log** se há mensagens de erro do Log Server (consulte [Ferramentas de solução de problemas](#), página 392).

## Nenhum Log Server está instalado para um Policy Server

O Websense Log Server coleta informações de uso da Internet e as armazena no banco de dados de log para aplicação em relatórios investigativos, relatórios de apresentação e os gráficos e resumos nas páginas Hoje e Histórico do Websense Manager.

O Log Server deve ser instalado para permitir a geração de relatórios.

A mensagem será exibida se:

- ◆ O Log Server estiver instalado em uma máquina que não tenha o Policy Server, e o endereço IP do Log Server estiver incorretamente definido como localhost no Websense Manager.
- ◆ O Log Server estiver instalado em uma máquina com Linux.
- ◆ Você não estiver usando as ferramentas de relatórios do Websense.

Para verificar se o endereço IP correto do Log Server está definido no Websense Manager:

1. Selecione a guia **Configurações** do painel de navegação esquerdo e vá para **Geral > Registro em log**.
2. Insira o endereço IP da máquina com o Log Server no campo **Endereço IP ou nome do Log Server**.
3. Clique em **OK** para salvar a alteração em cache e clique em **Salvar tudo**.

Se o Log Server estiver instalado em uma máquina com Linux ou se você não estiver usando as ferramentas de relatórios do Websense, será possível ocultar a mensagem de alerta no Websense Manager.

1. Na guia Principal do painel de navegação esquerdo, vá para **Status > Alertas**.
2. Em Alertas ativos, clique em **Avançado**.
3. Marque **Ocultar este alerta** para a mensagem Nenhum Log Server está instalado.
4. Clique em **Salvar agora**. A alteração será implementada imediatamente.

## O banco de dados de log não foi criado

Há ocasiões em que o programa de instalação não pode criar o banco de dados de log. A lista a seguir descreve as causas e as soluções mais comuns.

---

**Problema:** Existem alguns arquivos que usam os nomes que o software Websense usa para o banco de dados de log (wslogdb70 e wslogdb70\_1), mas os arquivos não se associam corretamente ao mecanismo do banco de dados; portanto, não podem ser usados pelo programa de instalação do Websense.

**Solução:** Remova ou renomeie os arquivos e execute o programa de instalação novamente.

---

**Problema:** A conta usada para fazer logon para instalação tem permissões inadequadas na unidade em que o banco de dados está sendo instalado.

---

---

<b>Solução:</b>	Atualize a conta de logon para ter as permissões de leitura e gravação para o local de instalação, ou conecte-se com outra conta que já tenha essas permissões. Em seguida, execute o programa de instalação novamente.
<b>Problema:</b>	Não há espaço em disco suficiente para criar e manter o banco de dados de log no local especificado.
<b>Solução:</b>	Libere espaço suficiente no disco selecionado para instalar e manter o banco de dados de log. Em seguida, execute o programa de instalação novamente. Você também pode escolher outro local.
<b>Problema:</b>	A conta usada para fazer logon para instalação tem permissões inadequadas do SQL Server para a criação de um banco de dados.
<b>Solução:</b>	Atualize a conta de logon ou conecte-se com uma conta que já tenha as permissões necessárias. Em seguida, execute o programa de instalação novamente.  As permissões necessárias dependem da versão do Microsoft SQL Server: <ul style="list-style-type: none"><li>■ SQL Server 2000 ou MSDE: são necessárias permissões <b>dbo</b> (proprietário de banco de dados)</li><li>■ SQL Server 2005: são necessárias permissões <b>dbo</b> e <b>SQLServerAgentReader</b></li></ul>

---

## O banco de dados de log não está disponível

O banco de dados de log do Websense armazena informações de uso na Internet para aplicação em relatórios de apresentação, relatórios investigativos e os gráficos e resumos nas páginas Hoje e Histórico do Websense Manager.

Se o software Websense não puder se conectar ao banco de dados de log, primeiro verifique se o mecanismo do banco de dados (Microsoft SQL Server ou Microsoft SQL Server Desktop Engine [MSDE]) está em execução na máquina com o banco de dados de log.

1. Abra a caixa de diálogo Serviços do Windows (consulte [A caixa de diálogo Serviços do Windows](#), página 392) e verifique se os seguintes serviços estão em execução:
  - Microsoft SQL Server:
    - MSSQLSERVER
    - SQLSERVERAGENT
  - Microsoft SQL Desktop Engine (MSDE):
    - MSSQL\$WEBSSENSE (se você obteve o MSDE da Websense, Inc.)
    - SQLAgent\$WEBSSENSE
2. Se algum serviço foi interrompido, clique no nome do serviço e clique em **Iniciar**.

Se o serviço não reiniciar, verifique no Windows Event Viewer (consulte [O Windows Event Viewer](#), página 393) para se informar sobre erros e avisos de Microsoft SQL Server ou MSDE.

Se o mecanismo do banco de dados estiver em execução:

- ◆ Verifique se o SQL Server Agent está em execução na máquina que executa o mecanismo do banco de dados.
- ◆ Use a caixa de diálogo Serviços do Windows para verificar se o **Websense Log Server** está em execução.
- ◆ Se o Log Server e o banco de dados de log estiverem em máquinas diferentes, verifique se as duas estão funcionando e se a conexão de rede entre elas não está danificada.
- ◆ Verifique se há espaço em disco suficiente na máquina com o banco de dados de log e se ele tem um volume suficiente de espaço em disco alocado (consulte [O Log Server não está registrando dados no banco de dados de log](#), página 385).
- ◆ Certifique-se de que a senha do Microsoft SQL Server ou do MSDE não foi alterada. Se a senha mudar, será preciso atualizar as informações de senha que o Log Server usa para se conectar ao banco de dados. Consulte [Atualizando a senha de conexão do Log Server](#), página 386.

## Tamanho do banco de dados de log

O tamanho do banco de dados de log é sempre uma preocupação. Se você tem gerado relatórios do Websense com êxito e perceber que agora a exibição está mais demorada, ou se começar a receber mensagens de tempo limite do navegador da Web, é recomendável desativar algumas partições do banco de dados.

1. No Websense Manager, vá para **Configurações > Reporting > banco de dados de log**.
2. Localize a seção **Partições disponíveis** da página.
3. Desmarque a caixa de seleção **Habilitar** para as partições que não são necessárias às operações de relatório em andamento.
4. Clique em **Salvar agora** para implementar a alteração.

## O Log Server não está registrando dados no banco de dados de log

Normalmente, quando o Log Server não pode gravar dados no banco de dados de log, é porque não há espaço em disco alocado suficiente. Isso pode ocorrer quando a unidade de disco está cheia ou, no caso do Microsoft SQL Server, se houver um tamanho máximo definido para o limite de crescimento do banco de dados.

Se a unidade de disco que hospeda o banco de dados de log estiver cheia, será preciso adicionar espaço em disco à máquina para restaurar o recurso de log.

Se o administrador do banco de dados do SQL Server tiver definido um tamanho máximo para o crescimento do banco de dados no Microsoft SQL Server, use um dos seguintes métodos:

- ◆ Entre em contato com o administrador do banco de dados do SQL Server para aumentar o limite máximo.
- ◆ Informe-se sobre o tamanho máximo e vá para **Configurações > Reporting > banco de dados de log** para configurar o banco de dados de log para que seja substituído quando atingir cerca de 90% do tamanho máximo. Consulte [Configurando opções de substituição](#), página 321.

Se o departamento de TI tiver estabelecido um volume máximo de espaço em disco para as operações do SQL Server, entre em contato com eles para obter ajuda.

## Atualizando a senha de conexão do Log Server

Se você alterar a senha da conta que o software Websense usa para se conectar ao banco de dados de log, terá que atualizar também o Log Server para que ele use a nova senha.

1. Na máquina com o Log Server, vá para **Iniciar > Programas > Websense > Utilitários > Configuração do Log Server**. O utilitário Configuração do Log Server é aberto.
2. Clique na guia **Banco de dados** e verifique se o banco de dados correto (por padrão, **wslogdb70**) aparece no campo DSN (nome da fonte de dados do ODBC).
3. Clique em **Conexão**. A caixa de diálogo Selecionar fonte de dados é exibida.
4. Clique na guia **Fonte de dados na máquina** e clique duas vezes em **wslogdb70** (ou no nome do seu banco de dados de log). A caixa de diálogo Login do SQL Server é exibida.
5. Verifique se o campo LoginID contém o nome de conta correto (em geral **sa**) e insira a nova senha.
6. Clique em **OK** e, na caixa de diálogo Configuração do Log Server, clique em **Aplicar**.
7. Clique na guia **Conexão**, pare e reinicie o Log Server.
8. Quando o Log Server estiver novamente em execução, clique em **OK** para fechar o utilitário.

## Configurando permissões de usuário para o Microsoft SQL Server 2005

O Microsoft SQL Server 2005 define funções do SQL Server Agent que administram a acessibilidade à estrutura de trabalhos. Os trabalhos do SQL Server Agent para SQL Server 2005 são armazenados no banco de dados msdb do SQL Server.

Para instalar o Websense Log Server com êxito, a conta de usuário que possui o banco de dados do Websense deve ter associação em uma das seguintes funções no banco de dados msdb:

- ◆ Função SQLAgentUser
- ◆ Função SQLAgentReader

- ◆ Função SQLAgentOperator

**Obs.:**

A conta de usuário do SQL também deve estar associada à função de servidor fixa *DBCreator*.

Vá para Microsoft SQL Server 2005 para conceder à conta de usuário do SQL Server as permissões necessárias para instalar com êxito os componentes de relatórios do Websense.

1. No computador do SQL Server, vá para **Iniciar > Programas > Microsoft SQL Server 2005 > Microsoft SQL Server Management Studio**.
2. Selecione a árvore **Object Explorer**.
3. Selecione **Logins > de Segurança**.
4. Selecione a conta de login que será usada durante a instalação.
5. Clique com o botão direito na conta de login e selecione **Propriedades** para este usuário.
6. Selecione **Mapeamento de Usuários** e faça o seguinte:
  - a. Selecione **msdb** em mapeamento do banco de dados.
  - b. Conceda associação para uma destas funções:
    - Função SQLAgentUser
    - Função SQLAgentReader
    - Função SQLAgentOperator
  - c. Clique em **OK** para salvar.
7. Selecione **Funções de Servidor** e selecione **dbcreator**. A função dbcreator é criada.
8. Clique em **OK** para salvar.

## O Log Server não pode se conectar ao serviço de diretório

Se um dos erros indicados abaixo ocorrer, o Log Server não poderá ter acesso ao serviço de diretório, que é necessário para a atualização de mapeamentos de usuários para grupos dos relatórios. Esses erros aparecem no Windows Event Viewer (consulte [O Windows Event Viewer](#), página 393).

- ◆ EVENT ID:4096 - Não é possível inicializar o serviço de diretório. O Websense Server pode estar desativado ou inacessível.
- ◆ EVENT ID:4096 – Não foi possível conectar ao serviço de diretório. Os grupos deste usuário não serão resolvidos neste momento. Verifique se esse processo pode acessar o serviço de diretório.

A causa mais comum é o Websense Log Server e o Websense User Service estarem em lados opostos de um firewall que está limitando o acesso.

Para solucionar este problema, configure o firewall para permitir o acesso pelas portas usadas para a comunicação entre esses componentes.

## Os dados sobre o tempo de navegação na Internet estão distorcidos

A consolidação pode distorcer os dados dos relatórios sobre o tempo de navegação na Internet. Esses relatórios indicam o tempo que os usuários gastam no acesso à Internet e podem incluir detalhes sobre o tempo em cada site. O tempo de navegação na Internet é calculado com o uso de um algoritmo especial; a ativação da consolidação pode distorcer a precisão dos cálculos desses relatórios.

## A largura de banda é maior que o esperado

Muitas das integrações do Websense fornecem informações sobre largura de banda. Se a sua integração não fornecer informações sobre largura de banda, você poderá configurar o Network Agent para fazer o registro em log de modo a incluir dados sobre largura de banda.

Quando um usuário solicita o download de um arquivo permitido, o produto de integração ou o Network Agent envia o tamanho integral do arquivo, que o software Websense registra como bytes recebidos.

Se depois o usuário cancelar o download, ou o arquivo não baixar completamente, o valor dos bytes recebidos no banco de dados de log ainda representará o tamanho integral do arquivo. Nessas circunstâncias, os bytes reportados recebidos serão maiores que o número real de bytes recebidos.

Isso também afeta os valores de largura de banda reportados, que representam uma combinação de bytes recebidos e bytes enviados.

## Algumas solicitações de protocolo não estão sendo registradas

Alguns protocolos, como os usados por ICQ e AOL, solicitam que os usuários se conectem a um servidor usando um endereço IP e, em seguida, enviam outro endereço IP identificador e um número de porta ao cliente para fins de mensagens. Nesse caso, todas as mensagens enviadas e recebidas podem não ser monitoradas e registradas em log pelo Websense Network Agent, pois o servidor de mensagens não é conhecido no momento da troca de mensagens.

Como resultado, o número de solicitações registradas pode não corresponder ao número de solicitações de fato enviadas. Isso afeta a precisão dos relatórios produzidos pelas ferramentas de relatórios do Websense.

## Todos os relatórios estão vazios

Se não houver dados para qualquer um dos seus relatórios, verifique se:

- ◆ As partições ativas do banco de dados incluem informações para as datas incluídas nos relatórios. Consulte [Partições de banco de dados](#), página 389.
- ◆ O trabalho do SQL Server Agent está ativo no Microsoft SQL Server ou no MSDE. Consulte [SQL Server Agent job](#), página 389.

- ◆ O Log Server está configurado corretamente para receber informações de log do Filtering Service. Consulte *Configuração do Log Server*, página 389.

## Partições de banco de dados

Os registros do Websense estão armazenados em partições do banco de dados. Novas partições podem ser criadas com base em tamanho ou data, dependendo da configuração e do mecanismo do banco de dados.

Você pode ativar ou desativar partições individuais no Websense Manager. Se você tentar gerar o relatório com base em informações baseadas em partições desativadas, nenhuma informação será localizada e o relatório estará vazio.

Para saber se as partições apropriadas do banco de dados estão ativas:

1. Vá para **Configurações > Reporting > banco de dados de log**.
2. Role a página até a seção **Partições disponíveis**.
3. Marque a caixa de seleção **Habilitar** para cada partição que contém dados a serem incluídos nos relatórios.
4. Clique em **Salvar agora** para implementar a alteração.

## SQL Server Agent job

É possível que o trabalho de banco de dados do SQL Server Agent tenha sido desativado. Esse trabalho deve estar em execução para que os registros sejam processados no banco de dados pelo trabalho do banco de dados ETL.

Se você estiver executando com o MSDE:

1. Vá para **Iniciar > Ferramentas administrativas > Serviços**.
2. Verifique se os serviços SQL Server e SQL Server Agent foram iniciados. Se você obteve o MSDE da Websense, Inc., esses serviços chamam-se MSSQL\$WEBSSENSE e SQLAgent\$WEBSSENSE.

Se você está executando o Microsoft SQL Server integral, peça ao administrador de banco de dados que verifique se o trabalho do SQL Server Agent está em execução.

## Configuração do Log Server

As definições de configuração devem estar corretas no Websense Manager e no Log Server para que o Log Server receba informações de log do Filtering Service. Caso contrário, os dados do log nunca serão processados no banco de dados de log.

Primeiro, verifique se o Websense Manager está se conectando ao Log Server corretamente.

1. Faça logon no Websense Manager com permissões incondicionais de Super administrador.
2. Vá para **Configurações > Geral > Registro em log**.
3. Insira o **nome da máquina** ou o **endereço IP** onde o Log Server está localizado.

4. Especifique a **porta** em que o Log Server está ouvindo (o padrão é 55805).
5. Clique em **Verificar status** para determinar se o Websense Manager é capaz de se comunicar com o Log Server especificado.  
Uma mensagem indica se o teste de conexão foi aprovado. Atualize o endereço IP ou o nome da máquina e a porta, se necessário, até o teste ser bem-sucedido.
6. Quando terminar, clique em **OK** para colocar as alterações em cache. As alterações só serão implementadas quando você clicar em **Salvar tudo**.

Em seguida, verifique as configurações no utilitário Configuração do Log Server.

1. Na máquina em que o Log Server está em execução, vá para **Iniciar > Programas > Websense > Utilitários > Configuração do Log Server**.
2. Na guia **Conexões**, verifique se a porta corresponde ao valor inserido no Websense Manager.
3. Clique em **OK** para salvar as alterações.
4. Use o botão na guia **Conexões** para interromper e iniciar o Log Server.
5. Clique em **Sair** para fechar o utilitário Configuração do Log Server.

## Nenhum gráfico é exibido nas páginas Hoje ou Histórico

Em organizações que usam administração delegada, verifique as permissões de relatório para a função de administrador delegado. Se a opção **Exibir relatórios nas páginas Hoje e Histórico** não estiver selecionada, esse gráfico não será exibido para administradores delegados nessa função.

Em ambientes que usam vários Policy Servers, o Log Server é instalado para se comunicar somente com um Policy Server. É preciso fazer logon nesse Policy Server para exibir os gráficos das páginas Hoje e Histórico ou para ter acesso a outros recursos de relatório.

## Não é possível acessar determinados recursos de relatório

Se o navegador da Web bloqueia pop-ups com uma configuração muito restrita, determinados recursos de relatório podem ser bloqueados. Para usá-los, você deve diminuir o nível de bloqueio ou desativar totalmente o bloqueio a pop-ups.

## A saída do Microsoft Excel não contém alguns dados de relatório

O maior número de linhas que pode ser aberto em uma planilha do Microsoft Excel é 65.536. Se você exportar um relatório com mais de 65.536 registros para o formato do Microsoft Excel, o registro número 65.537 e todos os subseqüentes não estarão disponíveis na planilha.

Para assegurar o acesso a todas as informações no relatório exportado, use um dos seguintes métodos:

- Para os relatórios de apresentação, edite o filtro de relatório para definir um relatório menor, talvez configurando um intervalo de datas menor, selecionando menos usuários e grupos, ou menos ações.
- Para relatórios investigativos, aprofunde o nível de acesso aos dados para definir um relatório menor.
- Selecione outro formato de exportação.

## Salvando a saída de relatórios de apresentação como HTML

Se você gerar um relatório diretamente na página Reporting > Relatórios de apresentação, poderá escolher entre três formatos de exibição: HTML, PDF e XLS. Se você preferir o formato de exibição HTML, poderá visualizar o relatório na janela do Websense Manager.

Não é recomendável imprimir nem salvar relatórios de apresentação no navegador. A saída impressa inclui toda a janela do navegador. A abertura de um arquivo salvo inicia o Websense Manager.

Para imprimir ou salvar relatórios com mais eficácia, escolha o formato de saída PDF ou XLS. Você pode abrir esses tipos de arquivo imediatamente se o software de visualização (Adobe Reader ou Microsoft Excel) estiver instalado na máquina local. Você também pode salvar o arquivo em disco (a única opção se o software de visualização apropriado não estiver disponível).

Depois de abrir um relatório no Adobe Reader ou no Microsoft Excel, use as opções de imprimir e salvar do programa para produzir a saída final desejada.

## Problemas de pesquisa de relatórios investigativos

Há duas possíveis preocupações relacionadas à pesquisa em relatórios investigativos.

- ◆ Os caracteres ASCII estendidos não podem ser inseridos
- ◆ O padrão de pesquisa não pode ser encontrado

### Caracteres ASCII estendidos

Os campos de pesquisa acima do gráfico de barras na página principal dos relatórios investigativos permitem que você busque um termo ou uma seqüência de texto específica no elemento gráfico selecionado.

Se você está usando o Mozilla Firefox em um servidor Linux para ter acesso ao Websense Manager, não poderá inserir caracteres ASCII estendidos nesses campos. Essa é uma limitação conhecida do Firefox em Linux.

Se você precisar pesquisar um relatório investigativo em busca de uma seqüência de texto que inclua caracteres ASCII estendidos, acesse o Websense Manager em um servidor Windows, usando qualquer navegador compatível.

### Pesquisa de padrão não encontrada

Algumas vezes, os relatórios investigativos não localizam URLs associados a um padrão inserido nos campos de pesquisa da página principal dos relatórios investigativos. Se isso ocorrer e você acreditar que o padrão existe nos URLs informados, tente inserir outro padrão que também pudesse localizar os URLs em questão.

## Problemas gerais de relatórios investigativos

- ◆ Algumas consultas são bem demoradas. Você pode ver uma tela vazia ou receber uma mensagem informando que sua consulta atingiu o tempo limite. Isso pode ocorrer pelos seguintes motivos:
  - Tempo limite do servidor Web
  - Tempo limite do MSDE ou do Microsoft SQL Server
  - Tempo limite do servidor proxy ou cacheVocê talvez precise aumentar manualmente o valor de tempo limite desses componentes.
- ◆ Se os usuários não estiverem em qualquer grupo, também não aparecerão em um domínio. As opções de grupo e de domínio estarão inativas.
- ◆ Mesmo que o Log Server esteja registrando visitas em vez de acessos, os relatórios investigativos denominam essas informações de **Acessos**.

## Ferramentas de solução de problemas

---

- ◆ *A caixa de diálogo Serviços do Windows, página 392*
- ◆ *O Windows Event Viewer, página 393*
- ◆ *O arquivo de log do Websense, página 393*

### A caixa de diálogo Serviços do Windows

Em máquinas com o Microsoft Windows, os recursos Filtering Service, Network Agent, Policy Server, User Service e todos os agentes de identificação transparente do Websense são executados como serviços. Você pode usar a caixa de diálogo Serviços do Windows para verificar o status desses serviços.

1. No Painel de controle do Windows, abra a pasta **Ferramentas administrativas**.
2. Clique duas vezes em **Serviços**.
3. Percorra a lista para localizar o serviço para o qual você está solucionando problemas.

A entrada inclui o nome do serviço, uma descrição resumida do serviço, o status do serviço (iniciado ou interrompido), como o serviço é iniciado e a conta que ele usa para realizar suas tarefas.

4. Clique duas vezes no nome de um serviço para abrir uma caixa de diálogo de propriedades com informações mais detalhadas sobre o serviço.

## O Windows Event Viewer

O Windows Event Viewer registra mensagens de erro sobre eventos do Windows, incluindo as atividades do serviço. Essas mensagens podem ajudá-lo a identificar os erros da rede ou do serviço que podem estar causando problemas de filtragem na Internet ou de identificação de usuário.

1. No Painel de controle do Windows, abra a pasta **Ferramentas administrativas**.
2. Clique duas vezes em **Event Viewer**.
3. Em Event Viewer, clique em **Aplicativo** para obter uma lista de mensagens de erro, avisos e mensagens informativas.
4. Percorra a lista para identificar os erros ou avisos dos serviços Websense.

## O arquivo de log do Websense

O software Websense grava mensagens de erro no arquivo **websense.log**, localizado no diretório **bin** do Websense (C:\Arquivos de Programas\Websense\bin ou /opt/Websense/bin, por padrão).

As informações nesse arquivo podem ser comparadas às encontradas no Windows Event Viewer. Em ambientes Windows, o Event Viewer apresenta mensagens em um formato mais amigável ao usuário. O arquivo **websense.log** está disponível em sistemas Linux e pode ser enviado ao Suporte técnico da Websense se você precisar de ajuda com a solução de problemas.



# Índice remissivo

## A

- acessando o Websense Manager, 15, 243
- acesso com senha, 45
  - em ambiente com vários Policy Servers, 276
- ações, 42
  - Bloquear, 42
  - Bloquear palavras-chave, 43
  - Bloquear tipos de arquivo, 44
  - Confirmar, 43
  - Cota, 43
  - Permitir, 42
  - selecionando para relatórios de apresentação, 103
- Active Directory
  - Native Mode, 61
- ActiveX, conteúdo
  - removendo, 148
- adicionando
  - a protocolos definidos pelo Websense, 189
  - clientes, 66
  - diretivas, 74
  - entradas nas listas Sempre verificar e Nunca verificar, 150
  - filtros de acesso limitado, 168
  - filtros de categoria, 47
  - filtros de protocolo, 50
  - tipos de arquivo, 193
- Adicionar
  - diretivas, 74
  - filtro de acesso limitado, 168
  - filtro de categoria, 47
  - filtro de protocolo, 50
  - grupos LDAP personalizados, 65
  - palavras-chave, 179
- administração delegada
  - acessando o Websense Manager, 248
  - acesso a relatórios, 301
  - adicionando administradores, 258
  - adicionando funções, 253, 254
    - aplicando diretivas, 243
    - configurando, 241
    - conflitos entre funções, 261
    - editando funções, 254
    - excluindo clientes de funções, 262
    - excluindo funções, 253
    - exclusão de funções, efeitos de, 262
    - notificando administradores, 243
    - permissões de diretiva, 237
    - permissões de relatório, 238
    - primeiros passos, 241
    - Proteção de filtro, 264
    - usando, 252
    - visão geral, 235
- administradores, 236
  - acessando o Websense Manager, 249
  - acesso simultâneo à mesma função, 263
  - adicionando à função, 255, 258
  - Contas de usuário do Websense, 250
  - delegados, 239
  - em várias funções, 240, 258, 263
  - excluindo da função, 255
  - exibindo definição de função, 245
  - monitorando alterações feitas, 281
  - notificação de responsabilidades, 243
  - permissões, 237
    - permissões de diretiva condicionais, 238
    - permissões de diretiva incondicionais, 238
    - permissões de relatório, 238, 256
    - permissões, definindo, 255, 259
    - Proteção de filtro, efeitos de, 264
  - relatórios, 237, 245, 264
  - Super administrador, 237
  - tarefas do Super administrador, 241
  - tarefas para delegados, 244
  - visão geral, 236
- administradores delegados, 239
- Agendador, relatórios de apresentação, 108

- alertas, 291
  - Atualizações de segurança em tempo real, 291
  - atualizações do banco de dados em tempo real, 291
  - configurando limites, 285
  - configurando métodos, 285
  - e-mail, 286
  - evitando excesso, 285
  - métodos de envio, 284
  - pop-up, 286
  - Resumo de saúde, 20
  - saúde do Websense, 291
  - sistema, 284
  - sistema, configurando, 287
  - SNMP, 286
  - uso de categoria, 284
  - uso de categoria, adicionando, 288
  - uso de categoria, configurando, 288
  - uso de protocolo, 284
  - uso de protocolo, adicionando, 290
  - uso de protocolo, configurando, 289
- alertas de e-mail, 286
- alertas de saúde, 291
  - descrição, 377
  - Resumo, 20
  - soluções, 378
- alertas de uso, 284
  - categoria, adicionando, 288
  - categoria, configurando, 288
  - categorias de registro em log, 304
  - protocolo, adicionando, 290
  - protocolo, configurando, 289
- alertas de uso de categoria
  - adicionando, 288
  - configurando, 288
  - e registro em log, 304
  - excluindo, 288
- alertas de uso de protocolo
  - adicionando, 290
  - configurando, 289
- alertas do sistema, 284
  - configurando, 287
- alertas pop-up, 286
- alertas SNMP, 286
- alteração de endereço IP
  - Policy Server, 277
- alterações
  - cache, 18
  - revendo, 19
  - salvando, 18
- alterações em cache, 18
- alterando a categoria de URL, 182
- alterando funções, 238
- alternando funções, 238
- ameaças
  - em arquivos, 147
  - em páginas da Web, 146
  - verificação de, 146
- amostras
  - diretivas, 71
  - filtros de categoria e protocolo, 52
- Aplicar a clientes, 75
- Aplicar diretiva a clientes, 77
- aplicativos, verificação, 147
- applets
  - tempo de cota, 44
- aprofundar, relatórios investigativos, 117
- arquivo de cache
  - registro em log, 311
- arquivo de cache de log, 311
- arquivo de log
  - Remote Filtering, 162
- arquivo de registro, 393
- arquivos, verificação, 147
- assinaturas, 26
  - excedidas, 26
  - expiração, 26
  - portal MyWebsense, 26
- atualização
  - usuários ausentes, 350
- atualização do banco de dados de verificação em tempo real, 144
- Atualizações de segurança em tempo real, 30, 291
- atualizações do banco de dados, 30
  - Real-Time Security, 30, 291
  - tempo real, 30, 291
  - verificação em tempo real, 144
- atualizações do banco de dados em tempo real, 30, 291

atualizar  
  configurações do banco de dados de log, 320  
autenticação  
  Log Server, 316  
  seletiva, 204  
autenticação manual, 201  
  habilitando, 203  
autenticação seletiva, 204  
avaliando diretivas de filtragem, 93

## B

banco de dados  
  Atualizações de segurança em tempo real, 30  
  atualizações do banco de dados em tempo real, 30  
  banco de dados de log, 317  
  catálogo, 317  
  Master Database, 29  
  para verificação em tempo real, 144  
  partições do banco de dados de log, 318  
  Policy Database, 275  
  trabalho de manutenção, 325  
  trabalhos do banco de dados de log, 318  
banco de dados de log, 273, 299, 300, 302  
  administrando, 302, 319  
  apresentando, 317  
  ativo, 320  
  banco de dados de catálogo, 317  
  conexão confiável, 310  
  conexão para relatórios investigativos, 330  
  conexões com o Log Server, 309  
  configuração de manutenção, 325  
  configurações, 320  
  consolidação, 312  
  criando partições, 327  
  excluindo erros, 327  
  não criado, 383  
  não disponível, 384  
  partições de banco de dados, 318  
  reindexação, 326  
  requisitos de espaço em disco, 300  
  selecionando partições para relatórios, 328  
  sem espaço em disco, 385  
  tamanho, 385

  trabalho de IBT, 95, 318  
  trabalho de manutenção, 318, 325  
  trabalhos, 318  
  visualizando o log de erros, 329  
banco de dados inicial, 29  
banda registrada, solicitações bloqueadas, 126  
batches com falha, 326  
BCP, 308, 309  
BCP (Bulk Copy Program), 308  
bloqueado e protegido, 265  
  categorias, 265  
  palavras-chave, 265  
  protocolos, 266  
  tipos de arquivo, 266  
bloqueando  
  com base em palavras-chave, 179  
  protocolos, 183  
  tipos de arquivo, 191  
Bloquear, 42  
  Palavras-chave, 43  
  Tipos de arquivo, 44  
bloqueio a pop-ups  
  acesso a relatórios, 390  
bloqueio de palavras-chave  
  solução de problemas, 359  
bloqueio de placa de rede, 343  
botão Continuar, 43  
botão Editar categorias, 172  
botão Editar protocolos, 172  
BrandWatcher, 27

## C

caixa de diálogo Serviços, 392  
Caixa de ferramentas, 195  
caracteres ASCII estendidos  
  no nome de máquina do DC Agent, 212  
  no nome de máquina do eDirectory Agent, 224  
  no nome de máquina do Logon Agent, 215  
  no nome de máquina do RADIUS Agent, 219  
  pesquisando em relatórios investigativos, 391  
catálogo  
  banco de dados, 317  
  relatório, 96  
catálogo de relatórios, 96

- nome, 104
- catálogo global, 61
- categoria de Segurança, 38
- categoria Largura de banda, 38
- categoria Produtividade, 38
- categorias
  - adicionadas ao Master Database, 37
  - adicionando personalizada, 176
  - definição, 29, 36
  - editando personalizadas, 173
  - Eventos especiais, 38
  - Largura de banda, 38
  - lista completa de, 36
  - personalizar, 173
  - Produtividade, 38
  - Proteção estendida, 38
  - protegendo para todas as funções, 265
  - registro em log, 304
  - renomeando personalizada, 176
  - Segurança, 38
  - selecionando para relatórios de apresentação, 102
  - uso da largura de banda, 189
- categorias personalizadas, 173
  - adicionando, 176
  - criando, 172
  - editando, 173
  - renomeando, 176
- chave, 26
- chave de assinatura, 26
  - inserindo, 28
  - inválida ou expirada, 349
  - verificando, 352
- classes de risco, 39, 301, 302
  - atribuindo categorias, 302
  - em relatórios, 302
  - Perda de largura de banda de rede, 40
  - Perda de produtividade, 40, 41
  - Responsabilidade legal, 40
  - Risco de segurança, 40
  - selecionando para relatórios de apresentação, 102
  - selecionando para relatórios investigativos, 125
  - Uso empresarial, 40
- classificando conteúdo, 146
- cliente do Remote Filtering, 156
- clientes, 57
  - adicionando, 66
  - administrando, 58
  - aplicando diretivas, 57
  - atribuindo diretivas, 75, 77
  - computadores, 57, 59
  - editando, 68
  - grupos, 60
  - mover para função, 68
  - redes, 57, 59
  - selecionando para relatórios de apresentação, 101
  - usuários, 57, 60
- clientes gerenciados, 236
  - adicionando em funções, 243
  - designando à função, 256, 259
  - excluindo de funções, 256, 262
  - movendo para funções, 242
- clientes, gerenciados, 236
  - adicionando em funções, 243
  - aplicando diretivas, 248
  - designando a funções, 246, 256, 259
  - em várias funções, 246, 259
  - excluindo de funções, 256, 262
  - movendo para função, 241
  - sobrepondo funções, 261
- colunas
  - para relatórios investigativos de detalhes, 124
- componentes, 270
  - banco de dados de log, 273
  - cliente do Remote Filtering, 156
  - DC Agent, 274
  - eDirectory Agent, 274
  - Filtering Service, 271
  - Log Server, 273
  - Logon Agent, 274
  - Master Database, 271
  - Network Agent, 271
  - Policy Broker, 271
  - Policy Database, 271
  - Policy Server, 271
  - RADIUS Agent, 274

- Remote Filtering Client, 272
- Remote Filtering Server, 155, 272
- Usage Monitor, 272
- User Service, 274
- Websense Content Gateway, 272
- Websense Manager, 272
- Websense Security Gateway, 272
- componentes do filtro, 172
- computadores
  - clientes, 57
- conexão confiável, 310
- configuração da placa de rede, 339
  - bloqueando, 343
  - configurações, 343
  - monitoramento, 343
- configuração da rede, 338
- configuração de diretivas
  - restaurar padrões, 53
- configurações
  - Alertas e notificações, 285
  - banco de dados de log, 320
  - Conta, 28
  - Diretório de logon, 249
  - Download do banco de dados, 31
  - Filtragem, 54
  - Identificação do usuário, 202
  - Network Agent, 340
  - Policy Server, 276
  - Remote Filtering, 162
  - Serviços de diretório, 61
  - Verificação em tempo real, 145
- configurações de diretório
  - avançadas, 63
- configurações de filtragem
  - configurando, 54
- configurações de firewall
  - download do banco de dados, 353
- configurações de proxy
  - download do banco de dados, 353
  - verificando, 354
- configurando as opções em tempo real, 145
- Confirmar, 43
  - em ambiente com vários Policy Servers, 276
- conjunto de caracteres
  - MBCS, 350
- conjuntos de caracteres
  - usados com o LDAP, 64
- consolidação
  - e registro de URLs completos, 323
  - e tempo de navegação na Internet, 388
  - logs, 300, 313
- conta de rede
  - definindo o diretório de logon, 249
- contas de usuário
  - adicionando ao Websense, 251
  - senha, 239
  - Websense, 239, 250
  - WebsenseAdministrator, 237
  - WebsenseAdministrator., 235, 236
- Contas de usuário do Websense, 239, 250
  - adicionando, 251
  - gerenciando, 253
  - senha, 239
- contas de usuário do Websense
  - WebsenseAdministrator, 16
- Content Gateway, 272
- conteúdo
  - classificação, 146
  - verificação, 143, 146
- conteúdo ativo
  - removendo, 148
- conteúdo dinâmico
  - classificando, 146
- controlador de domínio
  - teste de visibilidade, 368
- controle de inundação, alertas, 285
- copiando
  - filtros de acesso limitado, 46
  - filtros de categoria, 46
  - filtros de protocolo, 46
  - relatórios de apresentação, 99
- Copiar para função, 171
  - diretivas, 73
  - filtros, 47
- Cota, 43
- credenciais de rede
  - acessando o Websense Manager, 249
- criando
  - diretivas, 74
  - filtros de acesso limitado, 76

filtros de categoria, 76  
filtros de protocolo, 76

## D

DC Agent, 211, 274  
  configurando, 212  
  solução de problemas, 365  
definição de diretiva  
  programar, 75  
desativando  
  serviços Websense, 283  
desbloqueando URLs, 181  
diagnóstico  
  eDirectory Agent, 370  
diretiva Exemplo - Usuário padrão, 71  
diretiva Irrestrito, 71  
diretiva Padrão, 72  
  aplicada incorretamente, 366  
diretivas  
  adicionando, 73, 74  
  aplicando, 78  
  aplicando a clientes, 75, 77  
  aplicando a clientes gerenciados, 243, 248  
  aplicando a usuários e grupos, 60  
  aplicáveis, determinando, 78  
  copiando para funções, 73, 242  
  copiar para função, 171  
  criando para função, 247  
  de grupo, várias, 78  
  definição, 35, 71  
  descrições, 74  
  editando, 73, 75  
  editando para função, 247  
  Exemplo - Usuário padrão, 71  
  exibindo, 73  
  imprimindo em arquivo, 73  
  Irrestrito, 71  
  Padrão, 72  
  precedência de filtragem, 79  
  renomeando, 75  
Diretório de logon  
  definindo, 249  
download do banco de dados, 29  
  Atualizações de segurança em tempo real, 30

  atualizações em tempo real, 30  
  configurando, 31  
  continuando, 281  
  problemas da assinatura, 352  
  problemas de aplicativos com restrições, 356  
  requisitos de espaço em disco, 354  
  requisitos de memória, 355  
  solução de problemas, 352  
  status, 280  
  verificação em tempo real, 144  
  verificar acesso à Internet, 353  
  via proxy, 32

## E

economia de largura de banda  
  Página Histórico, 25  
  página Histórico, 23  
economia de tempo  
  Página Histórico, 25  
  página Histórico, 23  
eDirectory, 63  
eDirectory Agent, 222, 274  
  configurando, 224  
  diagnóstico, 370  
  modo de console, 371  
  solução de problemas, 369  
editando  
  configurações de cliente, 68  
  diretivas, 75  
  filtros de acesso limitado, 169  
  filtros de categoria, 48  
  filtros de protocolo, 50  
Editar  
  filtro de categoria, 48  
  grupo LDAP personalizado, 65  
e-mail  
  distribuição de relatórios, 304  
entrando em contato com o suporte técnico, 26  
erro de logon, 380  
espaço em disco  
  requisitos de download de banco de dados, 354  
  requisitos do banco de dados de log, 300  
  uso de relatórios de apresentação, 97  
esqueci senha do WebsenseAdministrator, 26  
estimativas

- economia de largura de banda, 25
- economia de tempo, 25
- Event Viewer, 393
- Eventos especiais, 38
- excluindo clientes gerenciados, 380
- excluindo entradas das listas Sempre verificar e Nunca verificar, 151
- executando o Websense Manager, 15
- exemplos
  - diretivas, 71
- exibição de detalhes
  - colunas, 124
  - configurando padrões, 331
  - modificando, 123
  - relatórios investigativos, 122
- Exibir alterações pendentes, 19
- Explorer for Linux, 93, 301
- expressões regulares, 172, 194
  - e URLs não filtrados, 181
  - em um filtro de acesso limitado, 169
  - recategorizando URLs, 174
- extensões de arquivos
  - adicionando a tipo de arquivo predefinido, 193
  - adicionando ao tipo de arquivo, 194
  - em tipos de arquivo predefinidos, 192
  - filtrando por, 191
  - para verificação em tempo real, 148
- F**
- falha ao abrir
  - Remote Filtering, 160
- Favoritos
  - relatórios de apresentação, 94, 96, 98, 104, 106
  - relatórios investigativos, 115, 133, 134, 135
- fazendo backup de dados do Websense, 292
- fazendo logon no, 16
- fechamento por falha
  - Remote Filtering, 160, 162
  - timeout, 160, 162
- ferramenta Acesso ao URL, 197
- ferramenta Categoria de URL, 196
- ferramenta Investigar usuário, 197
- ferramenta Testar filtragem, 196
- ferramenta Verificar diretiva, 196
- ferramentas
  - Acesso ao URL, 197
  - Categoria de URL, 196
  - Investigar usuário, 197
  - opção Localizar usuário, 197
  - Testar filtragem, 196
  - Verificar diretiva, 196
- ferramentas de solução de problemas
  - caixa de diálogo Serviços, 392
  - Event Viewer, 393
  - websense.log, 393
- fila de trabalhos
  - relatórios de apresentação, 99
  - relatórios investigativos, 116, 138
- Filtering Service, 271
  - alteração de endereço IP, 362
  - atualizando o UID, 363
  - descrição, 279
  - downloads do banco de dados, 280
  - gráfico de Resumo, 21
  - página Detalhes, 280
- filtragem
  - ações, 42
  - diagrama, 79
  - ordem de, 78
  - precedência, 79
- filtragem por reputação, 39
- filtrando
  - caixa de ferramentas, 195
  - com palavras-chave, 178
  - precedência, URLs personalizados, 180
  - protocolos, 183
  - tipos de arquivo, 191
- filtro
  - relatórios de apresentação, 98
- filtro Bloquear tudo, 52
  - e precedência de filtragem, 79
- filtro de relatório, relatórios de apresentação, 96, 98, 100
  - confirmando, 106
  - selecionando ações, 103
  - selecionando categorias, 102
  - selecionando classes de risco, 102
  - selecionando clientes, 101

- selecionando protocolos, 103
  - filtro Permitir tudo
    - e funções de administração, 242
    - e precedência de filtragem, 79
  - filtros, 46
    - acesso limitado, 46, 166
    - ativos, editando, 76
    - categoria, 35, 46
    - copiando para funções, 242
    - copiar para função, 171
    - criando para função, 247
    - determinando o uso, 76
    - editando para função, 247
    - Permitir tudo, 242
    - protocolo, 35, 46
    - relatórios de apresentação, 96
    - restaurar padrões, 53
  - filtros de acesso limitado, 46, 166
    - adicionando, 76
    - criando, 168
    - expressões regulares, 169
    - precedência de filtragem, 166
    - renomeando, 169
  - filtros de categoria, 46
    - adicionando, 76
    - criando, 47
    - definição, 35
    - duplicando, 46
    - editando, 48
    - modelos, 47, 53
    - renomeando, 48
  - filtros de protocolo, 46
    - adicionando, 76
    - criando, 50
    - definição, 35
    - editando, 50
    - modelos, 50, 53
    - renomeando, 51
  - filtros Permitir tudo, 52
  - formato Excel
    - log de auditoria, 281
    - relatórios de apresentação, 97, 108, 112
    - relatórios incompletos, 390
    - relatórios investigativos, 116, 137
  - formato HTML
    - relatórios de apresentação, 97
    - salvando relatórios de apresentação, 391
  - formato HTML, relatórios de apresentação, 108
  - formato PDF
    - relatórios de apresentação, 97, 108, 112
    - relatórios investigativos, 116, 137, 140
  - formato XLS
    - log de auditoria, 281
    - relatórios de apresentação, 97, 108
    - relatórios investigativos, 116, 140
  - funções
    - adicionando, 253, 254
    - adicionando administradores, 255, 258
    - adicionando clientes gerenciados, 243, 246, 256, 259
    - administradores em várias, 258
    - administrativas, 236
    - alternando, 238
    - aplicando diretivas, 243, 248
    - clientes em várias, 261
    - criando diretivas, 247
    - criando filtros, 247
    - editando, 254
    - editando diretivas, 247
    - editando filtros, 247
    - excluindo, 253
    - excluindo administradores, 255
    - excluindo clientes, 256
    - excluindo um Super administrador, 236, 262
    - exclusão, efeitos de, 262
    - exibindo definição, 245
    - filtros Permitir tudo em, 242
    - nomes, 253
    - prioridade, 253, 261
    - Proteção de filtro, efeitos de, 264
    - protegendo categorias, 265
    - protegendo protocolos, 266
    - sobrepondo clientes, 246
    - Super administrador, 235, 236, 237
  - funções administrativas, 236
- ## G
- gerenciamento de categorias, 172

gráfico de barras, 119  
gráfico de Carga de filtragem atual, 20  
gráfico de pizza, 119  
gráfico do Valor de hoje, 20  
gráficos  
  Carga de filtragem atual, 20  
  escolhendo para a página Hoje, 22  
  página Histórico, 23  
  página Hoje, 20  
  Resumo do Filtering Service, 21  
  valor de Hoje, 20  
grupos, 60  
Grupos de protocolos de segurança, 41  
grupos LDAP personalizados, 64  
  adicionando, 65  
  editando, 65  
  gerenciando, 253  
guia Configurações, 18  
guia Principal, 18

## H

HTTP Post, 315

## I

identificação de usuário  
  solução de problemas, 364  
identificação do usuário  
  manual, 201  
  transparente, 199  
  usuários remotos, 200  
identificação transparente do usuário, 199  
  agentes, 199  
  configurando, 202  
  DC Agent, 211  
  eDirectory Agent, 222  
  Logon Agent, 214  
  RADIUS Agent, 217  
identificadores  
  protocolo, 185  
identificadores de protocolo, 185  
  endereços IP, 185  
  portas, 185  
imprimindo  
  página Histórico, 24

  página Hoje, 21, 291  
  relatórios de apresentação, 108  
  relatórios investigativos, 140  
Imprimir diretivas em arquivo, 73  
informações da conta  
  configurando, 28  
informações de configuração do Websense, 275  
informações do usuário, registro em log, 304  
iniciando  
  Log Server, 307, 308, 317  
  serviços Websense, 283  
iniciando o Websense Manager, 15  
interrompendo  
  Log Server, 307, 308, 317  
intervalo de datas  
  trabalho de relatórios de apresentação  
    agendado, 111  
  trabalho programado de relatórios  
    investigativos, 137

## J

JavaScript, conteúdo  
  removendo, 148

## L

largura de banda  
  configuração de limites, 190  
  gerenciando, 189  
  maior que o esperado, 388  
  registro para solicitações bloqueadas, 118  
  usada pelas categorias, 189  
  usada pelos protocolos, 189  
LDAP  
  conjuntos de caracteres, 64  
  grupos personalizados, 64  
letras vermelhas, relatórios investigativos, 118  
liberar permissões da diretiva, 244  
limite de tempo de leitura, 324  
Linux, relatórios, 93, 301  
lista de trabalhos agendados  
  relatórios de apresentação, 99  
  relatórios investigativos, 138  
lista Nunca verificar, 145  
  adicionando sites, 150  
  excluindo entradas, 150

- lista Sempre verificar
  - adicionando sites, 150
  - excluindo entradas, 150
- localizando informações sobre produtos, 26
- log
  - auditoria, 281
    - método de inserção, 308
- log de auditoria, 281
- log de erros
  - Event Viewer, 393
  - excluindo do banco de dados de log, 327
  - visualizando para o banco de dados de log, 329
  - Websense.log, 393
- Log Server, 273, 299
  - atualizando informações do usuário/grupo, 307
  - autenticação, 316
  - conectando ao serviço de diretório, 387
  - conexão com o banco de dados de log, 310
  - configuração, 389
  - iniciando, 307, 308, 317
  - interrompendo, 307, 308, 317
  - não instalado, 383
  - usando o servidor proxy, 316
  - utilitário de Configuração, 301, 302, 306
- Logon Agent, 214, 274
  - configurando, 215
  - solução de problemas, 366
- logotipo
  - alterando na página de bloqueio, 87
  - relatórios de apresentação, 100
- logotipo personalizado
  - páginas de bloqueio, 87
  - relatórios de apresentação, 100, 105
- logotipo, relatórios de apresentação, 105
  
- M**
- mapa da categoria
  - Relatório Detalhe de atividade do usuário, 129
- Master Database, 29, 271
  - agendamento do download, 31
  - aprimorando, 314
  - Atualizações de segurança em tempo real, 30
  - atualizações em tempo real, 30
  - categorias, 36
  - continuando o download, 281
  - fazendo download, 29
  - problemas de download, 352
  - protocolos, 37
  - status de download, 280
- mecanismos de banco de dados
  - suportados, 299
- mensagem de e-mail
  - personalizando para relatórios de apresentação, 113
  - personalizando para relatórios investigativos, 137
- mensagens de bloqueio
  - alterando o tamanho do quadro, 87
  - criando alternativas, 90
  - criando personalizadas, 86
  - para tipos de arquivo, 192
  - personalizando, 85
  - protocolo, 84
- mensagens de bloqueio alternativas, 90
- mensagens de bloqueio personalizadas, 86
- método de inserção de log, 309
- Microsoft Excel
  - relatórios incompletos, 390
- Microsoft SQL Server, 299
- Microsoft SQL Server Desktop Engine, 299
- Mixed Mode
  - Active Directory, 61
- modelos, 53
  - filtro de categoria, 47, 53
  - filtro de protocolo, 50, 53
- modelos de filtro, 53
- modo de console
  - eDirectory Agent, 371
- monitoramento de placa de rede, 343
- monitorando
  - alterações do sistema, 281
  - atividade da Internet, 284
- movendo sites para outra categoria, 182
- mover para função, 68
  - clientes, 242
- MSDE, 299
  
- N**
- Native Mode

Active Directory, 61  
navegando no Websense Manager, 17  
NetBIOS  
  ativando, 368  
Network Agent, 271, 337  
  bloqueio de placa de rede, 343  
  comunicação com o Filtering Service, 362  
  configuração da placa de rede, 343  
  configuração de hardware, 338  
  configurações globais, 340  
  configurações locais, 341  
  e Remote Filtering, 156  
  mais de 2 placas de rede, 363  
  monitoramento de placa de rede, 343  
nome do arquivo  
  relatório de apresentação agendado, 97  
Novell eDirectory, 63

## O

obtendo suporte, 32  
ocorrências  
  definição, 311  
  registro em log, 300  
ocultando nomes de usuário  
  relatórios investigativos, 120  
ODBC, 308  
opções de exibição  
  relatórios investigativos, 332  
opções de saída  
  relatórios investigativos, 332  
opções de substituição, partições do banco de dados, 321  
opções em tempo real, 146, 151  
  classificando conteúdo, 146  
  relatórios, 151  
  removendo conteúdo, 148  
  salvando alterações, 150  
  verificação de arquivos, 147  
opções, relatórios investigativos, 116  
Open Database Connectivity (ODBC), 308  
ordem  
  filtragem, 79

## P

página de bloqueio de segurança, 303

Página Histórico  
  personalizando, 25  
página Histórico, 22  
  gráficos, 23  
  personalizando, 24  
página Hoje, 19  
  gráficos, 20  
  personalizando, 21, 22  
  Resumo de alertas de saúde, 20  
página Identificação do usuário, 202  
páginas de bloqueio, 83  
  acesso com senha, 45  
  alterando o logotipo, 87  
  arquivos-fonte, 85  
  botão Continuar, 43  
  botão Utilizar cota de tempo, 43  
  revertendo ao padrão, 89  
  variáveis de conteúdo, 88  
palavras-chave, 172, 178  
  bloqueando, 43  
  definindo, 179  
  não são bloqueadas, 359  
  protegendo para funções, 265  
partições  
  banco de dados de log, 318  
  criando, 327  
  excluindo, 300, 329  
  opções de substituição, 321  
  selecionando para relatórios, 328  
partições de banco de dados  
  criando, 327  
  excluindo, 326, 329  
  opções de substituição, 321  
  selecionando para relatórios, 328  
patches, 26  
perfil de usuário  
  problemas de script de logon, 369  
permissões, 236  
  definindo, 255, 256, 259  
  diretiva, 237, 239  
  diretiva condicional, 238  
  diretiva incondicional, 238  
  liberando diretiva, 244  
  relatórios, 238, 239, 248

- SQL Server, 384
    - unidade de instalação, 384
    - várias funções, 240
  - permissões de diretiva, 237, 239
    - condicionais, 238
    - incondicionais, 238
  - permissões de diretiva condicionais, 238
  - permissões de diretivas
    - liberando, 244
  - permitindo URLs para todos os usuários, 181
  - Permitir, 42
  - personalizar
    - mensagens de bloqueio, 85
    - Página Histórico, 25
    - página Histórico, 24
    - página Hoje, 21, 22
  - pesquisa de usuário, 67
  - pesquisando
    - clientes de diretório, 67
    - na barra de endereços, 359
    - relatórios investigativos, 120, 391
  - pesquisar padrão
    - relatórios investigativos, 392
  - Policy Broker, 271
    - e o Policy Database, 275
  - Policy Database, 271, 275
  - Policy Server, 271, 275
    - adicionando ao Websense Manager, 276
    - alterando o endereço IP, 277
    - e o Policy Database, 275
    - e Websense Manager, 275
    - removendo do Websense Manager, 276
    - várias instâncias, 276
    - várias instâncias, configurando o registro em log, 304
  - portal MyWebsense, 26
  - precedência
    - diretiva de filtragem, 57
    - filtragem, 79
    - função de administração delegada, 261
  - preferências, relatórios, 304
  - prioridade, função, 253, 261
  - programar
    - definição de diretiva, 75
  - Proteção de filtro
    - configurando, 241
    - criando, 238, 265
    - efeito nas funções, 239, 248, 264
    - protegendo categorias, 265
    - protegendo palavras-chave, 265
    - protegendo protocolos, 266
    - protegendo tipos de arquivo, 266
    - registro em log de protocolos, 266
  - Proteção estendida, 38
  - protocolo
    - definições, 182
    - gerenciamento, 172
    - mensagens de bloqueio, 84
  - protocolos
    - adicionados ao Master Database, 37
    - coletando informações de uso, 29
    - criando novo, 184
    - definição, 29, 37
    - definições, 182
    - definindo personalizada, 172
    - filtragem, 50
    - filtrando, 183
    - Grupos de protocolos de segurança, 41
    - lista completa de, 37
    - modificando definições do Websense, 189
    - não registrados em log, 388
    - protegendo para todas as funções, 265, 266
    - registro em log para todas as funções, 266
    - renomeando personalizados, 186
    - selecionando para relatórios de apresentação, 103
    - selecionando para relatórios investigativos, 125
    - Suporte a TCP e UDP, 51
    - uso da largura de banda, 189
  - protocolos personalizados, 182
    - criando, 187
    - editando, 185
    - identificadores, 185
    - não é possível criar, 381
    - renomeando, 186
  - pulsção, Remote Filtering, 157, 158
- R**
- RADIUS Agent, 217, 274

- configurando, 219
- redefinir senha do WebsenseAdministrator, 26
- redes
  - clientes, 57
- registrando
  - opções em tempo real, 151
  - opções em tempo real em comparação com filtragem, 152
- registro
  - Remote Filtering, 159
- registro de log aprimorado, 309
- registro de URLs completos, 300, 314, 323
- registro em log
  - anônimo, 305
  - aprimorado, 309
  - categorias, 304
  - configurando, 304
    - vários Policy Servers, 304
  - consolidando registros, 313
  - definição, 302
  - estratégia, 300
  - informações do usuário, 304
  - ocorrências, 311
  - seletivo de categorias, 300, 305
  - URLs completos, 314, 323
  - visitas, 311
- registro em log anônimo, 305
- registro em log de protocolos
  - para todas as funções, 266
- registro seletivo de categorias em log, 300, 305
- registros em log, 151
- reindexando o banco de dados de log, 326
- Relatório Detalhes da atividade do usuário por dia, 127
  - mapa da categoria, 129
- Relatório Detalhes da atividade do usuário por mês, 128
- relatório próprio, 260
  - ativando, 304
  - configurando, 334
  - notificando usuários, 335
- relatórios
  - acessar, 300
  - administrador, 245, 264
  - apresentação, 93
  - bloqueio a pop-ups, 390
  - componentes, 299
  - configurando investigativos, 330
  - configurando o servidor de e-mail, 304
  - configurando relatório próprio, 334
  - definindo permissões, 256
  - Detalhes da atividade do usuário por dia, 127
  - Detalhes da atividade do usuário por mês, 128
  - distribuição por e-mail, 304
  - estratégia, 300
  - incompletos, 390
  - investigativos, 93, 94
  - Linux, 93, 301
  - mantendo, 97
  - opções em tempo real, 151
  - permissões, 238, 239, 248, 256
  - preferências, 304
  - relatório próprio, 260
  - restrições de administrador, 240
  - tempo limite, 385
  - usando, 93
  - vazios, 388
- relatórios de apresentação, 93, 299
  - agendando, 99, 108, 109
  - catálogo de relatórios, 96
  - confirmando filtro de relatório, 106
  - copiando, 99
  - definindo o intervalo de datas para trabalho, 111
  - executando, 107
  - Favoritos, 94, 96, 98, 104, 106
  - fila de trabalhos, 99, 113
  - filtro de relatório, 96, 98, 100
  - formato de saída, 112
  - formato Excel, 97, 108, 112
  - formato HTML, 97, 108
  - formato PDF, 97, 108, 112
  - formato XLS, 97, 108
  - histórico de trabalhos, 114
  - imprimindo, 108
  - logotipo personalizado, 100, 105
  - mantendo, 97
  - nome do arquivo, 97
  - nome do Catálogo de relatórios, 104

- salvando, 108
  - uso de espaço em disco, 97
  - visão geral, 94
  - relatórios de resumo
    - em vários níveis, 121
    - relatórios investigativos, 117
  - relatórios de Usuário por dia/mês, 115, 127
  - relatórios de valores atípicos, 116, 138
  - relatórios investigativos, 93, 94, 299
    - acessando, 23
    - anônimo, 120
    - Atividade do usuário, 115
    - configurações padrão, 331
    - configurando, 330
    - definindo agendamento para, 136
    - Detalhes da atividade do usuário por dia, 127
    - Detalhes da atividade do usuário por mês, 128
    - escolhendo um banco de dados de log, 330
    - exibição de detalhes, 122, 123, 124
    - Favoritos, 115, 133, 134
    - fila de trabalhos, 116, 138
    - formato Excel, 116, 137, 140
    - formato PDF, 116, 137, 140
    - formato XLS, 140
    - gráfico de barras, 119
    - gráfico de pizza, 119
    - imprimindo, 140
    - letras vermelhas, 118
    - ocultando nomes de usuário, 120
    - opções, 116
    - opções de exibição, 332
    - opções de saída, 332
    - padrão, 115, 131
    - personalizando e-mail, 137
    - pesquisando, 120, 391
    - pesquisar padrões, 392
    - relatório próprio, 334
    - relatórios próprios, 141
    - resumo, 117
    - resumo em vários níveis, 121
    - salvando Favoritos, 133
    - trabalhos agendados, 116, 135
    - valores atípicos, 116, 138
    - visão geral, 115
  - relatórios padrão, investigativos, 115, 131
  - relatórios próprios, 141
  - remoção de conteúdo, 148
  - Remote Filtering, 155
    - arquivo de log, 159, 162
    - cliente, 272
    - comunicação, 160
    - configurações, 162
    - dentro da rede, 157
    - e Network Agent, 156
    - falha ao abrir, 160
    - fechamento por falha, 160, 162
    - filtragem de banda, 155
    - fora da rede, 158
    - protocolos suportados, 155, 156
    - pulsção, 157, 158
    - servidor, 272
    - Suporte a VPN, 161
    - tempo limite de fechamento por falha, 160, 162
    - Zona Desmilitarizada (DMZ), 157, 158
  - Remote Filtering Server, 155
  - removendo
    - conteúdo ativo, 148
    - entradas nas listas Sempre verificar e Nunca verificar, 150
    - instâncias do Policy Server do Websense Manager, 276
    - VB Script, conteúdo, 148
  - removendo conteúdo ativo, 148
  - renomear
    - categoria, 176
    - diretivas, 75
    - filtros de acesso limitado, 169
    - filtros de categoria, 48
    - filtros de protocolo, 51
    - protocolo personalizado, 186
  - réplicas do servidor eDirectory
    - configurando, 225
  - requisitos de memória
    - download do banco de dados, 355
  - restaurando dados do Websense, 292
- S**
- salvando relatórios de apresentação, 108

- Salvar tudo, 18
  - script de logon
    - ativando NetBIOS, 368
    - problemas de perfil de usuário, 369
    - problemas de visibilidade do controlador de domínio, 368
  - Security Gateway, 272
  - senha
    - alterando para usuário do Websense, 252, 253
    - usuário do Websense, 239, 250
    - WebsenseAdministrator, 237
  - senha do WebsenseAdministrator
    - redefinindo senha esquecida, 26
  - serviços
    - parando e iniciando, 283
  - serviços de diretório
    - configurando, 61
    - configurando para logon no Websense Manager, 249
    - Log Server conectando a, 387
    - pesquisando, 67
    - Windows NT Directory/Active Directory (Mixed Mode), 61
  - Servidor de interceptação
    - configuração de alerta SNMP, 286
  - servidor proxy
    - configuração do download do banco de dados, 32
    - Log Server usando, 316
  - sessão de navegação, 324
  - sessão, navegação, 324
  - SiteWatcher, 27
  - Software Websense
    - componentes, 270
  - solicitações bloqueadas
    - largura de banda registrada, 118
  - solicitações bloqueadas, banda registrada, 126
  - SQL Server
    - permissões, 384
  - SQL Server Agent
    - trabalho, 389
  - Status
    - Alertas, 291
    - Histórico, 22
    - Hoje, 19
    - Log de auditoria, 281
  - Status do Websense
    - Histórico, 22
    - Hoje, 19
  - status do Websense, 291
    - Alertas, 291
    - Log de auditoria, 281
  - substituir ação
    - categorias, 175
    - protocolos, 186
  - Sun Java System Directory, 63
  - Super administrador
    - adicionando clientes à função, 241
    - alternando funções, 238
    - condicionais, 238
    - copiando diretivas, 242
    - copiando filtros, 242
    - excluindo uma função, 236, 262
    - função, 235, 236, 237
    - incondicional, 238, 255
    - movendo clientes da função, 241, 242
    - permissões, 237
    - Proteção de filtro, efeitos de, 264
    - WebsenseAdministrator, 16
  - Super administrador condicional, 238
  - Super administrador incondicional, 238, 255
  - Suporte a TCP e UDP, 51
  - Suporte Técnico, 32
- ## T
- tamanho máximo para verificação de arquivos, 148
  - tempo de cota, 44
    - aplicando a clientes, 44
    - applets, 44
    - em ambiente com vários Policy Servers, 276
    - sessões, 44
  - tempo de leitura, 325
  - tempo de navegação
    - Internet (IBT), 95, 324
  - tempo de navegação na Internet (IBT)
    - configuração, 324
    - e consolidação, 388
    - explicação, 95
    - relatórios, 324

- tempo de leitura, 324, 325
  - trabalho de banco de dados, 95
  - tempo limite
    - desabilitar para Websense Manager, 21
    - relatórios, 385
  - tempo limite da sessão, 16
  - Testar filtragem
    - Localizar usuário, 197
  - ThreatWatcher, 27
  - tipos de arquivo, 172
    - adicionando, 193
    - bloqueando, 44
    - editando, 193
    - protegendo para funções, 266
  - título do relatório, relatórios de apresentação, 104
  - título, relatórios de apresentação, 104
  - trabalho de manutenção
    - banco de dados de log, 318, 325
    - configurando, 325
  - trabalho ETL, 318
  - Trabalho Extract, Transform, and Load (ETL), 318
  - trabalhos
    - banco de dados de log, 318
    - ETL, 318
    - IBT, 318
    - manutenção do banco de dados de log, 318
    - relatórios de apresentação agendados, 109, 113
    - relatórios investigativos agendados, 135, 138
    - SQL Server Agent, 389
  - trabalhos agendados
    - agendar, 109, 136
    - ativando, 114
    - desativando, 114
    - excluindo, 114
    - formato de saída, 112
    - histórico de trabalhos, 114
    - intervalo de datas, 111, 137
    - nome do arquivo de relatório, 97
    - personalizando e-mail, 113, 137
    - relatórios de apresentação, 109, 111, 113
    - relatórios investigativos, 116, 135
  - trabalhos de banco de dados
    - ETL, 318
    - manutenção, 318
    - SQL Server Agent, 389
    - tempo de navegação na Internet (IBT), 318
  - tutoriais
    - Guia rápido, 16
  - tutoriais do Guia rápido, 16
    - iniciando, 16
- U**
- URLs não filtrados, 172, 180
    - definindo, 181
    - não aplicados, 381
  - URLs personalizados
    - definição, 180
    - precedência de filtragem, 180
  - URLs recategorizados, 180
    - adicionando, 182
    - editando, 182
    - explicação, 172
    - não aplicados, 381
  - Usage Monitor, 272
  - Usar filtros personalizados, 64
  - User Service, 60, 274
  - usuário padrão, 236, 237
    - excluindo, 236
  - usuários, 57, 60
    - autenticação manual, 201
    - identificação transparente, 199
    - identificando, 199
    - identificando remotos, 159
  - usuários ausentes
    - após atualização, 350
  - usuários remotos, identificando, 159
  - utilitário de backup, 292
  - utilitário de Configuração
    - acessando, 306
    - Log Server, 306
  - utilitário de restauração, 292
  - utilitários
    - Configuração do Log Server, 306
  - Utilizar bloqueio mais restritivo, 167
    - com filtros de acesso limitado, 167
  - Utilizar cota de tempo, 44
    - botão de página de bloqueio, 43

**V**

várias diretivas  
  precedência de filtragem, 57  
várias diretivas de grupo, 78  
várias funções, permissões, 240  
vários Policy Servers, 276  
verificação de ameaças, 146  
verificação de aplicativos, 147  
verificação de arquivos  
  configurando o tamanho máximo, 148  
  extensões de arquivos, 148  
verificação de conteúdo, 143, 145  
verificação em tempo real, 143  
  atualizações do banco de dados, 144  
  configurações, 145  
  visão geral, 144  
Verificar diretiva  
  Localizar usuário, 197  
visitas  
  definição, 311  
  registro em log, 300, 311  
VPN  
  Remote Filtering, 161  
  túnel dividido, 161

**W**

WebCatcher, 314  
Websense Explorer for Linux, 93, 301  
Websense Manager, 15, 272

  acessando com conta de rede, 249  
  acessando com conta de usuário do  
    Websense, 250  
  acesso de administrador, 248  
  acesso simultâneo pelos administradores, 263  
  banner do Websense, 18  
  desabilitar tempo limite, 21  
  fazendo logon no, 16  
  iniciando, 15  
  navegação, 17  
  tempos limites da sessão, 16  
Websense Master Database, 29  
Websense Web Protection Services, 27  
websense.log, 393  
WebsenseAdministrator, 16, 237  
  excluindo, 236  
  senha, 237  
WebsenseAdministrator.  
  usuário, 235, 236  
Windows  
  caixa de diálogo Serviços, 392  
  Event Viewer, 393  
Windows Active Directory (Native Mode), 61  
Windows NT Directory/Active Directory (Mixed  
  Mode), 61

**Z**

Zona Desmilitarizada (DMZ), 157, 158

