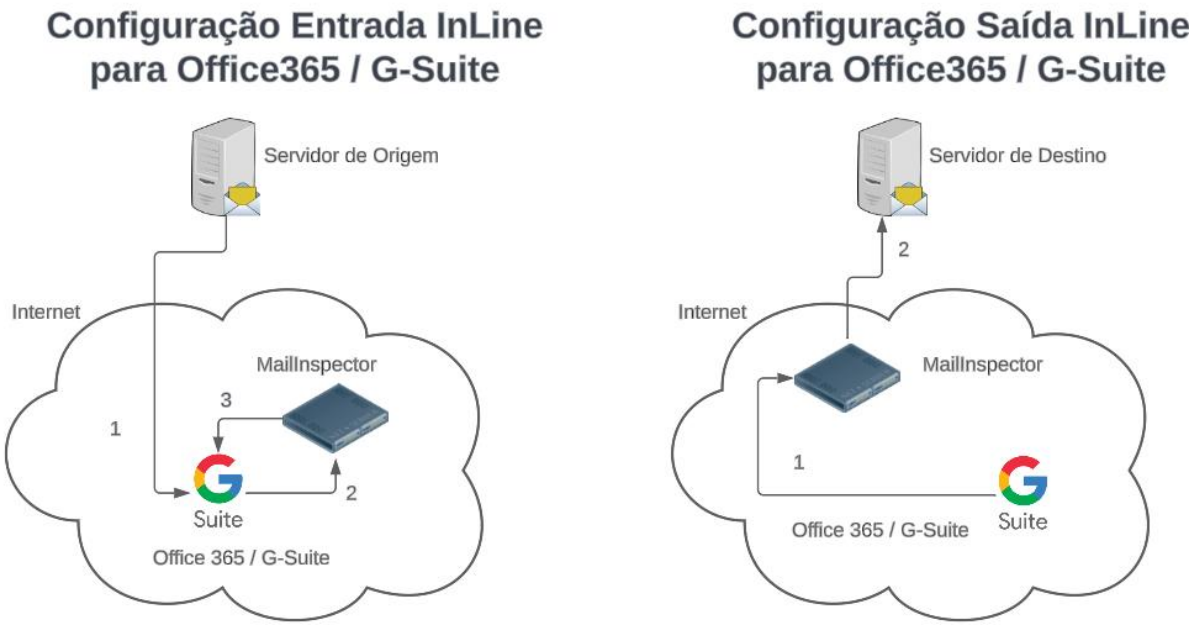
Documentação de Integração
MailInspector V5.2 com G-Suite
sem alteração no apontamento MX/DNS

MAILINSPECTOR

powered by HSC

Integração MailInspector

Exibe documento tem por finalidade mostrar a integração do MailInspector com Offi365, sem necessidade de mudança de MX e integração e importação de contas via API.



Solução com redirecionamento dos emails sem necessidade de alteração do DNS da empresa

Configuração Entrada InLine (sem mudança no MX) para Office365 / G-Suite

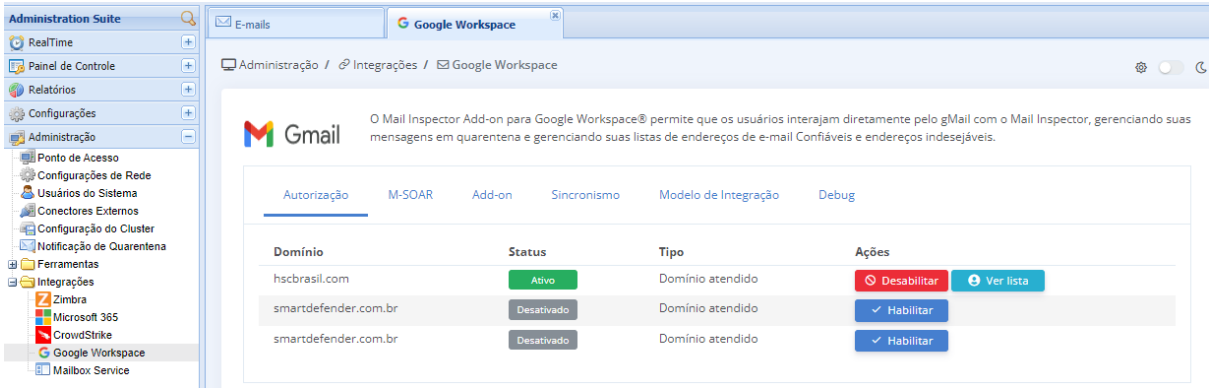
1. Os e-mails são direcionados ao Office365/G-Suite (que é o padrão quando se usa Office365 ou G-Suite), portanto, não há necessidade de mexer no MX/DNS;
2. Ao receber o e-mail, o Office365/G-Suite efetua a filtragem e encaminha para o MailInspector;
3. Após a filtragem por parte da Microsoft/Google, as mensagens são escaneadas novamente pelo MailInspector e os devolve ao Office365/G-Suite;

Configuração Saída InLine (sem mudança no MX) para Office365 / G-Suite

1. Email sai do Office365 / G-Suite e é entregue ao MailInspector;
2. É feita a filtragem do email no MailInspector e entregue a Internet (servidor destino);

Configuração de conexão com G-Suite via API e configuração de M-SOAR

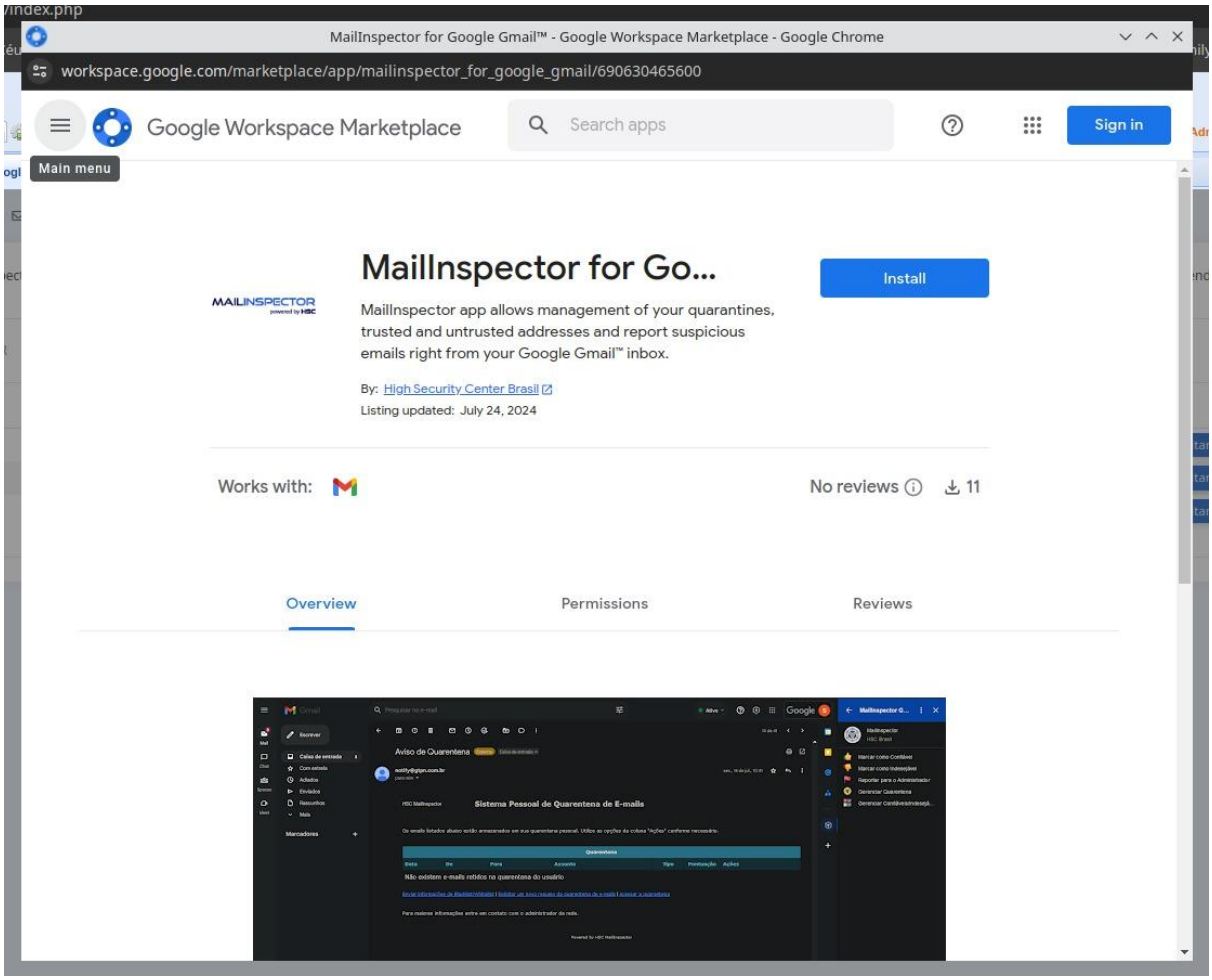
Primeiramente temos que configurar a conexão do MailInspector com o G-Suite. Para isso, vá em: Administração > Integrações > Google Workspace



1. Serão exibidos todos os domínios protegidos pelo Mail Inspector. Escolha o domínio que deseja ativar a integração e clique em Habilitar.

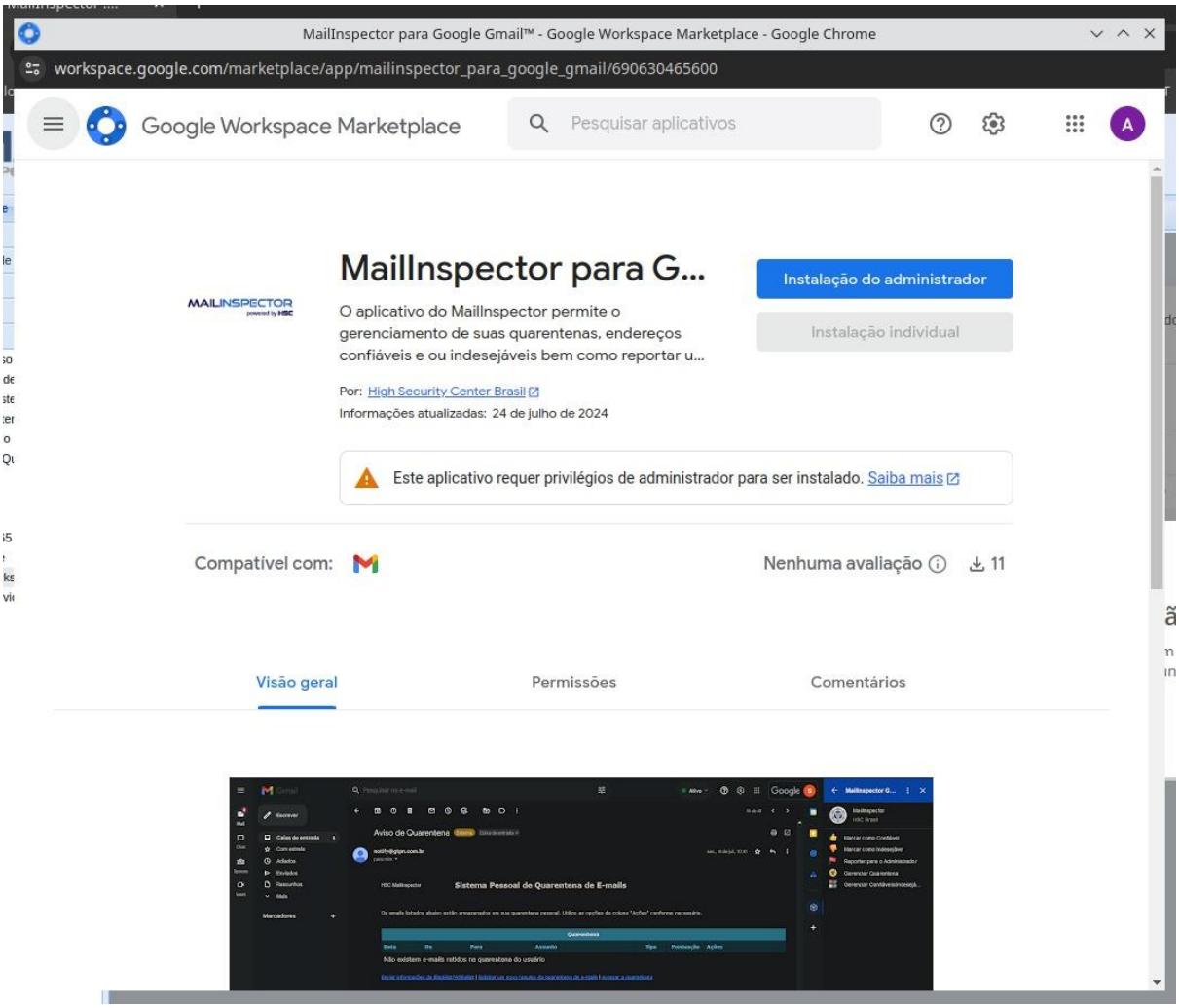
2. Na nova janela, informe a conta do administrador do serviço G-Suite

3. Ao fazer isso, será aberta a tela de login (canto superior direito).



Ao mesmo tempo aparecerá uma tela de Autorização de integração com contador em segundos, para você autenticar a sua senha.

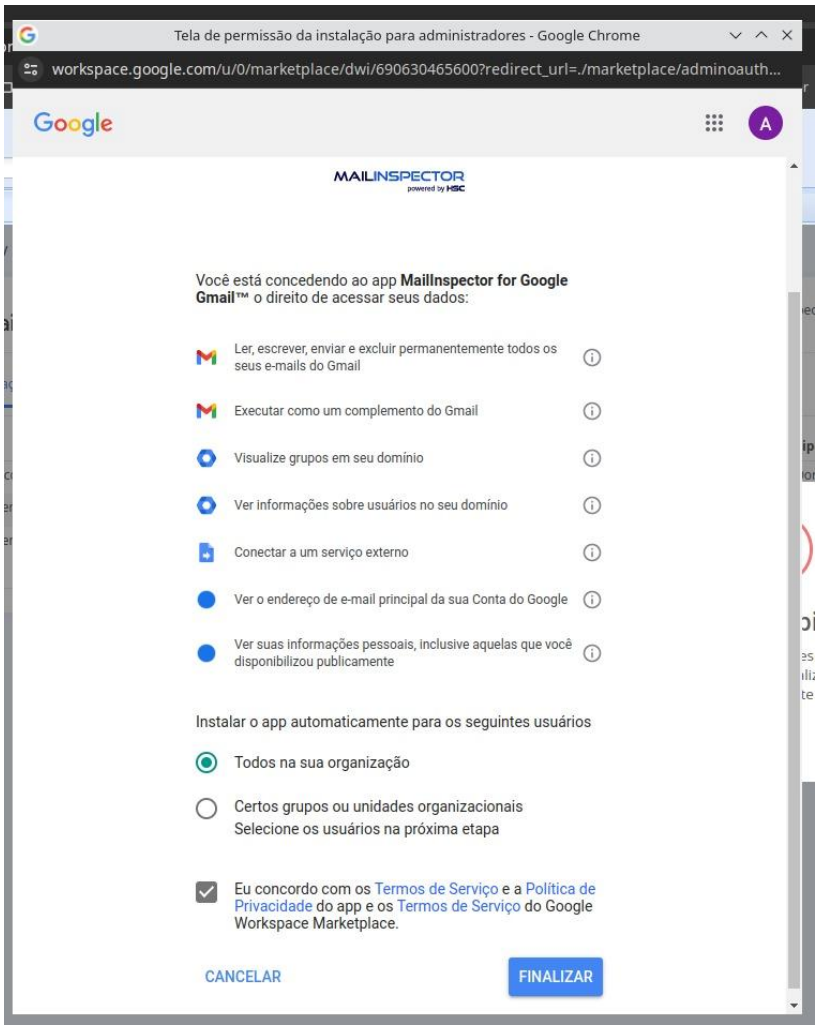
4. Uma vez autenticado, clique em Instalação do Administrador



5. Depois de clicar em Instalação do administrador, será aberta janela de aviso. Clique em continuar.

6. Será apresentada a tela de concordância com os termos de uso, bem como indicação das permissões necessárias para a integração do MailInspector com o G-Suite. Marque o box de Eu concordo com os Termos de Serviço e Política de Privacidade do app e os Termos de Serviço do Google Workspace Marketplace.

Depois marcado o box, clique em FINALIZAR

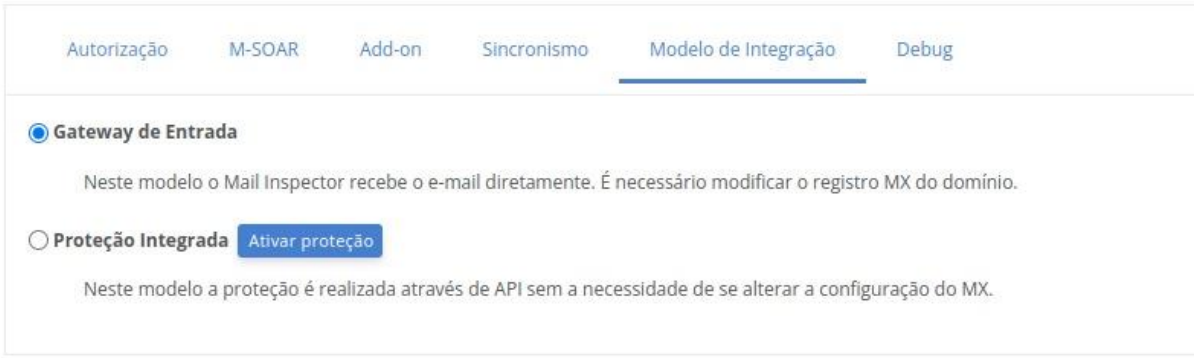


7. Será indicado que o MailInspector foi instalado no G-Suite. clique em CONCLUÍDO.

8. Após clicado em CONCLUÍDO, você pode configurar as ações de M-SOAR, ou deixar parta depois. Sugerimos que seja - **Não, manter o padrão** - Ao qual serão mantidas as ações padrão do M-SOAR, sem necessidade de alteração.

Configuração Entrada e Saída de Emails para G-Suite Inline (sem alteração de MX)

Por padrão o MailInspector permite que as configurações InLine sejam automáticas, bastando selecionar a opção Proteção Integrada.



Caso ocorra alguma falha de configuração automática, será necessária a configuração manual, para isso, basta seguir as etapas indicadas a seguir, de acordo com o tipo de servidor de email utilizado (G-Suite ou Office365).

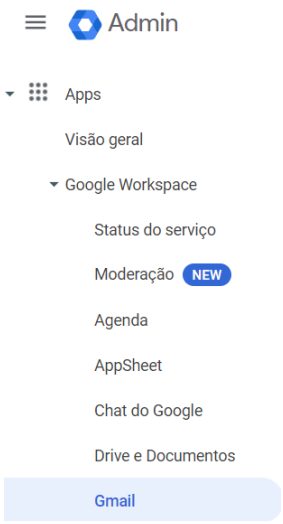
- **Por Gateway de Entrada:** É o processo em que é feito o apontamento dos emails para o MailInspector. Esse apontamento é através de mudança do MX no DNS da empresa.
- **Proteção Integrada:** Não há a necessidade de apontar o MX no DNS da empresa, basta configurar o Office365/G-Suite para que ao receberem os emails, eles sejam redirecionados ao MailInspector, que os filtrarão e os devolverá ao servidor Office365/G-Suite.
  Essa configuração poderá ser de forma automática, sem necessidade de intervenção ou criação de regras por parte do administrador, somente será necessária a intervenção manual em determinados casos, como por exemplo falta de permissão do administrador para acesso automático do MailInspector sobre o Office365/G-Suite, ou falha de comunicação, etc.

Caso ocorra alguma falha de configuração automática, será necessária a configuração manual, para isso, basta seguir as etapas indicadas a seguir, de acordo com o tipo de servidor de email utilizado (G-Suite ou Office365).

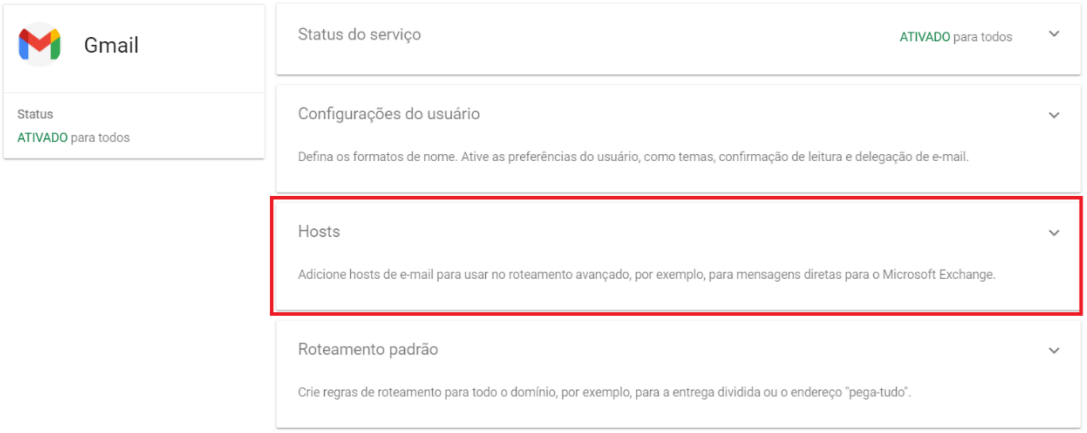
Acesse a sua conta de G-Suite pelo Google Admin Console.

Etapa 1: Adicionar os nodes de filtragem

1. Entre no Google Admin Console. (admin.google.com)
2. No painel de navegação esquerdo, clique em Apps > Google Workspace > Gmail.

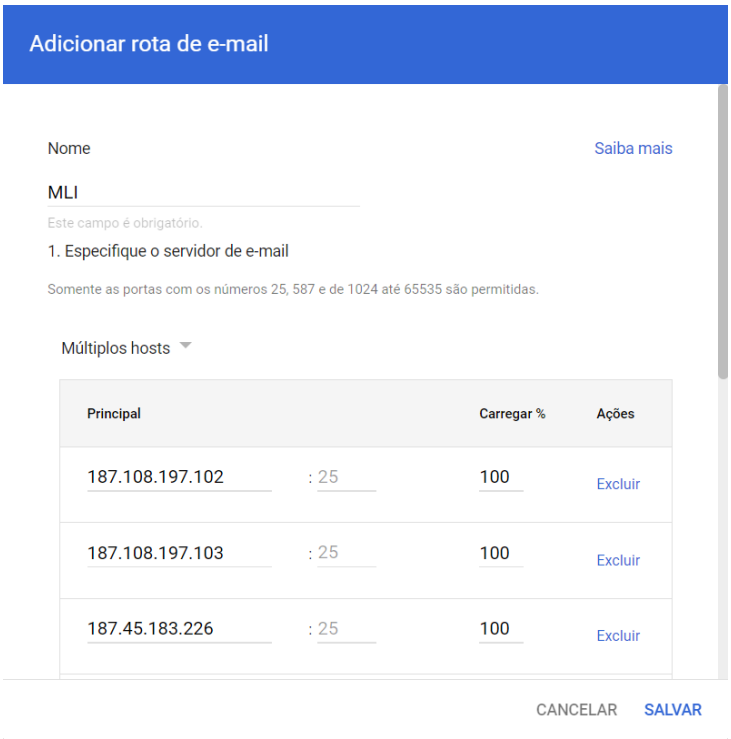


3. Clique em Hosts.



4. Clique em ADICIONAR ROTA.
5. Em Nome do rupo de NODES que você irá cadastrar. Para saber quais são os hostnames destes node, entre em contato com o suporte da HSCBRASIL. Como exemplo, vamos criar os nodes da nuvem CLICLOUD, através dos IPs.
6. Você pode adicionar uma única máquina ou múltiplas máquinas. No exemplo, vamos colocar múltiplas máquinas, ao qual o próprio Google irá gerenciar a alta disponibilidade e preferência de

entrega.

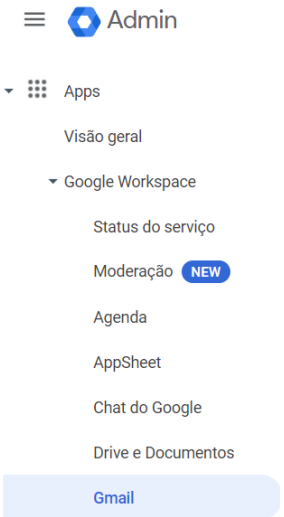


Repare que adicionei vários principais, não usamos os secundários.
Obs: Também é possível usar HOSTNAME por exemplo: **mx-balancer.mlicloud.com** em vez de IP.

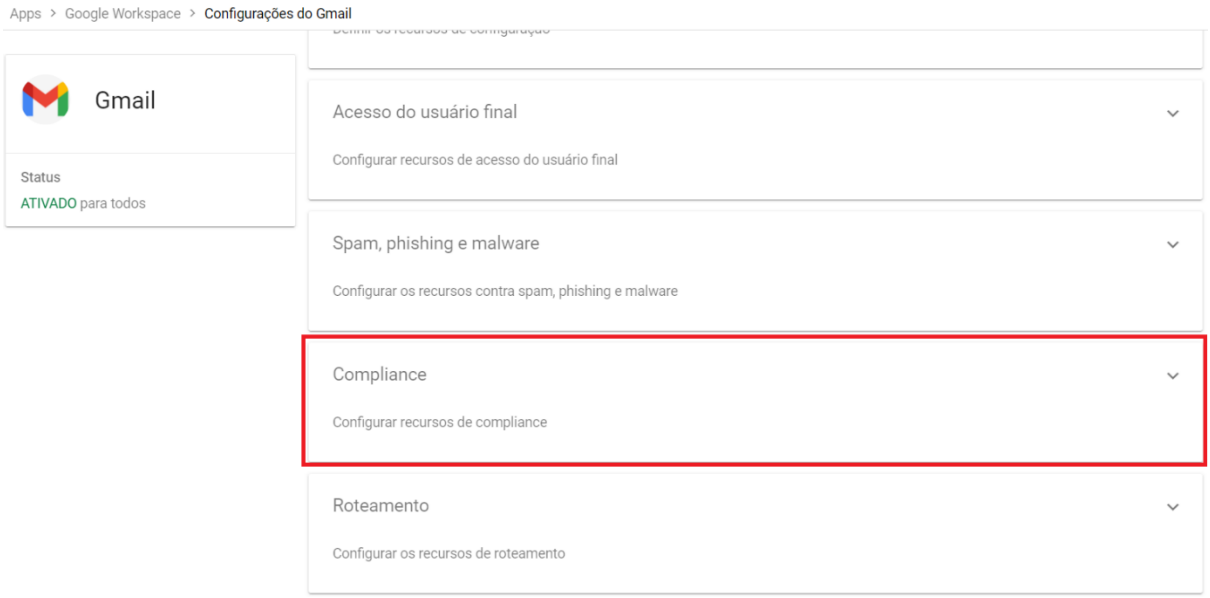
7. Digite o número das portas como 25 e 100% em carregar, para todas os nodes incluídos.
8. Em Opções, **desmarque** a caixa de seleção - Exigir um certificado assinado pela autoridade de certificação (recomendado).
9. Clique em Salvar.

Etapa 2: Criar regra de Entrada de Emails e redirecionamento se necessário

1. No painel de navegação esquerdo, clique em Apps > Google Workspace > Gmail



2. Role para baixo e clique em Compliance

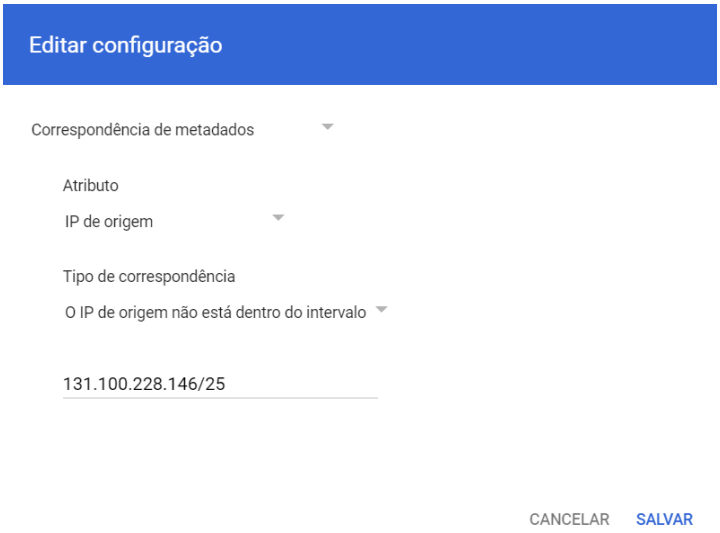


3. Clique em Compliance de conteúdo.
4. Essa opção nos permite criar regra de redirecionamento perante determinadas condições.
5. Vamos criar três regras de compliance:
    a. Inbound (Emails de Entrada);
    b. Interno (Emails Internos);
    c. Outbound (Emails de Saída);

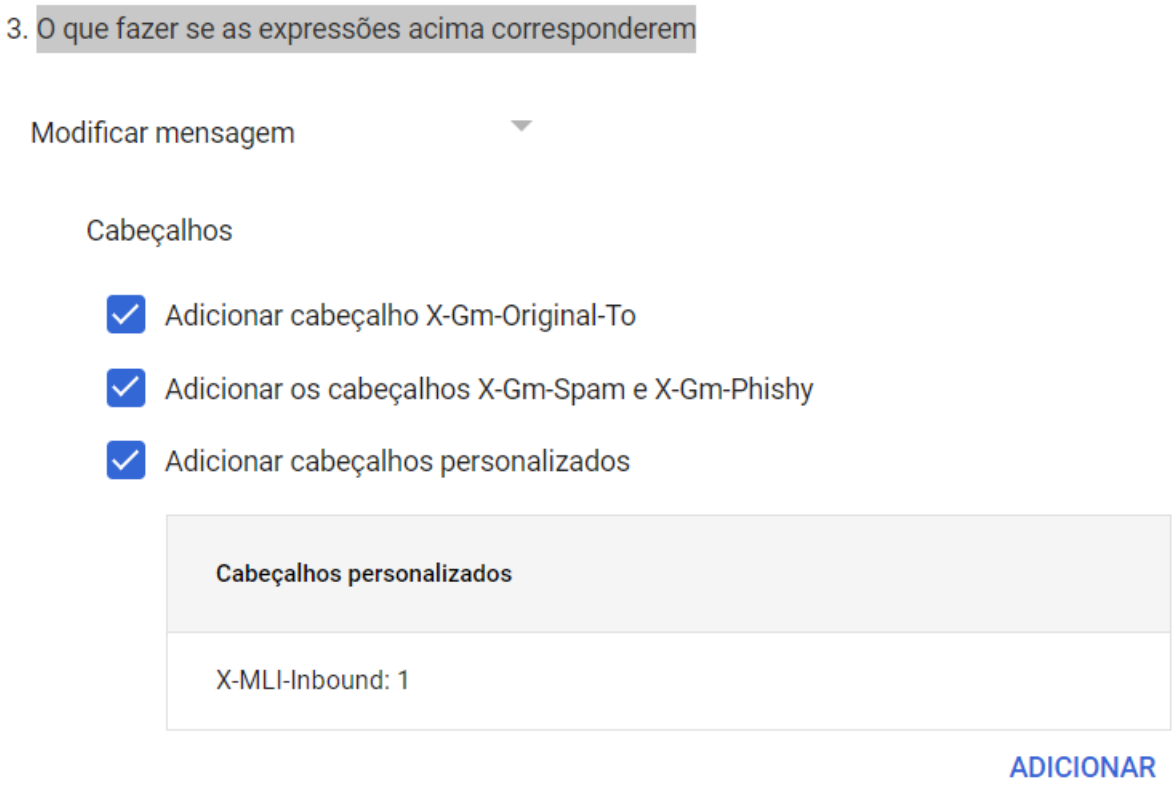
Regra Inbound

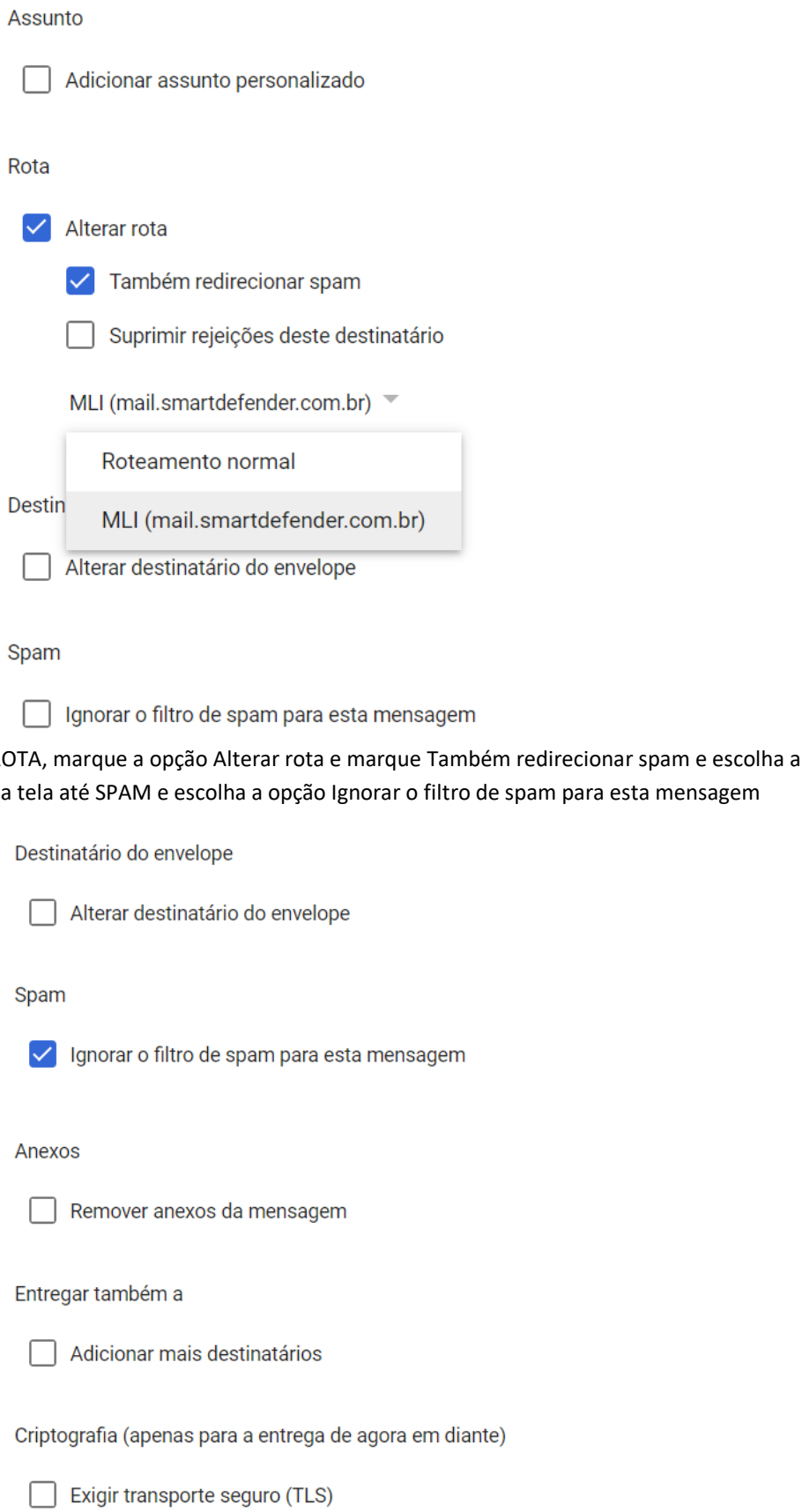
6. Clique em ADICIONAR REGRA
7. Na regra Inbound indique em Compliance do conteúdo o nome da regra (Inbound)
    a. Mensagens de e-mails afetadas: Recebidas
    b. Adicionar as expressões que descrevem o conteúdo que você quer pesquisar em cada mensagem: Se QUALQUER UMA das seguintes opções coincidirem com a mensagem
    c. Correspondência de Metadados
    d. Atributo: IP de origem
    e. Tipo de correspondência: O IP de origem não está dentro do intervalo

f. Repetir a entrada dos IP's, caso tenha mais de um IP a ser acrescentado, clicando em adicionar e repetir a ação de inserir IP.



8. O que fazer se as expressões acima corresponderem: Modificar mensagem

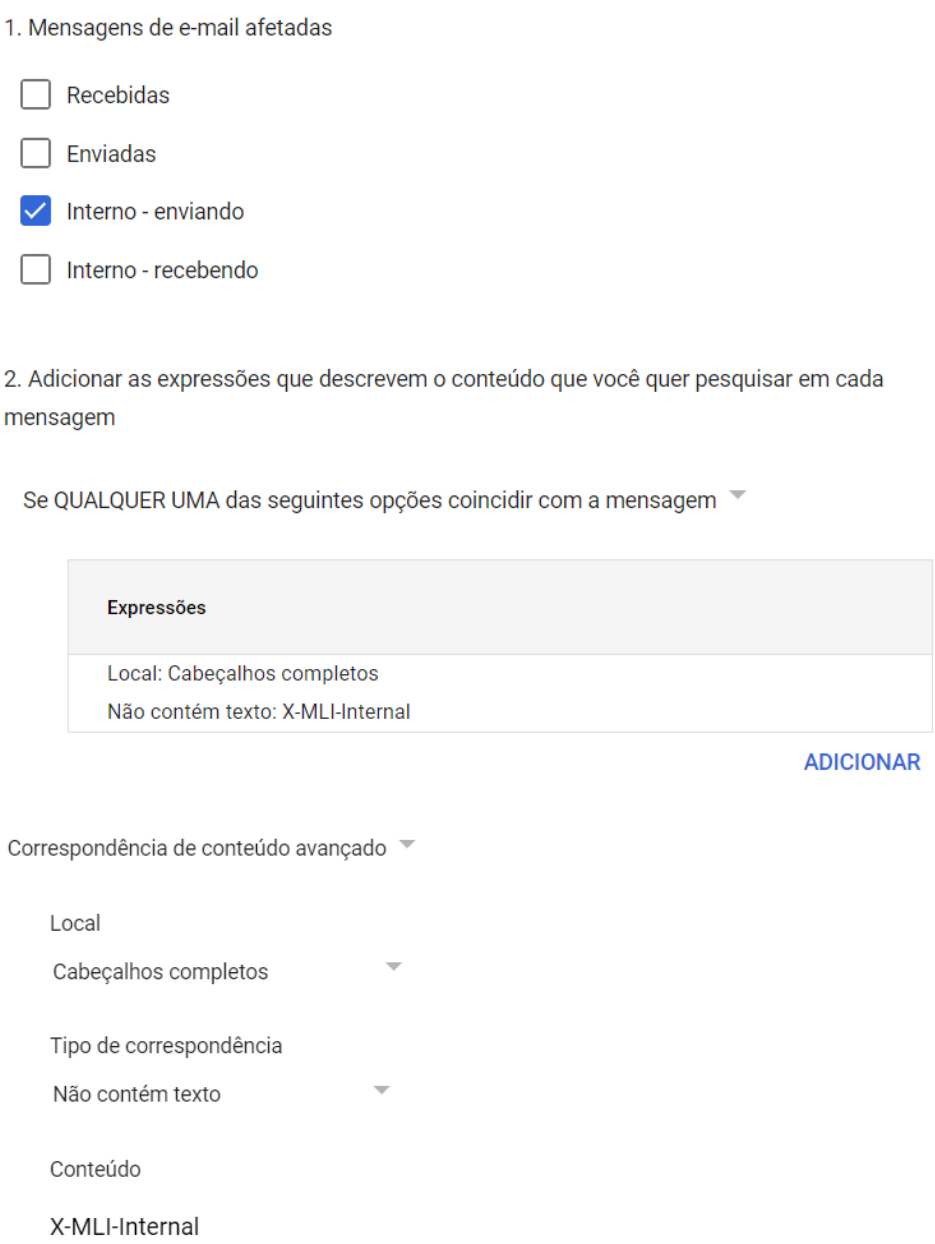




Em ROTA, marque a opção Alterar rota e marque Também redirecionar spam e escolha a opção MLI
Role a tela até SPAM e escolha a opção Ignorar o filtro de spam para esta mensagem

Regra Interno

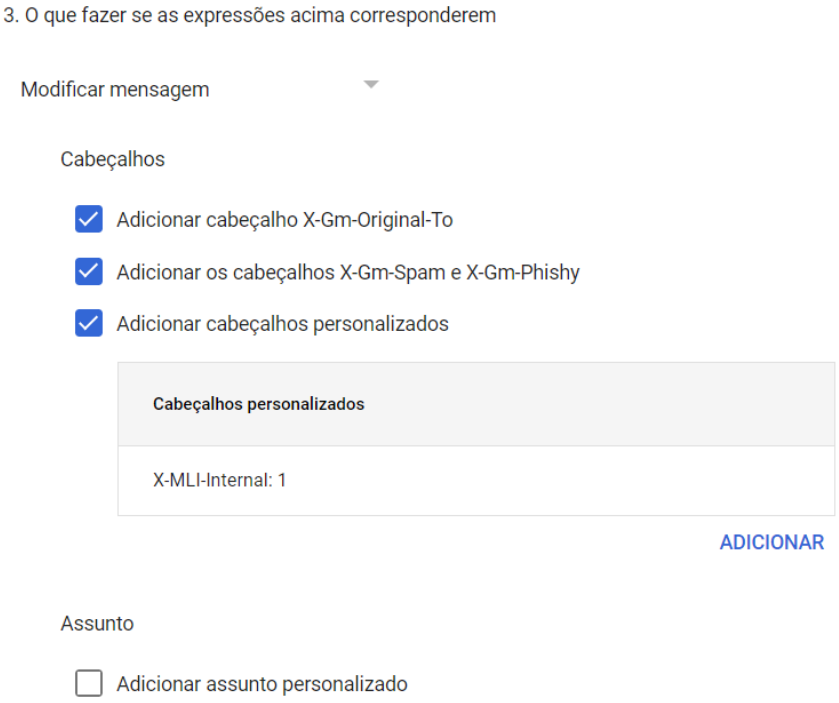
1. Clique em ADICIONAR OUTRA REGRA
2. Na regra Interno indique em Compliance do conteúdo o nome da regra (Interno)
3. Selecione Interno – enviando
   Adicionar as expressões que descrevem o conteúdo que você quer pesquisar em cada mensagem
   Se QUALQUER UMA das seguintes opções coincidir com a mensagem
   Expressões
   Local: Cabeçalhos completos
   Não contém texto: X-MLI-Internal



Marque as opções Cabeçalhos:

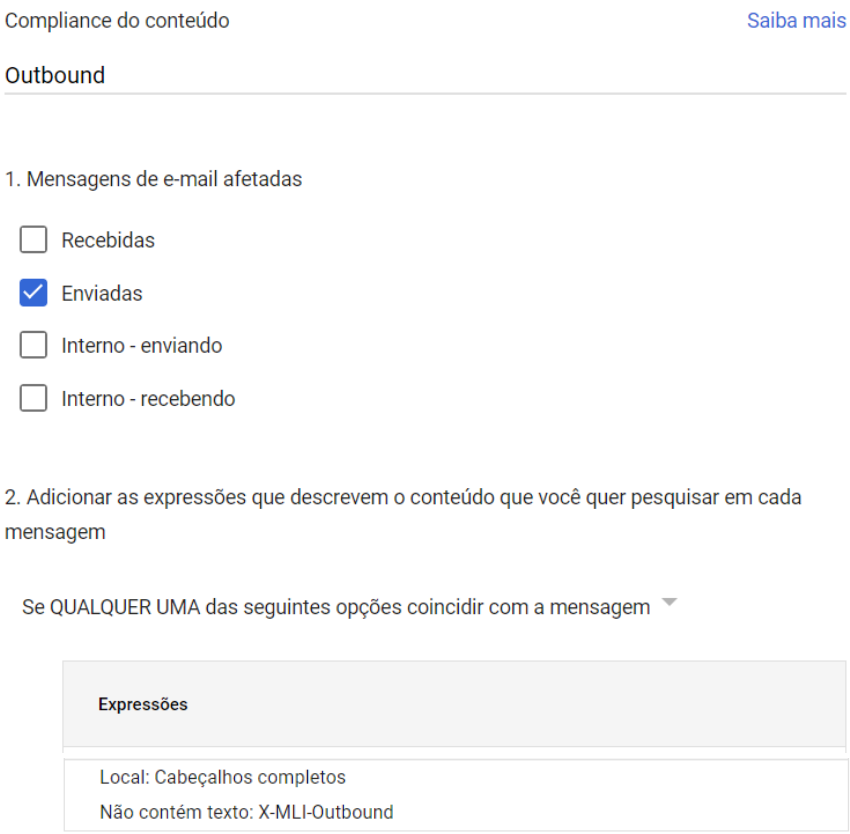
a. Adicionar cabeçalho X-Gm-Original-To
b. Adicionar os cabeçalhos X-Gm-Spam e X-Gm-Phishy

c. Adicionar cabeçalhos personalizados: X-MLI-Internal: 1

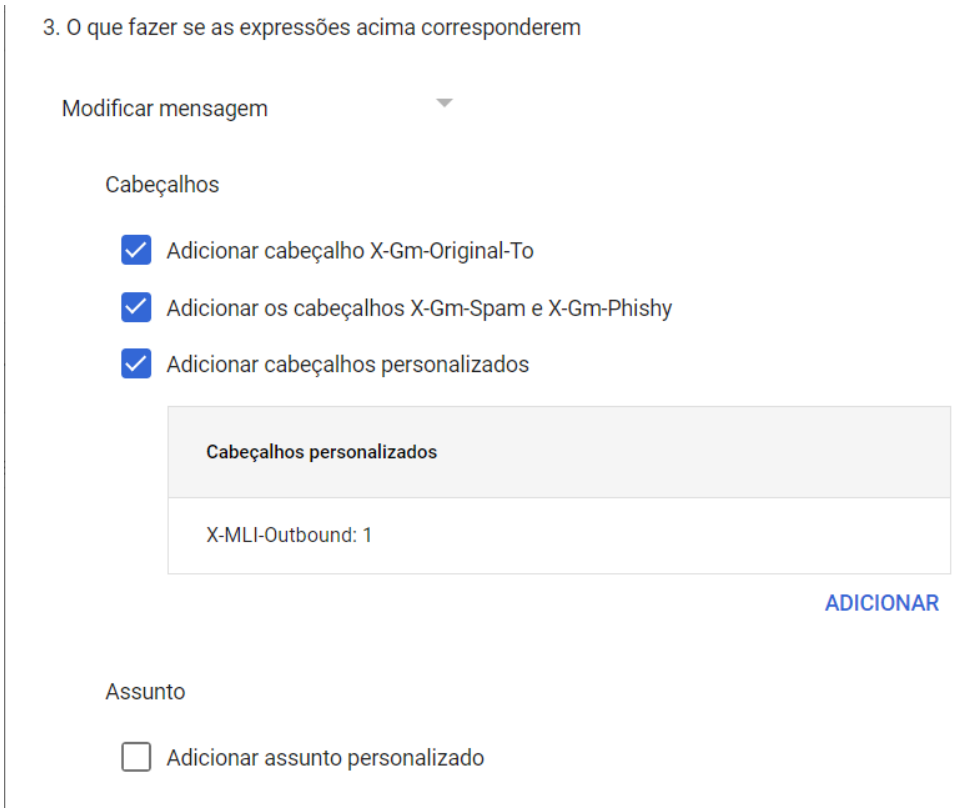


Regra Oubound

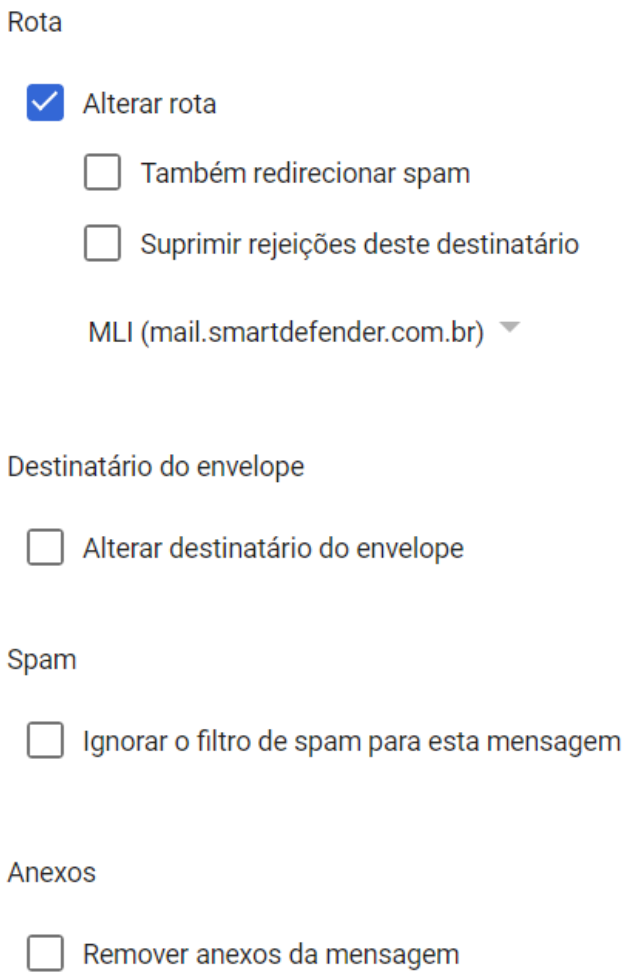
1. Clique em ADICIONAR OUTRA REGRA
   Na regra Outbound indique em Compliance do conteúdo o nome da regra (Outbound)
2. Selecione Enviadas
   Adicionar as expressões que descrevem o conteúdo que você quer pesquisar em cada mensagem
   Se QUALQUER UMA das seguintes opções coincidir com a mensagem
   Expressões
   Local: Cabeçalhos completos
   Não contém texto: X-MLI-Outbound



3. Marque as opções Cabeçalhos:
   a. Adicionar cabeçalho X-Gm-Original-To
   b. Adicionar os cabeçalhos X-Gm-Spam e X-Gm-Phishy
   c. Adicionar cabeçalhos personalizados: X-MLI-Outbound: 1



4. Em ROTA, marque a opção Alterar rota e indique a opção de rota MLI



5. Clique em Salvar

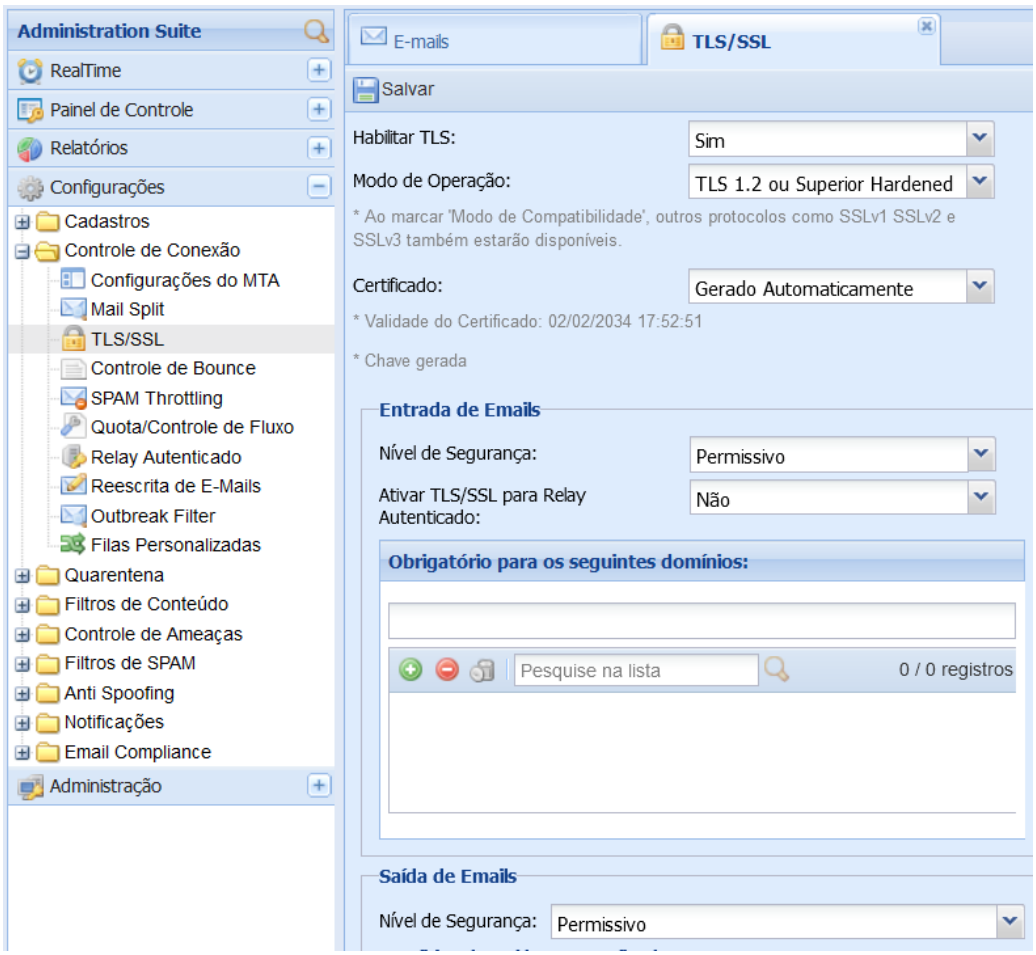
Comunicação segura entre MailInspector e Microsoft 365 / G-Suite

Verifique se está ativado o protocolo TLS no MailInspector.
É necessário que esteja habilitado e configurado no modo de operação TLS 1.2 ou Superior Hardened. As outras versões foram mantidas por questão de compatibilidade, mas oferecem menor segurança, não sendo recomendado o uso delas.

Para esse processo, vá em:
Configurações > Controle de Conexão > TLS/SSL

Marque as seguintes opções:

1. Habilitar TLS: Sim
2. Modo de Operação: TLS1.2 ou Superior Hardened
3. Entrada de Emails > Nível de Segurança: Permissivo
4. Saída de Emails > Nível de Segurança: Permissivo



Com essas configurações você está indicando a comunicação com TLS ativado entre G-Suite e MailInspector, dessa forma a comunicação de e-mails (tanto envio, quanto recebimento) é completamente segura.

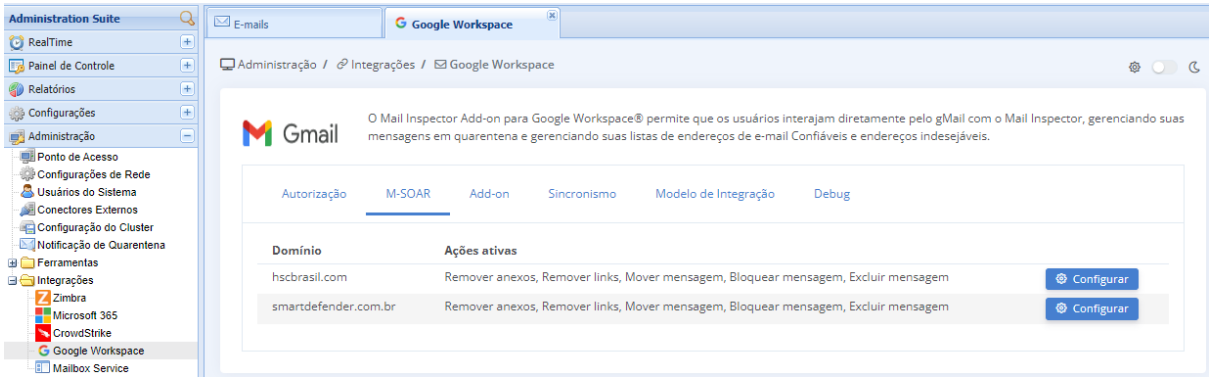
TLS v1.2	Cifra		Order	Strengh
TLS 1.2 ou Superior Hardened	xc030	ECDHE-RSA-AES256-GCM-SHA384	ECDH	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	x9f	DHE-RSA-AES256-GCM-SHA384	DH	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

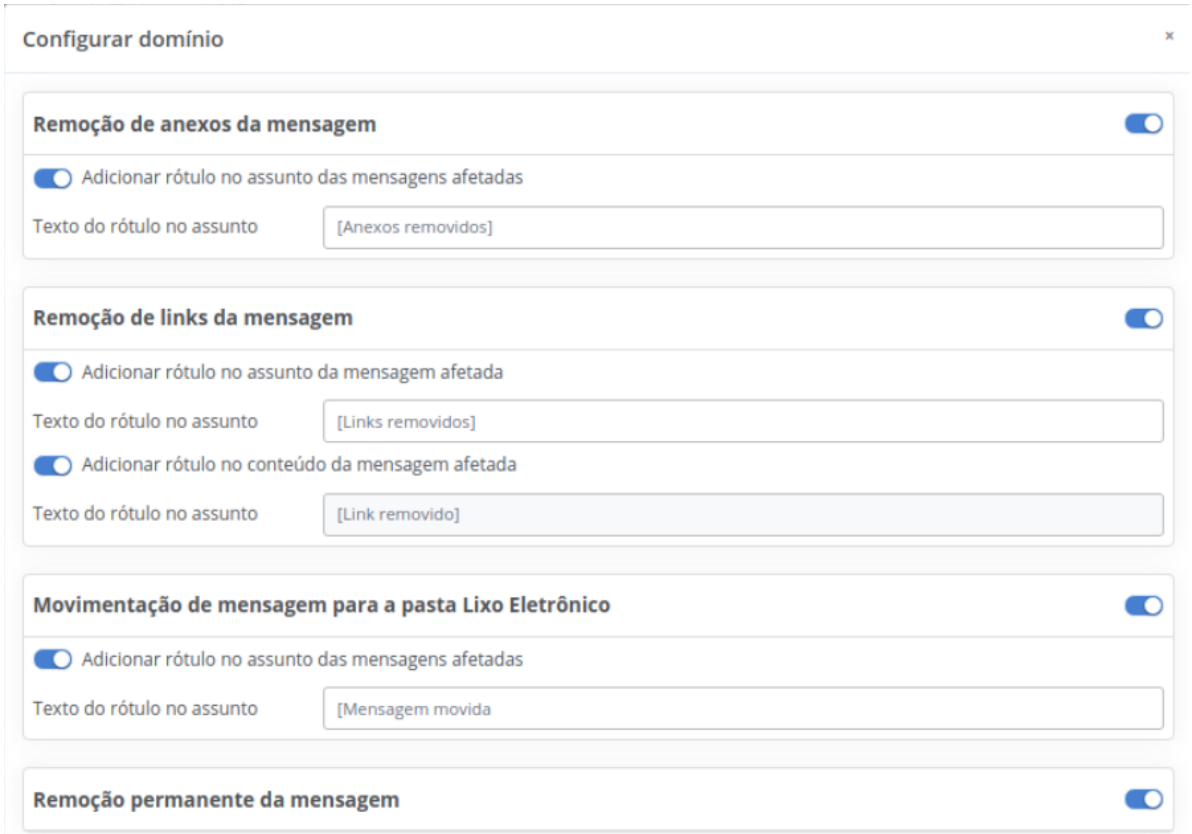
Configuração de Orquestração (M-SOAR)

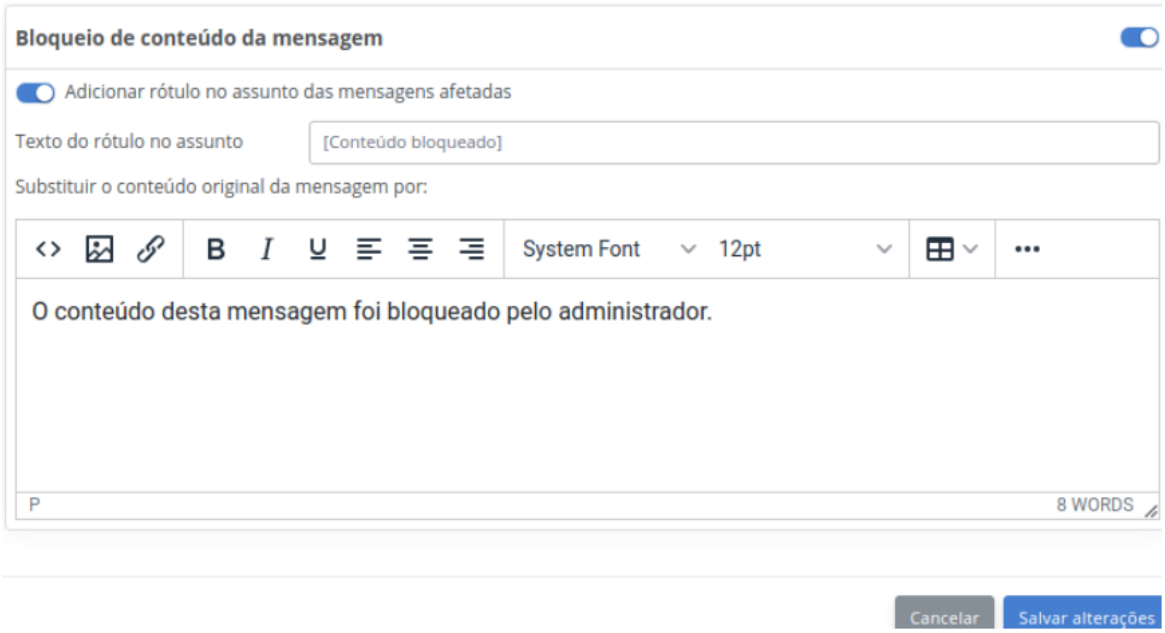
Configuração do M-SOAR permite personalizar quais ações o Administrador do MailInspector poderá efetuar em tempo real na caixa de e-mail do usuário do G-Suite (diretamente na caixa da conta Google do usuário).

Como durante a etapa de autenticação de usuário administrador, o G-Suite já libera para você o acesso ao M-SOAR, basta você configurar as ações desejadas no M-SOAR, para personalização dele (opcional).

Escolha o domínio que já foi anteriormente ativado na autenticação e sincronização e clique em Configurar, que serão abertas as telas de configuração do M-SOAR para o seu G-Suite.

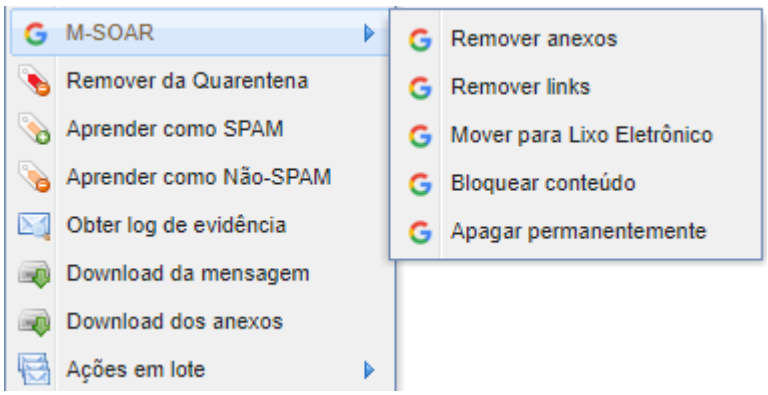






Edite as ações desejadas e clique em Salvar Alterações.

Para executar as ações acima, basta localizar a mensagem desejada no Painel Real Time → E-mail e clicar com o botão direito sobre a mensagem e escolher a ação desejada:



Ações do M-SOAR

Remover anexos da mensagem - remove os anexos do e-mail selecionado no G-Suite do usuário final
Remover links da mensagem - remove os links contidos no -mail selecionado no G-Suite do usuário final
Mover para Lixeira - move a mensagem para a pasta Lixeira no G-Suite do usuário final
Bloquear Conteúdo - impede a visualização da mensagem no G-Suite do usuário final
Apagar a mensagem - apaga a mensagem no G-Suite do usuário final

Requisito para ações

O Administrador do MailInspector deve levar em consideração que as ações do M-SOAR são disponibilizadas exclusivamente para as mensagens já entregues no G-Suite

Ativação de Add-On do MLI no G-Suite

O Add-on para G-Suite permite que os usuários dos serviços do Google interagirem a partir de seu G-Suite com o Mail Inspector. O usuário pode visualizar as suas mensagens em quarentena e liberar alguns tipos de quarentena além de adicionar ou remover registros de sua lista de endereços Confiáveis e Indesejáveis.
O procedimento a seguir descreve a ativação do Add-on do Mail Inspector no G-Suite.

Requisitos

- Ter ativado o M-SOAR (Orquestração)
- Possuir acesso administrativo ao MailInspector 5.2
- Já ter configurado o certificado digital no MailInspector (não pode ser o auto-assinado)

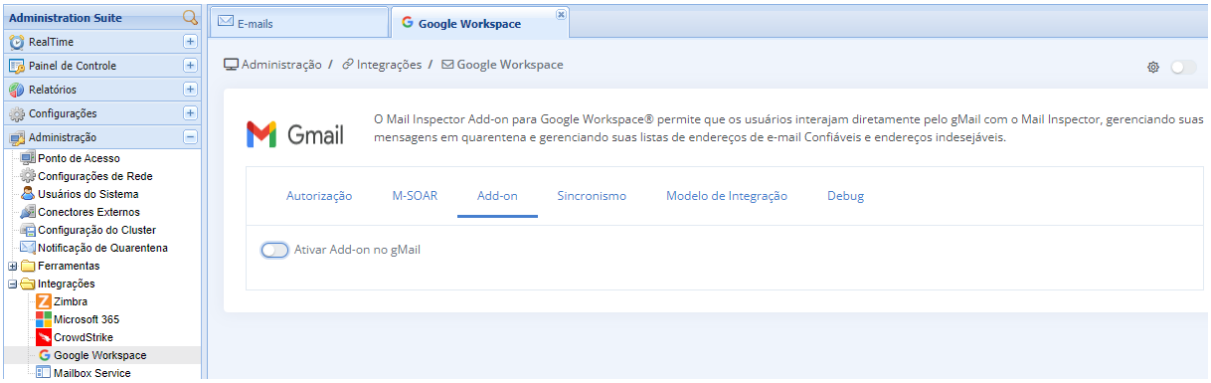
Guia Passo-a-Passo

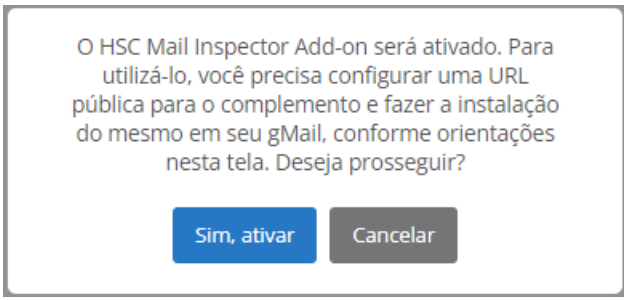
Este guia é dividido em algumas etapas que são executadas em sequência:

1. Ativação do Add-On;
2. Configuração das Ações do Usuário no Add-On e
3. Deploy para os usuários do G-Suite.

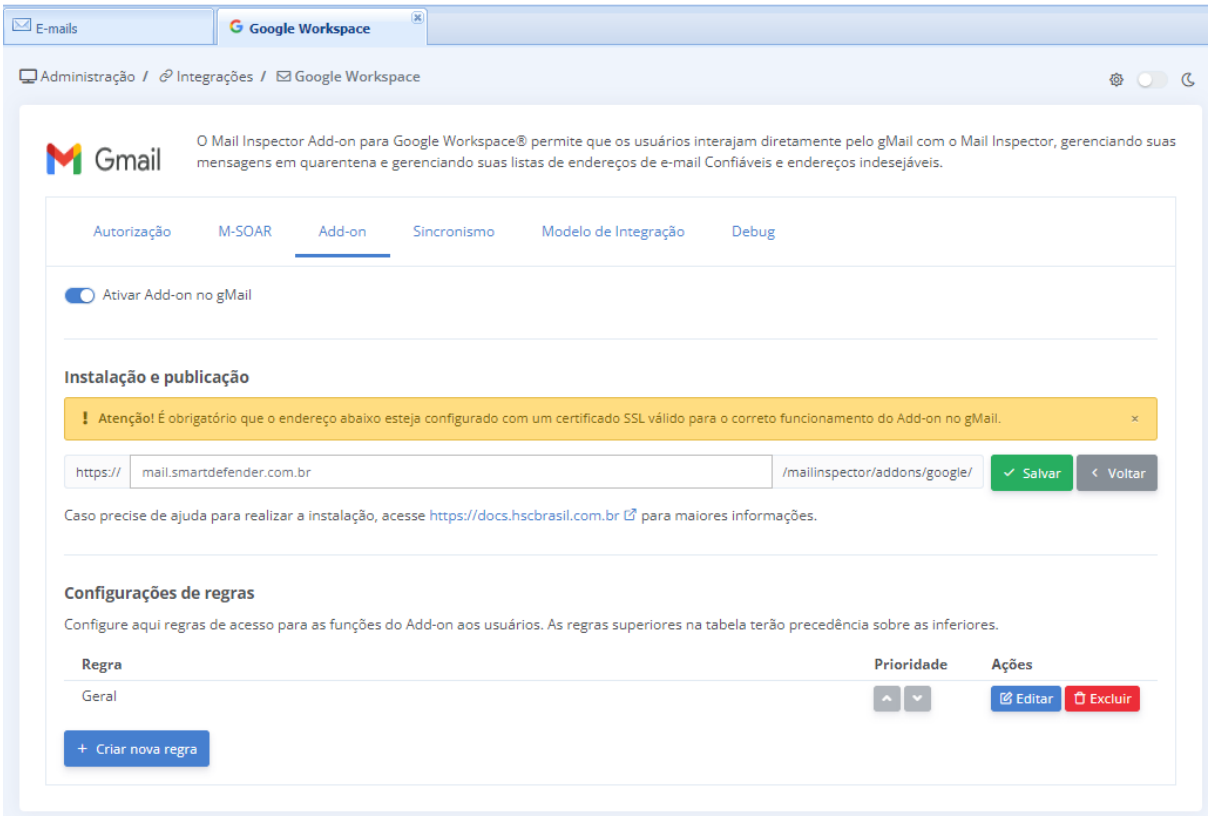
Primeira Etapa

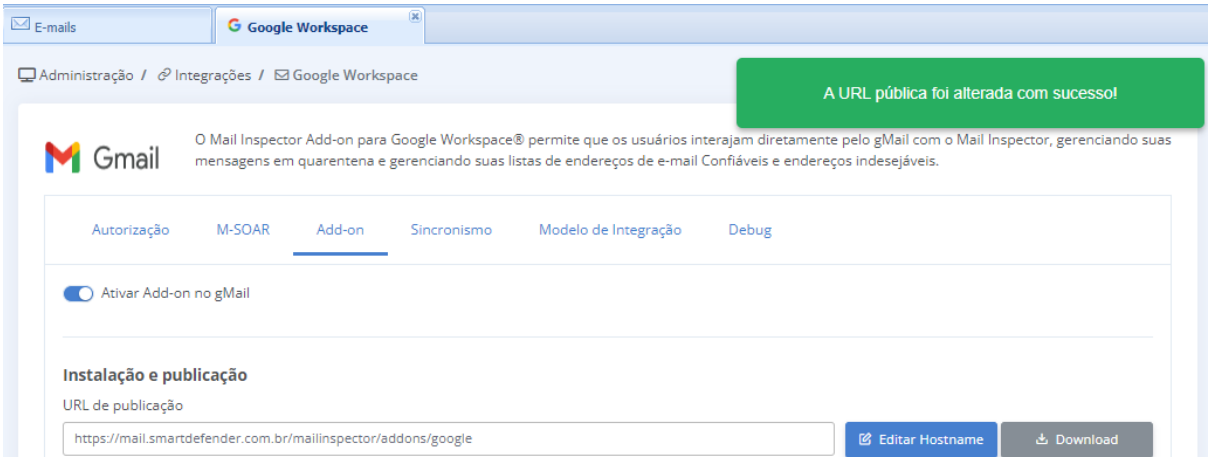
1. Vá em Administração > Integrações > Google Workspace e selecione a aba Add-On
   Ative o Add-On, pelo botão deslizante.





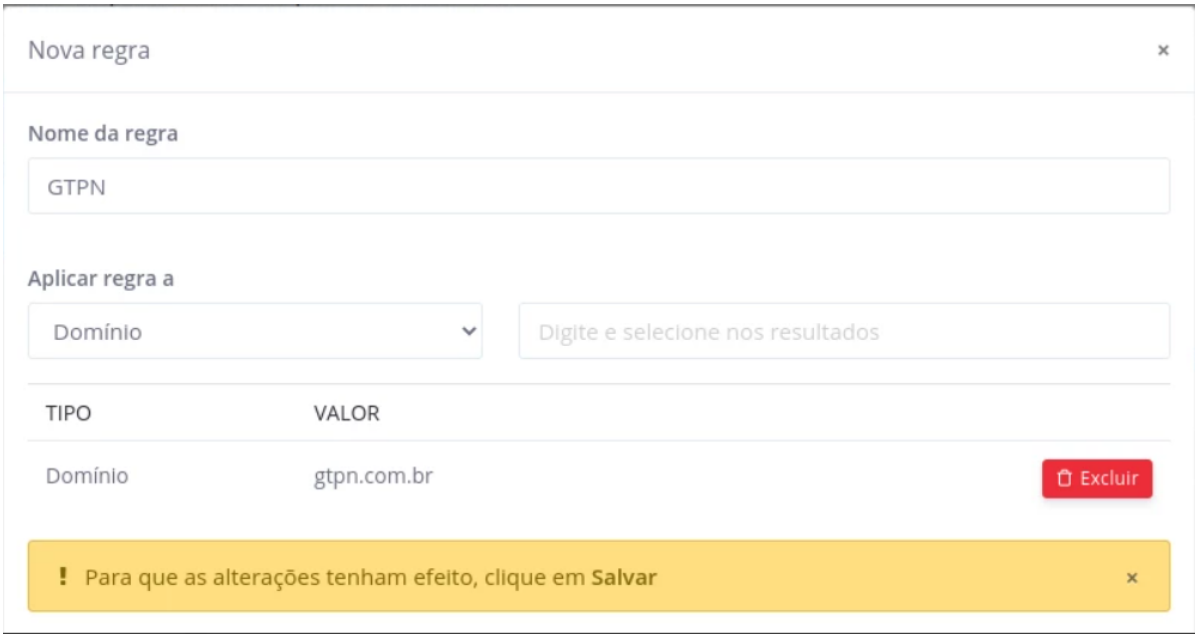
   Selecione Sim, ativar
2. Informe o FDQN do seu Mail Inspector, clique em salvar (no exemplo o que utilizamos foi o mail.smartdefender.com.br).



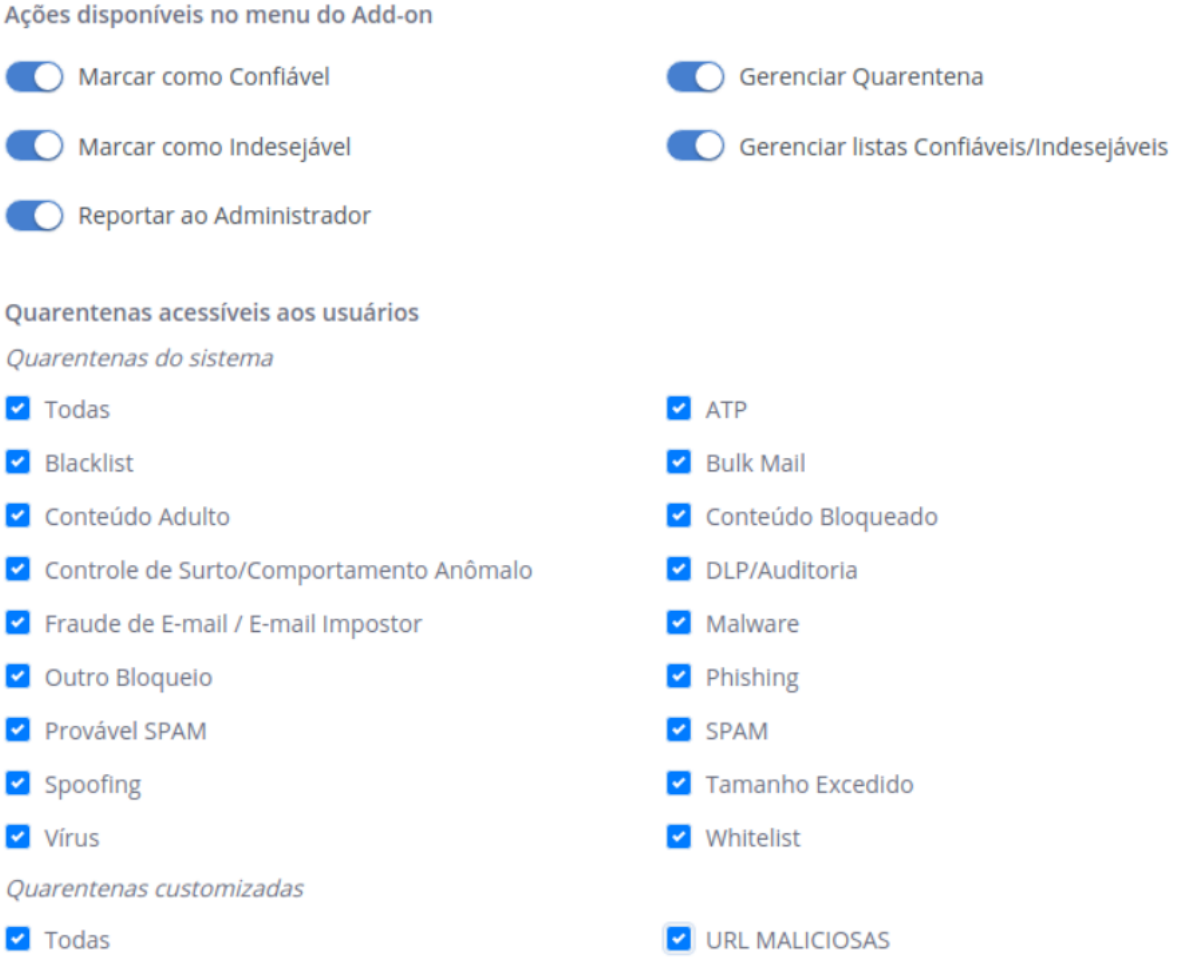


3. Configure as ações o usuário poderá executar em sua caixa de e-mail do G-Suite

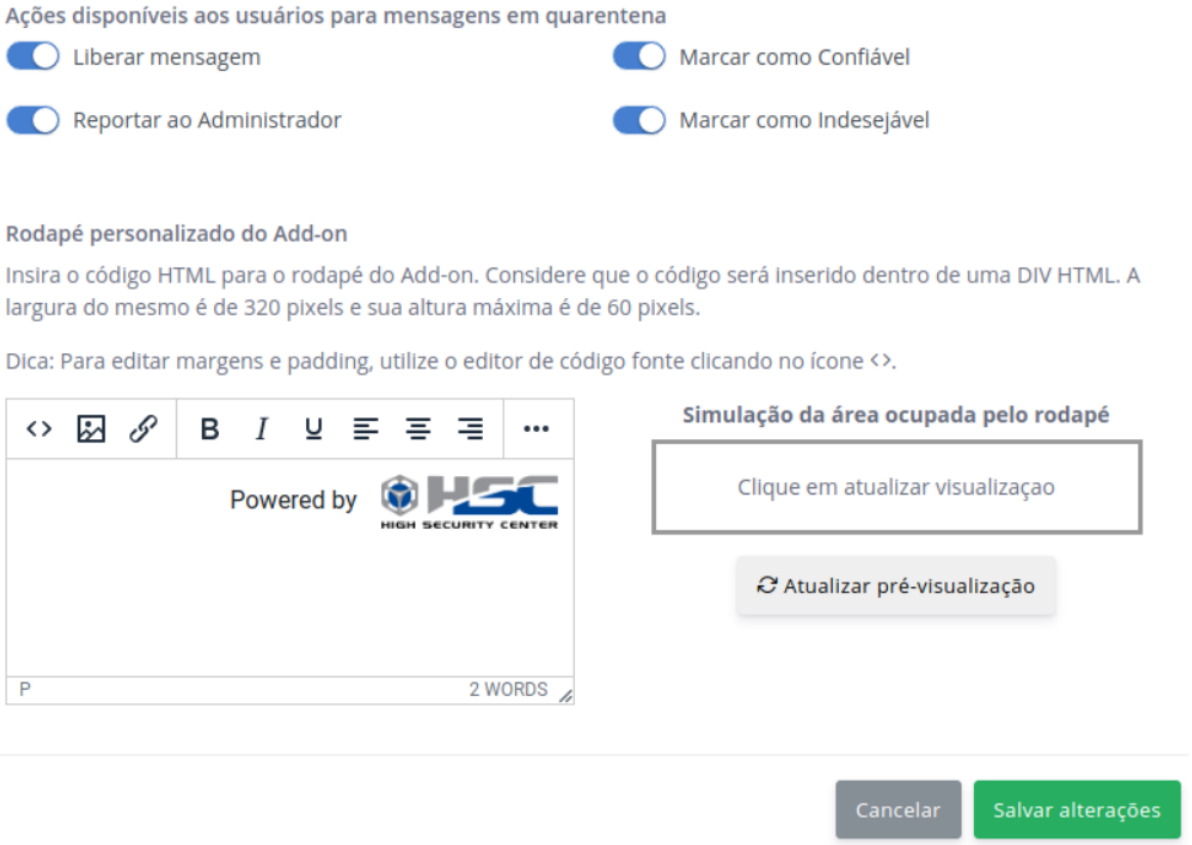
4. Edite a regra Geral ou crie uma nova regra personalizada. Será permitido aplicar regras diferentes por domínio, Grupos LDAP, Grupos de Usuários ou Usuário.



5. Determine as ações e quarentenas que serão disponibilizadas na interface do usuário do G-Suite



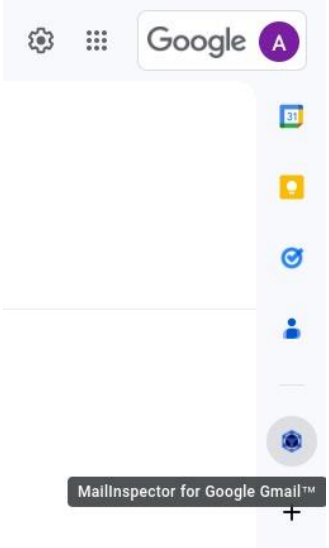
6. Determine as ações permitidas paras mensagens em quarentena. É possível personalizar o rodapé.



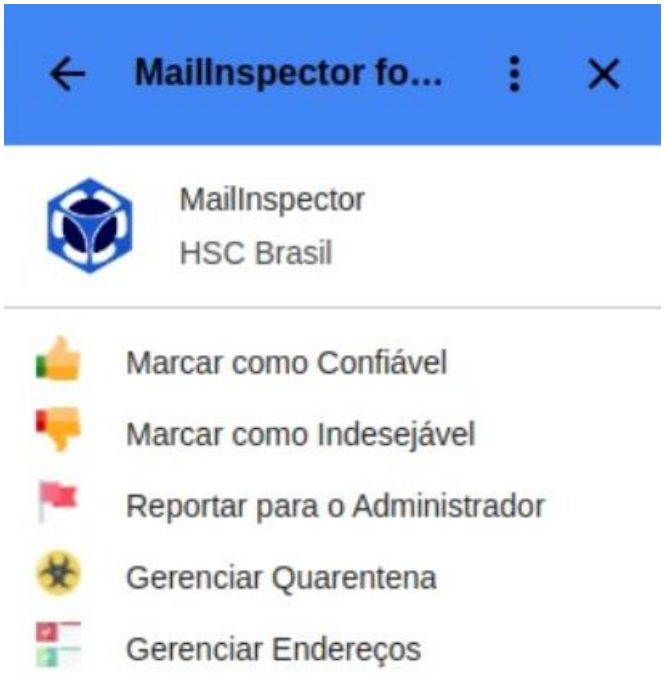
Somente é permitido ao usuário liberar mensagens em quarentena do tipo SPAM, Provável SPAM e Bulk Mail.
Não é possível liberar ameaças como vírus, malware e phishing.

Uma vez configurado o Add-On, não é necessário fazer mais nenhuma ação, pois todo o processo é automatizado.

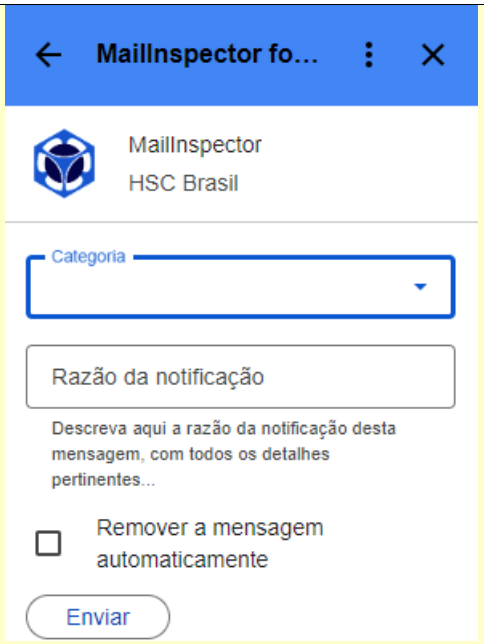
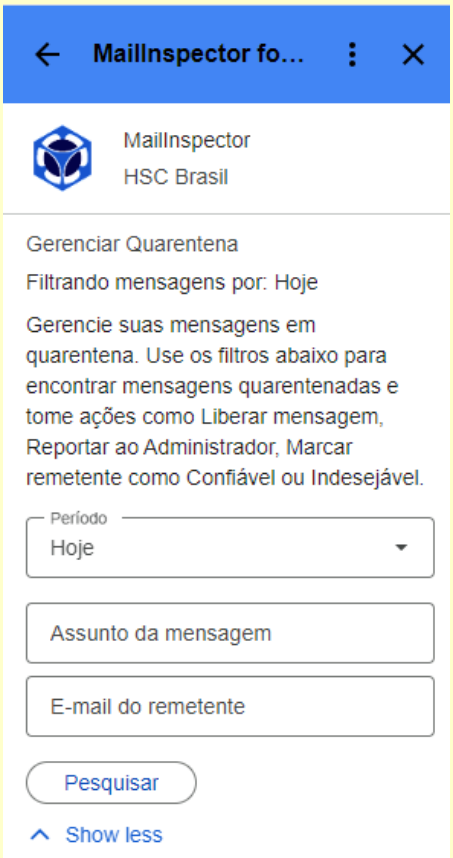
Para testar, basta acessar a sua conta G-Suite e verificar se já aparece o ícone do Add-On, conforme imagem a seguir:

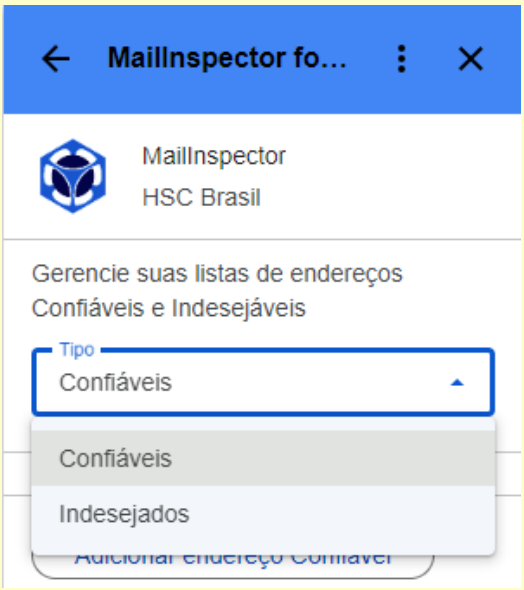


Dê um duplo clique sobre a mensagem que você deseja gerenciar e verifique as ações disponibilizadas pelo ícone do MailInspector.



Ações do Add-On	
Marcar como Confiável	Adiciona o remetente da mensagem na lista Confiável do usuário no MailInspector (Whitelist)
Marcar como Indesejável	Adiciona o remetente da mensagem na lista Indesejável do usuário no MailInspector (Blacklist)
Reportar para o Administrador	Remete uma cópia da mensagem para o Administrador do MailInspector • Como SPAM; • Como PHISHING; • Como AMEAÇA (Virus/Malware); Uma vez reportado, o sistema de Inteligência Artificial atua sobre o email, validando se é realmente o tipo de email informado pelo usuário, ao mesmo tempo em que é enviada uma cópia do email ao administrador do sistema, permitindo análise manual e ações manuais sobre ele. O sistema de Inteligência Artificial além de validar o email, faz a aprendizagem automática de acordo com a classificação do email, analisando vários pontos dele, desde conteúdo, até origem/destino, frequência de envio/recebimento, características do anexo contido no email, etc. Ainda na opção de Reportar para o Administrador, o usuário pode indicar a razão da notificação e selecionar a opção de Remover a mensagem automaticamente, dessa forma, ao enviar o email como amostra para o administrador, ele será removido automaticamente da caixa postal do usuário.

	
Gerenciar Quarentena	Permite aos usuários visualizarem as mensagens que estão retidas na sua quarentena pessoal, podendo liberar as mensagens do tipo Provável SPAM, SPAM e Bulk Mail. Ao selecionar esta opção, abre o menu de seleção de opções de: • Período; • Assunto; • E-mail do remetente. 

Gerenciar Confiáveis / Indesejáveis	Permite ao usuário adicionar ou remover registros de sua lista de remetentes: • Confiáveis; • Indesejados;  Ao selecionar uma das opções, apresenta-se a lista de usuários já registrados no MailInspector como Confiáveis e/ou Indesejados;

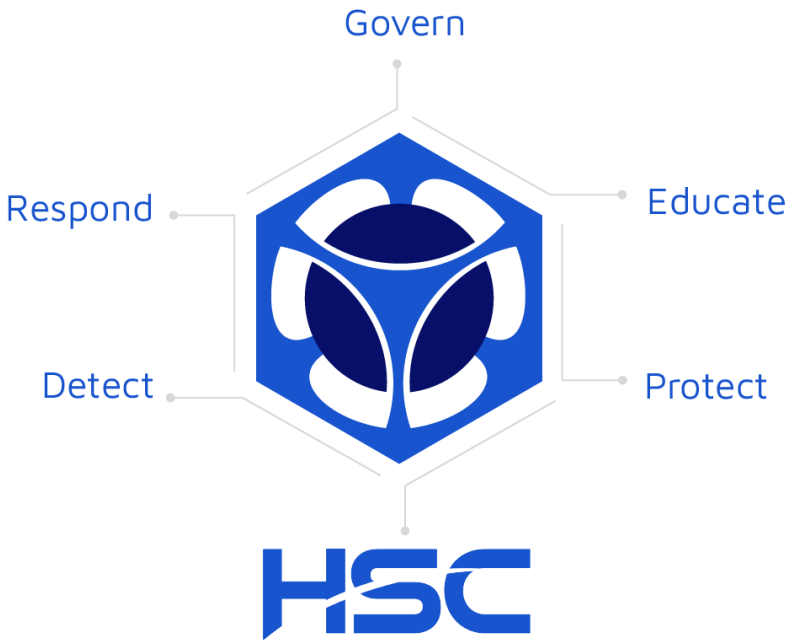
Todo o processo de Importação dos Usuários, importação de e-mails, importação de grupos, ativação de Add-On, ativação de M-SOAR, é feito através de API's, mas de modo a ficar o mais transparente possível ao administrador e aos usuários da solução.

Sobre a **HSC**

A HSC tem quase duas décadas de atuação em cibersegurança e conscientização de usuários, atendendo organizações de vários segmentos, dos setores público e privado.

Atualmente atuamos no Brasil, nos EUA e na América Latina.

Nossa experiência se reflete em números: todos os dias, protegemos mais de 10 milhões de mailboxes e filtramos mais de 100 milhões de e-mails



Material exclusivo da HSC, referente ao MailInspector.

hsclabs.com

+55 51 3500 8255