

Cliente de filtragem de conteúdo SonicWall™ 3.1

Guia de agente

SONICWALL™

Copyright © 2017 SonicWall, Inc. Todos os direitos reservados.

SonicWall é uma marca comercial ou marca comercial registrada da SonicWall Inc. e/ou respectivos afiliados nos EUA e/ou em outros países. Todas as outras marcas comerciais e marcas comerciais registradas são propriedade dos respectivos proprietários.

As informações neste documento são fornecidas em conexão com os produtos da SonicWall Inc. e/ou respectivos afiliados. Nenhuma licença, explícita ou implícita, por preclusão ou de outra forma, para qualquer direito de propriedade intelectual é concedida por este documento ou em conexão com as vendas de produtos SonicWall. EXCETO CONFORME DISPOSTO NOS TERMOS E CONDIÇÕES, COMO ESPECIFICADO NO CONTRATO DE LICENÇA PARA ESTE PRODUTO, A SONICWALL E/OU RESPECTIVOS AFILIADOS NÃO ASSUMEM QUALQUER RESPONSABILIDADE E NEGAM QUALQUER GARANTIA, EXPRESSA, IMPLÍCITA OU LEGAL RELACIONADA A SEUS PRODUTOS INCLUINDO, MAS NÃO LIMITANDO, A GARANTIA IMPLÍCITA DE COMERCIALIZAÇÃO, ADAPTAÇÃO PARA UMA DETERMINADA FINALIDADE OU NÃO INFRAÇÃO. EM NENHUMA CIRCUNSTÂNCIA A SONICWALL E/OU RESPECTIVOS AFILIADOS DEVEM SER CONSIDERADOS RESPONSÁVEIS POR QUALQUER DANO DIRETO, INDIRETO, EVENTUAL, PUNITIVO, ESPECIAL OU INCIDENTAL (INCLUINDO, SEM LIMITAÇÕES, DANOS POR PERDAS DE LUCROS, INTERRUPÇÃO DO TRABALHO OU PERDA DE INFORMAÇÕES) DEVIDO AO USO OU INCAPACIDADE DE USO DESTES DOCUMENTOS, MESMO QUE A SONICWALL E/OU RESPECTIVOS AFILIADOS TENHAM SIDO ALERTADOS QUANTO À POSSIBILIDADE DE TAIS DANOS. A SonicWall e/ou respectivos afiliados não garantem as representações ou fazem garantias no que diz respeito à precisão e integridade dos conteúdos deste documento e reservam o direito a alterar as especificações e descrições dos produtos a qualquer momento sem aviso prévio. A SonicWall Inc. e/ou respectivos afiliados não estabelecem nenhum compromisso para a atualização das informações contidas neste documento.

Para obter mais informações, visite <https://www.sonicwall.com/br-pt/legal/>.

Legenda



AVISO: O ícone AVISO indica risco de danos ao equipamento, ferimentos ou morte.



CUIDADO: O ícone CUIDADO indica um possível dano ao hardware ou perda de dados se as instruções não forem seguidas.



IMPORTANTE, NOTA, DICA, DISPOSITIVOS MÓVEIS ou VÍDEO: Um ícone de informação indica informações de suporte.

Cliente de filtragem de conteúdo Guia de agente
Atualizado – Julho de 2017
Versão de software – 3.1
232-003867-00 Rev. A

Cliente de filtragem de conteúdo

A SonicWall™ oferece uma segurança de conteúdo da Web abrangente que bloqueia determinados conteúdos da Web e impõe políticas de produtividade e proteção. Os componentes principais são o Serviço de filtragem de conteúdo (CFS), o Cliente de filtragem de conteúdo (CFC) e a EPRS (Proteção de política e sistema de relatório). O CFS protege os dispositivos atrás do firewall, o CFC protege os dispositivos independentemente da sua localização, mesmo que esteja conectado fora do firewall e a EPRS fornece aos administradores os meios para gerenciar o CFC a partir de uma interface da Web central.

Este documento descreve como usar a interface do Cliente de filtragem de conteúdo SonicWall nos sistemas de usuário. Você pode visualizar o status básico, incluindo informações da política, tal como o nome da política ativa, a última atualização bem-sucedida da política e o último relatório enviado. Além disso, pode visualizar o status para substituição, se permitido pela política, e detalhes da licença, tal como o número de série, a expiração e a versão. Este guia descreve as diferentes exibições da interface do usuário e as ações que podem ser tomadas para cada uma.

Para esta versão, a interface do Cliente de filtragem de conteúdo foi simplificada para um uso mais fácil e unificada para trabalhar com clientes Windows, Mac OS e Chrome.

Tópicos:

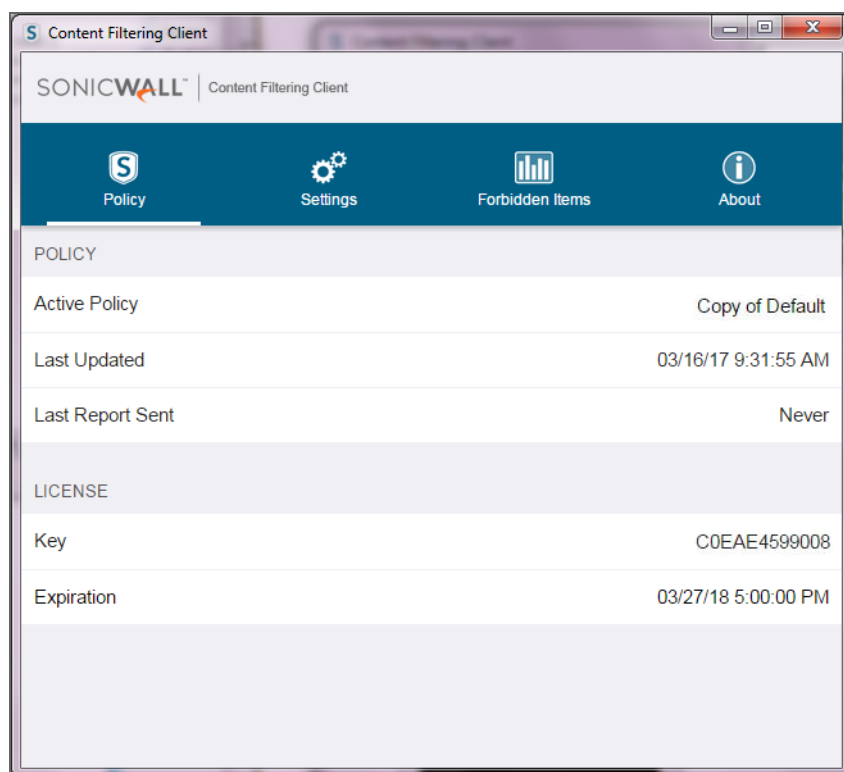
- [Política](#)
- [Configurações](#)
- [Itens proibidos](#)
- [Suporte SonicWall](#)

Política

A página Policy (Política) da interface mostra ambos os status da política e da licença.

Tópicos:

- [Seção Política](#)
- [Política ativa](#)
- [Seção Licença](#)



Seção Política

Na seção Policy (Política), cada campo listado é um link ativo. Quando passa o cursor sobre este, o link fica em **negrito e itálico** para indicar que está selecionado.

Os campos na vista Policy (Política) são definidos abaixo:

Campo	Função
Active Policy (Política ativa)	Quando selecionado, ele expande para mostrar o status das políticas ativas atuais. Para obter mais informações, consulte Política ativa . Clique em Active Policy (Política ativa) novamente para ocultar o status da política.
Last Updated (Última atualização)	Solicita uma atualização das políticas a partir da EPRS. Se a atualização for bem-sucedida, a data e hora atuais mudam para refletir o tempo de atualização. NOTA: Se uma atualização não for bem-sucedida, o carimbo de data/hora não mudará. Você pode abrir os logs para ver o erro que está impedindo a atualização.
Last Report Sent (Último relatório enviado)	Envia os relatórios mais recentes para a EPRS. Se a atualização for bem-sucedida, a data e hora atuais mudarão para refletir a hora em que o relatório foi enviado para a EPRS.

Política ativa

Quando selecionado, o campo Active Policy (Política ativa) é um link ativo que expande para mostrar o status das políticas padrão. Clique em Active Policy (Política ativa) novamente para ocultar o status da política.

Política	Status	Definição
Filter HTTP (Filtro HTTP)	Desligado/ Ligado	Quando ligado, filtra os sites HTTP que o usuário tenta acessar.
Filter HTTPS (Filtro HTTPS)	Desligado/ Ligado	Quando ligado, filtra os sites HTTPS que o usuário tenta acessar.
Safe Search (Pesquisa segura)	Desligado/ Ligado	Quando ligado, habilita as políticas de Pesquisa segura para Google e Bing.
Suspend behind FW (Suspende atrás do FW)	Desligado/ Ligado	Quando ligado, suspende o cliente de filtragem de conteúdo integrado e permite ao dispositivo de segurança de rede filtrar conteúdo da Web quando o sistema de usuário final está no escritório e atrás do firewall.

The screenshot shows the SonicWall Content Filtering Client interface. At the top, there is a navigation bar with four icons: Policy (selected), Settings, Forbidden Items, and About. Below the navigation bar, the main content area is titled 'POLICY'. It displays the 'Active Policy' as 'Copy of Default'. A list of policies is shown with their status:

Policy Name	Status
Filter HTTP	On
Filter HTTPS	On
Safe Search	On
Suspend Behind Firewall	On

Additional information at the bottom of the policy list:

Last Updated	03/16/17 9:31:55 AM
Last Report Sent	Never

Seção Licença

Na seção License (Licença), cada campo é informativo, em vez de um link ativo.

Campo	Função
Key (Chave)	Exibe o número de série do firewall ou o Grupo de distribuição de clientes associado à sua configuração.
Expiration (Expiração)	Indica quando a licença do CFC expira.

LICENSE	
Key	C0EAE4599008
Expiration	05/11/17 5:00:00 PM

Configurações

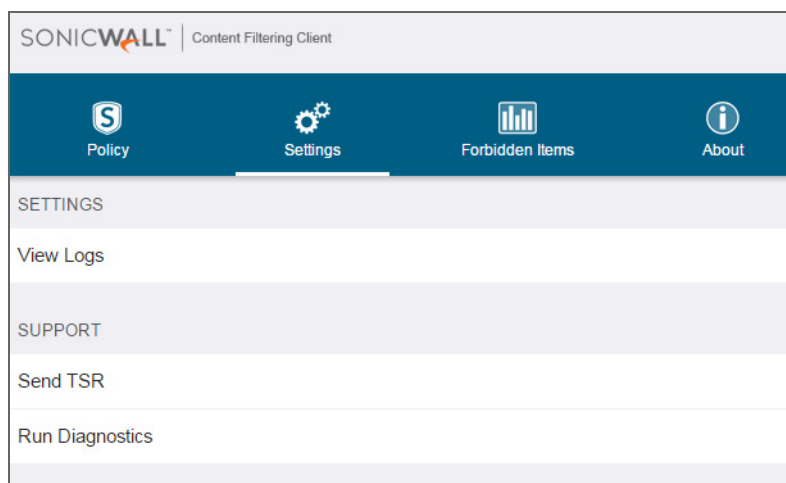
A página Settings (Configurações) agrupa informações de diagnóstico e suporte. As configurações de Windows e Mac OS são iguais, mas um sistema Chrome possui opções adicionais.

Tópicos:

- [Configurações em Windows e Mac OS](#)
- [Configurações do Chrome OS](#)

Configurações em Windows e Mac OS

A janela Settings (Configurações) de sistemas Windows e Mac OS mostra as opções **View Logs (Exibir logs)**, **Send TSR (Enviar TSR)** e **Run Diagnostics (Executar diagnóstico)**.



Visualizar logs

Em **Settings (Configurações)**, clique em **View Logs (Exibir logs)** e o arquivo de log do CFC abre em outra janela. O arquivo de log mantém um registro dos tipos diferentes de eventos gerados pelo CFC e a data e hora em que ocorreram. Quatro tipos de mensagens são rastreados:

- Informações
- Aviso
- Erro
- Depuração

Enviar um TSR

Na seção **Support (Suporte)**, você pode optar por **Send TSR (Enviar TSR)**. Um TSR é um Relatório do suporte técnico. Quando você clica em **Send TSR (Enviar TSR)**, um relatório de diagnóstico é enviado para a equipe de suporte na SonicWall. O Cliente de filtragem de conteúdo também exibe uma mensagem solicitando que entre em contato com o Suporte da SonicWall e fornece o nome do host do seu sistema, o qual é necessário para obter suporte. Consulte a captura de tela abaixo para obter um exemplo da mensagem.



Executar diagnóstico

Se você escolher **Run Diagnostics (Executar diagnóstico)**, o CFC executa uma verificação de diagnóstico e gera um relatório que abre um navegador. O relatório inclui as seguintes informações:

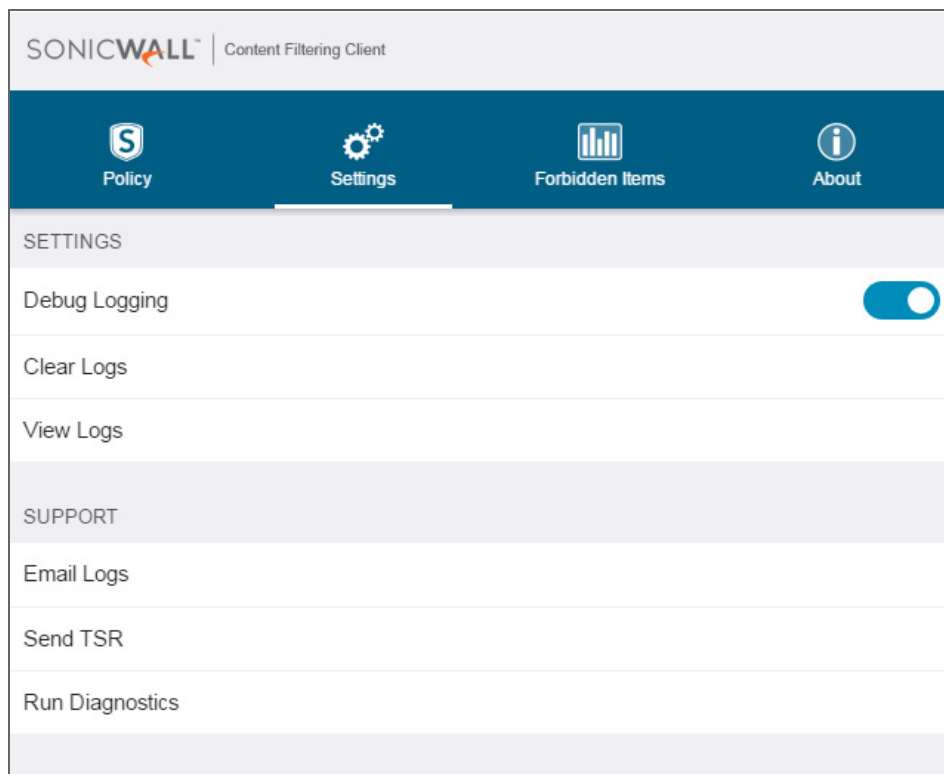
- Checking installation (Verificar instalação)
- Checking configuration (Verificar configuração)
- Checking license server (Verificar servidor da licença)
- Checking policy server (Verificar servidor da política)
- Checking botnet server (Verificar servidor de botnets)
- Checking WebRDS server (Verificar servidor WebRDS)
- Checking WebCFS server (Verificar servidor WebCFS)
- Checking TSR uploads server (Verificar servidor de carregamentos de TSR)
- Checking reporting server (Verificar servidor de relatório)

Você pode usar o relatório de diagnóstico para identificar a origem dos possíveis problemas. Um segmento desse relatório de diagnóstico é mostrado como um exemplo abaixo:

Checking installation	Fail	
Checking install location	Pass	
Checking for install directory	Pass	
Checking for service binary	Pass	Version is 3.1.20.0928
Checking for dashboard binary	Pass	Version is 3.1.20.0928
Checking for driver binary	Pass	Version is 3.1.20.0928
Checking for CA certificates	Pass	
Checking if Content Filtering Client service is installed	Pass	
Checking if Content Filtering Client service is running	Pass	
Checking if Content Filtering Driver service is installed	Pass	
Checking if Content Filtering Driver service is running	Fail	Content Filtering Driver service 'dswcfdrv' is not running
Checking configuration	Pass	
Checking for config database	Pass	
Validating serial number	Pass	Serial number CB0000005DB4 is valid
Getting 'Behind UTM' flag	Pass	The 'Behind UTM' flag is set to false

Configurações do Chrome OS

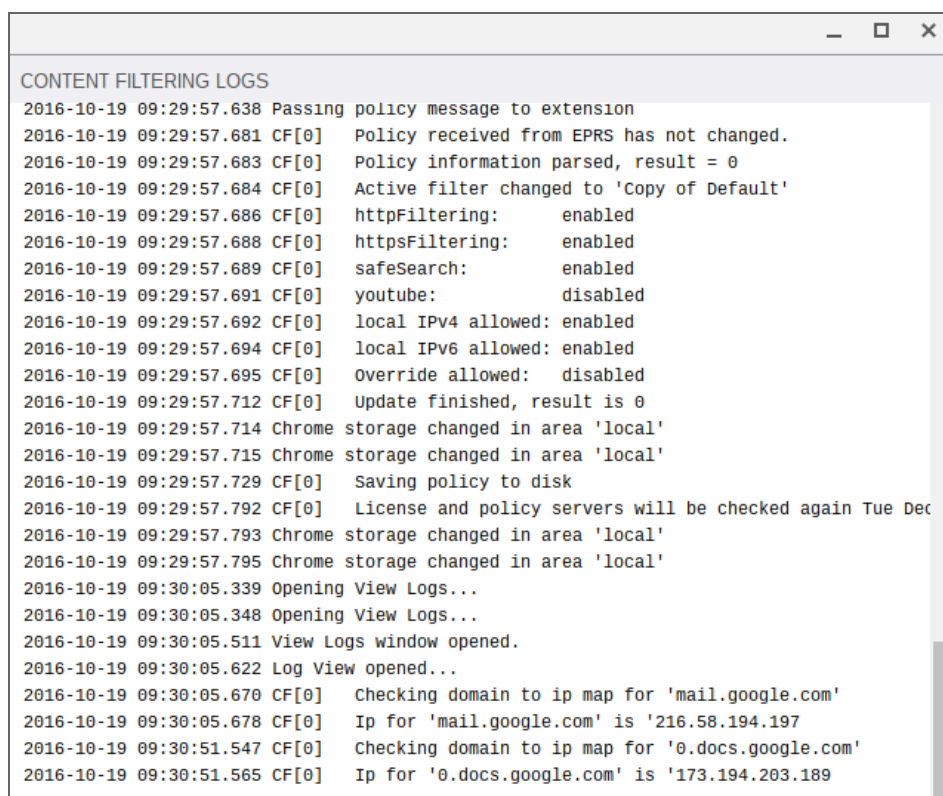
A janela Settings (Configurações) para sistemas Chrome OS mostra as opções de **Settings (Configurações)** e **Support (Suporte)**.



Opções de configuração do Chrome OS

A seção Settings (Configurações) da página tem diversas opções para um sistema Chrome.

Opção de configuração	Definição
Debug Logging (Registro em log da depuração)	O registro em log da depuração pode ser habilitado ou desabilitado no sistema de usuário final. Quando o botão está à esquerda com um fundo cinza, conforme mostrado na figura acima, o registro em log está desabilitado. Deslize o botão para a direita para habilitar o registro em log de depuração e o fundo fica azul.
Clear Logs (Limpar logs)	Limpa os Logs de filtragem de conteúdo. É-lhe pedido para confirmar se deseja limpar os logs, uma vez que esta ação não pode ser desfeita.
View Logs (Visualizar logs)	Exibe os Logs de filtragem de conteúdo. Um trecho de exemplo do arquivo de log é mostrado abaixo.



```
CONTENT FILTERING LOGS
2016-10-19 09:29:57.638 Passing policy message to extension
2016-10-19 09:29:57.681 CF[0] Policy received from EPRS has not changed.
2016-10-19 09:29:57.683 CF[0] Policy information parsed, result = 0
2016-10-19 09:29:57.684 CF[0] Active filter changed to 'Copy of Default'
2016-10-19 09:29:57.686 CF[0] httpFiltering: enabled
2016-10-19 09:29:57.688 CF[0] httpsFiltering: enabled
2016-10-19 09:29:57.689 CF[0] safeSearch: enabled
2016-10-19 09:29:57.691 CF[0] youtube: disabled
2016-10-19 09:29:57.692 CF[0] local IPV4 allowed: enabled
2016-10-19 09:29:57.694 CF[0] local IPV6 allowed: enabled
2016-10-19 09:29:57.695 CF[0] Override allowed: disabled
2016-10-19 09:29:57.712 CF[0] Update finished, result is 0
2016-10-19 09:29:57.714 Chrome storage changed in area 'local'
2016-10-19 09:29:57.715 Chrome storage changed in area 'local'
2016-10-19 09:29:57.729 CF[0] Saving policy to disk
2016-10-19 09:29:57.792 CF[0] License and policy servers will be checked again Tue Dec
2016-10-19 09:29:57.793 Chrome storage changed in area 'local'
2016-10-19 09:29:57.795 Chrome storage changed in area 'local'
2016-10-19 09:30:05.339 Opening View Logs...
2016-10-19 09:30:05.348 Opening View Logs...
2016-10-19 09:30:05.511 View Logs window opened.
2016-10-19 09:30:05.622 Log View opened...
2016-10-19 09:30:05.670 CF[0] Checking domain to ip map for 'mail.google.com'
2016-10-19 09:30:05.678 CF[0] Ip for 'mail.google.com' is '216.58.194.197
2016-10-19 09:30:51.547 CF[0] Checking domain to ip map for '0.docs.google.com'
2016-10-19 09:30:51.565 CF[0] Ip for '0.docs.google.com' is '173.194.203.189
```

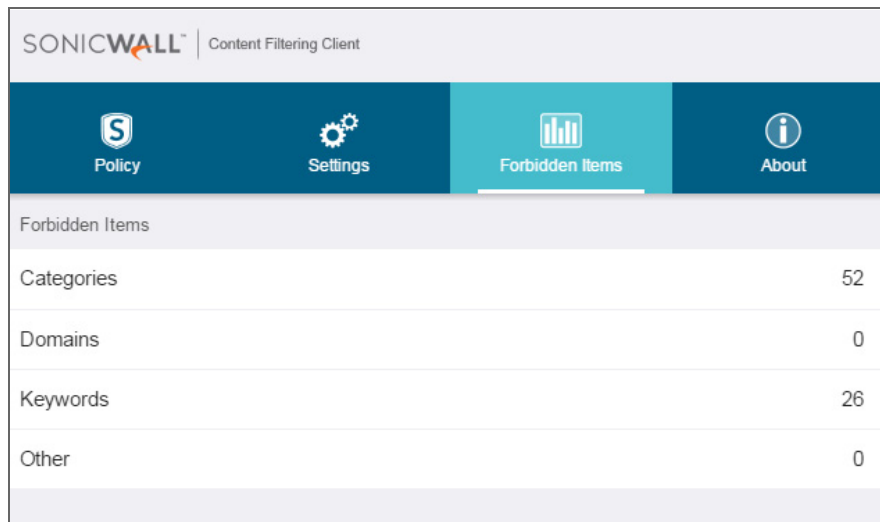
Opções de suporte do Chrome OS

Na seção **Support (Suporte)**, pode optar por **Email Logs (Logs de e-mail)**, **Send TSR (Enviar TSR)** ou **Run Diagnostics (Executar diagnóstico)**.

Opções de suporte	Definição
Email Logs (Logs de e-mail)	<p>Se necessitar de suporte, pode optar por enviar um e-mail ao seu administrador local. Quando você clica em Email Logs (Logs de e-mail), um arquivo é criado a partir dos Logs de filtragem de conteúdo e um modelo de e-mail com informações do sistema é aberto para si (ver abaixo). Insira o endereço de e-mail do destinatário, anexe o arquivo <code>tsr.zip</code> a partir do arquivo Downloads e envie o e-mail.</p> <div data-bbox="416 600 1401 875" style="border: 1px solid black; padding: 5px;"><p>SonicWALL Content Filtering Client for Chrome OS Version 3.1.24.124 OS: Chrome OS OS Version: 53.0.2785.154 OS Platform: 8530.96.0 OS Architecture: x86_64 Device ID: 3E191F3C-E01D-10A4-C542-F127E7CAD519</p><p>Note: You Must Attach the Downloaded file TSR.zip that was saved in the Downloads folder. You can also drag and drop the TSR.zip file from the Downloads folder into this email.</p></div>
Send TSR (Enviar TSR)	<p>Um TSR é um Relatório do suporte técnico. Quando você clica em Send TSR (Enviar TSR), um relatório de diagnóstico é enviado para a equipe de suporte técnico na SonicWall. O Cliente de filtragem de conteúdo também exibe uma mensagem solicitando que entre em contato com o suporte da SonicWall, Inc. e pede que mencione o seu ID de login durante o contato.</p> <div data-bbox="416 1037 943 1290" style="border: 1px solid black; padding: 5px;"><p>The TSR was sent successfully. Please contact SonicWall support at www.sonicwall.com/support and mention your login email 'ismimov@gedu.demo.sonicwallchromedemo.com'</p><div style="text-align: center;">Ok</div></div>
Run Diagnostics (Executar diagnóstico)	<p>Se você escolher Run Diagnostics (Executar diagnóstico), o CFC executa uma verificação de diagnóstico e gera um relatório que abre um navegador. O relatório inclui as seguintes informações:</p> <ul style="list-style-type: none">• Checking configuration (Verificar configuração)• Checking license server (Verificar servidor da licença)• Checking policy server (Verificar servidor da política)• Checking botnet server (Verificar servidor de botnets)• Checking WebRDS server (Verificar servidor WebRDS)• Checking WebCFS server (Verificar servidor WebCFS)• Checking TSR uploads server (Verificar servidor de carregamentos de TSR)• Checking reporting server (Verificar servidor de relatório)

Itens proibidos

A página **Forbidden Items (Itens proibidos)** permite ver os itens **Categories (Categorias)**, **Domains (Domínios)**, **Keywords (Palavras-chave)**, **Botnets** e **Other (Outro)** que foram bloqueados devido à configuração da política. Este mostra os contadores de eventos bloqueados para cada item. O exemplo abaixo mostra três eventos bloqueados por correspondência de Categorias. Não há detalhes disponíveis.

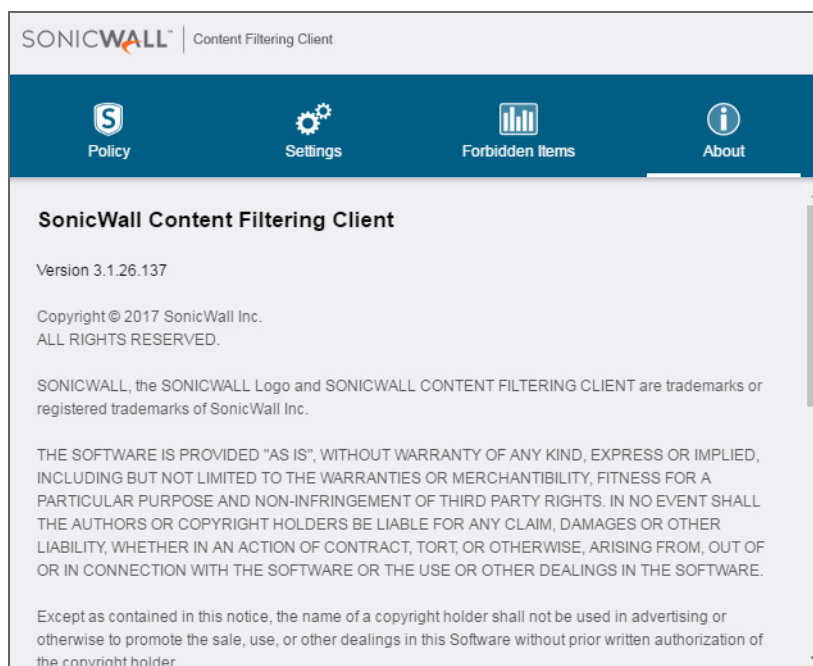


Forbidden Items	
Categories	52
Domains	0
Keywords	26
Other	0

NOTA: A opção Botnet não é mostrada nos sistemas Chrome OS.

Sobre

A página About (Sobre) exibe as informações de propriedade intelectual e garantia referente ao Cliente de filtragem de conteúdo SonicWall. A captura de tela abaixo mostra uma parte deste texto. É aqui que você também pode encontrar o número da versão do Cliente de filtragem de conteúdo caso necessite deste para fins de suporte.



SonicWall Content Filtering Client

Version 3.1.26.137

Copyright © 2017 SonicWall Inc.
ALL RIGHTS RESERVED.

SONICWALL, the SONICWALL Logo and SONICWALL CONTENT FILTERING CLIENT are trademarks or registered trademarks of SonicWall Inc.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT, OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use, or other dealings in this Software without prior written authorization of the copyright holder.

Suporte SonicWall

O suporte técnico está disponível para clientes que tiverem comprado produtos da SonicWall com um contrato de manutenção válido e para clientes com versões de avaliação.

O Portal de suporte fornece ferramentas de autoajuda que você pode usar para solucionar problemas com rapidez e de forma independente, 24 horas por dia, 365 dias por ano. Acesse o Portal de suporte em <https://support.sonicwall.com>.

O Portal de suporte permite:

- Visualizar artigos da base de conhecimentos e documentação técnica
- Baixar software
- Visualizar tutoriais em vídeo
- Colaborar com pares e especialistas em fóruns de usuários
- Obter assistência de licenciamento
- Acessar o MySonicWall
- Conhecer os serviços profissionais SonicWall
- Registrar-se para treinamento e certificação

Para contatar o Suporte da SonicWall, consulte <https://support.sonicwall.com/contact-support>.

Para visualizar o Contrato de produtos do usuário final (EUPA) da SonicWall, consulte <https://www.sonicwall.com/legal/eupa.aspx>. Selecione o idioma com base em sua localização geográfica para ver o EUPA que se aplica à sua região.