

# Boas praticas contra Spam

**i** Infelizmente o recebimento de Spams atualmente é um problema bastante incômodo. Na maioria das vezes você tem que excluir diversas mensagens Spam por dia, para que sua caixa de e-mail não lote e venha acarretar maiores transtornos. Existem alguns procedimentos que você pode realizar para ajudar a minimizar o recebimento de Spam. São eles:

1

## Habilitar o Apache SpamAssassin

O SpamAssassin é uma ferramenta que atua na análise das mensagens que chegam para suas contas. Além de analisar o conteúdo, a ferramenta pode classificar ela como Spam e direcionar para o diretório spam ou excluir automaticamente. Para maiores detalhes, nossa equipe também elaborou um tutorial informando maiores detalhes sobre a ferramenta, basta pesquisar por **SpamAssassin**.

**i** **Observação:** Essa ferramenta utiliza um tipo de pontuação (score) que vai de 0 à 10, onde: score menor que cinco, a ferramenta torna-se mais agressiva, podendo até bloquear mensagens legítimas. Pontuação superior à cinco, o SpamAssassin torna-se mais conservador, nesse caso podendo deixar algumas mensagens Spam chegar na caixa de entrada das contas.

2

## Boxtrapper

O BoxTrapper é uma ferramenta que também filtra os e-mails de sua caixa de entrada, assim como o SpamAssassin, porém ele possui etapas de verificação de e-mail. Caso algum endereço de e-mail que não esteja presente na Whitelist da ferramenta, envie e-mail para uma de suas contas, a ferramenta irá enviar uma mensagem de confirmação para o remetente, essa mensagem contém um link de confirmação, com isso a partir do momento que o remetente clicar nesse link, o endereço será adicionado na lista branca da ferramenta e as mensagens chegarão para suas contas.

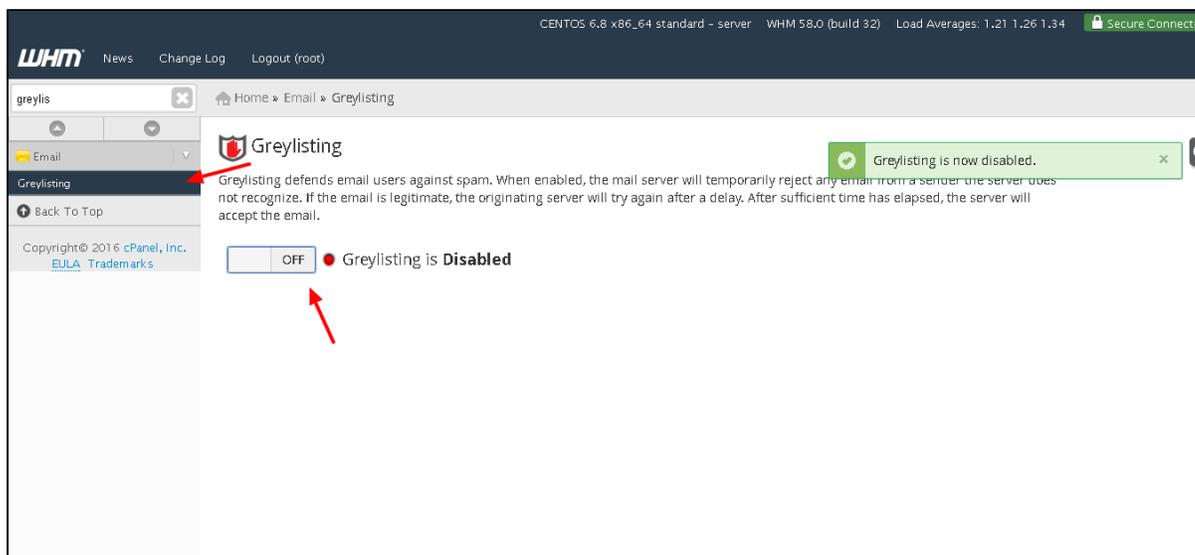
**i** **Observação:** A ferramenta em questão está disponível apenas para nossos planos corporativos ( VPS e servidores dedicados que utilizam CentOS + cPanel).

3

## Greylisting

A Greylisting protege os usuários de email contra spam. Quando habilitado, o servidor de email rejeita temporariamente qualquer email de destinatários não reconhecidos pelo servidor. Caso o email seja legítimo, o servidor de origem tentará novamente após um intervalo. Após decorrido tempo suficiente, o servidor aceitará o email.

Caso você deseje habilitar a ferramenta em questão, acesse o seu painel WHM e localize a opção "**Greylisting**", veja:



The screenshot shows the WHM interface for the 'Greylisting' configuration page. At the top, there is a navigation bar with 'WHM', 'News', 'Change Log', and 'Logout (root)'. Below that, the page title is 'greylisting' and the breadcrumb is 'Home » Email » Greylisting'. The main content area features a 'Greylisting' section with a shield icon and a description: 'Greylisting defends email users against spam. When enabled, the mail server will temporarily reject any email from a sender the server does not recognize. If the email is legitimate, the originating server will try again after a delay. After sufficient time has elapsed, the server will accept the email.' Below the description, there is a toggle switch labeled 'OFF' and a red dot indicating that 'Greylisting is Disabled'. A red arrow points to the 'OFF' button. In the top right corner, there is a green notification box that says 'Greylisting is now disabled.' with a close button (X).

A greylisting também pode acabar por bloquear mensagens autênticas para seus domínios, mas é possível adicionar o ip do domínio remetente como host confiável, para assim normalizar o envio:

The screenshot displays the WHM Greylisting interface. At the top, the status bar shows 'WHM 59.0 (build 32)' and 'Load Averages: 2.28 1.43 1.37'. The main content area is titled 'Trusted Hosts' and includes a sub-header 'Greylisting will never defer emails from entries on the Trusted Hosts list.' Below this, there is a 'New Trusted Hosts' section with a text input field for IP addresses and a 'Comment' field. A table of existing trusted hosts is shown, with columns for 'Host IP Address', 'Comment', and 'Actions'. The table contains six entries, each with a unique IP address and a comment indicating it was populated for a specific mail service. The 'Actions' column for each entry includes 'Edit' and 'Delete' options. A notification banner at the top right indicates that neighboring IP addresses are not in the trusted hosts list. Red arrows in the image point to the 'Add' button and the 'New Trusted Hosts' form.

Quando habilitada, a Greylisting irá atuar em todas as contas cPanel do servidor, porém, caso você deseje é possível desativar a ferramenta de forma individualmente, por conta cPanel.



**Observação:** A ferramenta Greylisting está disponível apenas para os nossos planos corporativos: Servidores dedicados e VPS que utilizam CentOS + cPanel.

Este artigo te ajudou?



✖

Your Rating:



Results:



1 rates

Ainda precisa de ajuda?

ABRIR UM CHAMADO