

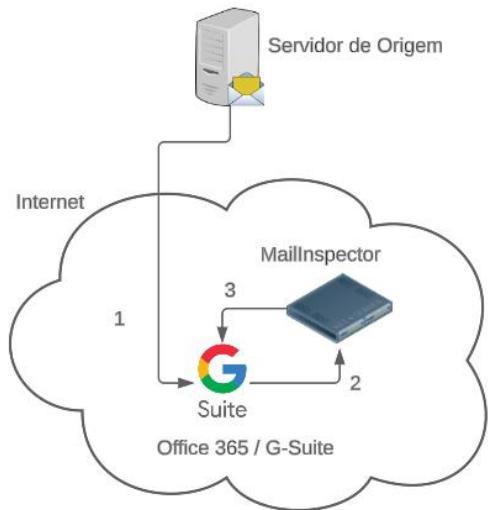
Documentação de Integração
Maillnspector V5.2 com G-Suite
sem alteração no apontamento MX/DNS

MAILINSPECTOR
powered by **HSC**

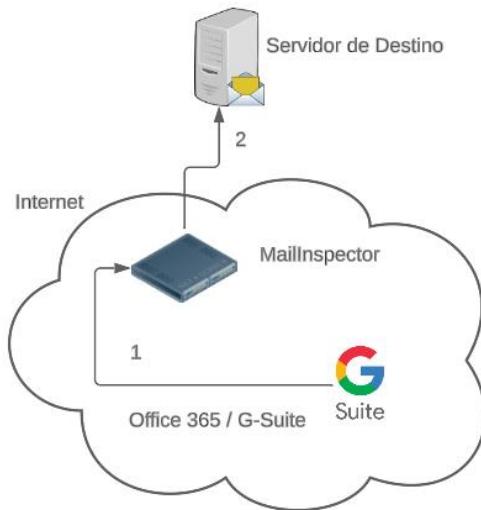
Integração MailInspector

Este documento tem por finalidade mostrar a integração do MailInspector com Office365, sem necessidade de mudança de MX e integração e importação de contas via API.

Configuração Entrada InLine para Office365 / G-Suite



Configuração Saída InLine para Office365 / G-Suite



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;

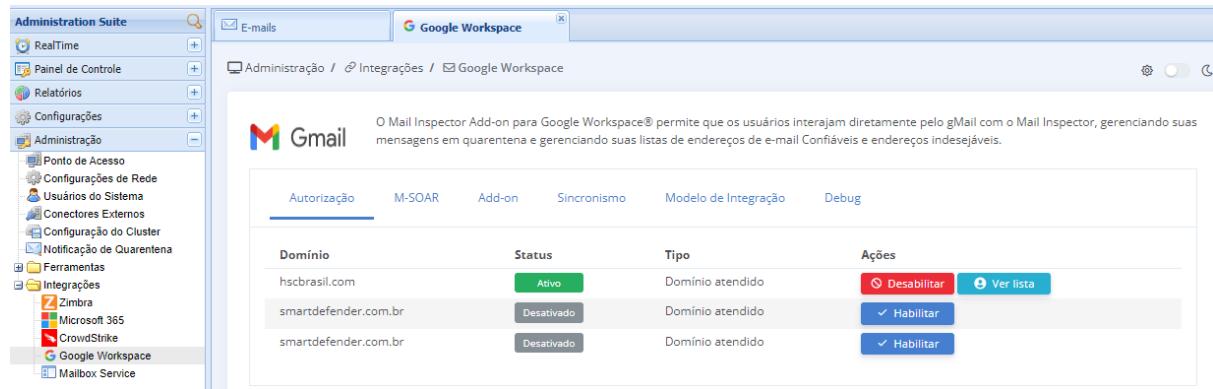
Configuração Saída InLine (sem mudança no MX) para Office365 / G-Suite

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



Domínio	Status	Tipo	Ações
hscbrasil.com	Ativo	Domínio atendido	Desabilitar Ver lista
smartdefender.com.br	Desativado	Domínio atendido	Habilitar
smartdefender.com.br	Desativado	Domínio atendido	Habilitar

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



Google Workspace
Autorização de domínio

Para a ativação do M-SOAR no domínio **hscbrasil.com** no Google, você deverá se autenticar com sua conta de administrador do domínio e autorizar que o Mail Inspector gerencie sua conta. Todas as permissões requisitadas deverão ser concedidas para o correto funcionamento da integração.

Deseja prosseguir?

Prosseguir Cancel

Atenção! Somente domínios que utilizam o serviço Google Workspace® poderão ser atendidos pelo serviço de integração do Mail Inspector.

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

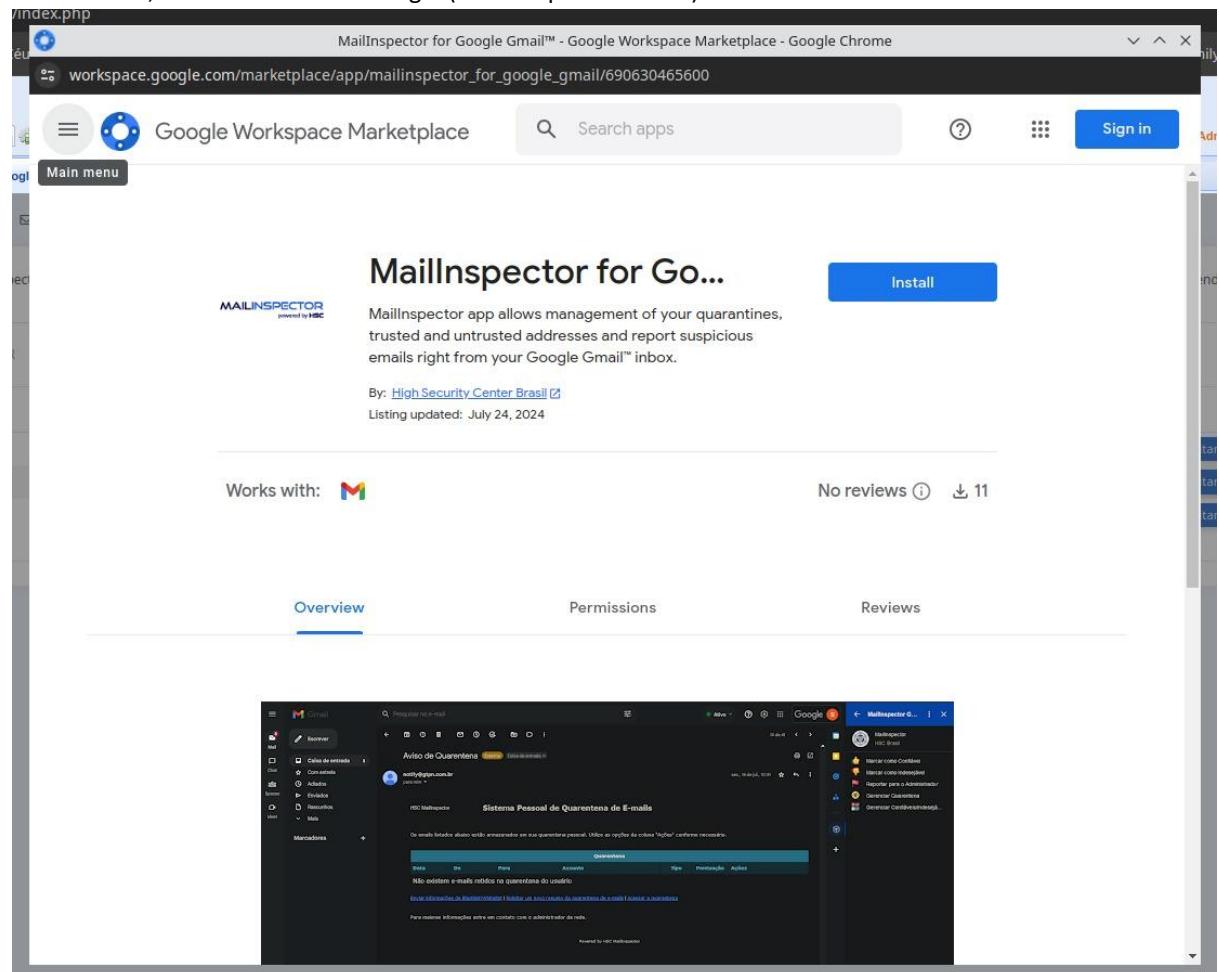


Insira o endereço de e-mail do administrador do domínio

admin@hscbrasil.com

Prosseguir Cancelar

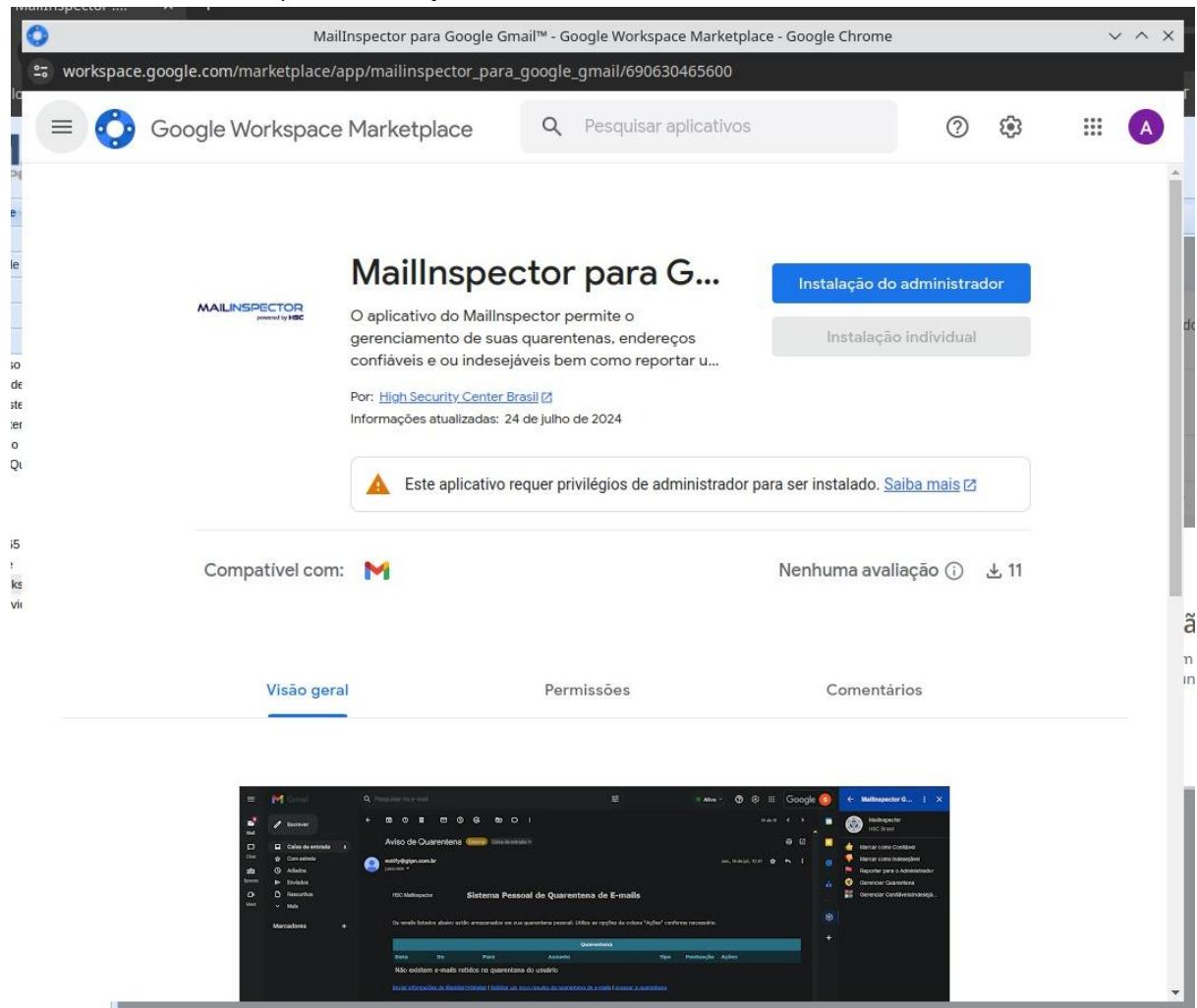
3. Ao fazer isso, será aberta a tela de login (canto superior direito).



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



MailInspector para Google Gmail™ - Google Workspace Marketplace - Google Chrome
workspace.google.com/marketplace/app/mailinspector_para_google_gmail/690630465600

Google Workspace Marketplace Pesquisar aplicativos

MailInspector para G...

MAILINSPECTOR powered by HSC

O aplicativo do MailInspector permite o gerenciamento de suas quarentenas, endereços confiáveis e ou indesejáveis bem como reportar u...

Por: [High Security Center Brasil](#)
Informações atualizadas: 24 de julho de 2024

Este aplicativo requer privilégios de administrador para ser instalado. [Saiba mais](#)

Instalação do administrador Instalação individual

Compatível com: Gmail Nenhuma avaliação 11

Visão geral Permissões Comentários

Sistema Pessoal de Quarentena de E-mails

Este aplicativo adiciona uma nova interface de usuário para gerenciar e-mails recebidos em sua caixa de entrada. Utilize as regras de quarentena "HighRisk" conforme necessário.

Quarentena

Destinatário Re Envio Prioridade Assunto

Não existem e-mails na quarentena do usuário.

MailInspector para Google Gmail

MailInspector para Google Gmail

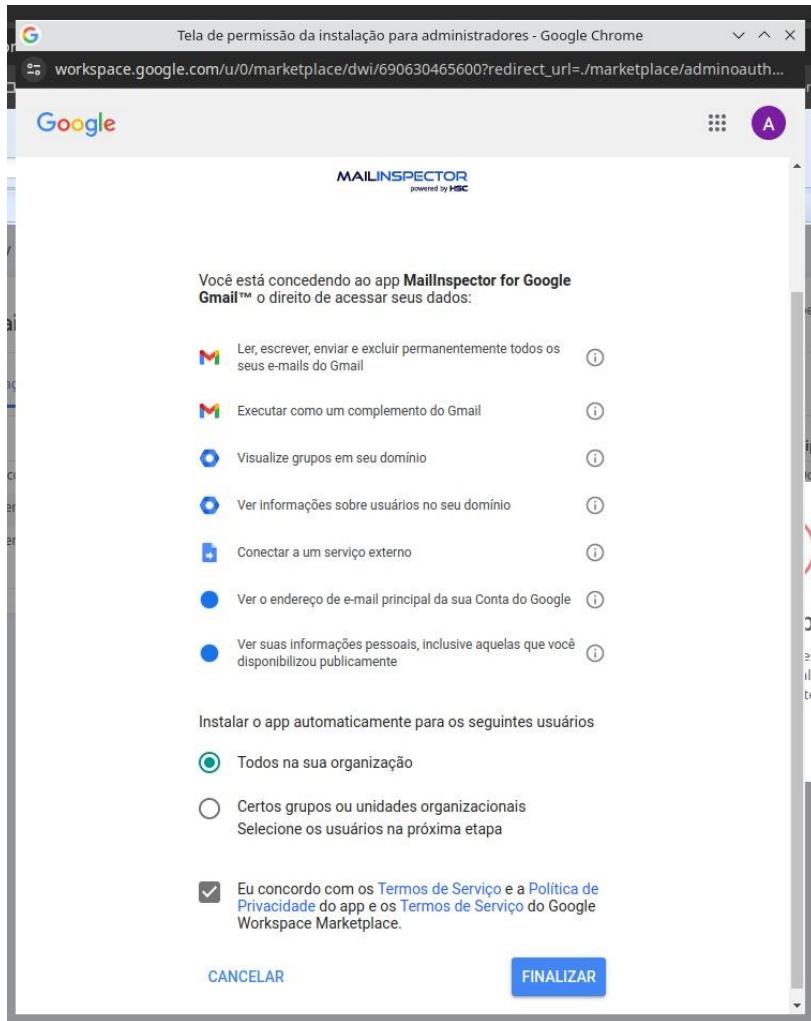
Manter como Confidencial Manter como Indisponível Desmarcar como Indisponível Desmarcar como Confidencial Desmarcar como Indisponível Desmarcar como Confidencial

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

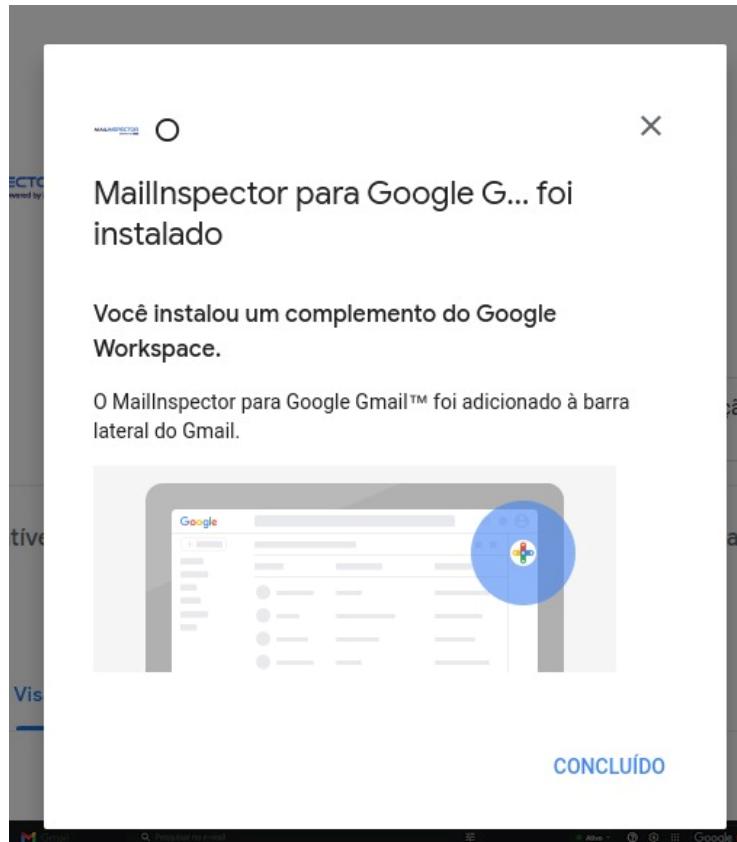


6. Será apresentada a tela de concordância com os termos de uso, bem como indicação das permissões necessárias para a integração do MailInspector com o G-Suite. Marque o box de Eu concordo com os Termos de Serviço e Política de Privacidade do app e os Termos de Serviço do Google Workspace Marketplace.

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 para 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.



Autorização M-SOAR Add-on Sincronismo **Modelo de Integração** Debug

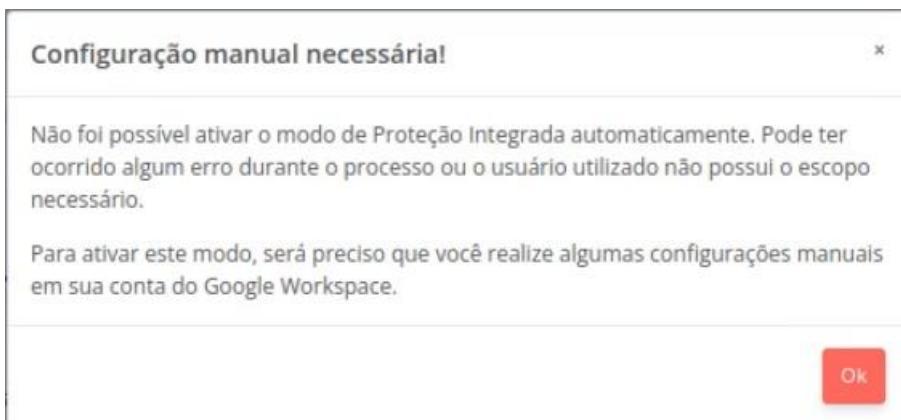
Gateway de Entrada
Neste modelo o Mail Inspector recebe o e-mail diretamente. É necessário modificar o registro MX do domínio.

Proteção Integrada **Ativar proteção**
Neste modelo a proteção é realizada através de API sem a necessidade de se alterar a configuração do MX.

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).



Configuração manual necessária!

Não foi possível ativar o modo de Proteção Integrada automaticamente. Pode ter ocorrido algum erro durante o processo ou o usuário utilizado não possui o escopo necessário.

Para ativar este modo, será preciso que você realize algumas configurações manualmente em sua conta do Google Workspace.

Ok

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

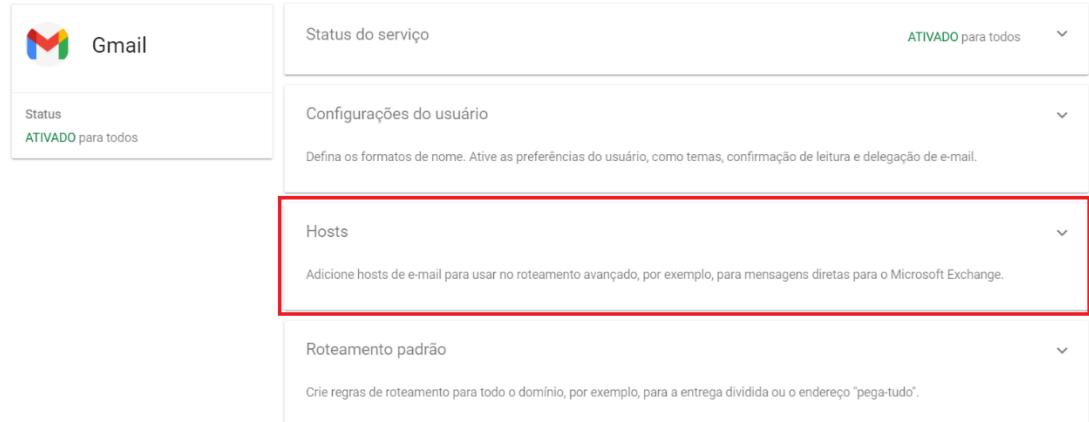
Etapa 1: Adicionar os nodes de filtragem

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



The screenshot shows the Google Admin Console interface. The left sidebar has a 'Admin' icon and a 'Gmail' tab highlighted. The main content area shows the 'Gmail' settings page. The 'Hosts' section is highlighted with a red box. The 'Hosts' section contains the following text: 'Adicione hosts de e-mail para usar no roteamento avançado, por exemplo, para mensagens diretas para o Microsoft Exchange.'

3. Clique em Hosts.



The screenshot shows the 'Hosts' section of the Gmail settings page. The 'Hosts' section is highlighted with a red box. It contains the following text: 'Adicione hosts de e-mail para usar no roteamento avançado, por exemplo, para mensagens diretas para o Microsoft Exchange.'

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.

Adicionar rota de e-mail

Nome	Saiba mais	
MLI	Este campo é obrigatório.	
1. Especifique o servidor de e-mail		
Somente as portas com os números 25, 587 e de 1024 até 65535 são permitidas.		
Múltiplos hosts ▾		
Principal	Carregar %	Ações
187.108.197.102 : 25	100	Excluir
187.108.197.103 : 25	100	Excluir
187.45.183.226 : 25	100	Excluir

[CANCELAR](#) [SALVAR](#)

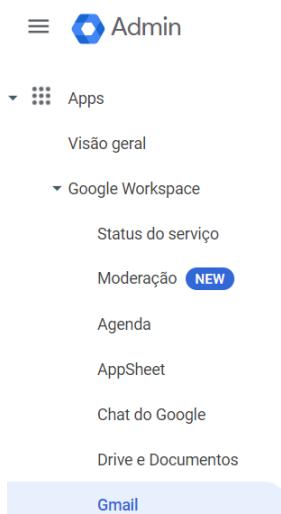
Repare que adicionei vários principais, não usamos os secundários.

Obs: Também é possível usar HOSTNAME por exemplo: **mx-balancer.mlicloud.com** em vez de IP.

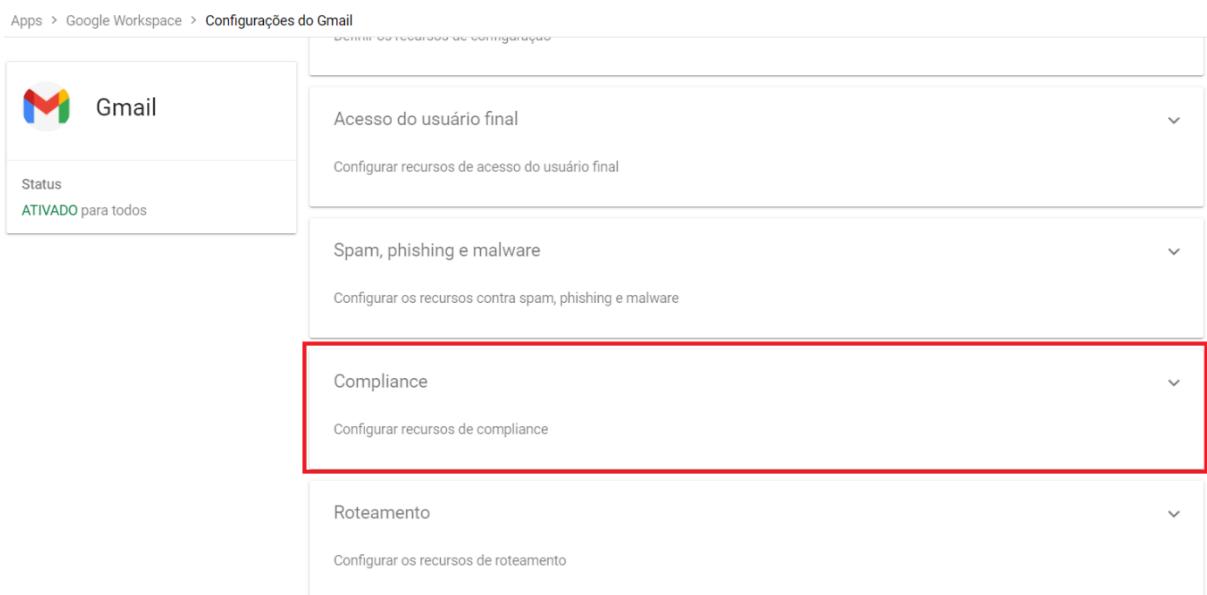
7. Digite o número das portas como 25 e 100% em carregar, para todas os nodes incluídos.
8. Em Opções, **desmarque** a caixa de seleção - Exigir um certificado assinado pela autoridade de certificação (recomendado).
9. Clique em Salvar.

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



The screenshot shows the 'Configurações do Gmail' (Gmail settings) page in the Google Workspace Admin Console. On the left, there's a sidebar with the Gmail logo and a status box indicating 'ATIVADO para todos' (Enabled for everyone). The main area contains several sections: 'Acesso do usuário final' (User access), 'Spam, phishing e malware' (Spam, phishing and malware), 'Compliance' (highlighted with a red box), and 'Roteamento' (Routing). Each section has a 'Configurar recursos' (Configure resources) link below it.

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.

Editar configuração

Correspondência de metadados

Atributo

IP de origem

Tipo de correspondência

O IP de origem não está dentro do intervalo

131.100.228.146/25

CANCELAR SALVAR

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

3. O que fazer se as expressões acima corresponderem

Modificar mensagem

Cabeçalhos

- Adicionar cabeçalho X-Gm-Original-To
- Adicionar os cabeçalhos X-Gm-Spam e X-Gm-Phishy
- Adicionar cabeçalhos personalizados

Cabeçalhos personalizados

X-MLI-Inbound: 1

ADICIONAR

Assunto

- Adicionar assunto personalizado

Rota

- Alterar rota

- Também redirecionar spam

- Suprimir rejeições deste destinatário

MLI (mail.smartdefender.com.br) ▾

Roteamento normal

Destin

MLI (mail.smartdefender.com.br)

- Alterar destinatário do envelope

Spam

- Ignorar o filtro de spam para esta 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

Destinatário do envelope

- Alterar destinatário do envelope

Spam

- Ignorar o filtro de spam para esta mensagem

Anexos

- Remover anexos da mensagem

Entregar também a

- Adicionar mais destinatários

Criptografia (apenas para a entrega de agora em diante)

- Exigir transporte seguro (TLS)

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

1. Mensagens de e-mail afetadas

- Recebidas
- Enviadas
- Interno - enviando
- Interno - recebendo

2. 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

[ADICIONAR](#)

Correspondência de conteúdo avançado ▾

Local

Cabeçalhos completos ▾

Tipo de correspondência

Não contém texto ▾

Conteúdo

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

3. O que fazer se as expressões acima corresponderem

Modificar mensagem ▾

Cabeçalhos

Adicionar cabeçalho X-Gm-Original-To

Adicionar os cabeçalhos X-Gm-Spam e X-Gm-Phishy

Adicionar cabeçalhos personalizados

Cabeçalhos personalizados

X-MLI-Internal: 1

ADICIONAR

Assunto

Adicionar assunto personalizado

Regra Outbound

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

Compliance do conteúdo

[Saiba mais](#)

Outbound

1. Mensagens de e-mail afetadas

- Recebidas
- Enviadas
- Interno - enviando
- Interno - recebendo

2. 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

3. O que fazer se as expressões acima corresponderem

Modificar mensagem ▾

Cabeçalhos

- Adicionar cabeçalho X-Gm-Original-To
- Adicionar os cabeçalhos X-Gm-Spam e X-Gm-Phishy
- Adicionar cabeçalhos personalizados

Cabeçalhos personalizados

X-MLI-Outbound: 1

[ADICIONAR](#)

Assunto

- Adicionar assunto personalizado

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

- Alterar rota
- Também redirecionar spam
- Suprimir rejeições deste destinatário

MLI (mail.smartdefender.com.br) ▾

Destinatário do envelope

- Alterar destinatário do envelope

Spam

- Ignorar o filtro de spam para esta mensagem

Anexos

- Remover anexos da mensagem

5. Clique em Salvar

Comunicação segura entre MailInspector e Microsoft 365 / G-Suite

Verifique se está ativado o protocolo TLS no MailInspector.

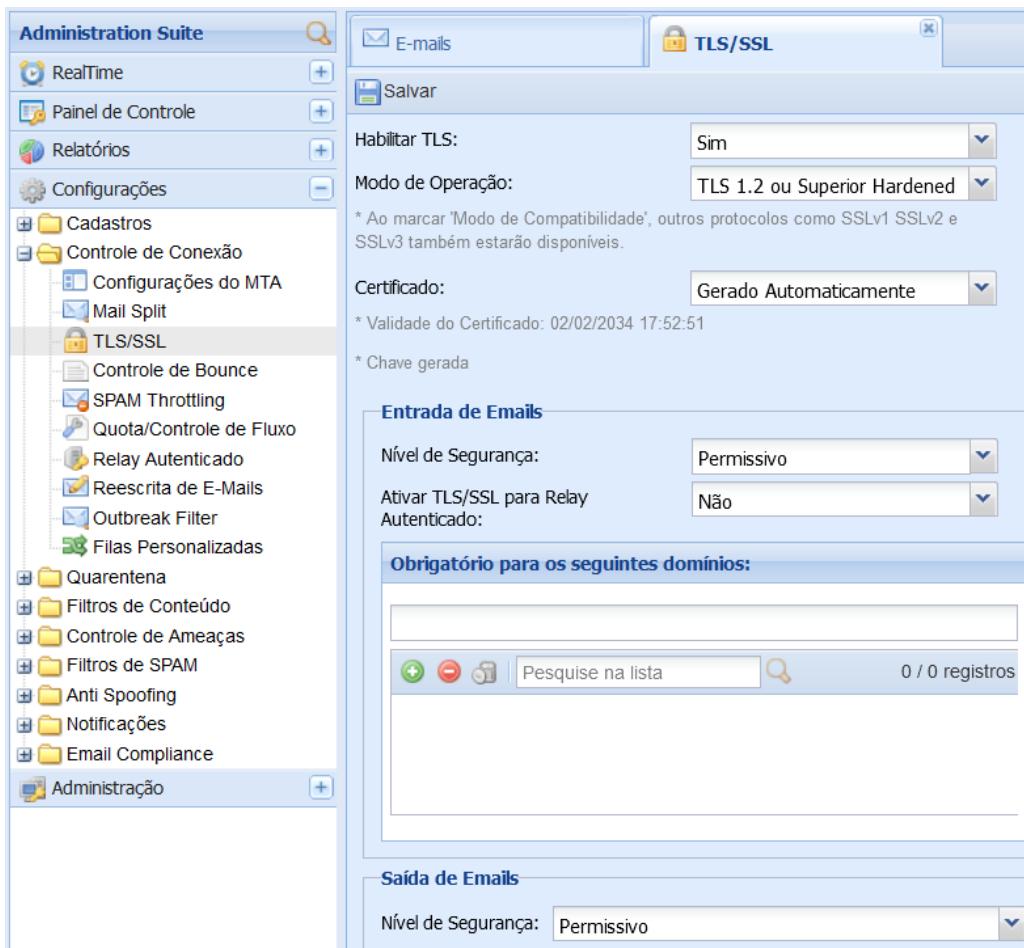
É necessário que esteja habilitado e configurado no modo de operação TLS 1.2 ou Superior Hardened. As outras versões foram mantidas por questão de compatibilidade, mas oferecem menor segurança, não sendo recomendado o uso delas.

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.

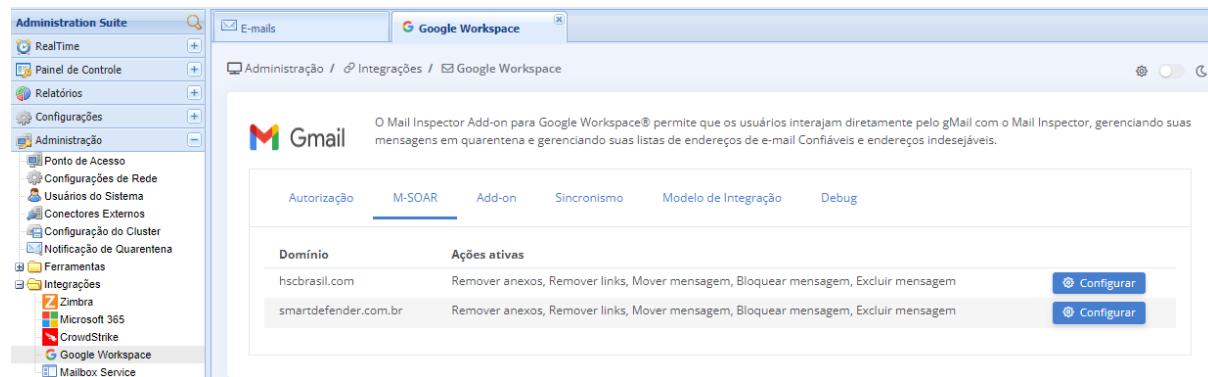
TLS v1.2	Cifra		Order	Strength
TLS 1.2 ou Superior	xc030	ECDHE-RSA-AES256-GCM- SHA384	ECDH	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Hardened	x9f	DHE-RSA-AES256-GCM-SHA384	DH	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Configuração de Orquestração (M-SOAR)

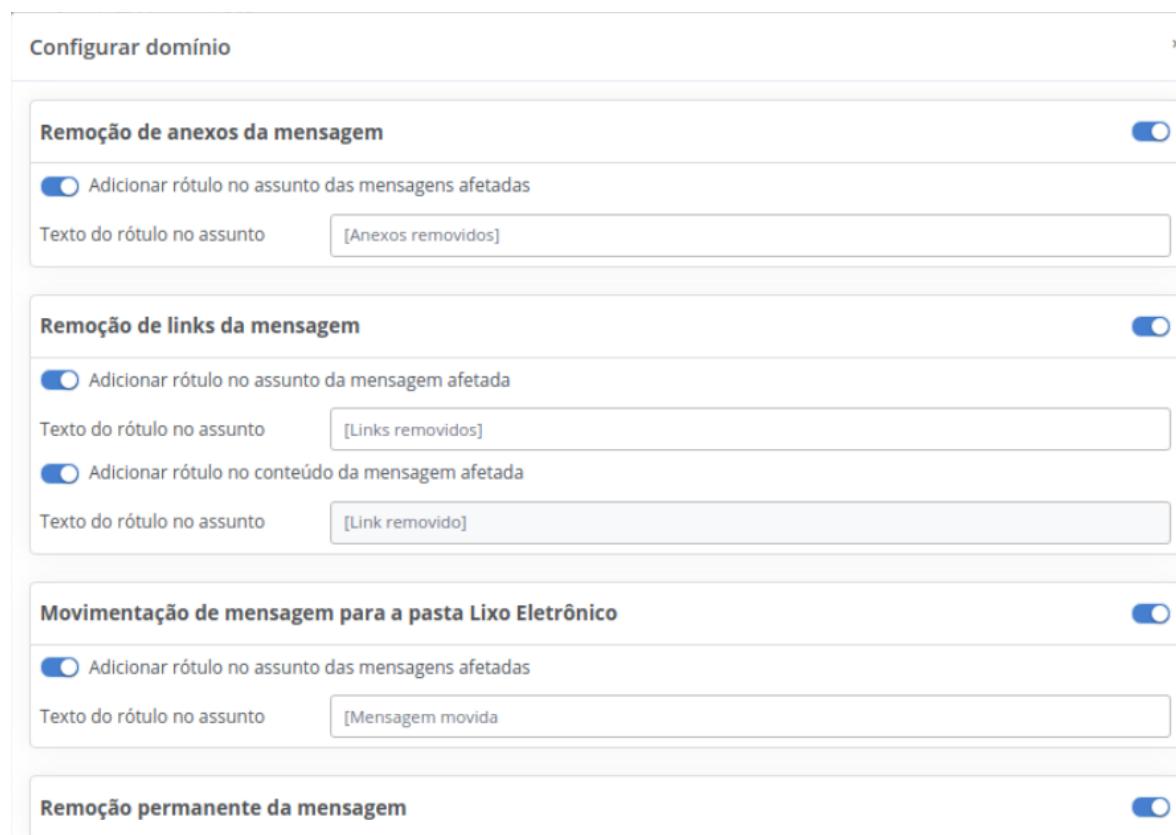
Configuração do M-SOAR permite personalizar quais ações o Administrador do MailInspector poderá efetuar em tempo real na caixa de e-mail do usuário do G-Suite (diretamente na caixa da conta Google do usuário).

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.



The screenshot shows the 'Administration Suite' interface with 'Integrations' selected. The main panel is for 'Gmail' with two domains listed: 'hscbrasil.com' and 'smartdefender.com.br'. Each domain has a list of active actions: 'Remover anexos, Remover links, Mover mensagem, Bloquear mensagem, Excluir mensagem'. There are 'Configurar' buttons next to each domain entry.



The 'Configurar domínio' interface has four sections:

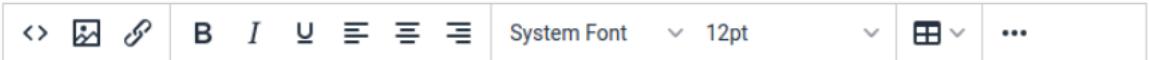
- Remoção de anexos da mensagem:**
 - Enabled switch:
 - Option: Adicionar rótulo no assunto das mensagens afetadas
 - Text input: Texto do rótulo no assunto [Anexos removidos]
- Remoção de links da mensagem:**
 - Enabled switch:
 - Option: Adicionar rótulo no assunto da mensagem afetada
 - Text input: Texto do rótulo no assunto [Links removidos]
 - Option: Adicionar rótulo no conteúdo da mensagem afetada
 - Text input: Texto do rótulo no assunto [Link removido]
- Movimentação de mensagem para a pasta Lixo Eletrônico:**
 - Enabled switch:
 - Option: Adicionar rótulo no assunto das mensagens afetadas
 - Text input: Texto do rótulo no assunto [Mensagem movida]
- Remoção permanente da mensagem:**
 - Enabled switch:

Bloqueio de conteúdo da mensagem

Adicionar rótulo no assunto das mensagens afetadas

Texto do rótulo no assunto

Substituir o conteúdo original da mensagem por:

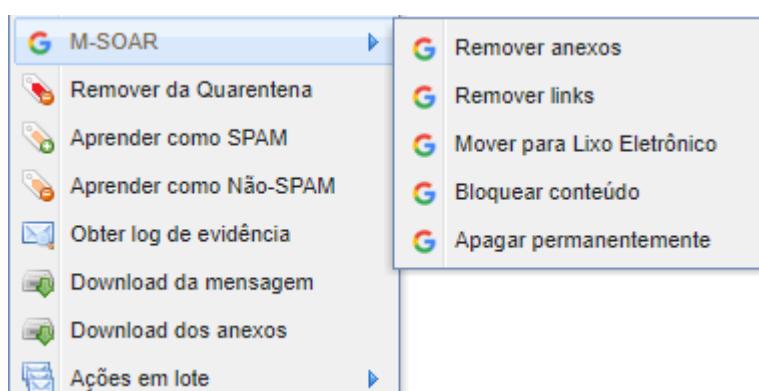


O conteúdo desta mensagem foi bloqueado pelo administrador.

P 8 WORDS 

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 e-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)

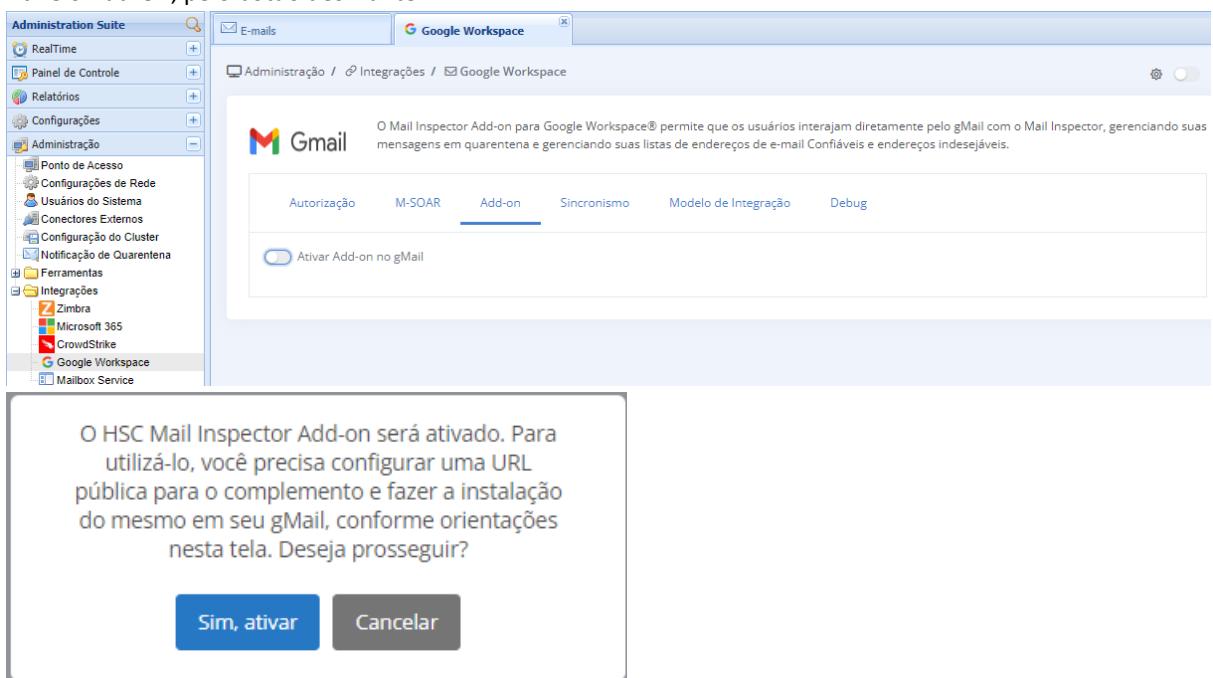
Guia Passo-a-Passo

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 > Interações > 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).

E-mails Google Workspace

Administração / Integrações / Google Workspace

Gmail O Mail Inspector Add-on para Google Workspace® permite que os usuários interajam diretamente pelo gMail com o Mail Inspector, gerenciando suas mensagens em quarentena e gerenciando suas listas de endereços de e-mail Confiáveis e endereços indesejáveis.

Autorização **M-SOAR** **Add-on** **Sincronismo** **Modelo de Integração** **Debug**

Ativar Add-on no gMail

Instalação e publicação

Atenção! É obrigatório que o endereço abaixo esteja configurado com um certificado SSL válido para o correto funcionamento do Add-on no gMail.

https:// mail.smartdefender.com.br /mailinspector/addons/google/ Salvar Voltar

Caso precise de ajuda para realizar a instalação, acesse <https://docs.hscbrasil.com.br> para maiores informações.

Configurações de regras

Configure aqui regras de acesso para as funções do Add-on aos usuários. As regras superiores na tabela terão precedência sobre as inferiores.

Regra	Prioridade	Ações
Geral		<input type="button"/> Editar <input type="button"/> Excluir

Criar nova regra

E-mails Google Workspace

Administração / Integrações / Google Workspace

Gmail O Mail Inspector Add-on para Google Workspace® permite que os usuários interajam diretamente pelo gMail com o Mail Inspector, gerenciando suas mensagens em quarentena e gerenciando suas listas de endereços de e-mail Confiáveis e endereços indesejáveis.

Autorização **M-SOAR** **Add-on** **Sincronismo** **Modelo de Integração** **Debug**

Ativar Add-on no gMail

Instalação e publicação

URL de publicação

https://mail.smartdefender.com.br/mailinspector/addons/google/ Editar Hostname Download

A URL pública foi alterada com sucesso!

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

Configurações de regras

Configure aqui regras de acesso para as funções do Add-on aos usuários. As regras superiores na tabela terão precedência sobre as inferiores.

Regra	Prioridade	Ações
Geral		<input type="button"/> Editar <input type="button"/> Excluir

Criar nova regra

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.

Nova regra

Nome da regra
GTPN

Aplicar regra a

Domínio

TIPO	VALOR	
Domínio	gtpn.com.br	<input type="button" value="Excluir"/>

! Para que as alterações tenham efeito, clique em Salvar

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

[Ações disponíveis no menu do Add-on](#)

- | | |
|--|---|
| <input checked="" type="radio"/> Marcar como Conflável | <input checked="" type="radio"/> Gerenciar Quarentena |
| <input checked="" type="radio"/> Marcar como Indesejável | <input checked="" type="radio"/> Gerenciar listas Confláveis/Indesejáveis |
| <input checked="" type="radio"/> Reportar ao Administrador | |

Quarentenas acessíveis aos usuários

Quarentenas do sistema

- | | |
|---|--|
| <input checked="" type="checkbox"/> Todas | <input checked="" type="checkbox"/> ATP |
| <input checked="" type="checkbox"/> Blacklist | <input checked="" type="checkbox"/> Bulk Mail |
| <input checked="" type="checkbox"/> Conteúdo Adulto | <input checked="" type="checkbox"/> Conteúdo Bloqueado |
| <input checked="" type="checkbox"/> Controle de Surto/Comportamento Anômalo | <input checked="" type="checkbox"/> DLP/Auditória |
| <input checked="" type="checkbox"/> Fraude de E-mail / E-mail Impostor | <input checked="" type="checkbox"/> Malware |
| <input checked="" type="checkbox"/> Outro Bloqueio | <input checked="" type="checkbox"/> Phishing |
| <input checked="" type="checkbox"/> Provável SPAM | <input checked="" type="checkbox"/> SPAM |
| <input checked="" type="checkbox"/> Spoofing | <input checked="" type="checkbox"/> Tamanho Excedido |
| <input checked="" type="checkbox"/> Vírus | <input checked="" type="checkbox"/> Whitelist |

Quarentenas customizadas

- | | |
|---|--|
| <input checked="" type="checkbox"/> Todas | <input checked="" type="checkbox"/> URL MALICIOSAS |
|---|--|

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

Ações disponíveis aos usuários para mensagens em quarentena

Liberar mensagem

Marcar como Confiável

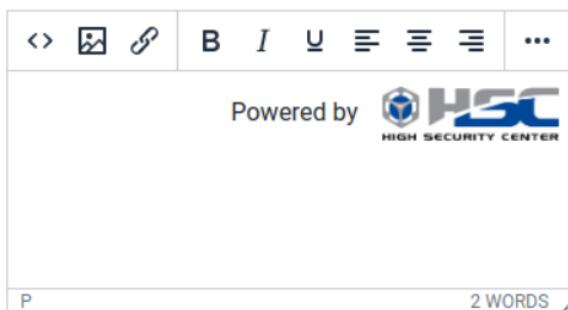
Reportar ao Administrador

Marcar como Indesejável

Rodapé personalizado do Add-on

Insira o código HTML para o rodapé do Add-on. Considere que o código será inserido dentro de uma DIV HTML. A largura do mesmo é de 320 pixels e sua altura máxima é de 60 pixels.

Dica: Para editar margens e padding, utilize o editor de código fonte clicando no ícone <>.



Simulação da área ocupada pelo rodapé

Clique em atualizar visualização

Atualizar pré-visualização

Cancelar

Salvar alterações

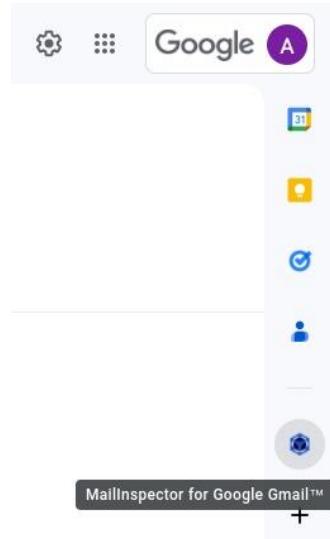


Somente é permitido ao usuário liberar mensagens em quarentena do tipo SPAM, Provável SPAM e Bulk Mail.

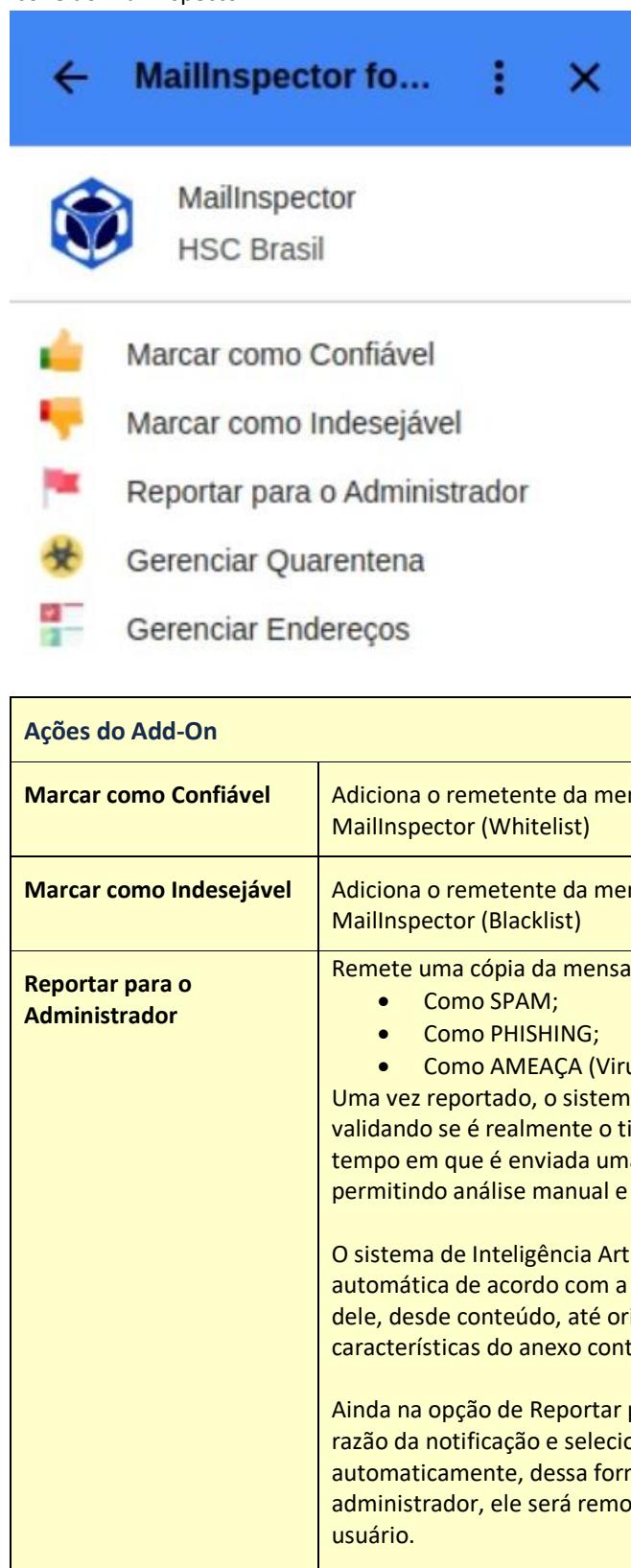
Não é possível liberar ameaças como vírus, malware e phishing.

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:

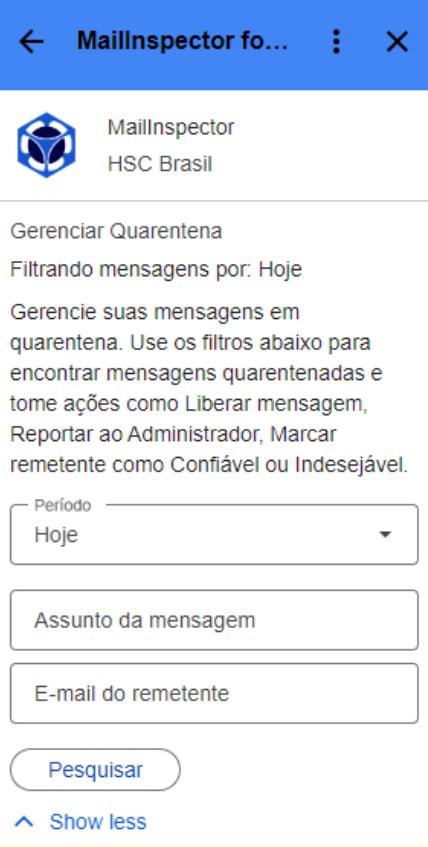


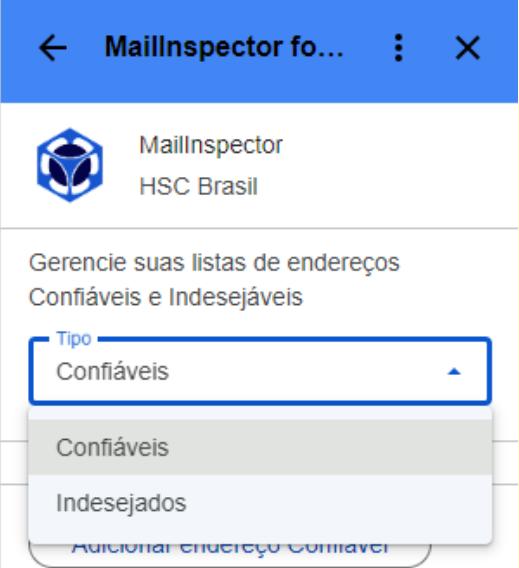
Dê um duplo clique sobre a mensagem que você deseja gerenciar e verifique as ações disponibilizadas pelo ícone do MailInspector.



The screenshot shows a blue header bar with a back arrow, the text 'MailInspector fo...', a vertical ellipsis, and a close 'X' button. Below the header, there is a logo for 'MailInspector' with a blue and white geometric design, and the text 'HSC Brasil'. A horizontal line separates this from a list of actions. The actions are listed with icons: a thumbs up for 'Marcar como Confiável', a thumbs down for 'Marcar como Indesejável', a flag for 'Reportar para o Administrador', a star for 'Gerenciar Quarentena', and a mail icon for 'Gerenciar Endereços'.

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	<p>Remete uma cópia da mensagem para o Administrador do MailInspector</p> <ul style="list-style-type: none">• Como SPAM;• Como PHISHING;• Como AMEAÇA (Virus/Malware); <p>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.</p> <p>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.</p> <p>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.</p>

	 <p>MaillInspector HSC Brasil</p> <p>Categoria</p> <p>Razão da notificação</p> <p>Descreva aqui a razão da notificação desta mensagem, com todos os detalhes pertinentes...</p> <p><input type="checkbox"/> Remover a mensagem automaticamente</p> <p>Enviar</p>
Gerenciar Quarentena	<p>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.</p> <p>Ao selecionar esta opção, abre o menu de seleção de opções de:</p> <ul style="list-style-type: none"> • Período; • Assunto; • E-mail do remetente.  <p>Gerenciar Quarentena</p> <p>Filtrando mensagens por: Hoje</p> <p>Gerencie suas mensagens em quarentena. Use os filtros abaixo para encontrar mensagens quarentenadas e tome ações como Liberar mensagem, Reportar ao Administrador, Marcar remetente como Confiável ou Indesejável.</p> <p>Período</p> <p>Hoje</p> <p>Assunto da mensagem</p> <p>E-mail do remetente</p> <p>Pesquisar</p> <p>Show less</p>

Gerenciar Confiáveis / Indesejáveis	<p>Permite ao usuário adicionar ou remover registros de sua lista de remetentes:</p> <ul style="list-style-type: none"> • Confiáveis; • Indesejados;  <p>Ao selecionar uma das opções, apresenta-se a lista de usuários já registrados no MailInspector como Confiáveis e/ou Indesejados;</p>
--	---



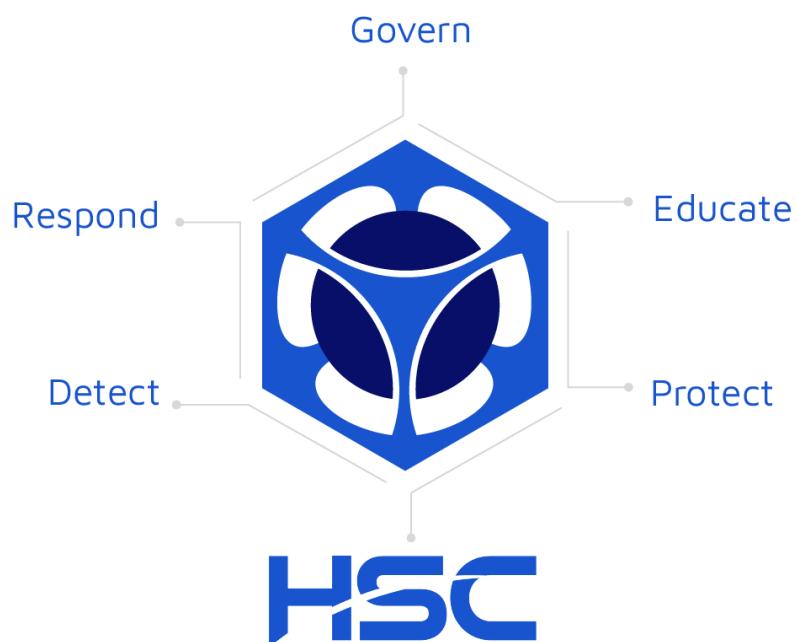
Todo o processo de Importação dos Usuários, importação de e-mails, importação de grupos, ativação de Add-On, ativação de M-SOAR, é feito através de API's, mas de modo a ficar o mais transparente possível ao administrador e aos usuários da solução.

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.

Copyright © 2024 HSC.
Não copie sem permissão.



hsclabs.com

+55 51 3500 8255