

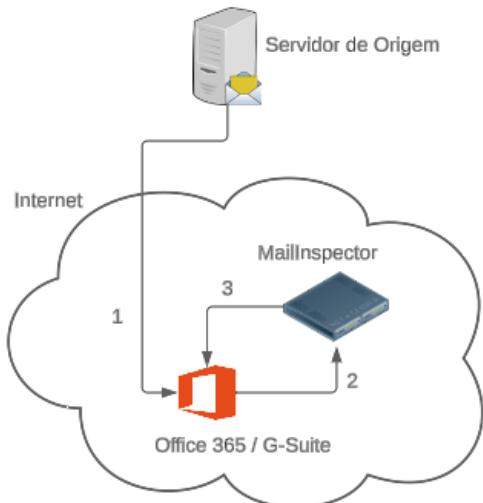
Documentação de Integração
MailInspector V5.2 com Microsoft Office365
sem alteração no apontamento MX/DNS

MAILINSPECTOR
powered by **HSC**

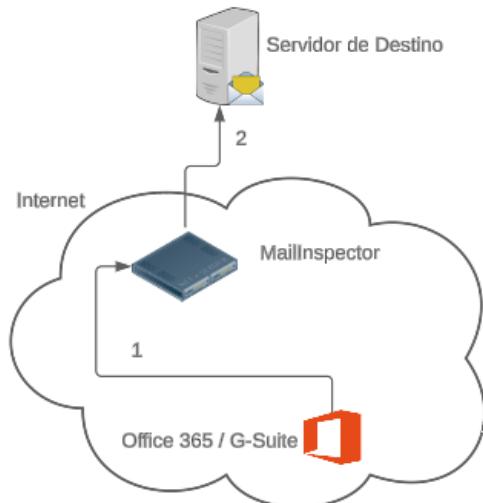
Integração MailInspector

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

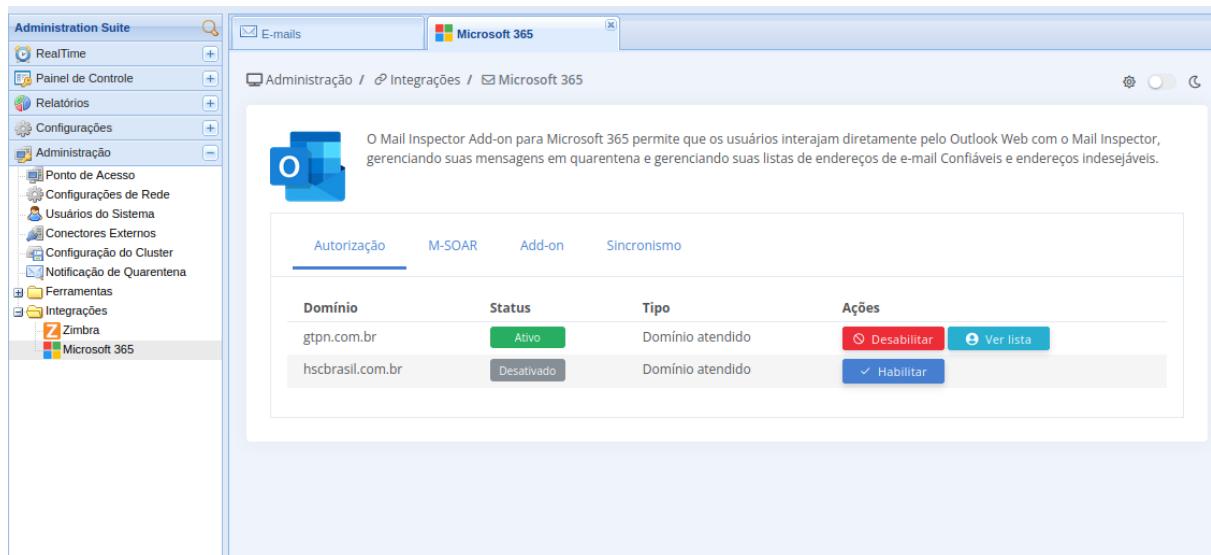
1. Os e-mails são direcionados ao Office365/G-Suite (que é o padrão quando se usa Office365 ou G-Suite), portanto, não há necessidade de mexer no MX/DNS;
2. Ao receber o e-mail, o Office365/G-Suite efetua a filtragem e encaminha para o MailInspector;
3. Após a filtragem por parte da Microsoft/Google,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

Primeiramente temos que configurar a conexão do MailInspector com o Office365. Para isso, vá em: Administração > Integrações > Microsoft 365



Domínio	Status	Tipo	Ações
gtpn.com.br	Ativo	Domínio atendido	Desabilitar Ver lista
hscbrasil.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.



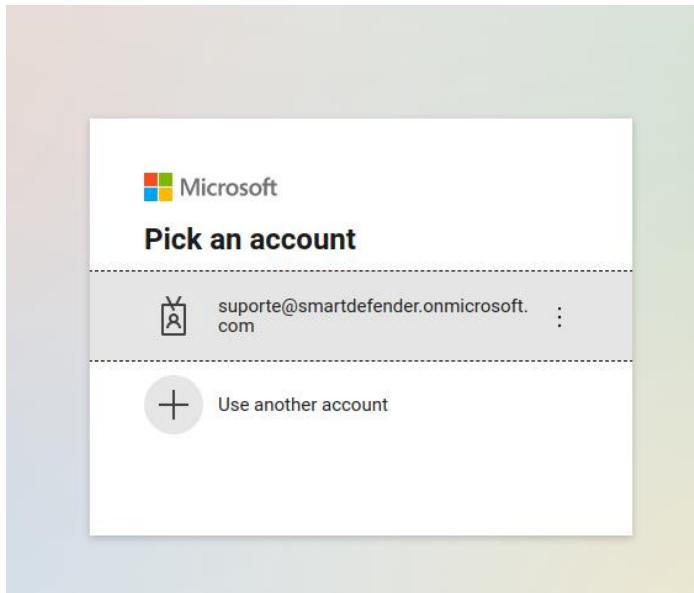
Para a ativação do M-SOAR no domínio **gtpn.com.br** na Microsoft, você deverá se autenticar com sua conta de administrador do domínio e autorizar que o Mail Inspector gerencie sua conta. Todas as permissões requisitadas deverão ser concedidas para o correto funcionamento da integração.

Deseja prosseguir?

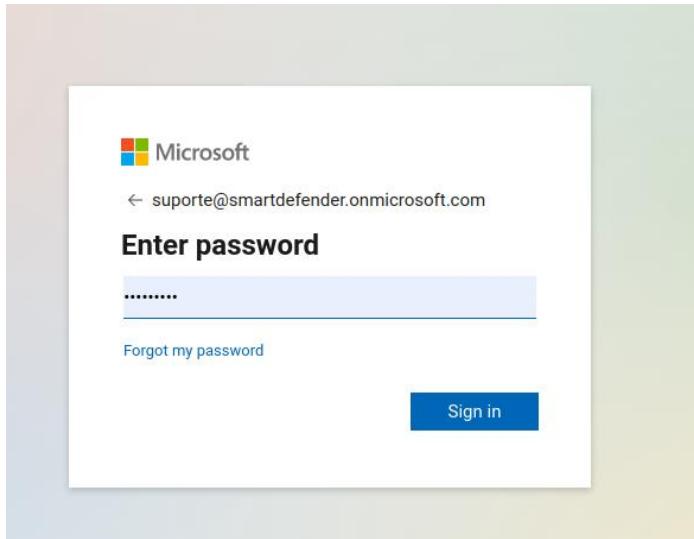
Prosseguir **Cancel**

Atenção! Somente domínios que utilizam o serviço Microsoft 365® poderão ser atendidos pelo serviço de integração do Mail Inspector.

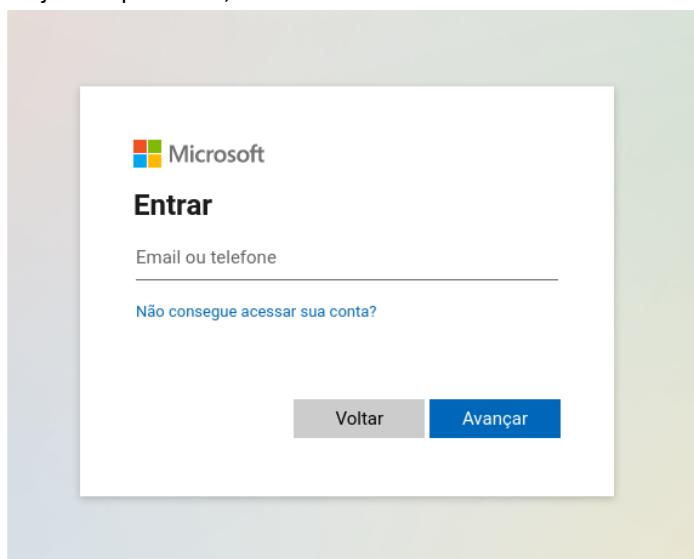
2. Na nova janela, informe as credenciais do administrador do serviço Microsoft 365



3. Informe a senha



4. Na janela que abrirá, informe as credenciais do Administrador da conta Microsoft 365



5. Confirme as permissões solicitadas

Permissions requested
Review for your organization



Mailinspector
gtpn.com.br

This application is not published by Microsoft.

This app would like to:

- ✓ Read and write directory data
- ✓ Read directory data
- ✓ Read and write mail in all mailboxes
- ✓ Read mail in all mailboxes
- ✓ Read all access reviews
- ✓ Manage all access reviews
- ✓ Read all users' full profiles
- ✓ Read and write all users' full profiles
- ✓ Manage access reviews for group and app memberships
- ✓ Read basic mail in all mailboxes
- ✓ Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

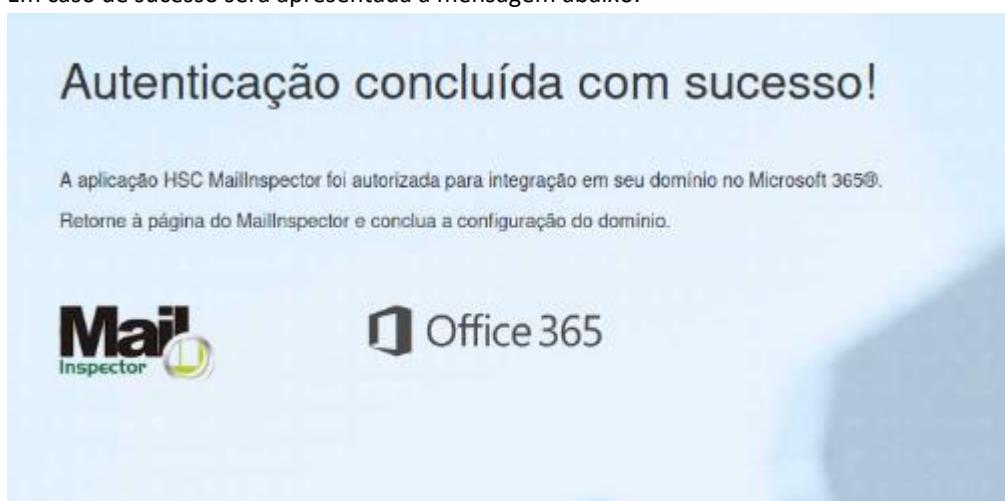
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. [The publisher has not provided links to their terms for you to review.](#) You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

[Cancel](#)

[Accept](#)

6. Em caso de sucesso será apresentada a mensagem abaixo:



7. Em caso de falha no acesso das credenciais fornecidas, será apresentada a mensagem:



Neste caso contate o administrador da conta Microsoft 365

8. Para importar os usuários, Grupos e Lista de Emails, clique na aba Sincronismo

Clique em Sincronizar, tanto para Cadastro automático de usuários, quanto para Cadastro de usuários válidos no domínio/Harvest Attack

Autorização M-SOAR Add-on Sincronismo Debug

Cadastro automático de usuários Habilita a importação e o cadastro automático dos usuários no Mail Inspector. Com isso, permite aos usuários gerenciar a sua quarentena, receber a notificação do digest e etc.

Ambiente Híbrido

Cadastro de usuários válidos no domínio / Harvest Attack Cria uma lista com todos os endereços válidos do domínio, e cria um dicionário que será utilizado para bloquear e-mails para contas desconhecidas e também para prevenir ataques como Harvest Attack e outros.

Para visualizar os usuários, emails e Grupos importados para autenticação por SSO (Single Sign-On), vá na aba Autorização e no domínio que você habilitou, clique no botão Ver Lista

O Mail Inspector Add-on para Microsoft 365 permite que os usuários interajam diretamente pelo Outlook Web 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	Debug
Domínio hsclatam.com	Status Ativo	Tipo Dominio atendido	Ações <input type="button" value="Desabilitar"/> <input checked="" type="button" value="Ver lista"/>	

Usuários E-mails Grupos

Mostrar 10 registros por página Procurar: ↑↓

	shared@gtpn.com.br	
	xshared@gtpn.com.br	
	xshared@smartdefender.onmicrosoft.com	

Mostrando página 1 de 1 Primeira Anterior 1 Próxima Última

Nessas abas você poderá visualizar:

- Usuários importados;

- E-mails importados;
- Grupos importados;



Caso você queira ativar outro domínio e importar os usuários, repita o processo.

Configuração Entrada de Emails para Office365 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.

- **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).



Vamos criar algumas etapas para o redirecionamento de email para o MailInspector, quando o email vier de fora. Para isso, vamos seguir a seguintes etapas:

1. Criar um Conector de Saída ao MailInspector
2. Criar regra de redirecionamento atrelado ao conector de saída
3. Criar Conector de Entrada InLine

1. Criando um Conector de Saída ao MailInspector

1. Acesse o seu Office365 como administrador;
2. Acesse o módulo de administração do Exchange;
3. Vá em Fluxo de e-mail > Conectores
4. Clique em Adicionar um conector
5. **Novo conector**
Conexão de: Office365
Conexão com: Organização parceira
Clique em Próxima
6. **Nome do conector**
Nome: Saída InLine MLI
Deixe marcada a caixa Ativar
Clique em Próxima
7. **Uso de conector**
Marque a opção:
Somente quando houver uma configuração de regra de transporte que redirecione mensagens para este conector
Clique em Próxima
8. **Roteamento**
Selecione a opção:
Rotear e-mail através desses hosts inteligentes
Insira os IPs dos nodes do MailInspector
Clique em Próxima
9. **Restrições de Segurança**
Deixe marcada a opção Sempre usar o protocolo TLS para proteger a conexão (recomendado)
Selecione a opção Qualquer certificado digital, inclusive certificados autoassinados
Clique em Próxima
10. E-mail de validação
Insira qualquer email, para validação
Clique em Próxima
11. Clique em Criar conector

2. Criando regra de redirecionamento atrelado ao conector de saída

1. Acesse o seu Office365 como administrador;
2. Acesse o módulo de administração do Exchange;
3. Vá em Fluxo de e-mail > Regras;
4. Clique em Adicionar uma regra;
5. Criar uma nova regra;
Nome: Roteamento Inbound InLine MLI
Aplicar esta regra se: O remetente

é externo/interno: Outside the organization
selecionar local do remetente

Outside the organization

Faça do seguinte:

Redirecionar a mensagem para: o seguinte conector > Saída InLine MLI

Exceto se:

O remetente > o endereço IP está em qualquer um desses intervalos ou correspondências exatas

Clique em Enter words

especificar intervalos de endereços IP

Insira todos os IPs do MailInspector disponibilizado para a sua empresa (fornecido pelo pessoal de suporte)

Clique em Salvar

Clique em Avançar

6. Definir configurações de regra

Deixe a opção Modo de regra em Impor

Mude a severidade para: Alto

Clique em Avançar

7. Revisar e concluir

Clique em Concluir

8. Regras

Mude a ordem de preferência da regra criada para o primeiro do grupo usando o botão ^Mover para cima, com isso, essa regra fará com que todos os emails de entrada sejam redirecionados para o

MailInspector, quando não vierem dos IPs do MailInspector. Caso vierem de algum IP do

MailInspector, o email será processado normalmente.

3. Criando um Conector de Entrada InLine

1. Acesse o seu Office365 como administrador;

2. Acesse o módulo de administração do Exchange;

3. Vá em Fluxo de e-mail > Conectores

4. Clique em Adicionar um Conector

5. Novo conector

Conexão de: Organização parceira

6. Nome do conector

Nome: Entrada InLine MLI

Deixe marcada a opção Ativar

Clique em Próxima

7. Autenticando e-mail enviado

Selecione a opção:

Ao verificar se o endereço IP do servidor de envio corresponde a um destes endereços IP que pertencem à sua organização

Insira todos os IPs do MailInspector (fornecidos pelo suporte da HSCBRASIL)

Clique em Próxima

8. Restrições de segurança

Verifique que esteja marcada a seguinte opção:

Rejeitar mensagens de e-mail que não forem enviadas por TLS

Desmarque a opção E exigir que o nome da entidade no certificado usado pelo parceiro para

autenticar o Office 365 corresponda a este nome de domínio

Clique em Próxima

9. Clique em Criar conector

Configuração Saída de Emails para Office365 Inline (sem alteração de MX)

Vamos criar algumas etapas para o redirecionamento de email para o MailInspector, quando o email vier de fora. Para isso, vamos seguir a seguintes etapas:

1. Criar um Conector de Saída ao MailInspector
2. Criação de regra de saída atrelado ao conector de Saída ao MailInspector



Caso você já tenha criado um conector de saída indicado na parte de **Configuração Entrada de Emails para Office365 Inline (sem alteração de MX)**, **pule para o item 2** que é **Criação de regra de saída** atrelado ao conector de Saída ao MailInspector.

1. Criando um Conector de Saída ao MailInspector

1. Acesse o seu Office365 como administrador;
2. Acesse o módulo de administração do Exchange;
3. Vá em Fluxo de e-mail > Conectores
4. Clique em Adicionar um conector
5. **Novo conector**
Conexão de: Office365
Conexão com: Organização parceira
Clique em Próxima
6. **Nome do conector**
Nome: Saída InLine MLI
Deixe marcada a caixa Ativar
Clique em Próxima
7. **Uso de conector**
Marque a opção:
Somente quando houver uma configuração de regra de transporte que redirecione mensagens para este conector
Clique em Próxima
8. **Roteamento**
Selecione a opção:
Rotear e-mail através desses hosts inteligentes
Insira os IPs dos nodes do MailInspector
Clique em Próxima
9. **Restrições de Segurança**
Deixe marcada a opção Sempre usar o protocolo TLS para proteger a conexão (recomendado)
Selecione a opção Qualquer certificado digital, inclusive certificados autoassinados
Clique em Próxima
10. **E-mail de validação**
Insira qualquer email, para validação
Clique em Próxima
11. Clique em Criar conector

2. Criando regra de saída atrelado ao conector de Saída ao MailInspector

1. Acesse o seu Office365 como administrador;
2. Acesse o módulo de administração do Exchange;
3. Vá em Fluxo de e-mail > Regras
4. Clique em Adicionar uma regra

5. Definir condições de regra

Nome: Saída InLine MLI

Aplicar esta regra se: O remetente

Selecionar local do remetente: Inside the organization

Faça do seguinte:

Redirecionar a mensagem para: o seguinte conector > Saída InLine MLI

Exceto se:

As propriedades da mensagem: incluir o tipo de mensagem > Calendaring

Clique em Salvar

Clique em Avançar

6. Definir configurações de regra

Modo de regra: Impor

Severidade: Alta

Clique em Avançar

7. Revisar e Concluir

Clique em Concluir

Comunicação segura entre MailInspector e Microsoft 365 / G-Suite

Verifique se está ativado o protocolo TLS no MailInspector.

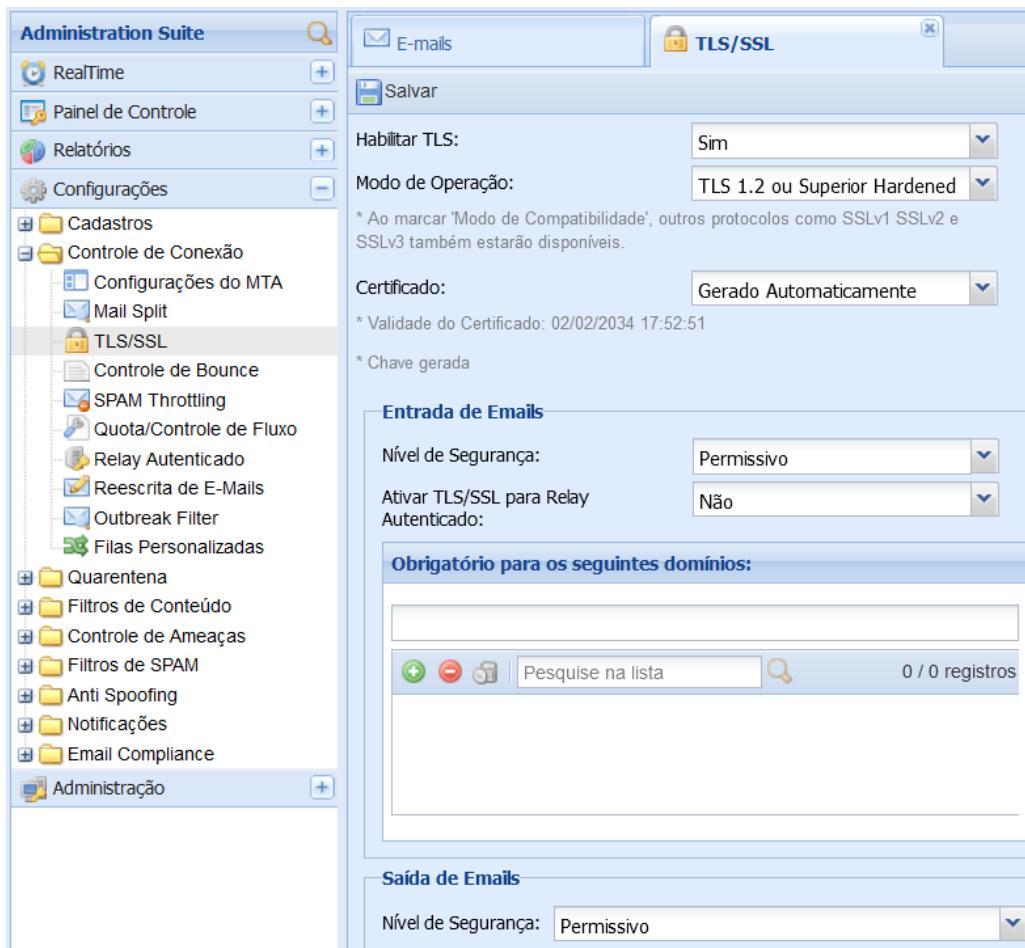
É necessário que esteja habilitado e configurado no modo de operação TLS 1.2 ou Superior Hardened. As outras versões foram mantidas por questão de compatibilidade, mas oferecem menor segurança, não sendo recomendado o uso delas.

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 Microsoft 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 Microsoft 365 (diretamente na caixa no Exchange).

1. No MailInspector vá em Interações > Microsoft 365 → M-SOAR e clique em Configurar. Logo com suas credenciais aprovadas na primeira etapa, clique em Sim, Configurar



2. Selecione Sim, configurar e configure as ações permitidas aos administradores do MailInspector e personalize os rótulos para as ações que serão registradas nas mensagens afetadas na caixa do usuário do Microsoft 365.

Configurar domínio x

Remoção de anexos da mensagem

Adicionar rótulo no assunto das mensagens afetadas

Texto do rótulo no assunto

Remoção de links da mensagem

Adicionar rótulo no assunto da mensagem afetada

Texto do rótulo no assunto

Adicionar rótulo no conteúdo da mensagem afetada

Texto do rótulo no assunto

Movimentação de mensagem para a pasta Lixo Eletrônico

Adicionar rótulo no assunto das mensagens afetadas

Texto do rótulo no assunto

Remoção permanente da mensagem

Bloqueio de conteúdo da mensagem

Adicionar rótulo no assunto das mensagens afetadas

Texto do rótulo no assunto

Substituir o conteúdo original da mensagem por:

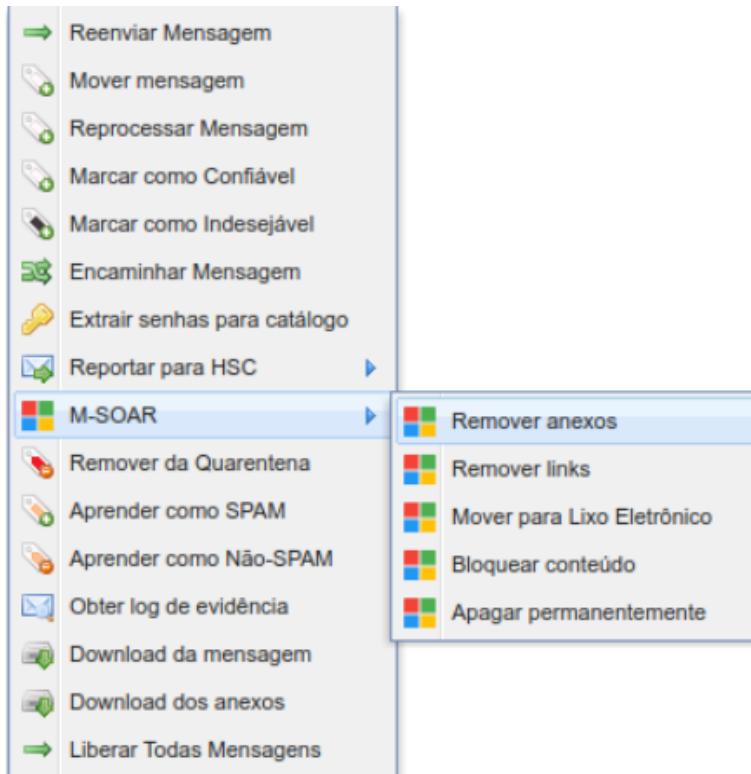
 P 8 WORDS A

O conteúdo desta mensagem foi bloqueado pelo administrador.

Cancelar Salvar alterações

3. Ao final clique em Salvar alterações.
4. Clique no botão SALVAR
5. A partir deste momento o Administrador do MailInspector pode executar ações sobre as mensagens já entregues na caixa do usuário do Microsoft 365.

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 Office 365 do usuário final

Remover links da mensagem - remove os links contidos no e-mail selecionado no Office 365 do usuário final

Mover para Lixo Eletrônico - move a mensagem para a pasta Lixo Eletrônico no Office 365 do usuário final

Bloquear Conteúdo - impede a visualização da mensagem no Office 365 do usuário final

Apagar a mensagem - apaga a mensagem no Office 365 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 Tenant da Microsoft 365

Ativação de Add-On do MLI no Office 365

O Add-on para Microsoft 365 permite que os usuários dos serviços da Microsoft interagirem a partir de seu MS Outlook Web, MS Outlook 2016 e MS Outlook 2019 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 Microsoft 365.

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)
- Acesso Administrativo ao Exchange Admin Center (<https://admin.exchange.microsoft.com/>)

Guia Passo-a-Passo

Este guia é dividido em 2 etapas que são executadas em sequência:

1. Configuração das Ações do Usuário no Add-On e
2. Deploy para os usuários do Microsoft 365.

Primeira Etapa

Configuração do Add-on: Corresponde à personalização das ações que o usuário do Add-on terá em seu cliente de e-mail Web ou instalação local do MS Outlook 2016 / 2019

1. Ative o Add-on no botão deslizante e informe o FDQN do seu Mail Inspector, clique em salvar e em seguida em Download. Salve o arquivo XML para a Segunda Etapa.

2. Configure as ações o usuário poderá executar em sua caixa de e-mail do Microsoft 365

3. 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

4. Determine as ações e quarentenas que serão disponibilizadas na interface do usuário do Office 365

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

<input checked="" type="checkbox"/> Marcar como Conflável	<input checked="" type="checkbox"/> Gerenciar Quarentena
<input checked="" type="checkbox"/> Marcar como Indesejável	<input checked="" type="checkbox"/> Gerenciar listas Confláveis/Indesejáveis
<input checked="" type="checkbox"/> 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/Auditoria
<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
---	--

5. 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

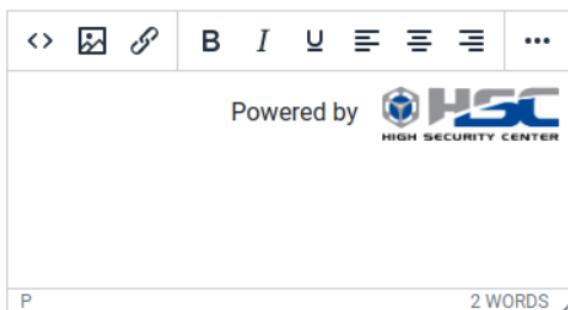
Reportar ao Administrador

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.

Segunda Etapa

Deploy do Add-on: Corresponde à implementação do Add-on nas configurações do domínio no ambiente de administração do Microsoft 365 (<https://admin.microsoft.com/>). Permite ao administrador do Microsoft 365 implementar apenas para alguns usuários ou grupos, conforme sua preferência.

1. Acesse o Portal de Administração do Microsoft 365 como Administrador.
2. Acesse <https://admin.microsoft.com/> e navegue em Configurações > Aplicativos Integrados
Clique em Add-ins (<https://admin.microsoft.com/Adminportal/Home#/Settings/AddIns>)

Modo escuro

Modo escuro

Aplicativos integrados

Descubra, adquira, gerencie e implante os aplicativos Microsoft 365 desenvolvido por parceiros da Microsoft.

Os aplicativos de linha de negócios desenvolvidos em sua própria organização não serão exibidos aqui. Para gerenciar esses aplicativos, acesse as respectivas centrais de administração ou página: [Azure Active Directory](#) | [SharePoint](#) | [Teams](#) | [Add-ins](#)

3. Em Add-ins, clique em + Implantar Suplemento

Add-ins

[+ Implantar Suplemento](#)

[Pesquisar](#)

Nome ↑

Descrição

4. Na janela lateral que será apresentada, clique em PRÓXIMO e selecione Implantar um Suplemento Personalizado

Implantar um suplemento personalizado

Crie um novo aplicativo Web ou carregue um suplemento/integração para o Office.

Carregar aplicativos personalizados

5. Clique em Escolher Arquivo e selecione o arquivo .XML obtido na Terceira Etapa. Clique em CARREGAR

Escolha como carregar o suplemento

Tenho o arquivo de manifesto (.xml) neste dispositivo.

Escolher Arquivo

Nenhum arquivo escolhido

Deve abrir o Add-On, conforme imagem a seguir:

HSC

Add-ins

[+ Implantar Suplemento](#)

[Pesquisar](#)

Nome ↑

Descrição



HSC Mail Inspector

Web protect your company from targeted and persistent attacks, using technologies such as Machin

Recomendação



Para minimizar impactos aos usuários finais, recomenda-se realizar a implementação para um usuário ou grupo de usuários, e então implementar para toda a corporação.

6. Selecione as opções da Implementação e IMPLANTAR



HSC Mail Inspector

Versão 1.0.0.0

Aplicativos de Host: Outlook

[Política de Privacidade](#)

[Termos de Uso](#)

[Obter Ajuda](#)

Web protect your company from targeted and persistent attacks, using technologies such as Machine Learning and Behaviour Analysis

Atribuir Usuários

Escolha quais usuários terão acesso ao HSC Mail Inspector

Todos

Usuários/grupos específicos

Procurar por usuários ou grupos específicos para adicionar ou remover

Comece a digitar um nome para pesquisar usu

suporte

7. É possível permitir ao usuário gerenciar a ativação e utilização ou não. Recomenda o método Fixo (Padrão)

Método de Implantação

Fixo (Padrão)

O suplemento será implantado automaticamente para os usuários atribuídos e não será possível removê-lo da faixa de opções deles.

Disponível

Os usuários podem instalar este suplemento clicando no botão obter mais suplementos na faixa de introdução inicial no Outlook e indo gerenciado pelo administrador.

Opcional

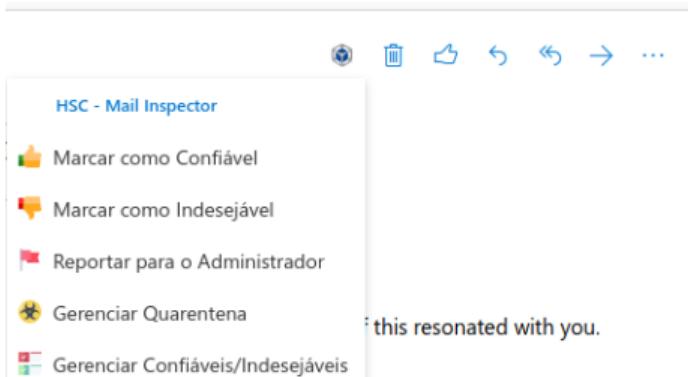
O suplemento será implantado automaticamente para os usuários atribuídos, mas eles podem optar por removê-lo da faixa de opções deles.

Atenção



É necessário aguardar 24h para disponibilizar o Add-on após sua ativação para os usuários ou grupos determinados.

8. Após o período de 24h, faça logoff e login, vá ao painel de e-mails e clique no ícone da HSC. Serão exibidas as ações a seguir:



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>
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.
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>



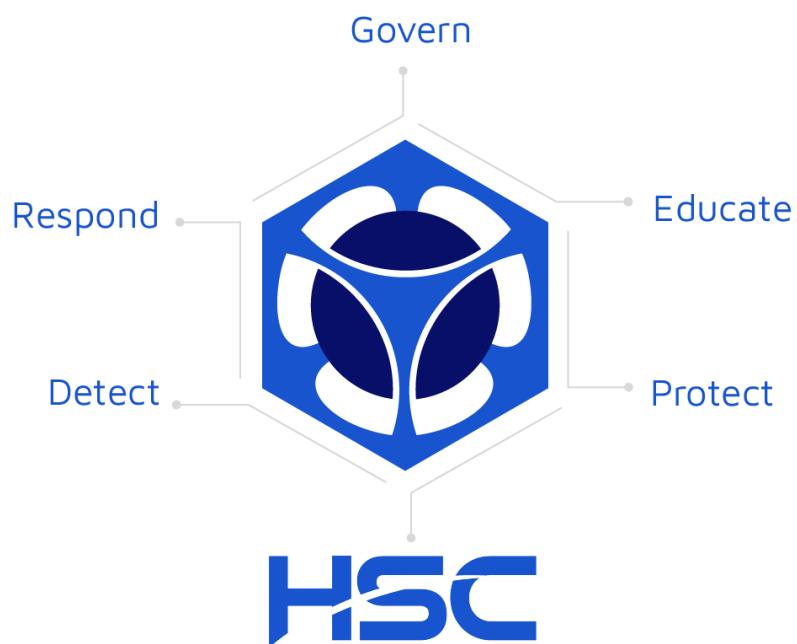
Todo o processo de Importação dos Usuários, importação de e-mails, importação de grupos, ativação de Add-On, ativação de M-SOAR, é feito através de API's, mas de modo a ficar o mais transparente possível ao administrador e aos usuários da solução.

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