Guia de administração

Revisão D

SaaS Email Protection

COPYRIGHT

ATRIBUIÇÕES DE MARCAS COMERCIAIS

INFORMAÇÕES SOBRE LICENÇA

Contrato de licença

Conteúdo

Prefácio **7**

Sobre este guia 7

Público-alvo 7

Convenções 7

O que há neste guia 8

Encontrar a documentação do serviço McAfee SaaS 8

1 Email Protection **9**

2 Visão geral **11**

Página Visão geral 11

Visualização da tela de estatísticas 12

3 Quarentena **15**

Pesquisar mensagens colocadas em quarentena 15

Página de quarentena 15

Exibição de mensagem segura 16

4 Email Continuity **17**

Recursos e limitações do Email Continuity 18

Abrir um e-mail no Email Continuity 18

Pesquisar e-mail no Email Continuity 19

Redigir um e-mail no Email Continuity 19

Email Continuity 20

Email Continuity para contas de e-mail externas 23

5 Políticas **27**

Página Políticas 27

Janela Novo conjunto de políticas 28

Gerenciando os conjuntos de políticas 29

Detalhes 30

Guia Detalhes 30

Vírus 30

Configurar ações a serem tomadas em relação a um vírus 30

Ações relacionadas a vírus 31

Notificações [Vírus] 32

Spam 32

O que é spam? 32

Configuração da política de classificação de spam 33

Classificação 34

Configuração de políticas de grupos de configurações 36

Subguia Grupos de conteúdo 36

Guia Geração de relatórios 37

ClickProtect 39

Atualizar as opções do ClickProtect para um conjunto de política de entrada 40

Guia Classificação . . . 41
Guia Avisos personalizados . . . 41
Guia Lista de permissão . . . 43
Conteúdo . . . 44
Grupos de conteúdo . . . 44
Grupos de conteúdo personalizados . . . 53
Documentos registrados . . . 55
Notificações [Conteúdo] . . . 56
Guia HTML Shield . . . 56
Anexos . . . 57
Tipos de arquivos . . . 57
Tipos de arquivo anexo . . . 58
Políticas de nome de arquivo . . . 59
Políticas adicionais . . . 61
Notificações [Anexos] . . . 62
Permitir/Negar . . . 62
Permissão de remetente . . . 63
Negação de remetente . . . 65
Blindagem de destinatário . . . 67
Autenticação de e-mail . . . 69
TLS imposto . . . 69
SPF imposto . . . 72
DKIM imposto . . . 74
Notificações [Autenticação de e-mail] . . . 77
Notificações . . . 77
Configurar um modelo de e-mail de notificação . . . 77
Guia Notificações . . . 78
Variáveis de notificação . . . 79
Recuperação de desastres . . . 79
Assinaturas de grupo . . . 79
Adição de uma assinatura de grupo . . . 80

6 Instalação 81

Servidores de entrada . . . 81
Verificar a configuração dos servidores de entrada . . . 81
Configurar um servidor de entrada . . . 82
Excluir um servidor de entrada . . . 82
Página Servidores de entrada . . . 83
Servidores de saída . . . 83
Configuração da filtragem de saída . . . 83
Configure os servidores de saída . . . 84
Excluir um servidor de saída . . . 85
Página de configuração de servidores de saída . . . 85
Aviso de isenção de responsabilidade sobre saída . . . 86
Adicionar um aviso de isenção de responsabilidade no e-mail de saída . . . 86
Página Aviso de isenção de responsabilidade sobre saída . . . 86
Recuperação de desastres . . . 87
Serviços de recuperação de desastres . . . 87
Configurar o spool automático para a recuperação de desastres . . . 87
Iniciar e interromper manualmente o spool para recuperação de desastres . . . 88
Configurar as notificações da recuperação de desastres . . . 88
Página Recuperação de Desastres . . . 89
Registros MX . . . 90
Redirecionando seus registros MX . . . 90
Selecione uma região para revisar os registros MX . . . 90
Página Configuração dos registros MX . . . 91

Página Configurações da criação de usuário . . . 93
Documentos registrados . . . 93
Como o registro de documentos impede a distribuição de documentos de propriedade . . . 93
Fazer upload de um documento registrado . . . 94
Página Documentos Registrados . . . 94
Instalação do DKIM . . . 95
Configurar DKIM . . . 95
Página Configuração de DKIM . . . 96

7 Auditoria de mensagens 97
Exibição de informações de disposição de mensagem . . . 97
Pesquisar por detalhes da mensagem . . . 97
Pesquisa por ID da mensagem . . . 99
Pesquisar por cabeçalho . . . 99
Auditoria de mensagens . . . 100
Definições do evento Visualização de detalhes da auditoria . . . 102
Visualizando os endereços de IP bloqueados . . . 106
Executar uma pesquisa de bloqueio de perímetro . . . 106
Janela Pesquisa de bloqueio de perímetro . . . 107
Exibição do histórico de pesquisa . . . 107
Analisar o histórico de pesquisa . . . 107
Janela de histórico de pesquisa . . . 108

8 Relatórios 111
Visão geral dos relatórios . . . 111
Configuração de cliente ou domínio e fuso horário . . . 113
Relatório Visão geral do tráfego . . . 113
Relatório **Tráfego: TLS** . . . 114
Relatório Tráfego: Criptografia . . . 115
Relatório Ameaças: Visão geral . . . 115
Relatório Ameaças: Vírus . . . 116
Relatório Ameaças: Spam . . . 117
Relatório Ameaças: Conteúdo . . . 118
Relatório Ameaças: Anexos . . . 119
Relatório TLS imposto: Detalhes . . . 120
Relatório SPF imposto . . . 121
Relatório DKIM imposto . . . 121
Relatório ClickProtect: Visão geral . . . 122
Relatório ClickProtect: Registro de cliques . . . 122
Relatório Quarentena: Visão geral da liberação . . . 123
Relatório Quarentena: Registro de liberação . . . 124
Relatório Atividades do usuário . . . 125
Relatório **Log de eventos** . . . 125
Relatório Trilha de auditoria . . . 126
Relatório Conexões de servidor de entrada . . . 127
Relatório Recuperação de desastres: Visão geral . . . 128
Relatório Recuperação de desastres: Log de eventos . . . 128

Índice 131

Prefácio

Este guia fornece as informações necessárias para configuração, uso e manutenção do seu serviço McAfee SaaS.

Conteúdo

- *Sobre este guia*
- *Encontrar a documentação do serviço McAfee SaaS*

Sobre este guia

Estas informações descrevem o público-alvo do guia, as convenções tipográficas e os ícones utilizados, além de como o guia é organizado.

Público-alvo

A documentação do McAfee SaaS passou por uma pesquisa cuidadosa e foi escrita direcionada ao público-alvo.

As informações neste guia destinam-se principalmente a:

- **Administradores** — Pessoas que configuram e gerenciam recursos específicos de um serviço.

Convenções

Este guia usa as seguintes convenções tipográficas e ícones.

Título do livro ou *Ênfase*	Título de um livro, capítulo ou tópico; introdução de um novo termo; ênfase.
Negrito	Texto que é rigidamente enfatizado.
`Entrada do usuário` ou `Caminho`	Comandos ou qualquer outro texto que o usuário digita; o caminho de uma pasta ou programa.
`Código`	Uma amostra de código.
Interface do usuário	Palavras na interface do usuário, que incluem opções, menus, botões e caixas de diálogo.
Hipertexto azul	Um link ativo para um tópico ou site.
	**Nota:** Informações adicionais, como um método alternativo de acessar uma opção.
	**Dica:** Sugestões e recomendações.
	**Importante/Atenção:** Conselho importante para proteger seu sistema de computador, instalação de software, rede, negócios ou dados.

O que há neste guia

Este guia foi organizado para ajudá-lo a encontrar as informações que você precisa.

Ele está dividido em partes funcionais destinadas a ajudá-lo na realização de seus objetivos ao usar seu serviço McAfee SaaS. Cada parte está dividida em capítulos que agrupam informações relevantes por recurso e tarefas associadas para que você possa ir diretamente ao tópico necessário para concretizar seus objetivos.

Encontrar a documentação do serviço McAfee SaaS

A McAfee fornece as informações necessárias durante cada fase da implementação do serviço, desde a instalação até o uso diário e a solução de problemas. Após o lançamento da atualização do serviço, as informações são adicionadas ao site de suporte do McAfee SaaS Email and Web Security.

Tarefa

1 Vá para a página do **ServicePortal for SaaS Email and Web Security**, em http://support.mcafeesaas.com/.

2 Clique ou selecione **Downloads**.

3 Em **Reference Materials** (Materiais de referência), role para baixo para acessar as informações necessárias:

- **Melhorias de serviço e notas de versão**
- **Materiais de treinamento**
- **Guias de referência de serviço**

1 Email Protection

O Email Protection fornece serviços de segurança que protegem as empresas de e-mails de spam não solicitados, lixo eletrônico, vírus, worms e conteúdo indesejado no perímetro da rede antes que eles possam entrar na sua rede interna. As diversas camadas do Email Protection fornecem uma filtragem de e-mails segura e completa para proteger seus usuários. Você pode ativar ou desativar camadas específicas alterando os pacotes de recursos licenciados ou por meio da configuração das políticas específicas no Control Console.

2 Visão geral

A página **Visão geral** fornece informações de alto nível sobre o tráfego de e-mails em direção ao seu domínio nas últimas 24 horas. Por padrão, a página exibe o **Status atual de recuperação de desastres** e a **Atividade de recuperação de desastres**.

Conteúdo

- *Página Visão geral*
- *Visualização da tela de estatísticas*

Página Visão geral

Use a página **Visão geral** para visualizar as informações da recuperação de desastres, bem como a amostra de 24 horas.

Tabela 2-1 Opções da página Visão geral

Opção	Definição
Visão geral	Clique na guia **Visão geral** para visualizar as informações padrão. • **Status atual de recuperação de desastres** • **Atividade de recuperação de desastres**
Estatísticas de exibição	Clique no botão **Estatísticas de exibição** para visualizar as informações da amostra. As estatísticas das últimas 24 horas são baseadas em seu fuso horário local. • **Amostra de 24 horas de entrada** • **Amostra de 24 horas de saída** • **Tráfego (Últimas 24 horas - fuso horário)** • **Imposição de política (Últimas 24 horas - fuso horário)** • **Status atual de recuperação de desastres** • **Atividade de recuperação de desastres**

Visualização da tela de estatísticas

Clique em **Exibir estatísticas** para visualizar uma amostra de 24 horas do tráfego de entrada e saída de e-mail.

Tabela 2-2 Visualização da tela de estatísticas

Opção	Definição
Instantâneo de 24 horas da entrada	Exibe um instantâneo de 24 horas do tráfego de e-mails recebidos: • **Largura de banda**: largura de banda média usada pelas mensagens de entrada. • **Tamanho médio**: tamanho médio das mensagens de entrada, incluindo os anexos. • **Negado**: mensagens negadas por serem mensagens devolvidas, conterem vírus, conteúdo indesejado, anexos, HTML, ou por provavelmente serem spam. A entrega é negada. • **Conteúdo**: todos os e-mails de entrada que violaram as políticas da palavra-chave de conteúdo. • **Vírus**: número de e-mails de entrada que continham vírus. • **Mensagens** — Número de mensagens de entrada processadas. Esse número inclui as mensagens enviadas a todos os domínios para o cliente. • **Em quarentena**: número total de e-mails de entrada que foram colocados em quarentena por algum motivo, incluindo spam, vírus, etc. • **Anexo**: todos os e-mails de entrada que continham anexos que violavam as políticas de anexo. • **Spam**: número de e-mails de entrada que tinham grandes chances de ser spam.
Instantâneo de 24 horas da saída	Exibe um instantâneo de 24 horas do tráfego de e-mails enviados: • **Largura de banda**: largura de banda média usada pelas mensagens de saída. • **Tamanho médio**: tamanho médio das mensagens de saída, incluindo os anexos. • **Negado**: mensagens negadas por serem mensagens devolvidas, conterem vírus, conteúdo indesejado, anexos, HTML, ou por provavelmente serem spam. A entrega é negada. • **Anexo**: todos os e-mails de saída que continham anexos que violavam as políticas de anexo. • **Vírus**: número de e-mails de saída que continham vírus. • **Mensagens** — Número de mensagens de saída processadas. Esse número inclui as mensagens enviadas de todos os domínios e de todos os usuários para o cliente, mesmo quando os usuários enviam mensagens de domínios não realmente administrados para o cliente (por exemplo, mensagens de contas do gmail). • **Em quarentena** — Número total de e-mails de saída que foram colocados em quarentena por algum motivo, incluindo spam, vírus etc. • **Criptografado**: todos os e-mails de saída que violavam as políticas de criptografia. • **Conteúdo**: todos os e-mails de saída que violavam quaisquer políticas da palavra-chave de conteúdo.
Tráfego (Últimas 24 horas)	Exibe uma representação gráfica do volume do tráfego nas últimas 24 horas do fuso horário designado que mostra o número total de e-mails de entrada e saída.
Imposição de política (Últimas 24 horas)	Exibe a porcentagem das mensagens que tiveram diferentes ações de e-mail aplicadas (por exemplo, removidas, bloqueadas, marcadas, colocadas em quarentena, descontaminadas, ou entregues normalmente) durante as últimas 24 horas do fuso horário designado.

Tabela 2-2 Visualização da tela de estatísticas *(continuação)*

Opção	Definição
Status atual de recuperação de desastres	Exibe uma lista dos domínios que estão atualmente na recuperação de desastres. O Email Protection atualmente está colocando o e-mail do domínio especificado no spool.
Atividade de recuperação de desastres	Exibe uma amostra das mensagens no spool e fora do spool se sua empresa estiver no modo de recuperação de desastres. O número de mensagens é listado em conjunto com o tamanho em KB que foi colocado ou retirado do spool. Escolha um dos três mecanismos fornecidos que permitem a você entrar no Web Protection System. O fuso horário padrão é a hora das montanhas.

3 Quarentena

O recurso quarentena em Email Protection permite que você revise mensagens de e-mail suspeitas e determine se estas são ou não spam.

Conteúdo

- *Pesquisar mensagens colocadas em quarentena*
- *Página de quarentena*
- *Exibição de mensagem segura*

Pesquisar mensagens colocadas em quarentena

Use as opções de pesquisa para filtrar mensagens colocadas em quarentena e executar ações, conforme necessário.

Para alterar os clientes, selecione o link no canto superior direito da janela aberta. Na janela de pop-up **Selecionar cliente**, digite o nome do cliente e selecione o nome quando a lista de opções for atualizada.

Tarefa

Para obter as Definições de opções, clique em **Ajuda** na interface.

1 EmEmail Protection, selecione **Quarentena**.

2 Selecione seus **Critérios de pesquisa**.

3 Clique em **Pesquisar**.

Revise os resultados e execute as ações nas mensagens colocadas em quarentena, conforme necessário.

Página de quarentena

A guia **Quarentena** permite que você pesquise e-mails colocados em quarentena e revise, libere, permita ou exclua-os para os usuários, se necessário.

Tabela 3-1 Definições de opções de critérios de pesquisa

Opção	Definição
Domínio	Especifica os domínios incluídos na pesquisa. Selecione para filtrar por domínio.
Para	Especifica o endereço de e-mail do destinatário para usar na pesquisa. Você pode usar caracteres curinga para pesquisar vários endereços de e-mail que correspondam à parte do endereço.

Tabela 3-1 Definições de opções de critérios de pesquisa *(continuação)*

Opção	Definição
De	Especifica o endereço de e-mail do remetente para usar na pesquisa. Você pode usar caracteres curinga para pesquisar vários endereços de e-mail que correspondam à parte do endereço.
Ameaça	Especifica o tipo de ameaça que deve ser usado na pesquisa.
Dia	Especifica a data que deve ser usada na pesquisa.
Direção	Especifica a direção do tráfego de e-mail que deve ser usada na pesquisa (entrada, saída ou ambas).

Tabela 3-2 Definições de opções de resultados de pesquisa

Opção	Definição
Liberar	Clique para liberar as mensagens selecionadas.
Sempre permitir para o usuário	Clique para adicionar os remetentes selecionados à lista **Permissão** do usuário e liberar as mensagens (aplica-se somente às mensagens de spam).
Excluir	Clique para excluir as mensagens selecionadas.
Excluir tudo	Clique para excluir todas as mensagens.
Exibir	Clique para visualizar uma mensagem na guia **Exibição de mensagem segura**.
Lista **Resultados da pesquisa**	• **Data** — Exibe a data da mensagem. • **De** — Exibe o endereço de e-mail da mensagem. • **Para**: exibe o endereço de e-mail da mensagem. • **Assunto** — Exibe o assunto da mensagem. • **Ameala** — Exibe o tipo de ameaça da mensagem. • **Pontuação** — Exibe a pontuação de quarentena da mensagem. • **Tamanho** — Exibe o tamanho da mensagem.

Exibição de mensagem segura

A janela **Exibição de mensagem segura** fornece mais informações sobre a mensagem em quarentena que você selecionou. Você também pode exibir o conteúdo da mensagem quando as configurações de políticas de Exibição de mensagem segura estiverem ativadas.

Tabela 3-3 Exibição de mensagem segura

Opção	Definição
Liberar	Clique para liberar uma mensagem selecionada da lista de quarentena e movê-la para sua caixa de entrada de e-mail.
Excluir	Clique para excluir uma mensagem selecionada da lista de quarentena.
Sempre permitir para o usuário	Clique para liberar mensagens para os destinatários de e-mail. Os endereços de e-mail de todos os remetentes serão adicionados à **Lista de permissão** dos destinatários. Todas as futuras mensagens dos remetentes não serão mais colocadas em quarentena.
Sempre negar	Clique para bloquear mensagens para os destinatários de e-mail.

4 Email Continuity

O Email Continuity fornece um serviço abrangente de recuperação de desastres gerenciado que protege seu tráfego de e-mail durante uma interrupção de rede. Quando ativo, os usuários e administradores podem exibir, enviar e gerenciar seus e-mails usando a interface online, enquanto o serviço armazena todas as atividades de envio e recebimento de e-mails na nuvem. Em seguida, quando a conectividade é restaurada, o serviço sincroniza os e-mails com seus servidores de e-mail, e o funcionamento normal do e-mail é retomado.

Conteúdo

- *Recursos e limitações do Email Continuity*
- *Abrir um e-mail no Email Continuity*
- *Pesquisar e-mail no Email Continuity*
- *Redigir um e-mail no Email Continuity*
- *Email Continuity*
- *Email Continuity para contas de e-mail externas*

Recursos e limitações do Email Continuity

Você pode usar a maioria dos recursos de um cliente de e-mail da Web padrão durante uma interrupção.

Tabela 4-1 Recursos e limitações do Email Continuity

Recursos de e-mail...	Descrição
Que você pode usar durante uma interrupção	• Opções de e-mail padrão. • Anexar arquivos • Pesquisar mensagens
Que estão indisponíveis durante uma interrupção	• Não é possível alterar o endereço de e-mail em **De:** . • Nenhum acesso à Lista de endereços global ou Lista de contatos pessoais. Essas Listas de distribuição estão no servidor corporativo e, durante uma interrupção, esse servidor não fica disponível. • Nenhuma Verificação ortográfica. • Nenhuma pasta de Rascunhos. • Nenhuma funcionalidade "Verificar nomes" para verificar o endereço de e-mail antes do envio. • Não é possível pesquisar texto no corpo de uma mensagem.
Talvez isso seja diferente do seu cliente de e-mail padrão	• Você deve separar vários endereços de e-mail com vírgulas, sem espaços após a vírgula. • Você deve inserir um endereço de e-mail totalmente qualificado no campo **Para:** quando redigir uma nova mensagem. • Se você tiver aberto várias mensagens, será exibida uma guia para cada mensagem. • Mensagens excluídas no Email Continuity não são excluídas permanentemente. Quando a interrupção de e-mail terminar, todas as atividades de e-mail serão sincronizadas com o(s) servidor(es) de e-mail da sua organização, que tratará da disposição final da mensagem.

Abrir um e-mail no Email Continuity

Quando a Recuperação de desastres está ativa, use a guia **Email Continuity** para acessar suas mensagens de e-mail.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 Clique na guia **Email Continuity**.

2 No painel **Critérios**, selecione uma pasta de e-mail.

A guia da pasta de e-mail será aberta.

3 Na lista, selecione uma mensagem de e-mail.

4 Clique em **Abrir**.

A mensagem é aberta em uma nova guia.

Use as opções para responder a mensagem, excluí-la ou imprimi-la.

Pesquisar e-mail no Email Continuity

Quando a Recuperação de desastres está ativa, use a guia **Email Continuity** para pesquisar suas mensagens de e-mail.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1. Clique na guia **Email Continuity**.
2. No painel **Critérios**, selecione uma pasta de e-mail.

   A guia da pasta de e-mail será aberta.
3. Clique no painel **Pesquisar**.

   As opções de critérios de pesquisa são abertas.
4. Insira um ou mais critérios de pesquisa.
5. Clique no botão **Pesquisar**.

   Os resultados da sua pesquisa serão exibidos em uma nova guia.

Use as opções para gerenciar os e-mails nos resultados da sua pesquisa.

Redigir um e-mail no Email Continuity

Quando a Recuperação de desastres está ativa, use a guia **Email Continuity** para acessar suas mensagens de e-mail.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1. Clique na guia **Email Continuity**.
2. No painel **Critérios**, selecione **Caixa de entrada**.

   A guia **Caixa de entrada** é aberta.
3. Clique em **Novo**.

   A guia **Nova mensagem** é aberta.
4. Crie seu e-mail.

Opção	Descrição
Selecionar endereço de e-mail do remetente	Selecione a partir da lista suspensa **De**.
Adicionar destinatários	Insira os endereços de e-mail nos campos **Para**, **Cc** ou **CCo**.
Inserir o assunto	

Opção	Descrição
Anexar arquivos	1 Clique em **Anexar arquivo** para adicionar um **Anexo**. 2 Clique em **Procurar** para selecionar um arquivo.
Redigir sua mensagem	Insira o texto da sua mensagem. Na exibição padrão, use as opções de HTML para formatar seu texto. Clique em **Alternar para texto sem formatação** para criar uma mensagem sem formatação HTML.

5 Clique em **Enviar**.

Sua mensagem será enviada aos seus destinatários.

A mensagem será exibida na pasta **Itens enviados**.

Email Continuity

Quando a Recuperação de desastres está ativa, você pode acessar seu e-mail a partir do console. Use essas ferramentas para receber e-mails, responder a mensagens, exibir anexos e pesquisar pastas disponíveis.

Tabela 4-2 Critérios

Opção	Definições
Pesquisar	Clique para executar uma pesquisa na pasta de e-mail selecionada usando seus critérios e suas datas escolhidas.
Redefinir	Clique para redefinir os valores de critérios de pesquisa.
Pastas de e-mail	Selecione uma pasta para exibir suas mensagens e pesquisar e-mails. • **Caixa de entrada** — Clique para exibir sua caixa de entrada. • **Itens excluídos** — Clique para exibir seus e-mails excluídos. • **Itens enviados** — Clique para exibir seus itens enviados.
Pesquisar e-mail	Selecione para executar uma nova pesquisa. • **Critérios** — Insira uma cadeia para pesquisar valores nos campos **Para**, **De** e **Assunto**. • **Data de início** — Insira ou selecione um valor de data. • **Data de término** — Insira ou selecione um valor de data.

Tabela 4-3 Email Continuity

Opção	Definições

Caixa de entrada	• **Novo** — Clique para redigir um novo e-mail.
	• **Abrir** — Clique para abrir o e-mail selecionado em uma nova guia.
	• **Visualizar** — Clique para exibir o e-mail selecionado no painel de visualização. Selecione a localização do painel de visualização ou clique no botão para percorrer as opções.
	  • **Inferior** — Exibe a mensagem na parte inferior da guia.
	  • **Direita** — Exibe a mensagem à direita da guia.
	  • **Ocultar** — Oculta a visualização.
	• **Responder**: clique para escrever uma resposta para o remetente do e-mail selecionado.
	• **Responder a todos** — Clique para escrever uma resposta para o remetente e todos os outros destinatários do e-mail selecionado.
	• **Encaminhar**: clique para encaminhar o e-mail selecionado.
	• **Excluir** — Clique para excluir o e-mail selecionado e movê-lo para a pasta **Itens excluídos**.
	• **Ações** — Selecione uma ação.
	  • **Marcar como lida** — Clique para selecionar as mensagens como lidas.
	  • **Marcar como não lida** — Clique para selecionar as mensagens como não lidas.
	• **Imprimir**: clique para imprimir o e-mail selecionado.
	• **Atualizar** — Clique para atualizar a lista de mensagens de e-mail.

Itens excluídos	• **Abrir** — Clique para abrir o e-mail selecionado em uma nova guia.
	• **Visualizar** — Clique para exibir o e-mail selecionado no painel de visualização. Selecione a localização do painel de visualização ou clique no botão para percorrer as opções.
	  • **Inferior** — Exibe a mensagem na parte inferior da guia.
	  • **Direita** — Exibe a mensagem à direita da guia.
	  • **Ocultar** — Oculta a visualização.
	• **Responder**: clique para escrever uma resposta para o remetente do e-mail selecionado.
	• **Responder a todos** — Clique para escrever uma resposta para o remetente e todos os outros destinatários do e-mail selecionado.
	• **Encaminhar**: clique para encaminhar o e-mail selecionado.
	• **Cancelar exclusão** — Clique para cancelar a exclusão do e-mail selecionado e movê-lo para a pasta **Caixa de entrada**.
	• **Ações** — Selecione uma ação.
	  • **Marcar como lida** — Clique para selecionar as mensagens como lidas.
	  • **Marcar como não lida** — Clique para selecionar as mensagens como não lidas.
	• **Imprimir**: clique para imprimir o e-mail selecionado.
	• **Atualizar** — Clique para atualizar a lista de mensagens de e-mail.

Tabela 4-3 Email Continuity *(continuação)*

Opção	Definições

Itens enviados	• **Abrir** — Clique para abrir o e-mail selecionado em uma nova guia.
	• **Visualizar** — Clique para exibir o e-mail selecionado no painel de visualização. Selecione a localização do painel de visualização ou clique no botão para percorrer as opções.
	  • **Inferior** — Exibe a mensagem na parte inferior da guia.
	  • **Direita** — Exibe a mensagem à direita da guia.
	  • **Ocultar** — Oculta a visualização.
	• **Responder**: clique para escrever uma resposta para o remetente do e-mail selecionado.
	• **Responder a todos** — Clique para escrever uma resposta para o remetente e todos os outros destinatários do e-mail selecionado.
	• **Encaminhar**: clique para encaminhar o e-mail selecionado.
	• **Imprimir**: clique para imprimir o e-mail selecionado.
	• **Atualizar** — Clique para atualizar a lista de mensagens de e-mail.

Painel **Visualizar**	• **Abrir** — Clique para abrir o e-mail selecionado em uma nova guia.
	• **Responder**: clique para escrever uma resposta para o remetente do e-mail selecionado.
	• **Responder a todos** — Clique para escrever uma resposta para o remetente e todos os outros destinatários do e-mail selecionado.
	• **Encaminhar**: clique para encaminhar o e-mail selecionado.
	• **Excluir** — Clique para excluir o e-mail selecionado e movê-lo para a pasta **Itens excluídos**.
	• **Ações** — Selecione uma ação.
	  • **Marcar como lida** — Clique para selecionar as mensagens como lidas.
	  • **Marcar como não lida** — Clique para selecionar as mensagens como não lidas.
	• **Imprimir**: clique para imprimir o e-mail selecionado.
	• **Mostrar cabeçalhos/Ocultar cabeçalhos** — Clique para mostrar ou ocultar os cabeçalhos de e-mails.

Tabela 4-3 Email Continuity *(continuação)*

Opção	Definições
Guia de mensagem aberta	• **Responder**: clique para escrever uma resposta para o remetente do e-mail selecionado. • **Responder a todos** — Clique para escrever uma resposta para o remetente e todos os outros destinatários do e-mail selecionado. • **Encaminhar**: clique para encaminhar o e-mail selecionado. • **Imprimir**: clique para imprimir o e-mail selecionado. • **Mostrar cabeçalhos/Ocultar cabeçalhos** — Clique para mostrar ou ocultar os cabeçalhos de e-mails.

Nova mensagem	• **Enviar** — Clique para enviar o e-mail.
	• **Anexar** — Clique para anexar arquivos ao e-mail.
	• **Alternar para texto sem formatação/Alternar para HTML** — Clique para selecionar o formato da mensagem.
	  • Texto sem formatação — Use o formato de texto simples.
	  • HTML — Use a ferramenta HTML WYSIWYG para formatar a mensagem.
	• **De:** — Selecione o endereço de origem.
	• **Para:** — Insira um ou mais endereços de e-mail.
	• **Cc:** — Insira um ou mais endereços de e-mail no campo Cc.
	• **Cco:** — Insira um ou mais endereços de e-mail no campo Cco.
	• **Assunto:** — Insira o texto de assunto.
	• **Anexo:** — Selecione um anexo de arquivo. Um novo campo **Anexo** será exibido sempre que você clicar em **Anexar** e adicionar o arquivo.
	  • Ícone Excluir — Clique para excluir o anexo.
	• Corpo da mensagem — Insira o corpo da mensagem.

Email Continuity para contas de e-mail externas

Quando a Recuperação de desastres está ativa, os administradores podem exibir as mensagens de e-mail órfãs pertencentes a usuários não atribuídos.

Tabela 4-4 Critérios

Opção	Definições
Pesquisar	Clique para executar uma pesquisa na pasta de e-mail selecionada usando seus critérios e suas datas escolhidas.
Redefinir	Clique para redefinir os valores de critérios de pesquisa.

Tabela 4-4 Critérios *(continuação)*

Opção	Definições
Pastas de e-mail	Selecione uma pasta para exibir suas mensagens e pesquisar e-mails. • **Caixa de entrada** — Clique para exibir sua caixa de entrada. • **Itens excluídos** — Clique para exibir seus e-mails excluídos.
Pesquisar e-mail	Selecione para executar uma nova pesquisa. • **Critérios** — Insira uma cadeia para pesquisar valores nos campos **Para**, **De** e **Assunto**. • **Data de início** — Insira ou selecione um valor de data. • **Data de término** — Insira ou selecione um valor de data.

Tabela 4-5 Email Continuity

Opção	Definições

Caixa de entrada	• **Abrir** — Clique para abrir o e-mail selecionado em uma nova guia.
	• **Visualizar** — Clique para exibir o e-mail selecionado no painel de visualização. Use o menu suspenso para selecionar o local do painel de visualização ou clique no botão para percorrer as opções.
	  • **Inferior** — Exibe a mensagem na parte inferior da guia.
	  • **Direita** — Exibe a mensagem à direita da guia.
	  • **Ocultar** — Oculta a visualização.
	• **Responder** — Clique para escrever uma resposta para o remetente do e-mail selecionado.
	• **Responder a todos** — Clique para escrever uma resposta para o remetente e todos os outros destinatários do e-mail selecionado.
	• **Encaminhar** — Clique para encaminhar o e-mail selecionado.
	• **Excluir** — Clique para excluir o e-mail selecionado e movê-lo para a pasta **Itens excluídos**.
	• **Ações** — Selecione uma ação.
	  • **Marcar como lida** — Clique para selecionar as mensagens como lidas.
	  • **Marcar como não lida** — Clique para selecionar as mensagens como não lidas.
	• **Imprimir** — Clique para imprimir o e-mail selecionado.
	• **Atualizar** — Clique para atualizar a lista de mensagens de e-mail.
	• **Ir para a Lista de usuários** — Clique para retornar à lista de contas do usuário. Disponível a partir do link **Gerenciamento de contas** | **Usuários** | **Contas de e-mail externas**.

Itens excluídos	• **Abrir** — Clique para abrir o e-mail selecionado em uma nova guia.
	• **Visualizar** — Clique para exibir o e-mail selecionado no painel de visualização. Use o menu suspenso para selecionar o local do painel de visualização ou clique no botão para percorrer as opções.
	  • **Inferior** — Exibe a mensagem na parte inferior da guia.
	  • **Direita** — Exibe a mensagem à direita da guia.
	  • **Ocultar** — Oculta a visualização.
	• **Responder** — Clique para escrever uma resposta para o remetente do e-mail selecionado.
	• **Responder a todos** — Clique para escrever uma resposta para o remetente e todos os outros destinatários do e-mail selecionado.
	• **Encaminhar** — Clique para encaminhar o e-mail selecionado.
	• **Cancelar exclusão** — Clique para cancelar a exclusão do e-mail selecionado e movê-lo para a pasta **Caixa de entrada**.
	• **Ações** — Selecione uma ação.
	  • **Marcar como lida** — Clique para selecionar as mensagens como lidas.
	  • **Marcar como não lida** — Clique para selecionar as mensagens como não lidas.
	• **Imprimir** — Clique para imprimir o e-mail selecionado.
	• **Atualizar** — Clique para atualizar a lista de mensagens de e-mail.

Tabela 4-5 Email Continuity *(continuação)*

Opção	Definições

Painel **Visualizar**	• **Abrir** — Clique para abrir o e-mail selecionado em uma nova guia.
	• **Responder** — Clique para escrever uma resposta para o remetente do e-mail selecionado.
	• **Responder a todos** — Clique para escrever uma resposta para o remetente e todos os outros destinatários do e-mail selecionado.
	• **Encaminhar** — Clique para encaminhar o e-mail selecionado.
	• **Excluir** — Clique para excluir o e-mail selecionado e movê-lo para a pasta **Itens excluídos**.
	• **Ações** — Selecione uma ação.
	  • **Marcar como lida** — Clique para selecionar as mensagens como lidas.
	  • **Marcar como não lida** — Clique para selecionar as mensagens como não lidas.
	• **Imprimir** — Clique para imprimir o e-mail selecionado.
	• **Mostrar cabeçalhos/Ocultar cabeçalhos** — Clique para mostrar ou ocultar os cabeçalhos de e-mails.

Guia de mensagem aberta	• **Responder** — Clique para escrever uma resposta para o remetente do e-mail selecionado. • **Responder a todos** — Clique para escrever uma resposta para o remetente e todos os outros destinatários do e-mail selecionado. • **Encaminhar** — Clique para encaminhar o e-mail selecionado. • **Imprimir** — Clique para imprimir o e-mail selecionado. • **Mostrar cabeçalhos/Ocultar cabeçalhos** — Clique para mostrar ou ocultar os cabeçalhos de e-mails.

5 Políticas

No Email Protection, as políticas definem regras para a filtragem de seus e-mails recebidos e enviados. As políticas de entrada protegem você contra spam, vírus e outros conteúdos nocivos. As políticas de saída, por outro lado, garantem a segurança e a adequação dos e-mails enviados a partir de seu sistema. O serviço inclui uma política de entrada e de saída padrão para cada um de seus domínios. Você também pode criar políticas personalizadas para qualquer domínio ou grupo.

Conteúdo

- *Página Políticas*
- *Janela Novo conjunto de políticas*
- *Gerenciando os conjuntos de políticas*
- *Detalhes*
- *Vírus*
- *Spam*
- *ClickProtect*
- *Conteúdo*
- *Anexos*
- *Permitir/Negar*
- *Autenticação de e-mail*
- *Notificações*
- *Recuperação de desastres*
- *Assinaturas de grupo*

Página Políticas

A página **Políticas** permite configurar conjuntos de políticas de entrada e saída.

Tabela 5-1 Opções da guia Políticas

Opção	Definição
Políticas de entrada	Exibe a lista de conjuntos de políticas de entrada. Selecione para configurar políticas de entrada para um domínio ou grupo.
Políticas de saída	Exibe a lista de conjuntos de políticas de saída. Selecione para configurar políticas de saída para um domínio ou grupo.

Tabela 5-2 Opções das páginas de políticas de entrada e saída

Opção	Definição
Barra de ferramentas Políticas	• **Aplicar** — Clique para salvar as alterações em uma política. • **Redefinir** — Clique para restaurar alterações anteriormente salvas. • **Novo** — Clique para criar uma nova política. • **Editar** — Clique para editar uma política existente. • **Excluir** — Clique para excluir uma política existente.
Lista de políticas	• **Nome**: especifica o nome da política. • **Proprietário**: especifica se a política pertence a um cliente ou grupo. • **Prioridade**: especifica a ordem de prioridade em que a política é aplicada em relação a outras políticas. • **Descrição**: especifica a descrição da política.

Janela Novo conjunto de políticas

Crie um novo conjunto de políticas para aplicar regras personalizadas de filtragem de e-mail em um cliente ou grupo.

Tabela 5-3 Opções da janela Novo conjunto de políticas

Opção	Definição
Salvar	Clique para salvar as alterações.
Cancelar	Clique nesta opção para fechar a janela sem salvar as alterações.
Nome	Insira o nome para a política.
Prioridade	Exibe a ordem de prioridade da política.
Direção	Mostra se a política é para o SMTP de entrada ou saída.
Descrição	Insira uma breve descrição da política.

Tabela 5-3 Opções da janela Novo conjunto de políticas *(continuação)*

Opção	Definição
Proprietário	Selecione o proprietário para especificar quem poderá editar a política: • **Cliente**: especifica que os administradores de clientes e superiores podem editar a política. • **Grupo**: especifica que os administradores de grupo do grupo especificado, bem como os administradores de clientes e superiores, podem editar a política. Selecione o grupo no menu suspenso.
Copiar de	Se necessário, selecione uma política existente para copiar as configurações para um novo conjunto de políticas. As opções a seguir se aplicam às opções de entrada: • **Copiar lista de permissão de remetente**: selecione esta opção para copiar a lista atual de permissão de remetente. • **Copiar lista de negação de remetente**: selecione esta opção para copiar a lista atual de negação de remetente. • **Copiar lista de blindagem de destinatário**: selecione esta opção para copiar a lista atual de blindagem de destinatário. • **Copiar lista de permissão do ClickProtect**: selecione esta opção para copiar a lista atual de permissão do ClickProtect.

Gerenciando os conjuntos de políticas

Os conjuntos de políticas permitem definir regras personalizadas de entrada e saída para cada um de seus domínios, além de regras padrão que se aplicam a todos os domínios.

Tabela 5-4 Opções de conjunto de políticas

Guia	Descrição	Entrada	Saída
Detalhes	Especifica o nome, a prioridade, a direção, o proprietário e a descrição do conjunto de políticas.	Sim	Sim
Vírus	Especifica as ações a serem executadas e as notificações a serem enviadas quando uma mensagem estiver infectada com um vírus.	Sim	Sim
Spam	Especifica o que fazer quando uma mensagem for identificada como spam.	Sim	Não
ClickProtect	Especifica formas de proteção contra endereços da Web em mensagens de e-mail que podem ter links para sites nocivos.	Sim	Não
Conteúdo	Especifica regras de filtragem para tipos específicos de conteúdo que podem ser inapropriados ou ofensivos.	Sim	Sim
Anexos	Especifica as regras de filtragem de anexos de e-mail.	Sim	Sim
Permitir/Negar	Especifica listas de remetentes que são automaticamente permitidos ou negados.	Sim	Não
Autenticação de e-mail	Especifica listas de domínios que devem ser verificados usando TLS, SPF ou uma assinatura DKIM antes que o e-mail seja enviado ou recebido.	Sim	Sim
Notificações	Especifica opções para as notificações de e-mail que são enviadas quando ocorre uma violação de política e uma ação é executada.	Sim	Sim

Tabela 5-4 Opções de conjunto de políticas *(continuação)*

Guia	Descrição	Entrada	Saída
Recuperação de desastres	Especifica regras para quando ocorre uma interrupção do e-mail e o Email Continuity está disponível.	Sim	Não
Assinaturas de grupo	Especifica a lista dos grupos que são afetados por esta política.	Sim	Sim

Detalhes

A guia **Detalhes** exibe as informações básicas de configuração para um conjunto de políticas existente.

Guia Detalhes

Visualize e edite o nome e a descrição do conjunto de políticas.

Tabela 5-5 Definições de opções da guia Detalhes

Opção	Definição
Salvar	Clique para salvar as alterações.
Cancelar	Clique para redefinir sem salvar as alterações.
Nome	Especifica o nome da política.
Prioridade	Especifica a ordem de prioridade da política (somente leitura).
Direção	Especifica se a política é para o SMTP de entrada ou saída (somente leitura).
Proprietário	Especifica quem pode editar a política (somente leitura).
Descrição	Especifica uma breve descrição para a política.

Vírus

O Email Protection fornece uma proteção contra vírus e worm altamente eficaz para toda a empresa. Através da identificação de vírus e worms no perímetro da rede antes que eles entrem ou deixem a infraestrutura de mensagens, o Email Protection minimiza os riscos de epidemia e infecção do seu sistema.

Proteção antivírus do Email Protection:

- Fornece proteção máxima usando diversos mecanismos antivírus líderes de mercado para permitir que o Email Protection personalize a proteção de forma a lidar com as ameaças mais recentes.
- Define as atualizações de definição de vírus a cada 5 minutos, oferecendo uma defesa imediata contra as ameaças mais recentes.
- Fornece varredura externa de vírus e gerenciamento de quarentena seguros para proteção contra vírus antes que eles alcancem a sua rede. Protege seus usuários, redes e dados contra danos.

Configurar ações a serem tomadas em relação a um vírus

Selecione as opções na subguia **Ações** para configurar como o sistema reagirá se um e-mail que contiver um vírus conhecido for recebido.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 No conjunto de políticas, selecione **Vírus** | **Ações**

2 No campo **Se uma mensagem contiver um vírus**, selecione a ação a ser tomada.

3 Se você selecionou, **Limpar a mensagem**, selecione uma outra ação em **Se uma mensagem não puder ser limpa**.

4 Clique em **Salvar**.

Ações relacionadas a vírus

A subguia **Ações** permite que você configure se os e-mails infectados serão colocados em quarentena, negados ou descontaminados. A tabela abaixo lista os tipos de configurações disponíveis.

Tabela 5-6 Definições de opções

Opção	Definição
Salvar	Clique para salvar as suas alterações.
Cancelar	Clique para restaurar valores anteriormente salvos.

Se uma mensagem contiver um vírus	• **Nenhuma ação** — Enviar o e-mail ao destinatário sem filtragem ou notificação (não recomendado).
	• **Colocar a mensagem em quarentena após o anexo ser removido** — Remover o anexo infectado do e-mail e enviá-lo para a área de quarentena de vírus sem notificação ao destinatário. Um texto é inserido no e-mail notificando o destinatário que um anexo foi removido.
	• **Remover o anexo** — Remover o anexo infectado do e-mail e enviá-lo para o destinatário. Um texto é inserido no e-mail notificando o destinatário que um anexo foi removido.
	• **Negar entrega** — Negar entrega da mensagem de e-mail.
	• **Limpar a mensagem** — Tenta remover o conteúdo com vírus e salvar o restante da mensagem.
	  • Se a limpeza for bem-sucedida, o e-mail será enviado ao destinatário com um texto inserido indicando que o e-mail passou por uma limpeza devido a um vírus.
	  • Se a limpeza não for bem-sucedida, o sistema executará a ação selecionada em **Se uma mensagem não puder ser limpa**.

Se uma mensagem não puder ser limpa	• **Colocar a mensagem em quarentena após o anexo ser removido** — Remover o anexo infectado do e-mail e enviá-lo para a área de quarentena de vírus sem notificação ao destinatário. Um texto é inserido no e-mail notificando o destinatário que um anexo foi removido. • **Remover o anexo** — Remover o anexo infectado do e-mail e enviá-lo para o destinatário. Um texto é inserido no e-mail notificando o destinatário que um anexo foi removido. • **Negar entrega** — Negar entrega da mensagem de e-mail.

Notificações [Vírus]

Use a subguia **Notificações** para selecionar quando as notificações de e-mail de uma ação são enviadas ao remetente e ao destinatário de um e-mail que está infectado por um vírus.

Tabela 5-7 Opções de notificação

Opção	Definição
Salvar	Clique para salvar as suas alterações.
Cancelar	Clique para restaurar valores anteriormente salvos.
Opções de remetente	Especifica que uma notificação foi enviada ao remetente, quando uma mensagem disparar a ação selecionada.
Opções de destinatário	Especifica que uma notificação foi enviada ao destinatário, quando uma mensagem disparar a ação selecionada.

Spam

O Email Protection fornece o produto de bloqueio de spam mais completo e eficiente disponível, bloqueando 98 por cento do spam e fornecendo uma baixa taxa de falsos positivos líder do setor. Uma probabilidade alta ou média de ser um spam é atribuída ao e-mail conforme apropriado e uma ação separada' pode ser atribuída a cada probabilidade.

Conteúdo

- *O que é spam?*
- *Configuração da política de classificação de spam*
- *Classificação*
- *Configuração de políticas de grupos de configurações*
- *Subguia Grupos de conteúdo*
- *Guia Geração de relatórios*

O que é spam?

Spam inclui e-mails comerciais não solicitados e indesejados que são enviados para vários endereços e que você deseja bloquear em sua caixa de entrada.

Em alguns casos, os criminosos usam o spam para coletar informações proprietárias ou causar danos a seu sistema de e-mail. Um spam desse tipo pode usar várias estratégias para ignorar filtros de spam, incluindo listas negras e listas de palavras-chave.

Bloqueio de spam e proteção contra inundação de devoluções

A Proteção de bloqueio de spam por meio de Listas de bloqueio em tempo real (RBLs) e a Proteção contra inundação de devoluções são dois métodos de proteção contra spam usados para bloquear endereços IP ou mensagens ofensivas.

Método de proteção contra spam	Definição
Proteção de bloqueio de spam por meio de RBLs	• As RBLs são usadas para identificar e-mails distribuídos por endereços IP de spammers conhecidos. • Elas são ativadas por padrão para todos os novos conjuntos de políticas. Essa configuração garante o mais alto nível de identificação de spam e bloqueia automaticamente as mensagens de endereços IP suspeitos. • As "listas de permissão" personalizadas têm precedência sobre RBLs em uma base por endereço. O endereço do remetente é sempre comparado às listas de permissão apropriadas antes da filtragem de RBL. O sistema entregará a mensagem se o endereço aparecer em uma lista de permissão. • Os clientes podem optar por não usar a proteção de RBL, mas, por motivos de segurança, isso não é recomendável.
Proteção contra inundação de devoluções	Nega o recebimento de mensagens de devolução não reconhecidas, mas permite as devoluções válidas que contenham um cabeçalho seguro fornecido pelo serviço de saída.

Filtragem de e-mail cinza (graymail)

O Email Protection inclui uma política de conteúdo pré-criada para a fácil identificação e bloqueio de e-mail cinza (graymail).

Ao contrário do spam, o graymail inclui mensagens de e-mail em massa, boletins informativos e anúncios legítimos. Por exemplo, um varejista que você uma vez aceitou, mas que agora deseja bloquear.

Definição de grupos de conteúdo

A filtragem de conteúdo de spam é controlada pela comparação do conteúdo de um e-mail com listas de palavras-chave ou frases predefinidas (grupos de conteúdo de spam). Você pode definir uma ação diferente para cada grupo de conteúdo de spam. A ação nesta janela substitui todas as outras ações de spam. Por exemplo, um e-mail que tenha uma probabilidade média de ser um spam também inclui conteúdo que está em um grupo de conteúdo de spam. Nesse caso, a ação definida para o grupo de conteúdo de spam se aplicará ao invés da ação para spam médio.

Esta política de e-mail é separada da filtragem de e-mail de Palavra-chave de conteúdo, controlada pela guia **Grupos de conteúdo**. Os e-mails colocados em quarentena são posicionados na área quarentena de conteúdo para a conta do usuário. Essa conta só pode ser acessada por gerenciadores de quarentena ou usuários de nível superior.

Quando o mesmo conteúdo estiver definido na guia **Spam** e na guia **Conteúdo**, as políticas de conteúdo serão utilizadas.

Configuração da política de classificação de spam

Use as configurações de política de classificação de spam para gerenciar e-mails indesejados automaticamente. Os diferentes níveis de classificação permitem que você selecione diferentes ações, dependendo do nível de risco das mensagens de e-mail.

Para obter definições de opções, clique em **Ajuda** na interface.

Tarefa

1 Em Email Protection, selecione **Políticas** e abra um conjunto de políticas.

2 Na janela do conjunto de políticas, selecione **Spam** | **Classificação**.

3 Selecione uma opção para cada nível de probabilidade de spam para especificar uma ação.

- **provavelmente spam (probabilidade média)**
- **quase certamente spam (probabilidade alta)**
- **e-mail cinza (graymail)**

4 Selecione as ações de política adicionais conforme necessário.

5 Clique em **Salvar**.

Classificação

Use a guia **Classificação** para configurar sua política de spam de entrada.

Tabela 5-8 Definições de opções

Opção	Definição
Salvar	Clique para salvar as alterações.
Cancelar	Clique para limpar as alterações.

Tabela 5-8 Definições de opções *(continuação)*

Opção	Definição

Quando uma mensagem é	• **provavelmente spam (probabilidade média)** — Especifica as mensagens que provavelmente são spam.
	  • **Marcar o assunto da mensagem com "[SPAM]"** — Acrescenta "[SPAM]" às mensagens, de forma que você possa classificar e analisá-las em seu cliente de e-mail local.
	  • **Colocar em quarentena** — Armazena as mensagens em quarentena.
	  • **Negar entrega** — Bloqueia as mensagens e notifica os remetentes quando as mensagens são rejeitadas.
	  • **Nenhuma ação** — Aceita todas as mensagens e não executa nenhuma outra ação.
	  Nenhuma ação é relatado no relatório **Ameaças: Spam** como **Outros** para mensagens de spam.
	• **quase certamente spam (probabilidade alta)** — Especifica as mensagens que muito provavelmente são spam.
	  • **Marcar o assunto da mensagem com "[SPAM]"** — Acrescenta "[SPAM]" às mensagens, de forma que você possa classificar e analisá-las em seu cliente de e-mail local.
	  • **Colocar em quarentena** — Armazena as mensagens em quarentena.
	  • **Negar entrega** — Bloqueia as mensagens e notifica os remetentes quando as mensagens são rejeitadas.
	  • **Nenhuma ação** — Aceita todas as mensagens e não executa nenhuma outra ação.
	  Nenhuma ação é relatado no relatório **Ameaças: Spam** como **Outros** para mensagens de spam.
	• **e-mail cinza (graymail)** — Especifica as mensagens que não são spam, mas podem incluir assinaturas de e-mail indesejadas e outras mensagens de e-mail em massa.
	  • **Marcar assunto com "[Graymail]"** — Acrescenta "[Graymail]" (e-mail cinza) às mensagens, de forma que você possa classificar e analisá-las em seu cliente de e-mail local.
	  • **Colocar em quarentena** — Armazena as mensagens em quarentena.
	  • **Negar entrega** — Bloqueia as mensagens e notifica os remetentes quando as mensagens são rejeitadas.
	  • **Nenhuma ação** — Aceita todas as mensagens e não executa nenhuma outra ação.
	  Nenhuma ação é relatado no relatório **Ameaças: Spam** como **Outros** para mensagens de spam.
	  • **Permitir** — Aceita todas as mensagens e fornece permissão aos remetentes no futuro.

Mais opções	• **Ativar listas de bloqueio em tempo real (RBLs)** — Selecione para ter uma proteção contra spam avançada, capaz de detectar e bloquear endereços IP que estão enviando campanhas de mala direta em massa. • **Bloquear mensagens devolvidas não reconhecidas ("backscatter")** — Selecione para impedir o recebimento de mensagens devolvidas não reconhecidas. • **Ativar prevenção contra inundação de spam** — Selecione para bloquear campanhas de spam com altos volumes e de curta duração, também conhecidas como spam "hailstorm". Desmarque para reduzir os falsos positivos quando a prevenção contra inundações de spam é a causa.

Configuração de políticas de grupos de configurações

Determine a ação a ser realizada se um e-mail tiver algum conteúdo definido como conteúdo de spam para grupos.

Tarefa

Para obter as definições das opções, clique em **Ajuda** na interface.

1. Em Email Protection, selecione **Políticas** e abra um conjunto de políticas.
2. Na janela do conjunto de políticas, selecione **Spam** | **Grupos de conteúdo**.
3. Clique em **Novo**.
4. Digite um **Nome do grupo** exclusivo para o novo grupo de conteúdo e configure as opções.
   a. Digite palavras-chave e frases associadas ao grupo de conteúdo no campo **Conteúdo**.
   b. Selecione a **Ação** apropriada.
      Por exemplo, **Quarentena**.
   c. Selecione **Ativar** para aplicar o grupo de conteúdo à política.
5. Clique em **Salvar**.

Subguia Grupos de conteúdo

Use a subguia **Grupos de conteúdo** para definir grupos de conteúdo e atribuir as ações a serem realizadas se um e-mail corresponder às palavras-chave ou frases determinadas.

Tabela 5-9 Definições da opção Grupos de conteúdo

Opção	Definição
Novo	Clique para criar um novo grupo de conteúdo.
Editar	Clique para editar um grupo de conteúdo existente.
Excluir	Clique para excluir um grupo de conteúdo.

Tabela 5-9 Definições da opção Grupos de conteúdo *(continuação)*

Opção	Definição
Tabela de grupos de conteúdo	Exibe uma lista dos grupos de conteúdo atuais. • **Nome do grupo** — Exibe o nome do grupo de conteúdo. • **Ação** — Exibe a ação a ser realizada. • **Ativado** — Exibe se o gripo de conteúdo está atualmente ativado ou não.

Opções de grupos de conteúdo	Especifica as configurações ao criar um novo grupo de conteúdo ou editar um nome de grupo existente.
	• **Nome do grupo** — Especifica o nome do grupo de conteúdo.
	• **Conteúdo** — Especifica as palavras-chave ou frases associadas ao grupo de conteúdo.
	• **Ação** — Especifica a ação a ser realizada.
	  • **Quarentena**
	  • **Negar**
	  • **Permitir**
	  • **Marcar assunto**
	• **Ativar** — Selecione para ativar o grupo de conteúdo.
	• **Salvar** — Clique para salvar as alterações.
	• **Cancelar** — Clique para fechar as opções de grupo de conteúdo sem salvar.
	  Você pode usar caracteres curinga — asterisco (*) e ponto de interrogação (?) — para definir o conteúdo de um grupo de conteúdo. O asterisco se aplica a um ou mais caracteres de uma cadeia de caracteres. O ponto de interrogação se aplica a um único caractere. Os caracteres curinga podem ser colocados dentro ou no final de uma cadeia de caracteres, mas não no início.

Guia Geração de relatórios

A guia **Geração de relatórios** permite que você configure o relatório de spam.

Tabela 5-10 Definições de opções de geração de relatórios

Opção	Definição
Salvar	Clique para salvar as alterações.
Cancelar	Clique para limpar as alterações.

Tabela 5-10 Definições de opções de geração de relatórios *(continuação)*

Opção	Definição

Configurações padrão	• **Enviar um relatório de spam por e-mail para** — Especifica quem recebe o relatório.
	  • **Todos os usuários atribuídos a esta política** — Todas as contas de usuário associadas ao conjunto de políticas.
	  • **Usuários selecionados** — Somente as contas de usuário configuradas para os relatórios de spam nas janelas de gerenciamento de usuários.
	  • **Nenhum usuário** — Nenhum usuário associado a esse conjunto de políticas.
	• **Formato** — Especifica o formato e o tipo de conteúdo a ser incluído no relatório de spam.
	  • **HTML - com ações** — Esse relatório HTML permite que o destinatário execute ações diretamente do relatório de spam. Você poderá aplicar **Liberar**, **Sempre permitir** ou (caso permitido) **Sempre negar** em cada mensagem do relatório. Também será possível aplicar **Excluir tudo** nas mensagens da quarentena de spam.
	  • **HTML - sem ações** — O relatório HTML não contém nenhum dos links de ação.
	  • **Texto claro** — O relatório está em texto claro.
	• **Tipo** — Especifica o que deverá estar incluído no relatório de spam.
	  • **Novos itens desde o último relatório** — Contém todas as novas mensagens de spam em quarentena adicionadas desde o último relatório gerado. Não se aplica aos relatórios de spam sob demanda.
	  • **Todos os itens colocados em quarentena** — Contém todas as mensagens de spam que foram colocadas em quarentena.
	• **Links do relatório de spam para o Control Console** — Especifica o número de dias que os links ficarão ativos antes de expirar. Dois valores adicionais permitem que você personalize o link:
	  • **Exigir autenticação** — O link não expira, mas exige que o usuário efetue logon.
	  • **Nunca expirar** — O link nunca expira.
	• **Mensagem personalizada** — Especifica o texto personalizado que pode ser adicionado ao relatório de spam. O texto pode ter no máximo 4.000 caracteres.

Programação e frequência	• **Frequência** — Especifica os dias da semana em que o relatório é enviado. Selecione um ou mais dias. • **Entregar relatórios às** — Especifica a hora do dia em que os relatórios estão programados para ser entregues. Você pode programar os Relatórios de spam para que sejam entregues uma ou duas vezes ao dia. Os relatórios são enviados pontualmente no horário especificado.  Todos os horários são baseados em sua configuração de fuso horário. Para configurar seu fuso horário, selecione **Gerenciamento de Contas** | **Clientes** | **Detalhes**. Selecione o link **atualizar** ao lado de **Fuso horário padrão**. Na janela pop-up, selecione o fuso horário e clique em **Atualizar**.

Tabela 5-10 Definições de opções de geração de relatórios *(continuação)*

Opção	Definição
Permitir a usuários.	• **personalizar opções de filtragem de spam** — Quando ativado, os usuários podem selecionar as ações para spam usando a guia **Preferências**. • **personalizar o tempo e a frequência de entrega do relatório de spam** — Quando ativado, os usuários podem selecionar a frequência dos relatórios usando a guia **Preferências**. • **personalizar o tipo de relatório** — Quando ativado, os usuários podem alterar o tipo de relatório usando a guia **Preferências**. • **desativar a filtragem de spam** — Quando ativado, os usuários podem desativar a filtragem de spam usando a guia **Preferências**. • **configurar endereço de e-mail alternativo para entrega de relatório de spam** — Quando ativado, os usuários podem especificar um endereço de e-mail alternativo usando a guia **Preferências**. O redirecionamento do relatório permite que o destinatário alternativo obtenha acesso total à conta do Control Console de um usuário. Incentive os usuários a escolherem endereços de e-mail alternativos com cautela. • **Clique aqui para fazer download o Spam Control for Outlook** ® — Quando ativado, os usuários podem baixar o utilitário Spam Control For Outlook. Você pode especificar o local para o download na página de configurações de marca. O acesso ao Spam Control for Outlook também pode ser ativado ou desativado direto do sistema.
Outras opções	Especifica outras opções ativadas para relatórios. • **Permitir que usuários que não são administradores efetuem login diretamente no Control Console** — Quando ativado, permite que os usuários efetuem login no Control Console usando a página de logon. Não afeta a capacidade de efetuar logon dos usuários selecionando um link no relatório de spam. Se o acesso ao Control Console não estiver ativado e os usuários não receberem o relatório de spam, as funções do gerenciador de quarentena ou de nível superior deverão realizar as alterações nas configurações do usuário. • **Exibir mensagens na quarentena usando a Exibição de mensagem segura** — Quando ativado, permite que os usuários exibam o conteúdo do corpo de um e-mail na janela de exibição de mensagem segura. Caso contrário, o usuário deverá liberar o e-mail para ver o que há no conteúdo do corpo. • **Exibir endereço de e-mail do usuário no relatório de spam** — Quando ativado, exibe os endereços de usuário e aliases no relatório de spam. • **Ativar o atalho "Negar" do relatório de spam** — Quando ativado, exibe o link **Sempre negar** no relatório de spam, a página **Quarentena de mensagem** e a página **Exibição de mensagem segura**. Caso contrário, os usuários deverão ir até a janela **Permitir/Negar listas de remetentes** para alterar as listas **Permitir** ou **Negar**. • **Mostrar a pontuação de spam no relatório de spam** — Quando ativado, exibe a pontuação de probabilidade de spam para cada mensagem em quarentena do relatório de spam.

ClickProtect

O ClickProtect protege sua organização contra ameaças baseadas na Web que podem chegar por e-mail usando a Reputação de URL do McAfee GTI®. Os URLs são avaliados durante o processamento

("no momento da varredura") e quando os usuários clicam em um link ("no momento do clique"). A varredura no momento do clique garante que os usuários estejam protegidos contra alterações na reputação de um site que podem ocorrer após a varredura inicial da mensagem.

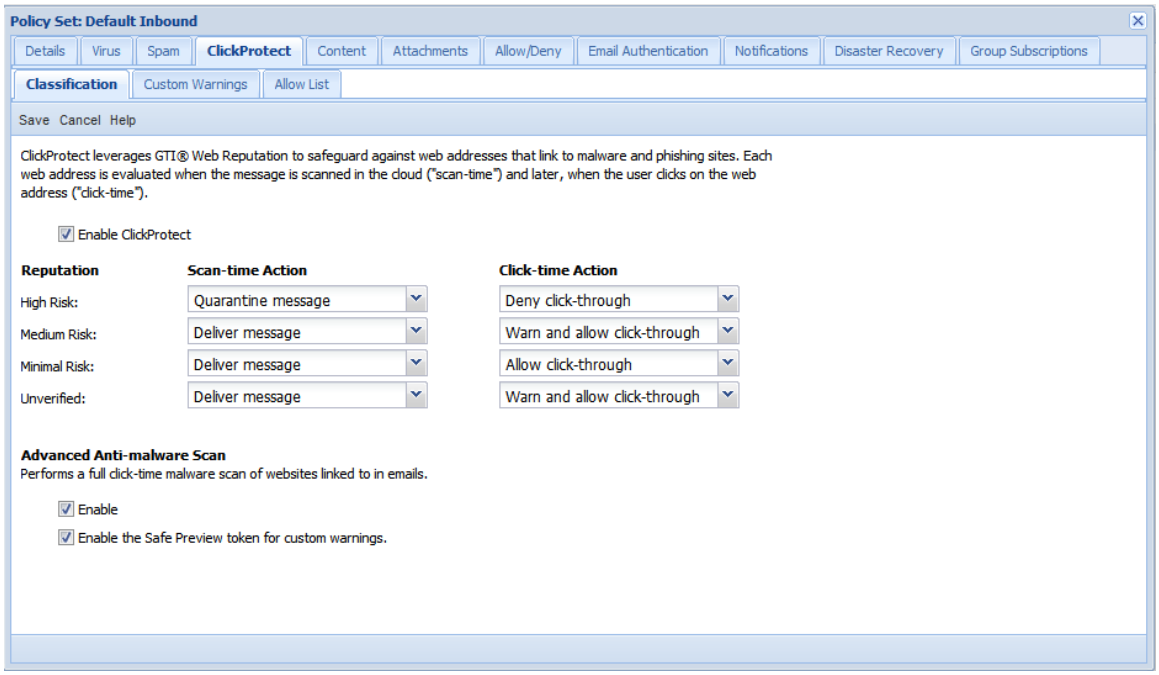

Figura 5-1 Nova guia ClickProtect na janela de política de entrada

Atualizar as opções do ClickProtect para um conjunto de política de entrada

Configure o ClickProtect para realizar ações específicas de momentos de varredura e de clique que protegem seus usuários de links de URL em mensagens de e-mail recebido que oferecem risco.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 Selecione **Email Protection** | **Políticas** | **Políticas de entrada**

2 Realce uma política personalizada ou selecione a política de Entrada padrão e clique em **Editar**.

3 Na janela **Conjunto de políticas**, selecione **ClickProtect**.

4 Selecione **Ativar o ClickProtect**.

5 Selecione as ações de momentos de varredura e de clique para cada tipo de reputação.

6 Em **Varredura antimalware avançada**, selecione as opções de varredura de malware, conforme necessário.

7 Clique em **Salvar**.

Depois de ativar o ClickProtect, você pode personalizar as mensagens de aviso que os seus usuários verão, bem como atualizar a lista de URLs aprovadas.

Guia Classificação

Use a guia **Classificação** para configurar as ações dos momentos de clique e varredura do ClickProtect.

Tabela 5-11 Definições de opções da guia Classificação

Opção	Definição
Salvar	Clique para salvar as alterações.
Cancelar	Clique para redefinir sem salvar as alterações.
Ativar o ClickProtect	Selecione para ativar o ClickProtect e configurar suas ações dos momentos de clique e varredura.
Reputação	Exibe as categorias de risco: • **Alto risco** — Especifica uma URL que apresenta comportamento prejudicial. Por exemplo, o site é conhecido por hospedar malware. • **Risco médio** — Especifica uma URL que apresenta comportamento questionável que pode ser prejudicial para o usuário. • **Risco mínimo** — Especifica uma URL que exibe comportamento adequado ou que é verificada como confiável. • **Não verificado** — Especifica uma URL de onde nenhuma informação de reputação foi obtida.
Ação do momento de varredura	Especifica a ação a ser realizada no momento de varredura, para cada tipo de reputação. • **Entregar mensagem** • **Mensagem em quarentena** • **Negar mensagem** • **Marcar assunto**
Ação do momento de clique	Especifica a ação a ser realizada no momento de clique, para cada tipo de reputação. • **Permite o click-through** — Selecione para redirecionar imediatamente o usuário ao site da Web. • **Avisa e permite o click-through**: selecione para exibir uma mensagem de aviso em um navegador e dar ao usuário a opção de prosseguir para o site solicitado. • **Negar click-through** — Selecione para exibir uma mensagem de bloqueio em um navegador e explicar o motivo pelo qual o site da Web foi negado. Você pode personalizar as páginas de aviso e de mensagem bloqueada na guia **Avisos personalizados**.
Varredura antimalware avançada	Especifica se você deseja ou não varrer links de e-mail quanto a malware no momento de clique. • **Ativar**: selecione para ativar a varredura antimalware. • **Ative o token Safe Preview para avisos personalizados**: selecione para ativar a opção **Safe Preview** na guia **Avisos personalizados**. Você pode personalizar a página de mensagem de aviso na guia **Avisos personalizados**.

Guia Avisos personalizados

A guia **Avisos personalizados** permite personalizar a página de aviso que é exibida quando um risco no site da Web é detectado no momento de clique. Cada campo de texto permite que você digite e formate o

texto usando as opções da barra de ferramentas. Você também pode adicionar tokens para exibir informações específicas sobre um link.

Tabela 5-12 Definições das opções da guia Avisos personalizados

Opção	Definição
Salvar	Clique para salvar o texto, os tokens e a formatação HTML.
Cancelar	Clique para descartar as alterações e restaurar o texto salvo anteriormente.
Avisa e permite	Especifica o texto exibido quando você seleciona **Avisa e permite o click-through** como a ação do momento de clique para um nível de risco. Esta página geralmente avisa o usuário do risco e oferece a opção de continuar ou abandonar o link.
Negar click-through	Especifica o texto exibido quando você seleciona **Negar click-through** como a ação do momento de clique para um nível de risco. Esta página geralmente avisa o usuário do risco e fornece uma explicação do motivo pelo qual o site foi bloqueado.
Malware encontrado	Especifica o texto exibido quando você ativa a opção **Varredura antimalware avançada** e o malware é encontrado.
Erro	Especifica o texto que é exibido quando ocorre um erro. Por exemplo, a reputação de um URL não pode ser verificada ou um site não pode ser verificado quanto a malware.

Tokens de avisos personalizados

Use esses tokens para incluir detalhes específicos sobre um link no texto da mensagem de aviso personalizado.

Tabela 5-13 Definições de tokens

Adicionar esse token	Para exibir
%URL%	O URL no qual o usuário clicou. Recomendado somente para a mensagem de aviso **Avisa e permite**.
%URL_REPUTATION%	O nível de risco do site com base em sua reputação. • Mínimo • Médio • Alto • Não verificado
%URL_CATEGORY%	A categoria do site.

Tabela 5-13 Definições de tokens *(continuação)*

Adicionar esse token	Para exibir

%IMAGE_PREVIEW%	Uma visualização segura do site da Web.
	Em determinadas situações, a visualização da imagem pode não ser exibida. Isso pode acontecer quando:
	• O acesso à pagina é negado devido ao valor %URL_REPUTATION%. Por exemplo, **Alto risco** está definido para **Negar click-through**.
	• A varredura de malware detectou um vírus.
	• Safe preview não está ativado para a **Varredura antimalware avançada**.
	• O valor %URL_CATEGORY% inclui conteúdo violento ou sexual.
	  • Extremo
	  • Conteúdo hediondo
	  • Nudez acidental
	  • Nudez
	  • Pornografia
	  • Roupas provocantes
	  • Materiais sexuais
	• Ocorre um erro durante a varredura de visualização, ou a varredura de visualização demora mais de 20 segundos.

%FROM_ADDRESS%	O endereço de e-mail que enviou o e-mail com o URL do site.
%DATE_TIME%	A data e a hora do e-mail.
%SUBJECT%	A linha de assunto do e-mail.
%MESSAGE_ID%	A ID da mensagem do e-mail.
%MALWARE_NAME%	O nome da ameaça de malware.

Exemplos de tokens de aviso personalizado

- O site que você solicitou é considerado risco de %URL_REPUTATION%.
- O link foi enviado a você por %FROM_ADDRESS% em %DATE_TIME%.
- A linha de assunto do e-mail era %SUBJECT%.
- Este site, %URL%, está associado à categoria %URL_CATEGORY%.

Guia Lista de permissão

A guia **Lista de permissão** permite configurar a lista de domínios, endereços IP e URLs que o ClickProtect sempre permite em um e-mail. Por exemplo, um site que você deseja excluir da reescrita de URL ou um site interno que o ClickProtect não consegue acessar.

- Cada domínio, endereço IP ou URL pode ter no máximo 256 caracteres.
- São permitidos caracteres curinga em domínios e endereços IP.
- Você pode adicionar no máximo 200 endereços IP.

Tabela 5-14 Definições de opções da guia Lista de permissão

Opção	Definição
Salvar	Clique para salvar as alterações da lista.
Cancelar	Clique para descartar as alterações e redefinir a lista.

Tabela 5-14 Definições de opções da guia Lista de permissão *(continuação)*

Opção	Definição
Domínio, Endereço IP ou URL	Campos do formulário: • **Domínio, endereço de e-mail ou endereço IP** — Digite um domínio, endereço de e-mail ou endereço IP válido. • **Adicionar >>** — Clique para adicionar um endereço à lista. • **<< Remover**: selecione um endereço na lista e clique em **<< Remover** para excluí-lo. • **<< Remover todos**: clique para excluir todos os endereços da lista. **Lista de permissão**: • **Endereço** — Exibe o domínio, o endereço de e-mail ou o endereço IP.
Mais opções	Fazer upload de uma lista: • **Procurar** — Clique para localizar um arquivo em sua unidade local. • **Fazer upload** — Clique para fazer upload do arquivo. Fazer download de uma lista: • **Fazer download** — Clique para fazer download da lista em um arquivo csv. Use as opções padrão: • **Assinar a lista ClickProtect da política de entrada padrão** — Especifica se a lista de Permissão de remetente da política padrão deve ser utilizada além de sua lista personalizada.

Conteúdo

As opções de filtragem de conteúdo permitem comparar o conteúdo de um e-mail em relação a listas de palavras-chave ou frases predefinidas (grupos de conteúdo).

Grupos de conteúdo

Os grupos de conteúdo permitem configurar como o sistema reage ao receber um e-mail contendo texto que viola as políticas de conteúdo.

Se o grupo de conteúdo estiver ativado, o conteúdo abaixo será filtrado no e-mail.

- Linguagem vulgar
- Racismo
- Conotação sexual

O Email Protection também fornece grupos de conteúdo predefinidos que contêm informações pessoais válidas e aceitáveis permitidas em mensagens de e-mail devido a políticas específicas. Esses grupos de conteúdo não podem ser editados, mas você poderá determinar se eles serão ou não usados. Veja abaixo os dois tipos de grupos de conteúdo predefinidos.

- Número do cartão de crédito
- CPF

Os cartões de crédito suportados são AMEX, VISA, MC e DISC.

Os números de cartão de crédito e de CPF podem ser representados ou formatados de diversas maneiras. É possível que o Email Protection não consiga capturar todas as mensagens que contenham essas informações.

Editar grupos de conteúdo [políticas de entrada]

Defina ações para grupos de conteúdo de política de entrada.

Tarefa

1. Selecione um grupo de conteúdo e clique em **Editar**.
2. No campo **Nome do grupo**, digite o grupo de conteúdo personalizado.
3. No menu **Ação**, selecione uma opção.
   - **Nenhum** — Encaminha o e-mail para o endereço de e-mail do destinatário.
   - **Quarentena** — Envia o e-mail para a quarentena.
   - **Negar** — Nega a entrega do e-mail.
   - **Permitir** — Envia o e-mail para o endereço de e-mail do destinatário.
   - **Marcar assunto** — Adiciona a frase "[CONTEÚDO]" à linha de assunto do e-mail. Envia o e-mail para o endereço de e-mail do destinatário.
4. Se desejar enviar uma cópia do e-mail para outro endereço, selecione uma lista de distribuição predefinida no menu **Cópia silenciosa**.
5. Selecione **Ativar**.
6. Clique em **Salvar**.

Grupos de conteúdo da política de saída

Uma varredura determinada dos **Grupos de conteúdo da política de saída** é disparada nas mensagens quando há o uso de palavras-chave pré-determinadas de dicionário de política. Uma biblioteca de regras de conformidade pré-definidas é fornecida.

Antes de iniciar

Essa função fica disponível para políticas de saída apenas para aqueles que assinaram o Email Encryption. Se o um cliente ou domínio assinar o Email Encryption, ele poderá escolher essa opção para forçar o Email Encryption caso a mensagem contenha a palavra [encrypt]. Essa palavra [encrypt] pode estar na linha de assunto da mensagem ou no corpo do texto da mensagem de saída.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 As opções abaixo estão disponíveis.

Opção	Descrição
Expandir todos	Clique para exibir e selecionar uma opção na lista de dicionários estendidos.
Recolher todos	Clique para fechar a lista estendida.
Criptografar mensagem	Estará disponível para grupos de conteúdo de saída se o cliente tiver assinado a criptografia.

A combinação para o tamanho máximo de mensagem criptografada inclui o cabeçalho, o corpo e o anexo da mensagem, não podendo ultrapassar 30 MB nas mensagens criptografadas.

2 Clique em **Iniciar validador** para abrir a janela **Validação de expressão regular**.

3 Digite a **Expressão regular**.

Copie o texto de amostra no campo **Texto de amostra**.

4 Clique em **Testar**. Se a expressão regular for encontrada dentro do texto de amostra, ela será marcada no campo **Resultado: Correspondência**.

COPIE SUA EXPRESSÃO REGULAR para o campo de conteúdo antes de fechar a janela **Validação de expressão regular**. As informações não são preenchidas automaticamente no campo de conteúdo. Você perderá suas informações.

Nomes dos grupos de conteúdo das políticas de saída

Escolha uma destas opções para configurar os grupos de conteúdo de sua política de saída. Estas configurações garantem que suas mensagens de e-mail de saída respeitem as regras regulamentares internacionais de conformidade, bem como as regras de conformidade operacional da sua empresa.

Tabela 5-15 Definições dos nomes dos gruposs

Categoria	Definições de opções
Uso aceitável	• **Memorandos confidenciais internos**: termos normalmente encontrados em memorandos internos da empresa. Termos geralmente usados para expressar confidencialidade. • **Substâncias controladas**: termos relacionados a substâncias ilegais. • **Discriminação**: termos relacionados a racismo e intolerância. • **Apostas**: termos relacionados a jogos de azar. • **Linguagem ofensiva**: termos relacionados à linguagem vulgar. • **Linguagem ameaçadora**: termos que geralmente estão relacionados a produtos químicos nocivos ou armas.
Política da Austrália	• **Carteira de habilitação de Nova Gales do Sul**: expressões normalmente usadas para oferecer suporte a números de carteira de habilitação. Padrões relacionados à carteira de habilitação de Nova Gales do Sul. • **Carteira de habilitação de Queensland**: expressões normalmente usadas para oferecer suporte a números de carteira de habilitação. Padrões relacionados à carteira de habilitação de Queensland. • **Número fiscal**: padrões relacionados ao número fiscal da Austrália. • **Carteira de habilitação de Vitória**: expressões normalmente usadas para oferecer suporte a números de carteira de habilitação. Padrões relacionados à carteira de habilitação de Vitória.
Política da Áustria	• **IBAN da Áustria**: padrões numéricos relacionados ao IBAN austríaco.
Setor financeiro e bancário	• **Número de roteamento ABA**: número de roteamento ABA com soma de verificação e validação de palavra-chave.
Política do Brasil	• **CEP do Brasil**: padrões relacionados ao CEP brasileiro. • **CNPJ do Brasil**: padrões relacionados ao Cadastro nacional de pessoas jurídicas. • **CPF do Brasil**: padrões relacionados ao Cadastro de Pessoas Físicas. • **Placa de carro do Brasil**: padrões relacionados a placas de carro brasileiras.

Tabela 5-15 Definições dos nomes dos gruposs *(continuação)*

Categoria	Definições de opções
Política do Canadá	• **Carteira de habilitação da província de Alberta**: expressões normalmente usadas para oferecer suporte a números de carteira de habilitação. Padrões numéricos relacionados à carteira de habilitação da província de Alberta. • **Serviços de saúde da província de Alberta**: padrões numéricos relacionados ao cartão de saúde da província de Alberta. • **Passaporte canadense**: padrões numéricos relacionados ao cartão de saúde da província de Ontário. • **Carteira de habilitação da província de Manitoba**: expressões normalmente usadas para oferecer suporte a números de carteira de habilitação. Padrões relacionados à carteira de habilitação da província de Manitoba. • **Serviços de saúde da província de Manitoba**: padrões numéricos relacionados ao cartão de saúde da província de Manitoba. • **Carteira de habilitação da província de Ontario**: expressões normalmente usadas para oferecer suporte a números de carteira de habilitação. Padrões numéricos relacionados à carteira de habilitação da província de Ontário. • **Serviços de saúde da província de Ontario**: padrões numéricos relacionados ao cartão de saúde da província de Ontario. • **Carteira de habilitação da província de Quebec**: expressões normalmente usadas para oferecer suporte a números de carteira de habilitação. Padrões numéricos relacionados à carteira de habilitação da província de Quebec. • **Serviços de saúde da província de Quebec**: padrões numéricos relacionados ao cartão de saúde da província de Quebec. • **Carteira de habilitação da província de Saskatchewan**: expressões normalmente usadas para oferecer suporte a números de carteira de habilitação. • **Serviços de saúde da província de Saskatchewan**: padrões numéricos relacionados ao cartão de saúde da província de Saskatchewan. • **Número de seguridade social**: padrões numéricos relacionados ao número de seguridade social Canadense.
Política da China	• **Passaporte chinês**: padrões relacionados ao passaporte chinês.
Política de Hong Kong	• **Documento de identificação de Hong Kong**: padrões relacionados ao documento de identificação de Hong Kong.
Política de Taiwan	• **ID do cidadão**: padrões relacionados ao número de identidade do cidadão de Taiwan.
Vantagem competitiva	• **Atas de reuniões do conselho**: termos normalmente encontrados em documentos que detalham as atividades da reunião do conselho. • **Informações sobre preços**: termos frequentemente encontrados em listas de preços.

Tabela 5-15 Definições dos nomes dos gruposs *(continuação)*

Categoria	Definições de opções
Descontentamento de funcionário	• **Comunicações de empregados descontentes**: termos geralmente usados por alguém para expressar o descontentamento com seu trabalho ou outros. • **Pesquisa de empregos executivos**: termos encontrados nas pesquisas de empregos executivos. • **Currículo**: termos frequentemente encontrados em um resumo pessoal ou curriculum vitae. • **Declaração de imposto ou dados relacionados**: expressão normalmente usada para o número de identificação do empregador.
IP da indústria de entretenimento	• **Programações registradas**: termos geralmente encontrados na programação do entretenimento ou transmissão.
Conformidade FERPA	• **Números de seguridade social e etnias**: número de seguridade social com verificação SSA e verificação de palavra-chave. Termos que descrevem o histórico étnico de uma pessoa. • **Números de seguridade social e níveis**: número de seguridade social com verificação SSA e verificação de palavra-chave. Termos frequentemente encontrados junto com informações sobre notas de alunos.
Conformidade financeira e de segurança	• **Documentos de auditorias financeiras**: termos relacionados a auditorias financeiras. • **Documentos de relatórios financeiros**: termos e expressões geralmente usados em relatórios financeiros. • **Documentos de declarações financeiras**: termos geralmente encontrados em declarações financeiras.
Conformidade FISMA	• **Avaliação de alto impacto FIPS**: classificação FIPS do sistema com avaliação de alto impacto. • **Avaliação de baixo impacto FIPS**: classificação FIPS do sistema com avaliação de baixo impacto. • **Avaliação de médio impacto FIPS**: classificação FIPS do sistema com avaliação de médio impacto.
Política da França	• **IBAN da França**: padrões numéricos relacionados ao IBAN francês. • **INSEE**: padrões numéricos relacionados ao código INSEE francês.
Política da Alemanha	• **IBAN da Alemanha**: padrões numéricos relacionados ao IBAN alemão.
Conformidade GLBA	• **Número de roteamento ABA**: número de roteamento ABA com soma de verificação e validação de palavra-chave. • **Violações de números de cartão de crédito**: número de cartão de crédito com verificação de palavra-chave. • **Violações de relatórios de crédito**: termos geralmente encontrados em um relatório de crédito. • **Violações de números de seguridade social**: número de seguridade social com verificação SSA e verificação de palavra-chave.

Tabela 5-15 Definições dos nomes dos gruposs *(continuação)*

Categoria	Definições de opções
Conformidade HIPAA	• **Termos médicos e números de cartão de crédito**: número de cartão de crédito com verificação de palavra-chave. Termos geralmente encontrados junto com um diagnóstico médico. • **Informações pessoais de saúde contendo dados de admissão e saída**: informações relacionadas à admissão e saída do paciente. • **Informações pessoais de saúde contendo números de seguridade social**: informações relacionadas à admissão e saída do paciente. Número de seguro social com verificações SSA e de palavra-chave. • **Informações pessoais de saúde contendo dados de diagnóstico**: termos normalmente encontrados em um diagnóstico médico. • **Termos médicos e números de seguridade social**: número de seguridade social com verificação SSA e verificação de palavra-chave. Termos geralmente encontrados junto com um diagnóstico médico.
Política da Índia	• **PAN da Índia**: padrões relacionados ao número de conta permanente indiano.
Política de Israel	• **IBAN de Israel**: padrões de texto relacionados à identificação israelense. • **Identificação de Israel**: padrões de numéricos relacionados à identificação israelense.
Política da Coreia	• **Número de registro de residente**: padrões relacionados ao número de registro de residente da Coreia.
Jurídico	• **Comunicações entre cliente e advogado** : termos normalmente encontrados em comunicações entre cliente e advogado. • **Ação judicial e assuntos jurídicos**: termos normalmente encontrados em documentos jurídicos.
Política do México	• **CURP do México**: padrões relacionados ao CURP mexicano (Clave Única de Registro de Población). • **NSS do México**: padrões relacionados ao número de seguro social mexicano. • **RFC do México**: padrões relacionados ao registro federal de contribuintes mexicano. • **CLABE do México**: Padrões relacionados ao CLABE mexicano.
Política da Holanda	• **IBAN da Holanda**: padrões numéricos relacionados ao IBAN holandês.

Tabela 5-15 Definições dos nomes dos gruposs *(continuação)*

Categoria	Definições de opções
PII da América do Norte	• **Violações em massa de números de seguridade social**: padrões numéricos relacionados ao número de seguridade social Canadense. • **Violações em massa dos números de seguridade social**: número de seguridade social com verificação SSA e verificação de palavra-chave. Limite numérico dos números do serviço social. O padrão é definido como superior a 100. • **Violações de informações de identificação pessoal do Canadá**: padrões numéricos relacionados ao número de seguridade social Canadense. • **Violações de números de identificação de empregados**: expressão normalmente usada para o número de identificação do empregado. • **Violações de números de seguridade social**: padrões numéricos relacionados ao número de seguridade social Canadense. • **SOMENTE violações de números de seguridade social**: número de seguridade social somente com verificação SSA, sem necessidade de palavra-chave. • **Violações de números de seguridade social**: número de seguridade social com verificação SSA e verificação de palavra-chave. • **Violações de número de cartão de crédito não criptografado** : número de cartão de crédito com verificação de palavra-chave. • **Violações de informações de identificação pessoal dos Estados Unidos**: número de seguridade social com verificações SSA e de palavra-chave.
Indústria dos cartões de pagamento	• **Violações em massa de números de cartões de crédito**: número de cartão de crédito com verificação de palavra-chave. Limite numérico dos números de cartão crédito. O padrão é definido como superior a 100 números de cartão de crédito. • **Violações de números de cartão de crédito**: número de cartão de crédito com verificação de palavra-chave.
Política da Polônia	• **Número PESEL**: padrões numéricos relacionados ao PESEL polonês. • **Número NIP**: padrões numéricos relacionados ao NIP polonês. • **Número de passaporte**: padrões numéricos relacionados ao número de passaporte polonês. • **Número Regon**: padrões numéricos relacionados à ID Regon polonesa. • **IBAN da Polônia**: padrões numéricos relacionados ao IBAN polonês.
Política da Rússia	• **Fundo de pensão da Rússia**: padrões relacionados ao número individual do fundo de pensão russo. • **Identificação fiscal pessoal da Rússia**: padrões relacionados à identificação fiscal pessoal russa. • **Passaporte externo da Rússia** : padrões relacionados ao passaporte externo russo. • **Passaporte interno da Rússia** : padrões relacionados ao passaporte interno russo.
Política de Singapura	• **Padrão de conta bancária** : termos relacionados a informações de contas bancárias. Padrões relacionados às contas bancárias na Singapura. • **NRIC** : padrões relacionados à carteira de identidade de registro nacional da Singapura. • **Número Sofinummer**: padrões numéricos relacionados ao Sofinummer holandês.

Tabela 5-15 Definições dos nomes dos gruposs *(continuação)*

Categoria	Definições de opções
Conformidade SOX	• **Atas de reuniões do conselho**: termos normalmente encontrados em documentos que detalham as atividades da reunião do conselho. Termos geralmente encontrados que são sensíveis à lei Sarbanes-Oxley. • **Remuneração e benefícios**: termos relativos à remuneração e benefícios. Termos geralmente encontrados que são sensíveis à lei Sarbanes-Oxley. • **Relatórios de conformidade**: termos geralmente encontrados em relatórios de conformidade. Termos geralmente encontrados que são sensíveis à lei Sarbanes-Oxley. • **Relatórios financeiros**: termos e expressões geralmente usados em relatórios financeiros. Termos geralmente encontrados que são sensíveis à lei Sarbanes-Oxley. • **Divulgações de declarações financeiras**: termos geralmente encontrados em declarações financeiras. Termos geralmente encontrados que são sensíveis à lei Sarbanes-Oxley. • **Fusão e aquisição**: termos geralmente usados em cenários de fusão ou aquisição. Termos geralmente encontrados que são sensíveis à lei Sarbanes-Oxley. • **Declarações de lucro e prejuízo**: termos frequentemente usados em declarações de lucro e prejuízo. Termos geralmente encontrados que são sensíveis à lei Sarbanes-Oxley. • **Ganhos projetados**: termos frequentemente encontrados em informações sobre ganhos projetados. Termos geralmente encontrados que são sensíveis à lei Sarbanes-Oxley. • **Previsão de vendas**: termos geralmente encontrados em uma previsão de vendas. Termos geralmente encontrados que são sensíveis à lei Sarbanes-Oxley. • **Relatórios de atividades suspeitas**: termos geralmente encontrados em um relatório de atividades suspeitas. Termos geralmente encontrados que são sensíveis à lei Sarbanes-Oxley.
Política da Espanha	• **DNI da Espanha**: padrões relacionados ao DNI (Documento Nacional de Identidad) espanhol. • **IBAN da Espanha**: padrões relacionados ao IBAN espanhol.
Leis de privacidade estaduais	• **Lei da carteira de habilitação da Califórnia**: expressões normalmente usadas para oferecer suporte a números de carteira de habilitação. • **Número de seguridade social**: número de seguridade social com verificações SSA e de palavra-chave.
Política da Turquia	• **Número do cidadão da Turquia**: padrões relacionados ao número do cidadão turco. • **IBAN da Turquia**: padrões relacionados ao IBAN turco.

Tabela 5-15 Definições dos nomes dos gruposs *(continuação)*

Categoria	Definições de opções
Política do Reino Unido	• **Número NHS**: padrões relacionados ao número do serviço nacional de saúde do Reino Unido. • **NINO**: padrões relacionados ao número de seguridade social do Reino Unido. • **SEDOL**: padrões relacionados à SEDOL do Reino Unido. • **IBAN do Reino Unido**: padrões relacionados ao IBAN do Reino Unido.
Grupos sem categoria	• **Política da China - Identificação nacional chinesa**: padrões relacionados à identificação nacional chinesa. • **Conteúdo sexual**: termos relacionados a sexo.

Grupos de conteúdo personalizados

Os grupos de conteúdo personalizados permitem definir suas próprias regras personalizadas. Ao configurar um grupo de conteúdo, você pode determinar como o sistema reage ao receber um e-mail contendo um texto que corresponde a uma determinada regra. Também é possível definir uma ação diferente para cada regra de grupo de conteúdo.

- Você pode adicionar até 2.000 grupos de conteúdo personalizados.
- Cada grupo de conteúdo personalizado está limitado a 255 caracteres.

Configurar políticas de grupos de conteúdo personalizados

Determine a ação a ser realizada se um e-mail tiver algum conteúdo definido como conteúdo personalizado para grupos.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 Em Email Protection, selecione **Políticas** e abra um conjunto de políticas.

2 Na janela Conjunto de políticas, selecione **Conteúdo** | **Grupos de conteúdo personalizados**.

3 Clique em **Novo**.

4 Digite um **Nome do grupo** exclusivo para o novo grupo de conteúdo e configure as opções.

a Digite palavras-chave e frases associadas ao grupo de conteúdo no campo **Conteúdo**.

As políticas de criptografia de saída são compatíveis com as expressões regulares do conteúdo. Se necessário, selecione **Ativar expressões regulares**. Use o **Validador de expressões regulares** para testar a precisão de suas expressões regulares.

b Selecione a **Ação** apropriada.

Por exemplo, **Quarentena**.

c Selecione **Ativar** para aplicar o grupo de conteúdo à política.

5 Clique em **Salvar**.

Grupos de conteúdo personalizados

Use a guia **Grupos de conteúdo personalizados** para definir grupos de conteúdo e atribuir as ações a serem executadas se um e-mail corresponder às palavras-chave ou frases determinadas.

Tabela 5-16 Grupos de conteúdo personalizados

Opção	Definição
Novo	Clique para criar um grupo de conteúdo.
Editar	Clique para editar um grupo de conteúdo existente.
Excluir	Clique para excluir um grupo de conteúdo.
Lista de grupos de conteúdo personalizados	Exibe uma lista dos grupos de conteúdo atuais. • **Nome do grupo** — Exibe o nome do grupo de conteúdo. • **Ação** — Exibe a ação a ser realizada. • **Lista de cópias silenciosas** — Exibe a lista de distribuição de e-mail que recebe cópias silenciosas. • **Ativado** — Exibe se o grupo de conteúdo está ativado.

Tabela 5-16 Grupos de conteúdo personalizados *(continuação)*

Opção	Definição

Adicionar ou alterar um grupo de conteúdo personalizado	Especifica as configurações ao criar um grupo de conteúdo ou editar um nome de grupo existente.
	• Nome do grupo
	• Conteúdo
	• Ação
	• Ativar
	• Salvar
	• Cancelar
	• **Nome do grupo** — Especifica o nome do grupo de conteúdo.
	• **Conteúdo** — Especifica as palavras-chave ou frases associadas ao grupo de conteúdo.
	• **Ativar expressões regulares** (apenas para políticas de criptografia de saída) — Selecione esta opção para ativar o uso de expressões regulares no campo **Conteúdo**.
	• **Iniciar validador** (apenas para políticas de criptografia de saída) — Clique nesta opção para abrir a janela **Validador de expressão regular**.
	• **Ação** — Especifica a ação a ser executada.
	  • **Quarentena**
	  • **Negar**
	  • **Permitir**
	  • **Marcar assunto**
	• **Cópia silenciosa** — Selecione a lista de distribuição que recebe cópias silenciosas.
	• **Ativar** — Selecione esta opção para ativar o grupo de conteúdo.
	• **Salvar** — Clique para salvar as alterações.
	• **Cancelar** — Clique para fechar as opções de grupo de conteúdo sem salvar.
	Você pode usar caracteres curinga – asterisco (*) e ponto de interrogação (?) – para definir o conteúdo de um grupo. O asterisco se aplica a um ou mais caracteres de uma cadeia de caracteres. O ponto de interrogação se aplica a um único caractere. Os caracteres curinga podem ser colocados dentro ou no final de uma cadeia de caracteres, mas não no início.

Janela **Validador de expressão regular** (apenas para políticas de saída)	Use o validador de expressão regular para testar suas expressões regulares. Se os resultados da pesquisa não corresponderem aos esperados, altere sua expressão regular. • **Expressão regular** — Digite seus critérios de expressão regular. • **Texto de amostra** — Digite o texto de amostra que contém os termos que você deseja pesquisar. • **Teste** — Clique para validar a expressão regular. • **Resultado** — Exibe os resultados da pesquisa.

Documentos registrados

Você pode filtrar os e-mails enviados para impedir que documentos registrados sejam enviados para usuários fora da organização.

Configurar ações para documentos registrados

Atribua ações apropriadas em suas políticas de saída para documentos registrados.

> **Antes de iniciar**
> Faça upload de seus documentos selecionando **Instalação** | **Documentos registrados**.

Tarefa

1 No Email Protection, selecione **Políticas** | **Políticas de saída**.

2 Selecione uma política e clique em **Editar**.

3 Na janela do conjunto de políticas, selecione **Conteúdo** | **Documentos registrados**.

4 Selecione um documento e clique em **Editar**.

5 Digite uma descrição.

6 Selecione uma ação na lista suspensa **Ação**.

Opção	Descrição
Nenhum	O e-mail é encaminhado ao endereço de e-mail do destinatário.
Quarentena	O e-mail é enviado para a área de quarentena de conteúdo do destinatário.
Negar	A entrega do e-mail é negada.
Permitir	O e-mail é enviado ao endereço de e-mail do remetente.
Marcar assunto	A palavra "[CONTEÚDO]" é adicionada à linha de assunto do e-mail no início do texto do assunto. O e-mail é enviado para o endereço de e-mail do destinatário.
Mensagem criptografada	As mensagens criptografadas não podem exceder 30 MB. Esse limite inclui o tamanho combinado do cabeçalho, do corpo e de todos os anexos da mensagem.

7 Selecione uma lista de distribuição predefinida na lista suspensa **Cópia silenciosa**.

8 Selecione **Ativar** e clique em **Salvar**.

Notificações [Conteúdo]

Use a subguia **Notificações** para selecionar quando as notificações de e-mail de uma ação são enviadas ao remetente e ao destinatário de um e-mail que viola uma política de grupo de conteúdo.

Tabela 5-17 Opções de notificação

Opção	Definição
Salvar	Clique para salvar as suas alterações.
Cancelar	Clique para restaurar valores anteriormente salvos.
Opções de remetente	Especifica que uma notificação foi enviada ao remetente, quando uma mensagem disparar a ação selecionada.
Opções de destinatário	Especifica que uma notificação foi enviada ao destinatário, quando uma mensagem disparar a ação selecionada.

Guia HTML Shield

A HTML Shield permite que você aplique uma camada adicional de segurança a e-mails formatados em HTML eliminando níveis variáveis de conteúdo HTML potentiacialmente prejudiciais. É útil para bloquear possíveis *ameaças recentes* ou ameaças que tenham como destino vulnerabilidades

anteriormente desconhecidas que possam estar ocultas no código HTML. A HTML Shield é útil especialmente para usuários que receberam e-mails perigosos anteriormente.

Tabela 5-18 Opções da HTML Shield

Opção	Definição
Salvar	Clique para salvar as alterações.
Cancelar	Clique para cancelar as alterações.
Proteção HTML Shield	Especifica o nível de proteção: • **Baixo** — lida com as origens baseadas em HTML mais comuns de possíveis explorações removendo as marcações de HTML maliciosas. • **Médio** — adiciona opções de segurança adicionais desabilitando o Javascript, o Java e o ActiveX, bem como removendo ameaças que possam estar ocultas nos comentários de HTML ou atributos de HTML inválidos. • **Alto** — fornece o nível mais alto de proteção removendo todo o conteúdo de HTML. • **Nenhum** — a proteção HTML Shield não está ativa.
Opções para configurações baixa e média	Especifica opções adicionais que você pode definir ao selecionar o nível de proteção HTML Shield Baixo ou Médio.

Anexos

A filtragem de anexos oferece a você a capacidade de controlar os tipos e tamanhos de anexos permitidos que entram na sua rede de e-mails.

- **Filtragem de anexos por tipo de arquivo** — Ative ou desative a filtragem de anexos por tipo de arquivo. O tipo de arquivo é determinado usando a extensão do arquivo, o tipo de conteúdo MIME e a composição binária.
- **Filtragem de anexos por tamanho** — Designa um tamanho máximo permitido para cada tipo de anexo ativado.
- **Regras de anexo personalizadas por nome de arquivo** — Configure regras personalizadas usando nomes de arquivo que substituam as configurações globais em um tipo de arquivo de anexo. Você pode designar que a regra use o nome de arquivo inteiro ou uma parte dele.
- **Filtragem de arquivos contidos em um anexo de arquivo ZIP** — Configure regras personalizadas para fazer com que o Email Protection analise os arquivos dentro de um anexo de arquivo ZIP, se possível, para determinar se há algum arquivo no ZIP que viole as políticas de anexo. Se o arquivo ZIP não puder ser analisado, designe a ação de e-mail a ser aplicada.
- **Regras de anexo de arquivo ZIP criptografado ou de "alto risco"** — Configure regras personalizadas para e-mails com arquivos ZIP criptografados e/ou arquivos ZIP considerados de alto risco (grandes demais, excesso de níveis aninhados, etc.).

Tipos de arquivos

A subguia **Tipos de arquivos** permite que você configure como o sistema reagirá se receber um e-mail de um tipo de anexo específico ou se um anexo violar políticas de anexo.

Por padrão, todos os anexos que não estejam na lista de permissão serão filtrados em relação à ação selecionada. Os anexos são investigados em termos de nome de arquivo, tipo de conteúdo MIME e composição binária.

Tipos de arquivo anexo

Tipos de arquivo anexo permitidos e suas extensões.

Tabela 5-19 Os tipos de arquivo permitidos.

Tipos de arquivo permitidos	Extensões de arquivo
Documentos do Microsoft Word	*.doc, *.dot, *.rtf, *.wiz
Documentos do Microsoft PowerPoint	*.pot, *.ppa, *.pps, *.ppt, *.pwz
Documentos do Microsoft Excel	*.xla, *.xlb, *.xlc, *.xlk, *.xls, *.xlt, *.xlw
Arquivos do Microsoft Access	*.adp, *.ldb, *.mad, *.mda, *.mdb, *.mdz, *.snp
Outros arquivos do Microsoft Office	*.cal, *.frm, *.mbx, *.mif, *.mpc, *.mpd, *.mpp, *.mpt, *.mpv, *.win, *.wmf
Documentos do Office Word 2007 XML	*.docx
Documento com capacidade de macro do Office Word 2007 XML	*.docm
Modelo do Office Word 2007 XML	*.dotx
Modelo com capacidade de macro do Office Word 2007 XML	*.dotm
Pasta de trabalho do Office Excel 2007 XML	*.xlsx
Pasta de trabalho com capacidade de macro do Office Excel 2007 XML	*.xlsm
Modelo do Office Excel 2007 XML	*.xltx
Modelo com capacidade de macro do Office Excel 2007 XML	*.xltm
Pasta de trabalho binária do Office Excel 2007 (BIFF12)	*.xlsb
Complemento com capacidade de macro do Office Excel 2007 XML	*.xlam
Apresentação do Office PowerPoint 2007 XML	*.pptx
Apresentação capacidade de macro do Office PowerPoint 2007 XML	*.pptm
Modelo do Office PowerPoint 2007 XML	*.potx
Modelo XML com capacidade de macro do Office PowerPoint 2007	*.potm
Complemento XML com capacidade de macro do Office PowerPoint 2007	*.ppam
Apresentação do Office PowerPoint 2007 em slide show	*.ppsx
Apresentação com capacidade de macro do Office PowerPoint 2007 XML em slide show	*.ppsm
Arquivos do Adobe Acrobat (PDF)	*.abf, *.atm, *.awe, *.fdf, *.ofm, *.p65, *.pdd, *.pdf
Arquivos Macintosh	*.a3m, *.a4m, *.bin, *.hqx, *.rs_
Arquivos compactados ou arquivados	*.arj, *.bz2, *.cab, *.gz, *.gzip, *.jar, *.lha, *.lzh, *.rar, *.rpm, *.tar, *.tgz, *.z, *.zip
Arquivos de áudio	*.aff, *.affc, *.aif, *.aiff, *.au, *.m3u, *.mid, *.mod, *.mp3, *.ra, *.rmi, *.snd, *.voc, *.wav

Tabela 5-19 Os tipos de arquivo permitidos. *(continuação)*

Tipos de arquivo permitidos	Extensões de arquivo
Arquivos de vídeo/filme	*.asf, *.asx, *.avi, *.lsf, *.lsx, *.m1v, *.mmm, *.mov, *.movie, *.mp2, *.mp4, *.mpa, *.mpe, *.mpeg, *.mpg, *.mpv2, *.qt, *.vdo
Arquivos de imagem	*.art, *.bmp, *.dib, *.gif, *.ico, *.jfif, *.jpe, *.jpeg, *.jpg, *.png, *.tif, *.tiff, *.xbm
Executáveis O padrão é **Não permitir**	*.bat, *.chm, *.class, *.cmd, *.com, *.dll, *.dmg, *.drv, *.exe, *.grp, *.hlp, *.lnk, *.ocx, *ovl, *.pif, *.reg, *.scr, *.shs, *.sys, *.vdl, *.vxd
Scripts O padrão é **Não permitir**	*.acc, *.asp, *.ccs, *.hta, *.htx, *.je, *.js, *.jse, *.php, *.php3, *.sbs, *.sct, *.shb, *.shd, *.vb, *.vba, *.vbe, *.vbs, *.ws, *.wsc, *.wsf, *.wsh, *.wst
Arquivos de texto ASCII	*.cfm, *.css, *.htc, *.htm, *.html, *.htt, *.htx, *.idc, *.jsp, *.nsf, *.plg, *.txt, *ulx, *.vcf, *.xml, *.xsf
Arquivos Postscript	*.cmp, *.eps, *.prn, *.ps

Políticas de nome de arquivo

A subguia **Políticas de nome de arquivo** designa as regras para os nomes de arquivos específicos. A estrutura permite que você especifique regras *personalizadas* que substituem as regras globais definidas na guia Tipos de arquivo.

Antes de iniciar

As políticas de filtragem de anexo são aplicadas na seguinte ordem.

1. Políticas de **Nome de arquivo**
2. Políticas **adicionais**
3. Políticas de **tipos de arquivos**

Tarefa

1 Na lista suspensa de filtro, selecione um dos seguintes itens.

Opção	Descrição
É	O Email Protection filtra os nomes de arquivo que possuem correspondência exata com o texto no campo de valor. Por exemplo, se você desejar filtrar o nome de arquivo config.exe e nenhum outro, você deve selecionar É e, em seguida, digitar config.exe no campo de valor. Para este exemplo, a opção *É* tem o significado de *O nome do arquivo É config.exe.*
Contém	O Email Protection filtra os nomes de arquivo que contenham o texto na descrição de valor em qualquer lugar no nome do arquivo. Por exemplo, se você desejar filtrar qualquer arquivo que contenha config em seu nome como, postconfig ou config.ini, selecione esta opção.
Termina com	O Email Protection filtra os nomes de arquivo que terminam com o texto na descrição de valor. Por exemplo, se você desejar filtrar qualquer arquivo executável que termina com .exe, selecione esta opção.

No campo **Valor**, digite o nome ou nome parcial com o qual o Email Protection deve pesquisar o e-mail de entrada.

2 Na lista suspensa **Ação**, selecione uma das seguintes opções.

Opção	Descrição
Quarentena	O e-mail é enviado para a área de quarentena de conteúdo do destinatário.
Negar	A entrega do e-mail é negada.
Permitir	O e-mail é enviado ao endereço de e-mail do destinatário.
Remover	O Email Protection remove o anexo do e-mail e o e-mail é enviado ao destinatário. Um texto é inserido no e-mail notificando o destinatário que um anexo foi removido.
Criptografar mensagem	Está disponível para grupos de conteúdo de saída se o usuário estiver assinado a criptografia.

A combinação para o tamanho máximo de mensagem criptografada inclui o cabeçalho, o corpo e o anexo da mensagem, não podendo ultrapassar 30 MB nas mensagens criptografadas.

3 Se desejar enviar uma cópia do e-mail para um outro endereço, selecione uma lista de distribuição pré-definida na lista suspensa **Cópia silenciosa**.

4 Clique em **Salvar**.

Políticas adicionais

Use a guia **Políticas adicionais** para especificar as ações adicionais a serem executadas durante o processamento de arquivos zip ou de anexos muito grandes. Essas regras permitem aperfeiçoar as políticas de tipos de arquivos permitidos e substituir as regras definidas na guia **Políticas de tipo de arquivo**.

Tabela 5-20 Definições de opções

Opção	Descrição
A mensagem contém um anexo zip de alto risco:	Especifica a ação a ser tomada quando um arquivo zip é considerado de alto risco. Um arquivo zip é um arquivo que contém outros arquivos e pastas, geralmente em um formato compactado. Existem diversas formas em que um attacker pode criar um arquivo zip que, ao ser entregue em uma mensagem de e-mail, representa uma ameaça ao destinatário. Essas ameaças incluem exceder o limite da caixa de e-mails de um destinatário, deixar o computador do destinatário sem espaço de armazenamento, travar ou causar pane no computador do destinatário. Um anexo zip é considerado de alto risco quando viola as regras relacionadas a tamanho de arquivo, taxa de compactação, número de arquivos e pastas aninhadas. • O próprio arquivo zip é maior que 500 MB. • O arquivo contido no arquivo zip é maior que 100 MB. • O arquivo zip contém mais de 1.500 arquivos. • A taxa de compressão é maior que 95%. • O arquivo zip contém mais de 3 níveis aninhados.
A mensagem contém um anexo zip criptografado:	Especifica a ação a ser tomada quando um arquivo zip está criptografado. Um anexo zip criptografado é um arquivo zip protegido por senha e criptografado. Os anexos zip criptografados em uma mensagem de e-mail representam uma ameaça ao destinatário porque eles podem estar infectados com vírus que podem não ser detectados pelo antivírus.
O arquivo no anexo zip viola a política de anexo:	Especifica a ação a ser tomada quando um arquivo zip viola a política de anexos. Um arquivo zip contém um índice que lista por nome cada arquivo incluído no arquivo zip. Os nomes de arquivos listados no índice do arquivo são examinados para determinar se um tipo de anexo ou política de nome de arquivo de anexo foi violado. As políticas de filtragem de anexo são aplicadas na seguinte ordem. 1 Políticas de **Nome de arquivo** 2 Políticas de **Anexo** 3 Políticas de **Tipo de arquivo**
Negar mensagens em que o tamanho total for excessivo:	Especifica a ação a ser tomada quando o tamanho total da mensagem é maior que o máximo permitido. • Uma mensagem de entrada pode ser negada caso ela exceda de 5 MB até 200 MB. • Uma mensagem de saída pode ser negada caso ela exceda de 10 MB até 200 MB. Não serão enviadas notificações ao remetente ou ao destinatário para informar sobre violações de tamanho máximo de mensagem.

Notificações [Anexos]

Selecione quando as notificações de e-mail de uma ação são enviadas ao remetente e ao destinatário de um e-mail que viola uma política de anexo.

Tabela 5-21 Definições de opções

Opção	Definição
Salvar	Clique para salvar as suas alterações.
Cancelar	Clique para restaurar valores anteriormente salvos.
Opções de remetente	Especifica que uma notificação foi enviada ao remetente, quando uma mensagem disparar a ação selecionada.
Opções de destinatário	Especifica que uma notificação foi enviada ao destinatário, quando uma mensagem disparar a ação selecionada.

Permitir/Negar

Com as opções Permitir/Negar, você pode criar listas de remetentes de e-mail que a política sempre permite ou nega, independentemente das circunstâncias. Essas listas de remetentes podem incluir endereços de e-mail individuais, endereços IP e domínios.

- **Permissão de remetente** — Adicionar os remetentes nos quais você confia e dos quais sempre deseja receber e-mails.
- **Negação de remetente** — Adicione os remetentes nos quais você não confie e dos quais não deseja receber e-mails.
- **Blindagem de destinatário** — Adicione os endereços de e-mail de sua própria organização que não estão mais ativos. Por exemplo, um ex-funcionário.

Listas de conjuntos de políticas versus listas de usuários

O Email Protection permite listas de remetentes permitidos e negados tanto no nível de conjunto de políticas quanto de usuário. Quando houver um conflito entre as listas, o conjunto de políticas com a classificação mais alta terá precedência.

Por exemplo, um usuário que adiciona um endereço a sua lista de permissão pessoal pode esperar receber e-mails desse remetente. No entanto, se esse endereço também estiver na lista de negação da política, o remetente será negado.

Listas de permissão versus listas de negação

A lista de permissão sempre tem precedência sobre a lista de negação dentro do mesmo conjunto de políticas quando há um conflito.

Por exemplo, quando um domínio está na lista de negação, mas um remetente desse domínio também está na lista de permissão, o remetente é permitido.

Não são permitidos endereços duplicados.

Não é possível adicionar o mesmo endereço de e-mail:

- Mais de uma vez para as listas de permissão ou negação.
- A ambas as listas de permissão e de negação.

Permitir/Negar e quarentena

Se um endereço de e-mail estiver bloqueado como spam e tiver sido adicionado à quarentena, não haverá necessidade de adicionar o remetente à lista de negação.

Permissão de remetente

A guia **Permissão de remetente** permite manter uma lista de remetentes confiáveis.

Adição de remetentes

Você pode adicionar endereços de e-mail, domínios, endereços IP e faixas de endereços IP. Também é possível utilizar caracteres curinga.

Tipo	Exemplo
Endereço de e-mail	• `user@example.com` • `user@sub.example.com` • `user@example.*.com`
Domínio	• `example.com` • `*.example.com` • `example.*` • `mysubdomain.*.*`
Endereço IP	• `10.20.0.4` • `10.20.*.4` • `10.*.*.*` • `*.20.*.16` • `10.0.62.0/24` Não use um caractere curinga e um número dentro do mesmo octeto. Por exemplo, `10.2*.0.4` não é válido.

Validação de SPF

O SPF (Sender Policy Framework) evita a falsificação de endereços de e-mail e garante que um e-mail de um endereço de remetente confiável é genuíno.

Dentro do SPF, um resultado `softfail` ou `permerror` indica que um remetente não passou na validação e que o e-mail não é permitido.

A validação de SPF não se aplica a endereços IP.

Fazer upload e download de listas

Você pode adicionar uma longa lista de endereços de uma só vez fazendo seu upload para um arquivo de texto.

Certifique-se de usar um arquivo de texto (.csv ou. txt, por exemplo), de adicionar um endereço por linha e de ter o arquivo disponível em sua unidade local.

O número máximo de valores permitidos em uma lista é 5.000. Valores duplicados ou inválidos são descartados automaticamente.

Você também pode fazer download de uma lista existente para um arquivo .csv se quiser editá-la ou reutilizá-la em outra política.

Lista de permissão de remetente da política de entrada padrão

Ao criar uma lista de permissão de remetente para um conjunto de políticas personalizado, você pode assinar a lista de permissão de remetente da política de entrada padrão. Essa assinatura adiciona os endereços padrão à sua política.

Se a lista padrão for alterada, a assinatura será atualizada automaticamente.

Gerenciar a lista de remetentes permitidos

Use a guia **Permissão de remetente** para gerenciar a lista de remetentes permitidos.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 Na janela **Conjunto de políticas**, selecione **Permitir/Negar** | **Permissão de remetente**

2 Execute uma ou mais tarefas para atualizar a lista.

Para...	Siga estas etapas...
Adicionar um domínio, endereço de e-mail ou endereço IP individual	1 Digite um endereço. 2 Clique em **Adicionar>>**. O endereço é atualizado na lista.
Remover um endereço	1 Selecione um ou mais endereços na lista. Use CTRL-clique ou SHIFT-clique para selecionar mais de um endereço. 2 Clique em **<<Remover**. Os endereços não são mais exibidos na lista.
Remover todos os endereços	1 Clique em **<<Remover tudo**. A página exibe uma mensagem de aviso. 2 Clique em **Continuar**. A lista de endereços fica vazia.
Alterar a configuração de validação de SPF de um ou mais endereços	1 Selecione um ou mais endereços na lista. Use CTRL-clique ou SHIFT-clique para selecionar mais de um endereço. 2 Selecione **Exigir validação de SPF** ou **Remover validação de SPF**. O valor de **Validar SPF** muda para a nova cadeia de caracteres.
Fazer upload de uma lista de endereços	1 Em **Mais opções**, clique em **Procurar**. 2 Localize o arquivo e clique em**Abrir**. 3 Clique em **Fazer upload**. Os novos endereços são exibidos como adições à lista existente.
Fazer download de uma lista de endereços	1 Em **Mais opções**, clique em **Fazer download**. 2 Salve a lista em uma unidade local. Agora você tem uma lista que você pode editar e da qual pode fazer upload para um conjunto de políticas.

3 Clique em **Salvar**.

Guia Permissão de remetente

Crie uma lista de endereços de e-mail, domínios e endereços IP que são sempre permitidos.

Tabela 5-22 Permissão de remetente

Opção	Descrição
Salvar	Clique para salvar as alterações da lista.
Cancelar	Clique para descartar as alterações e redefinir a lista.
Domínio, endereço de e-mail ou endereço IP	Campos do formulário: • **Domínio, endereço de e-mail ou endereço IP** — Digite um domínio, endereço de e-mail ou endereço IP válido. • **Exigir validação de SPF (não disponível para endereços IP)** — Selecione esta opção para exigir a validação SPF para o novo domínio ou endereço de e-mail. O SPF não se aplica a endereços IP. • **Adicionar >>** — Clique para adicionar sua entrada à lista. • **<< Remover** — Clique para remover um ou mais endereços selecionados da lista. • **<< Remover tudo** — Clique para remover todos os endereços da lista. Lista: • **Endereço** — Exibe o domínio, o endereço de e-mail ou o endereço IP. • **Validar SPF** — Especifica se a validação de SPF é necessária. • **Exigir validação de SPF** — Clique para exigir a validação de SPF para os endereços selecionados. • **Remove validação de SPF** — Clique para remover a validação de SPF dos endereços selecionados.
Mais opções	Fazer upload de uma lista: • **Procurar** — Clique para localizar um arquivo em sua unidade local. • **Fazer upload** — Clique para fazer upload do arquivo. Fazer download de uma lista: • **Fazer download** — Clique para fazer download da lista em um arquivo csv. Use as opções padrão: • **Assinar a lista de Permissão de remetentes da política de Entrada padrão** — Especifica se a lista de permissão de remetentes da política padrão deve ser utilizada além de sua lista personalizada.

Negação de remetente

A **Negação de remetente** permite que você defina uma lista de endereços de e-mail cujo e-mail não será aceito para entrega. Se um endereço de e-mail for digitado aqui, os usuários não poderão substituir essa configuração mesmo se o endereço de e-mail for digitado em suas listas de permissão no nível de usuário.

Para inserir valores na **Lista de Negação de remetente**, forneça as informações abaixo.

Tarefa

1 Digite um endereço no campo **Domínio, endereço de e-mail ou endereço IP:** . Use um dos formatos abaixo.

Opção	Descrição
Um endereço de e-mail, por exemplo:	• user@example.com • user@sub.example.com • user@example.*.com
Um Nome do domínio, por exemplo:	• example.com • *.example.com • example.* • mysubdomain.*.*
Um endereço IP. Os endereços IP devem conter 4 octetos; sendo cada octeto numérico, entre 0 e 255, OU um caractere curinga. **Caracteres curinga e números não podem estar misturados em um octeto.** **Os exemplos incluem:**	• 10.20.0.4 • 10.20.*.4 • 10.*.*.* • *.20.*.16 • 10.0.62.0/24

2 Clique em **Adicionar**.

3 Clique em **Salvar**.

Tarefas

- *Se o remetente estiver na lista de negação de remetentes* na página 66
  Para selecionar uma das opções de disposição de mensagem disponíveis, execute as etapas abaixo.
- *Upload em massa* na página 67
  Faça upload de um arquivo com uma lista predefinida.

Se o remetente estiver na lista de negação de remetentes

Para selecionar uma das opções de disposição de mensagem disponíveis, execute as etapas abaixo.

Clique em uma das opções de disposição de mensagem disponíveis (a seleção também se aplicará à lista de negação de usuário final).

- **Negar entrega** — Os remetentes na lista de negação do conjunto de políticas recebem uma notificação de que a mensagem foi negada pelo destinatário pretendido.
- **Aceitar e descartar discretamente a mensagem** — Os remetentes na lista de negação do conjunto de políticas *não* recebem nenhuma notificação de que suas mensagens nunca foram enviadas ao destinatário pretendido.

Tarefa

- **Assinar a lista de negação de remetente de entrada padrão** — Selecione a assinatura da lista padrão de **Negação de remetente de entrada padrão** para adicionar a política de domínio padrão a uma lista de negação de remetentes personalizada. Para exibir a lista padrão, selecione a opção de entrada padrão embaixo da guia de políticas.

  Se a lista padrão for alterada, a assinatura ao padrão será atualizada para refletir essas alterações.

Upload em massa

Faça upload de um arquivo com uma lista predefinida.

Antes de iniciar

A lista deve estar no formato a seguir.

- O arquivo deve ser de texto.
- Um endereço de e-mail por linha.
- O arquivo deve estar disponível para acesso pelo navegador.

Tarefa

1 Clique em **Procurar** e selecione um arquivo para upload.

2 Clique em **Fazer upload**.

O arquivo é adicionado à lista de domínios.

3 Edite a lista.

- Para remover um valor da lista, selecione-o na caixa de listagem e clique em **Remover**.
- Selecione **Remover tudo** para remover todas as entradas.

4 Clique em **Salvar**.

O número máximo de valores permitidos em qualquer lista é 5.000. Valores duplicados ou inválidos são descartados automaticamente.

Blindagem de destinatário

A **Blindagem de destinatário** permite que você defina uma lista de endereços de e-mail de destinatário e determine uma ação para cada um dos e-mails enviados para esse destinatário. Os e-mails recebidos em todos os endereços de e-mail; de alias referentes à conta de usuário determinada também serão incluídos no processamento de blindagem de destinatário. Por exemplo, você pode determinar que os e-mails recebidos para uma conta de usuário de um ex-funcionário sejam sempre negados.

Para um provedor de serviço cliente, os endereços de e-mail inseridos se aplicarão somente ao domínio que você está configurando. Para uma empresa cliente, os endereços de e-mail inseridos se aplicarão a todos os domínios dentro da empresa. No entanto, se os grupos forem administrados, a empresa cliente pode criar uma lista de destinatários exclusiva dentro de um conjunto de políticas personalizado e atribuir em seguida um ou mais grupos a esse conjunto de políticas.

Tarefa

1 Digite um endereço no campo **Endereço de e-mail**.

O endereço de e-mail deve conter um domínio válido do cliente atual.

2 Clique em **Adicionar**.

3 Clique em **Salvar**.

Tarefas

- *Se o destinatário estiver na lista Blindagem de destinatário* na página 68
  Selecione a ação a ser aplicada quando um e-mail for recebido para um dos endereços no campo **Lista Blindagem de destinatário**.
- *Upload em massa* na página 68
  Faça upload de um arquivo com uma lista predefinida.

Se o destinatário estiver na lista Blindagem de destinatário

Selecione a ação a ser aplicada quando um e-mail for recebido para um dos endereços no campo **Lista Blindagem de destinatário**.

Tarefa

1 Selecione a ação que deseja aplicar.

Opção	Descrição
Aceitar e descartar discretamente a mensagem	O e-mail é aceito, mas é descartado sem notificação.
Negar entrega	A entrega do e-mail é negada.
Nenhuma ação	O e-mail é encaminhado ao endereço de e-mail do destinatário sem nenhum processamento aplicado.

2 Assine a **Lista Blindagem de destinatário de entrada padrão**.

Selecione a assinatura na lista padrão **Blindagem de destinatário de entrada padrão** para adicionar o domínio ou a política de grupo padrão à sua lista personalizada de blindagem de destinatário de entrada. Para exibir a lista padrão, selecione a opção de entrada padrão na guia de políticas.

Se a lista padrão for alterada, a assinatura do padrão será atualizada para refletir essas alterações.

Upload em massa

Faça upload de um arquivo com uma lista predefinida.

Antes de iniciar

A lista deve estar no formato a seguir.

- O arquivo deve ser de texto.
- Um endereço de e-mail por linha.
- O arquivo deve estar disponível para acesso pelo navegador.

Tarefa

1 Clique em **Procurar** e selecione um arquivo para upload.

2 Clique em **Fazer upload**.

O arquivo é adicionado à lista de domínios.

3 Edite a lista.

- Para remover um valor da lista, selecione-o na caixa de listagem e clique em **Remover**.
- Selecione **Remover tudo** para remover todas as entradas.

4 Clique em **Salvar**.

O número máximo de valores permitidos em qualquer lista é 5.000. Valores duplicados ou inválidos são descartados automaticamente.

Autenticação de e-mail

O recurso de autenticação de e-mail permite validar remetentes de e-mail e proteger o conteúdo dos e-mails enquanto eles estão em trânsito. Essa autenticação de e-mail ajuda a identificar e bloquear alguns tipos de mensagens forjadas, bem como tentativas de phishing.

TLS imposto

O protocolo de criptografia **Transport Layer Security (TLS)** criptografa os e-mails recebidos e enviados. Ao especificar o **TLS imposto** para um domínio, você pode exigir que o TLS seja usado ao receber ou enviar e-mails para esse domínio.

- Quando o TLS não puder ser negociado, as mensagens serão negadas e notificações serão, opcionalmente, enviadas ao remetente, ao destinatário ou a ambos.
- Quando você trocar e-mails com alguém que também use o TLS, um certificado de uma autoridade de certificação (CA) reconhecida será gerado.
- O TLS imposto é exigido para o **Email Encryption**.

Ativar o TLS em seu sistema

Para ser bem-sucedido, o TLS imposto requer uma negociação entre o agente de transferência de mensagens do Email Protection e o seu sistema. O TLS precisa estar ativado no seu lado para acomodar esta transação.

Consulte o manual de seu software MTA para obter informações sobre como ativar o TLS. Certifique-se de que o TLS esteja implementado em seu sistema antes de configurar suas listas de domínio.

Utilizar caracteres curinga para domínios e subdomínios

O uso do caractere curinga (*) é uma forma conveniente de identificar o subdomínio de um Remetente/Destinatário.

Tabela 5-23 Exemplos de caracteres curingas

Exemplo de domínio	Correspondências
*.example.com	*subdomain1.example.com* e *subdomain2.example.com*
example.*	*example.com* e *example.net*
subdomain.*.*	*subdomain.example.com* e *subdomain.someplace.com*
subdomain.*.example.com	*subdomain.something.example.com* e *subdomain.else.example.com*

Fazer upload e download de listas

Você pode adicionar uma longa lista de domínios de uma só vez fazendo seu upload para um arquivo de texto.

Certifique-se de usar um arquivo de texto (.csv ou. txt, por exemplo), de adicionar um domínio por linha e de ter o arquivo disponível em sua unidade local.

O número máximo de valores permitidos em uma lista é . Valores duplicados ou inválidos são descartados automaticamente.

Você também pode fazer download de uma lista existente para um arquivo .csv se quiser editá-la ou reutilizá-la em outra política.

Adicionar um domínio à lista TLS imposto

Use a guia **TLS imposto** para adicionar um domínio ou subdomínio à lista TLS imposto.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 Na janela **Conjunto de políticas**, selecione **Autenticação de e-mail** | **TLS imposto**.

2 Execute uma ou mais tarefas para atualizar a lista.

Para...	Siga estas etapas...
Adicionar um domínio individual ou subdomínio individual	1 Digite um domínio. 2 Clique em **Adicionar>>**. O domínio é atualizado na lista.
Remover um domínio	1 Selecione um ou mais domínios na lista. Use CTRL-clique ou SHIFT-clique para selecionar mais de um endereço. 2 Clique em **<<Remover**. Os domínios não são mais exibidos na lista.
Remover todos os domínios	1 Clique em **<<Remover tudo**. A página exibe uma mensagem de aviso. 2 Clique em **Continuar**. A lista de domínios ficará vazia.
Alterar a configuração de validação de CA para um ou mais domínios	1 Selecione um ou mais endereços na lista. Use CTRL-clique ou SHIFT-clique para selecionar mais de um domínio. 2 Selecione **Exigir validação de CA** ou **Remover validação de CA**. O valor de **Validar CA** muda de acordo com a nova configuração.

Para...	Siga estas etapas...
Fazer upload de uma lista de domínios	1 Em **Mais opções**, clique em **Procurar**. 2 Localize o arquivo e clique em**Abrir**. 3 Clique em **Fazer upload**. Os novos domínios são exibidos como adições à lista existente.
Fazer download de uma lista de domínios	1 Em **Mais opções**, clique em **Fazer download**. 2 Salve a lista em uma unidade local. Agora você tem uma lista que você pode editar e da qual pode fazer upload para um conjunto de políticas.

3 Clique em **Salvar**.

Guia TLS imposto

Crie uma lista de domínios que exigem TLS.

Tabela 5-24 Guia TLS imposto

Opção	Descrição
Salvar	Clique para salvar as alterações da lista.
Cancelar	Clique para descartar as alterações e redefinir a lista.
Domínio	Campos do formulário: • **Domínio** — Digite um domínio válido. • **Exigir validação de CA** — Selecione para exigir a validação de CA para o novo domínio. • **Adicionar >>** — Clique para adicionar sua entrada à lista. • **<< Remover** — Clique para remover um ou mais domínios selecionados da lista. • **<< Remover tudo** — Clique para remover todos os domínios da lista. Lista: • **Domínio** — Exibe o domínio. • **Validar CA** — Especifica se a validação de CA é necessária. • **Exigir validação de CA** — Clique para exigir a validação de CA para os endereços selecionados. • **Remove validação de CA** — Clique para remover a validação de CA dos endereços selecionados.
Mais opções	Fazer upload de uma lista: • **Procurar** — Clique para localizar um arquivo em sua unidade local. • **Fazer upload** — Clique para fazer upload do arquivo. Fazer download de uma lista: • **Fazer download** — Clique para fazer download da lista em um arquivo csv. Use as opções padrão: • **Assinar a lista de TLS imposto da política de entrada padrão** — Especifica se a lista de TLS imposto da política de entrada padrão deve ser utilizada além de sua lista personalizada. • **Assinar a lista de TLS imposto da política de saída padrão** — Especifica se a lista de TLS imposto da política de saída padrão deve ser utilizada além de sua lista personalizada.

Autoridades de certificação

Use uma autoridade de certificação (CA) confiável para validar domínios na página **TLS imposto**.

Tabela 5-25 Lista de autoridades de certificação

CA		
AddTrust	GTE CyberTrust	Thawte
Comodo	IPS Servidores	Trustis FPS
DigiCert Inc	Netlock	Valicert
DST —— Digital Signature Trust	Network Solutions	Usertrust
Entrust.net	QuoVadis	Verisign
Equifax	RSA Data Security	Tata
GlobalSign	SecureNet	Starfield Tech
Go Daddy	StartCom	SwissSign
GeoTrust	TC TrustCenter	SecureTrust /Trustwave

SPF imposto

Estrutura da política do remetente (SPF) pode ser usada por destinatários de e-mail para determinar se as mensagens que eles recebem foram enviadas de um endereço IP autorizado pelo proprietário do domínio, que pode ajudar a detectar a falsificação. A SPF pode ajudar a detectar a falsificação somente quando os proprietários do domínio mantêm e implementam registros de SPF no DNS (Servidor de Nome do domínio).

Para implementar o SPF, os proprietários do domínio devem criar entradas especiais de DNS, das quais listam os endereços IP que estão autorizados a enviar e-mail a partir de seu domínio. Os destinatários de e-mail devem comparar um endereço IP de origem de e-mail ao endereço IP nos registros de SPF de DNS do proprietário do domínio. Se eles corresponderem, é possível suporte que a mensagem foi enviada pelo proprietário do domínio ou por um terceiro autorizado. Se eles não corresponderem, o destinatário deve suspeitar da mensagem porque ela pode ser uma tentativa de phishing inteligentemente mascarada.

Informações importantes sobre o SPF:

- Muitos proprietários de domínios não implementaram o SPF, incluindo vários domínios comerciais bem-conhecidos, uma vez que a implementação do SPF é voluntária.
- Mesmo aqueles que implementaram o SPF podem ter registros desatualizados ou imprecisos, resultando em falsos positivos. O único modo de resolver isso é entrar em contato com o proprietário do domínio e pedir que ele corrija o problema.
- Nada impede que spammers e hackers implementem o SPF, portanto, ele não é um indicador confiável para spam.
- Muitas organizações permitem que terceiros enviem e-mails em nome de seus domínios (falsificação autorizada). Os endereços IP desses terceiros devem ser incluídos nos registros de SPF do proprietário do domínio para que os destinatários possam validar com êxito esses tipos de mensagens.
- Os provedores de e-mail hospedado muitas vezes dão os mesmos registros de SPF para todos os seus proprietários de domínios, tornando, assim, impossível distinguir um proprietário de domínio do outro e reduzindo a utilidade da tecnologia.
- Mesmo com o SPF implementado e imposto, ainda é possível que os spammers criem e-mails muito convincentes, provenientes de domínios que são similares, porém não exatamente os mesmos, ao domínio usado pela organização que está sendo falsificada. Portanto, a cautela e o treinamento contínuo dos usuários são recomendados.

Você pode ativar o SPF imposto de duas maneiras diferentes: para domínios específicos e para todos os domínios.

Criar um domínio de SPF imposto

Exigir validação de SPF para domínios específicos. Para ativar o SPF imposto para domínios específicos, adicione-os à lista de domínios. Os domínios da lista devem passar por uma verificação de SPF, ou a mensagem será negada.

Tarefa

1 Insira um domínio no campo **Domínio**. Clique em **Adicionar >>**.

Para inserir valores na lista de domínios de SPF, digite o endereço completo do domínio e/ou subdomínio do remetente ou use uma parte do domínio utilizando caracteres curinga. A especificação de um domínio de remetente não inclui automaticamente nenhum subdomínio desse domínio. A lista a seguir demonstra exemplos diferentes de entradas usando um caractere curinga (*).

Tabela 5-26 Exemplos de caracteres curinga

Exemplo de domínio	Correspondências
*.example.com	*subdomain1.example.com* e *subdomain2.example.com*
example.*	*example.com* e *example.net*
subdomain.*.*	*subdomain.example.com* e *subdomain.someplace.com*
subdomain.*.example.com	*subdomain.something.example.com* e *subdomain.else.example.com*

Se o subdomínio não for ser inserido usando o caractere curinga, ele deverá ser explicitamente definido.

O número máximo de valores permitidos na lista **Domínio** é 1.500. Valores duplicados ou inválidos são descartados automaticamente.

2 Para remover um valor da lista, selecione-o na caixa de listagem e clique em **<< Remover**. Selecione **<< Remover tudo** para remover todas as entradas.

3 Selecione Mais opções.

Opção	Descrição
Para domínios que não estão na lista:	Nas listas suspensas, selecione a ação de SPF apropriada (entregar, negar, marcar assunto) para os seguintes critérios: • Quando o SPF estiver disponível, mas houver falha na validação. • Quando o SPF não estiver disponível. • Quando o SPF estiver disponível e a validação for bem-sucedida. Quando a ação for Marcar assunto, as marcas serão aplicadas ao final do assunto. As marcas são: AVISO: falha de validação do SPF, SPF verificado, AVISO: validação de SPF não disponível.
Lista de uploads (anexos):	Para fazer upload de um arquivo com uma lista predefinida de domínios, clique em **Procurar** e selecione um arquivo para fazer upload. Após selecionar o arquivo, clique em **Fazer upload**. O arquivo é adicionado à lista de domínios.

Opção	Descrição
Lista de downloads (salve as alterações primeiro):	Para baixar a lista de domínios para um arquivo CSV, clique em **Fazer download**.

4 Clique em **Salvar**.

Selecione **Inscrever-se na Lista de imposição de SPF da política de Entrada padrão** para incluir a lista de **SPF cumprido** da política padrão com a política atual.

Se as configurações de **SPF cumprido** na política padrão forem alteradas, a assinatura atualizará automaticamente todas as políticas assinadas.

Imposição do SPF em todos os domínios fora da lista

Selecione ações a serem aplicadas a todos os outros domínios que não estão na lista de domínios usando as listas suspensas.

Para domínios não adicionados a uma lista de domínios, as ações a seguir podem ser aplicadas.

Se um domínio estiver listado, a ação será *negar se o SPF falhar* ou *permitir se o SPF aprovar*.

Tarefa

1 Selecione a ação de SPF apropriada (entregar, negar, marcar assunto) usando as listas suspensas sob a opção **Para domínios que não estão na lista** para os seguintes critérios:

- quando o SPF estiver disponível mas a validação falhar — o proprietário do domínio implementou o SPF mas a mensagem não veio de um endereço IP incluído no registro de SPF
- quando o SPF não estiver disponível — o proprietário do domínio não implementou o SPF, não é possível verificar a mensagem em termos de SPF
- quando o SPF estiver disponível e a validação for realizada com êxito

Quando a ação for *marcar assunto*, as marcações serão aplicadas no final do assunto. As marcações são:

- [AVISO: falha de validação do SPF]
- [AVISO: validação de SPF não disponível]
- [SPF verificado]

2 Clique em **Salvar**.

Quando os domínios estiverem presente na lista de domínios e ações forem especificadas para todos os outros domínios, a ação de lista de domínio para negar será preferencial em relação a todas as ações que se apliquem aos outros domínios.

DKIM imposto

O **DomainKeys Identified Mail (DKIM)** faz parte do pacote de Autenticação de e-mail projetado para verificar o remetente do e-mail e a integridade da mensagem. A especificação DomainKeys adotou aspectos de e-mails de Internet identificados para criar um protocolo avançado, chamado DomainKeys Identified Mail.

Criação de um domínio de DKIM imposto

Exigir validação de DKIM para domínios específicos.

Tarefa

1 Insira um domínio no campo **Domínio**. Clique em **Adicionar >>**.

Para inserir valores na lista de domínios de DKIM, digite o endereço completo do domínio e/ou subdomínio do remetente ou use uma parte do domínio utilizando caracteres curinga. A especificação de um domínio de remetente não inclui automaticamente nenhum subdomínio desse domínio. A lista a seguir demonstra exemplos diferentes de entradas usando um caractere curinga (*).

Tabela 5-27 Exemplos de caracteres curinga

Domínio exemplo	Correspondências
*.example.com	*subdomain1.example.com* e *subdomain2.example.com*
example.*	*example.com* e *example.net*
subdomain.*.*	*subdomain.example.com* e *subdomain.someplace.com*
subdomain.*.example.com	*subdomain.something.example.com* e *subdomain.else.example.com*

Se o subdomínio não for ser inserido usando o caractere curinga, ele deverá ser explicitamente definido.

O número máximo de valores permitidos na lista **Domínio** é 1.500. Valores duplicados ou inválidos são descartados automaticamente.

2 Para remover um valor da lista, selecione-o na caixa de listagem e clique em **<< Remover**. Selecione **<< Remover tudo** para remover todas as entradas.

3 Selecione Mais opções.

Opção	Descrição
Para domínios que não estão na lista:	Nas listas suspensas, selecione a ação de DKIM apropriada (Entregar, Negar, Marcar assunto) para os seguintes critérios: • Quando uma assinatura DKIM está presente mas não é válida. • Quando não há uma assinatura DKIM presente. • Quando há uma assinatura DKIM válida presente. Quando a ação for Marcar assunto, as marcas serão aplicadas ao final do assunto. As marcas são: AVISO: falha na validação do DKIM, DKIM verificado, AVISO: validação de DKIM não disponível.
Lista de uploads (anexos):	Para fazer upload de um arquivo com uma lista predefinida de domínios, clique em **Procurar** e selecione um arquivo para fazer upload. Após selecionar o arquivo, clique em **Fazer upload**. O arquivo é adicionado à lista de domínios.

Opção	Descrição
Lista de downloads (salve as alterações primeiro):	Para baixar a lista de domínios para um arquivo CSV, clique em **Fazer download**.

4 Clique em **Salvar**.

Selecione a assinatura **Assinar a lista de DKIM imposto da política de entrada padrão** para adicionar a política de domínio padrão de entrada/saída apropriada à sua política de DKIM imposto personalizada. Para exibir a lista padrão, selecione a opção de entrada/saída padrão correspondente sob a guia de políticas. Essa opção só estará disponível em conjuntos de políticas personalizados (não padrão).

Se a lista padrão for alterada, a assinatura do padrão será atualizada para refletir essas alterações.

Impor DKIM para todos os domínios fora da lista

Selecione ações a serem aplicadas a *todos os outros* domínios que não estão na lista de domínios usando as listas suspensas.

Para domínios não adicionados a uma lista de domínios, as ações abaixo podem ser aplicadas.

Se um domínio estiver listado, a ação será *negar se o DKIM falhar* ou *permitir se o DKIM aprovar*.

Tarefa

1 Selecione a ação de DKIM apropriada (entregar, negar, marcar assunto) usando as listas suspensas sob a opção **Para domínios que não estão na lista**, para os seguintes critérios:

- quando uma assinatura DKIM estiver presente mas não for válida
- quando não há uma assinatura DKIM presente
- quando houver uma assinatura DKIM válida presente

Quando a ação for *marcar assunto*, as marcações serão aplicadas no final do assunto. As marcações são:

- [AVISO: falha na validação do DKIM]
- [AVISO: validação de DKIM não disponível]
- [DKIM verificado]

2 Clique em **Salvar**.

Quando os domínios estiverem presente na lista de domínios e ações forem especificadas para todos os outros domínios, a ação de lista de domínio para negar será preferencial em relação a todas as ações que se apliquem aos outros domínios.

Notificações [Autenticação de e-mail]

Use a subguia **Notificações** para selecionar quando as notificações de e-mail de uma ação são enviadas ao remetente e ao destinatário de um e-mail que viola uma política de Autenticação de e-mail imposta.

Tabela 5-28 Opções de notificação

Opção	Definição
Salvar	Clique para salvar as suas alterações.
Cancelar	Clique para restaurar valores anteriormente salvos.
Opções de remetente	Especifica que uma notificação foi enviada ao remetente, quando uma mensagem disparar a ação selecionada.
Opções de destinatário	Especifica que uma notificação foi enviada ao destinatário, quando uma mensagem disparar a ação selecionada.

Notificações

A guia **Notificações** permite configurar modelos de e-mail para as notificações de políticas disponíveis nas outras guias.

Personalização de modelos para cada combinação de destino e ação

Em cada guia existem modelos separados para cada combinação de destino de e-mail e ação de política.

Por exemplo, quando você tiver dois destinos (remetente e destinatário) e três ações (quarentena, negar entrega e remover), haverá seis modelos para configurar:

- remetente e quarentena
- remetente e negar entrega
- remetente e remover
- destinatário e quarentena
- destinatário e negar entrega
- destinatário e remover

Configuração de modelos de e-mail com texto e variáveis

Você pode personalizar o endereço de remetente, endereço responder a, linha de assunto de e-mail e texto de corpo em cada modelo. Também é possível usar variáveis de notificação para adicionar informações de sistema em cada um desses campos.

Por exemplo, ao adicionar a variável $(DATE) a data de quando o e-mail de notificação foi enviado é inserida.

Configurar um modelo de e-mail de notificação

Personalize o modelo de e-mail para cada tipo de notificação e cada combinação de destino e ação.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 Em Email Protection, selecione **Políticas** e abra uma política de entrada ou saída.

2 No conjunto de políticas, selecione **Notificações** e escolha o tipo de notificação que deseja modificar.

3 Clique no assunto do modelo que você deseja modificar e clique em **Editar**.

Os campos de formulário editáveis são exibidos.

4 Atualize o conteúdo de cada campo.

Opção	Descrição
De	Digite o endereço que você deseja usar como remetente da notificação.
Responder a	Digite o endereço que você deseja que os destinatários usem ao responderem à notificação.
Assunto	Digite a linha de assunto da notificação.
Corpo	Digite todas as informações relevantes que você deseja incluir com relação à violação de política e a ação realizada.

5 Clique em **Salvar**.

Guia Notificações

Use cada uma das subguias de **Notificações** para editar os modelos de e-mail de notificação para sua política.

Tabela 5-29 Definições de opções das guias Notificação

Opção	Definição
Editar	Clique para editar o modelo selecionado.
Lista de modelos	Especifica os detalhes de cada modelo. • **Assunto** — Especifica a linha de assunto do modelo. • **Destino** — Especifica o destino da notificação (remetente ou destinatário). • **Ação** — Especifica a ação realizada. • **Em uso** — Usa um ícone para indicar se a notificação foi selecionada para a política.
Campos editáveis	Especifica os valores de cada modelo. • **De** — Especifica o endereço que deseja usar como remetente da notificação. • **Responder a** — Especifica o endereço que você deseja que os destinatários usem ao responderem à notificação. • **Assunto** — Especifica a linha de assunto da notificação. • **Corpo** — Especifica o corpo de texto do e-mail. Ele deve incluir todas as informações relevantes sobre o e-mail, a violação de política e as ações realizadas. • **Salvar** — Clique para salvar suas alterações. Pode levar até 20 minutos para as alterações serem efetuadas. • **Cancelar** — Clique para fechar o modelo sem salvar as alterações.

Variáveis de notificação

Use essas variáveis de notificação para adicionar as informações de sistema a um modelo de e-mail. Todas as variáveis diferenciam maiúsculas de minúsculas e você deve digitá-las da mesma forma que aparecem aqui.

Tabela 5-30 Variáveis de notificação

Use essa sintaxe de variável...	Para inserir automaticamente...
$(SUBJECT)	O assunto do e-mail que violou a política.
$(FROM)	O endereço de e-mail do remetente que violou a política. Essa variável insere o endereço em De: exibido no e-mail.
$(SENDER)	O endereço de e-mail do remetente que violou a política. Essa variável insere o endereço em De: do envelope SMTP recebido do servidor de e-mail remetente.
$(TO)	O endereço de e-mail do destinatário ou Para: endereço do e-mail que violou a política.
$(DATE)	A data em que o e-mail foi recebido que violou a política.
$(REASON)	A razão pela qual o e-mail violou a política.
$(ACTION)	A ação que foi aplicada ao e-mail que violou a política.
$(DOMAIN)	O Domínio que recebeu do e-mail que violou a política.
$(MSG_HEADER)	As informações de cabeçalho do e-mail que violou a política.
$(SIZE)	O tamanho do e-mail que violou a política, incluindo os anexos.
$(POSTMASTER)	"postmaster@" e o seu domínio.

Recuperação de desastres

A **Recuperação de desastres** permite que você especifique as ações a serem realizadas quando um e-mail não puder ser entregue.

Um administrador de clientes ou superior deverá ser habilitado para fazer alterações nessa janela.

- Adie para o controle de acesso baseado em domínio Email Continuity em **Configuração de recuperação de desastres**. Selecione essa opção para usar as definições de configuração da janela **Configuração de recuperação de desastres**.
- Permite que os usuários usem o cliente de Webmail Email Continuity. Selecione essa opção para permitir que os usuários utilizem o cliente de Webmail **Email Continuity** quando e-mails não puderem ser entregues.
- Não permite que os usuários usem o cliente de Webmail Email Continuity. Selecione essa opção se não desejar permitir que os usuários utilizem o cliente de Webmail Email Continuity quando e-mails não puderem ser entregues.

Assinaturas de grupo

Assinaturas de grupo permite aplicar um conjunto de políticas a um ou mais grupos de usuários criados no Gerenciamento de Contas.

Adição de uma assinatura de grupo

Inscreva grupos no conjunto de políticas atual.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 Selecione um ou mais grupos na lista **Grupos disponíveis**.

Pressione e mantenha a tecla Ctrl para selecionar vários grupos.

2 Clique em **Adicionar** para adicionar o grupo à lista **Grupos assinados/subscritos neste conjunto de políticas**.

3 Clique em **Salvar**.

Para remover um valor da lista, selecione-o no grupo e clique em **Remover**.

6 Instalação

O Email Protection filtra o e-mail destinado ao seu servidor ou servidores de e-mail de SMTP (Simple Mail Transfer Protocol) de entrada. Seu provedor já deveria ter definido um ou mais servidores de SMTP no Control Console.

Conteúdo

- *Servidores de entrada*
- *Servidores de saída*
- *Aviso de isenção de responsabilidade sobre saída*
- *Recuperação de desastres*
- *Registros MX*
- *Página Configurações da criação de usuário*
- *Documentos registrados*
- *Instalação do DKIM*

Servidores de entrada

O Email Protection filtra o e-mail destinado para seus servidores de entrada de e-mail SMTP. Alguns servidores de entrada são configurados quando você é configurado no sistema, mas você também pode adicionar servidores adicionais, conforme necessário. É necessário adicionar todos os servidores de e-mail que recebem e-mails de entrada para um determinado domínio.

Conteúdo

- *Verificar a configuração dos servidores de entrada*
- *Configurar um servidor de entrada*
- *Excluir um servidor de entrada*
- *Página Servidores de entrada*

Verificar a configuração dos servidores de entrada

Se você for novo no Email Protection, seu provedor já terá configurado os servidores de SMTP para você. Antes de continuar, é necessário verificar se essas configurações estão corretas.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1. No Email Protection, selecione **Configuração**.
2. Na guia **Configuração**, verifique se você está visualizando o domínio correto. Clique no link para selecionar um domínio diferente.

3 Analise as configurações de SMTP de cada servidor na lista para saber se estão corretas.

4 Clique em **Salvar**.

Configurar um servidor de entrada

Adicione servidores adicionais de entrada para um domínio a fim de garantir que todos os servidores em um domínio recebem o e-mail de entrada.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 No Email Protection, selecione **Configuração**.

2 Se necessário, clique no link do domínio para alterar os domínios.

3 Clique em **Adicionar novo host**.

4 No campo **Endereço do host de SMTP**, digite o endereço IP ou nome do domínio completamente qualificado do host do servidor.

A notação CIDR não é permitida. Se você não possuir um nome de DNS válido para seus servidores de e-mail, será necessário usar o endereço IP.

5 Digite um valor para a **Porta**.

O valor padrão é 25.

6 Digite um valor para classificar a **Preferência** do servidor em relação aos outros servidores.

7 Selecione **Ativar**.

Ao menos um servidor deve ser marcado como ativo.

8 Clique em **Salvar**.

O Email Protection encaminha o e-mail imediatamente para os servidores ativos.

Excluir um servidor de entrada

Remova todas as entradas de servidor que não são mais usadas por um domínio.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 No Email Protection, selecione **Configuração**.

2 Se necessário, clique no link do domínio para alterar os domínios.

3 Localize o servidor de entrada que deseja remover e selecione **Excluir**.

4 Clique em **Salvar**.

Página Servidores de entrada

Use a página **Servidores de entrada** para configurar a entrega correta para os servidores de entrada SMTP. Para cada host SMTP, especifique um endereço, uma porta e um valor de preferência.

Tabela 6-1 Definições de opção de configuração do servidor de entrada

Opção	Descrição
Link do domínio	Especifica o domínio atual. Clique para selecionar um domínio diferente.
Salvar	Clique para salvar todas as alterações.
Cancelar	Clique para restaurar configurações anteriormente salvas.
Lista de host SMTP	• **Endereços de host SMTP** — especifica o host que fornece o tráfego do SMTP de entrada. Digite um endereço IP ou um nome de host totalmente qualificado que esteja registrado no DNS. Por exemplo, `mycompany.com`. Campo necessário. • **Porta** — especifica a porta SMTP. Normalmente, o valor é 25. Campo necessário. • **Preferência** — especifica a preferência do MX para este servidor. Ao entregar o e-mail, o serviço entrega primeiro os servidores de menor número. Se a entrega falhar, o serviço entregará ao endereço de host do SMTP com o próximo maior número, e assim por diante. Campo necessário. • **TLS imposto** — especifica se a conexão de e-mail com o servidor está ou não criptografada usando o TLS. Se você selecionar **TLS imposto** e o TLS não estiver ativado em seu servidor de e-mail de entrada, todas as mensagens de entrada no servidor de e-mail serão negadas. • **Ativo** — especifica se este endereço de host de SMTP atualmente está ou não aceitando tráfego. • **Exclusão** — seleciona a exclusão do host SMTP especificado.
Adicionar novo host	Clique para adicionar um novo endereço IP ou nome de host à lista.
Testar conectividade	Clique para testar o status de conexão do servidor em todos os endereços de host SMTP ativos.

Servidores de saída

O Email Protection permite que você filtre mensagens de saída enviadas de seus servidores de e-mail. Se seu serviço incluir filtragem de saída, use a página **Configuração dos servidores de saída** para configurar os endereços IP para seus servidores.

Conteúdo

- *Configuração da filtragem de saída*
- *Configure os servidores de saída*
- *Excluir um servidor de saída*
- *Página de configuração de servidores de saída*

Configuração da filtragem de saída

O Email Protection usa o endereço de "host inteligente" ou de "retransmissão" para garantir que seu e-mail de saída seja filtrado. Isso é realizado pelo roteamento de todos os seus e-mails de saída através do Email Protection antes que continuem até seu destino final.

Configure os servidores de saída

Configure um ou mais servidores de saída no Email Protection para ativar a filtragem de saída. Para cada servidor de saída, adicione e configure a faixa de endereços IP pela qual o servidor de e-mail terá que enviar os e-mails com o Email Protection.

> **Antes de iniciar**
>
> A configuração do servidor de saída detecta a região de forma automática. Antes de adicionar servidores de saída, selecione sua região em **Instalação** | **Registros MX**.

Tarefa

Para obter as Definições de opções, clique em **Ajuda** na interface.

1 Em Email Protection, selecione **Instalação** | **Servidores de saída**.

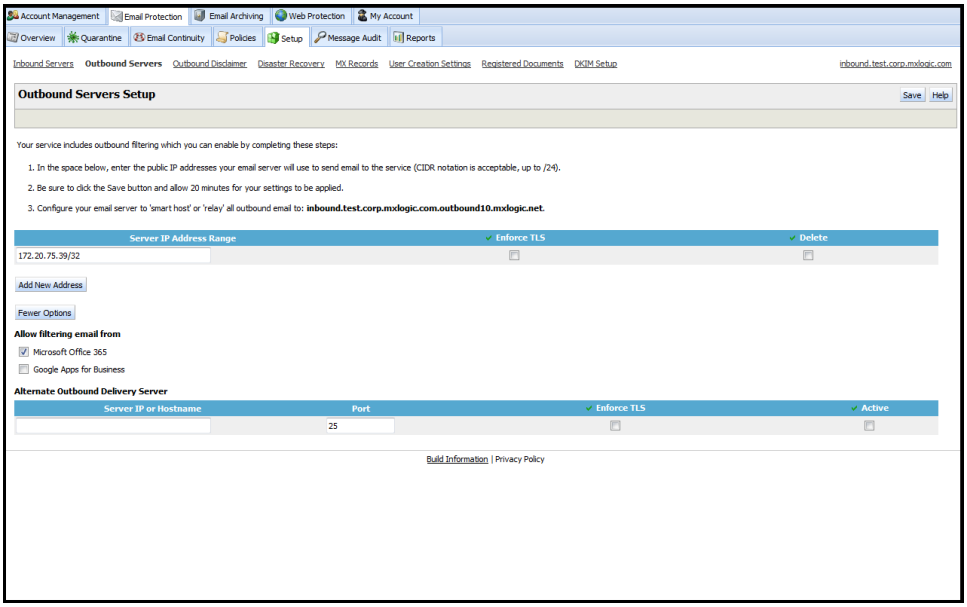

Figura 6-1 Configuração de servidores de saída

2 Se necessário, clique no link do domínio para alterar os domínios.

3 Clique em **Add New Address (Adicionar novo endereço)**.

4 No campo **Server IP Address Range (Faixa de endereço IP do servidor)**, digite o endereço IP ou endereços para todos os servidores de e-mail de saída. A notação CIDR é aceitável, até /24.

5 Se necessário, selecione **Impor TLS**.

Os usuários de criptografia devem selecionar essa opção para garantir que seu e-mail seja criptografado.

6 Se necessário, selecione **Mais opções** para visualizar e configurar opções adicionais.

- Selecione opções para **Permitir e-mail de filtragem em** Microsoft Office 365 ou Google Apps for Business.
- Configure um **Servidor de entrega de saída alternativo**.

  Após uma mensagem ser entregue ao servidor de entrega de saída alternativo, o Email Protection não estará mais associado à mensagem.

7 Clique em **Salvar**.

Espere pelo menos 30 minutos para que suas novas configurações entrem em vigor.

Após você configurar seus endereços de servidor de saída, é necessário configurar o endereço de "host inteligente" ou de "retransmissão" nos servidores de e-mail. Use o endereço especificado para você na página **Configuração do servidor de saída**.

Excluir um servidor de saída

Remova um servidor de saída se a faixa de endereços não for mais usada.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 No Email Protection, selecione **Instalação** | **Servidores de saída**.

2 Localize o servidor de saída que deseja remover em **Intervalo de endereços IP do servidor** e selecione **Excluir**.

3 Clique em **Salvar**.

Página de configuração de servidores de saída

Use a página **Servidores de saída** para configurar a filtragem para servidores de saída. Você pode configurar endereços IP individuais ou uma faixa de endereços usando a notação CIDR. Email Protection também oferece suporte a Microsoft Office 365 e Google Apps for Business.

Tabela 6-2 Definições de opção de configuração de servidores de saída

Opção	Definição
Link do domínio	Especifica o domínio atual. Clique para selecionar um domínio diferente.
Salvar	Clique para salvar todas as alterações.
Lista de servidores de saída	• **Faixa de endereços IP do servidor** — digite um endereço IP ou uma faixa de endereços. A notação CIDR é aceitável, até /24. • **TLS imposto** — especifica se a conexão de e-mail com o servidor está ou não criptografada usando o TLS. • **Exclusão** — seleciona a exclusão do host SMTP especificado.
Adicionar novo usuário	Clique para adicionar um novo endereço ou uma faixa de endereços.
Mais opções.	Clique para visualizar opções adicionais.
Permite a filtragem de e-mail a partir de	• **Microsoft Office 365** — selecione para ativar o suporte para Microsoft Office 365. • **Google Apps for Business**: selecione para ativar o suporte para Google Apps for Business.
Servidor de entrega de saída alternativo	• **IP ou nome de host do servidor** — especifica o host para entrega de saída alternativa. Digite um endereço IP ou um nome de host totalmente qualificado. • **Porta** — especifica a porta SMTP. Normalmente, o valor é 25. • **TLS imposto** — especifica se a conexão de e-mail com o servidor está ou não criptografada usando o TLS. • **Ativo** — especifica se o servidor está ou não atualmente ativo.

Aviso de isenção de responsabilidade sobre saída

Você pode criar o texto que será incluído em todos os e-mails de saída.

Conteúdo

- *Adicionar um aviso de isenção de responsabilidade no e-mail de saída*
- *Página Aviso de isenção de responsabilidade sobre saída*

Adicionar um aviso de isenção de responsabilidade no e-mail de saída

As ações da **Configuração de aviso de isenção de responsabilidade sobre saída** configuram o texto de aviso de isenção de responsabilidade para cada domínio que é exibido em todos os e-mails de saída.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1. No Email Protection, selecione **Configuração** | **Aviso de isenção de responsabilidade sobre e-mail de saída**.
2. Se necessário, clique no link do domínio para alterar os domínios.
3. Selecione a opção **Exibir aviso de isenção de responsabilidade em mensagens de e-mail de saída** para ativar a área de texto.
4. Insira seu **Texto de aviso de isenção de responsabilidade**.

   Você deve limitar seu texto para um máximo de 2.000 caracteres.
5. Clique em **Salvar**.

Página Aviso de isenção de responsabilidade sobre saída

Personalize o texto que deseja exibir em todos os e-mails de saída.

Tabela 6-3 Definições das opções de configuração do aviso de isenção de responsabilidade sobre saída

Opção	Definição
Salvar	Clique para salvar as suas alterações.
Cancelar	Clique para restaurar configurações anteriormente salvas.
Ação da mensagem do aviso de isenção de responsabilidade	• **Nenhum aviso de isenção de responsabilidade**: especifica que nenhum aviso de isenção de responsabilidade será incluído nos e-mails de saída. • **Exibir aviso de isenção de responsabilidade em mensagens de e-mail de saída**: especifica que seu texto personalizado será incluído nos e-mails de saída. • **Texto do aviso de isenção de responsabilidade**: especifica o texto que você deseja exibir em todos os e-mails de saída. Limite seu texto para 2.000 caracteres.

Recuperação de desastres

Os serviços de recuperação de desastres do Email Protection permitem que você armazene seus e-mails remotamente por tempo determinado quando a comunicação com seus servidores de e-mail for interrompida de forma inesperada.

Conteúdo

- *Serviços de recuperação de desastres*
- *Configurar o spool automático para a recuperação de desastres*
- *Iniciar e interromper manualmente o spool para recuperação de desastres*
- *Configurar as notificações da recuperação de desastres*
- *Página Recuperação de Desastres*

Serviços de recuperação de desastres

A recuperação de desastres inclui dois serviços, Segurança contra falhas e Email Continuity.

Segurança contra falhas

- A segurança contra falhas salva as mensagens para entrega posterior se o servidor de e-mail ficar indisponível.
- Quando o servidor de e-mail ficar disponível, a segurança contra falhas entregará as mensagens.
- Os usuários não poderão acessar suas mensagens porque elas só estarão na segurança contra falhas.
- A segurança contra falhas contém uma quantidade ilimitada de capacidade de armazenamento, mas remove as mensagens que estão na segurança contra falhas há mais de 5 dias.

Email Continuity

- O Email Continuity salva as mensagens para entrega posterior se o seu servidor de e-mail ficar indisponível.
- Quando o seu servidor de e-mail tornar-se disponível, o Email Continuity entregará as mensagens.
- Os usuários podem acessar suas mensagens através de uma interface com base na Web enquanto as mensagens estiverem somente no Email Continuity.
- O Email Continuity também tem capacidade de armazenamento ilimitado e remove mensagens que estão no armazenamento do Email Continuity há mais de 60 dias.

Configurar o spool automático para a recuperação de desastres

É possível configurar a recuperação de desastres para que comece automaticamente a armazenar ou fazer spool do seu e-mail após um período específico de inatividade.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1. No Email Protection, selecione **Configuração**.
2. Se necessário, clique no link do domínio para alterar os domínios.
3. Em **Definições de configuração**, selecione **Automático**.
4. Selecione um valor para o número de minutos de inatividade que o sistema deve esperar antes de iniciar automaticamente o spool.

5 Se necessário, selecione **Permitir que usuários usem o Email Continuity**.

6 Clique em **Salvar**.

Iniciar e interromper manualmente o spool para recuperação de desastres

Você pode iniciar ou interromper manualmente o spool sempre que souber que seus servidores de e-mail estão inativos.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 No Email Protection, selecione **Configuração**.

2 Se necessário, clique no link do domínio para alterar os domínios.

3 Em **Definições da configuração**, selecione **Manual**.

4 Selecione uma opção no menu suspenso.

- Selecione **Iniciar spool** para iniciar o spool manual.
- Selecione **Interromper spool** para encerrar o spool manual.

5 Como opção, selecione **Entregar o e-mail no spool quando a conectividade for restabelecida**.

6 Se necessário, selecione **Permitir que usuários usem o Email Continuity**.

7 Clique em **Salvar**.

Configurar as notificações da recuperação de desastres

Especifique um ou mais endereços de e-mail que devem ser notificados quando os eventos da recuperação de desastres ocorrerem.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 No Email Protection, selecione **Configuração**.

2 Se necessário, clique no link do domínio para alterar os domínios.

3 Em **Notificações**, digite um **Endereço de e-mail de destinatário**.

4 Clique em **Adicionar** para atualizar a lista.

Você pode adicionar até quatro endereços de e-mail.

5 Clique em **Salvar**.

Página Recuperação de Desastres

As informações abaixo explicam como configurar serviços de recuperação de desastres.

Tabela 6-4 Definições das opções de configuração da recuperação de desastres

Opção	Definição
Status	Especifica o status atual do spool, incluindo: • Se o spool está ativado ou desativado • Se necessário, por quanto tempo as mensagens foram colocadas no spool • Se necessário, a quantidade de mensagens que foram colocadas no spool, em kilobytes O gráfico animado é um auxílio visual que indica o status atual do spool, onde: • **Solução de filtragem**: os servidores de filtragem do Email Protection. • **E-mail armazenado**: servidores de spool do Email Continuity. • **Servidor do cliente**: seus servidores de e-mail. Clique em **Testar conectividade** para testar a conectividade com cada endereço de host SMTP ativo listado na janela **Servidores de entrada**. Quando o Email Continuity e o spool de e-mail estão ativos, um ícone de informações secundárias é exibido para as **Contas de e-mail não locais**. Os e-mails não locais ocorrem quando os usuários não são configurados em seu sistema. Estes e-mails são colocados em uma fila diferente. Clique no link **Visualizar contas de e-mail não locais agora** para abrir a caixa de e-mail não local e identificar os usuários que não estão configurados.
Configurações e definições	• **Automático**: configura o sistema para fazer automaticamente o spool de todos os e-mails de entrada quando o sistema detecta uma perda de conectividade com seu servidor de e-mail durante um período de tempo específico. Esteja ciente de que poderá levar vários minutos para determinar que o seu servidor de entrada está indisponível. Durante esse tempo, assim como durante o retardamento de tempo, os e-mails recebidos podem apresentar erro se o seu servidor de entrada estiver indisponível. • **Manual**: você pode iniciar e interromper manualmente o spool da **Recuperação de desastres** em interrupções planejadas de servidores de e-mail, como na manutenção de servidores. • A opção **Iniciar spool** inicia o spool manualmente • A opção **Interromper spool** interrompe o spool manualmente. Pode levar alguns minutos para que o spool manual de e-mails recebidos seja iniciado e interrompido. Selecione a opção **Entregar e-mails no spool quando a conectividade estiver disponível** para entregar e-mails no spool quando a conectividade ao servidor de e-mail for restaurada. • **Permitir que os usuários usem o Email Continuity**: permite que os usuários do domínio selecionado usem o Email Continuity. Isso só funciona com o Email Continuity e permite o acesso do usuário quando a conectividade está desativada.
Notificações	As notificações são entregues automaticamente para todos os destinatários listados quando estes eventos de **Recuperação de desastres** ocorrem: • Início do spool automático • Início da remoção automática do spool

Tabela 6-4 Definições das opções de configuração da recuperação de desastres *(continuação)*

Opção	Definição
	• A remoção automática ou manual do spool é concluída Para minimizar a possibilidade de que as notificações de **Recuperação de desastres** não possam ser entregues aos destinatários listados, a McAfee recomenda que as notificações sejam enviadas aos endereços de e-mail associados a dispositivos móveis.

Registros MX

Um registro MX (mail exchange) é um registro de recurso no DNS que especifica o servidor de e-mail responsável por aceitar e-mails em nome de um domínio. Cada registro MX especifica um nome de host e o valor de preferência que prioriza a entrega do e-mail quando diversos servidores estão disponíveis. Você deve configurar seus registros MX para que apontem para o Email Protection Service para que o e-mail seja corretamente encaminhado e filtrado. Por outro lado, se os seus registros MX forem inválidos ou obsoletos, você corre o risco de perder seu e-mail ou limitar a eficiência do serviço.

- Conclua o processo de configuração dos servidores de entrada para cada domínio antes de redirecionar seus registros MX.
- Configure os registros MX para cada um dos seus domínios clicando no nome do domínio atual na barra de menu.

Conteúdo

- *Redirecionando seus registros MX*
- *Selecione uma região para revisar os registros MX*
- *Página Configuração dos registros MX*

Redirecionando seus registros MX

Seus registros MX devem ser configurados como nomes de domínios completamente qualificados e, em seguida, redirecionados para apontar para o Email Protection. Essa alteração permite que o Email Protection filtre seu e-mail e encaminhe-o para seus servidores de e-mail. Seu administrador de redes ou registrador de domínio é normalmente a pessoa responsável por atualizar os registros MX.

As informações necessárias para que sua empresa faça essas alterações são fornecidas no *Guia de ativação do Email Protection*.

É possível que demore alguns dias para que seu registro MX seja redirecionado para se propagar a todos os servidores de e-mail que enviam mensagens ao seu servidor de e-mail. Durante esse tempo, seu servidor de e-mail ainda poderá receber e-mails diretamente destes servidores de e-mail.

Selecione uma região para revisar os registros MX

Selecione uma região para usar os registros MX para filtragem de e-mail.

Antes de iniciar

Antes de alterar os registros MX, você deve concluir o processo de configuração dos servidores de entrada.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1 Selecione **Email Protection** | **Configuração** | **Registros MX**

2 Em **Região**, selecione uma opção para atualizar a página.

3 Revise as informações em **Configuração recomendada**, **Configuração atual** e **Bloquear**.

Use essas informações para configurar seus registros MX, para que o e-mail seja direcionado aos serviços do Email Protection. As informações de bloqueio permitem configurar os servidores de e-mail para só aceitar as conexões do serviço.

Página Configuração dos registros MX

A página de **Configuração dos registros MX** permite que você determine quais registros MX serão usados com base na sua região, estejam seus registros MX configurados corretamente ou não, e fornece endereços IP para que você possa usá-los a fim de impedir atacantes de burlar o serviço.

Tabela 6-5 Definições das opções da página Configuração dos registros MX

Opção	Definição
Região	Especifica a localização dos seus servidores de e-mail. Selecionar uma região determina o conjunto de registros MX que deverá ser usado.
Configuração recomendada	Exibe os registros MX recomendados para a região que você selecionou. Use estes registros para redirecionar seu e-mail para o Email Protection Service. Para evitar problemas de entrega, você deve substituir sua configuração atual pelo conjunto completo de registros MX.

Tabela 6-5 Definições das opções da página Configuração dos registros MX *(continuação)*

Opção	Definição
Configuração atual	Exibe o conjunto atual de registros MX com base em uma consulta em seu provedor de DNS autoritativo. Cada registro inclui as seguintes informações de status: • **Inválido**: o registro é desconhecido e não pode encaminhar o e-mail para o Email Protection Service. • **Válido**: o registro é conhecido e pode encaminhar o e-mail para o Email Protection Service. • **Obsoleto**: o registro é reconhecido, mas não corresponde aos registros MX recomendados atuais exibidos em **Configuração recomendada**. Você deve atualizar seus registros para que correspondam ao que é exibido. Verifique novamente sua configuração atual: • **Verificar novamente**: clique nesta opção para consultar seu provedor de DNS autoritativo. • **Usar este servidor de DNS**: insira o nome de host ou um servidor de DNS alternativo e clique em **Verificar novamente**.
Bloquear	Exibe uma lista dos arquivos que você pode usar para limitar as conexões de SMTP e impedir atacantes de burlar o Email Protection. Cada arquivo contém a lista dos endereços IP que você deve permitir no Email Protection. Todos os outros devem ser bloqueados. Existem quatro formatos diferentes. Selecione um que melhor funcionará em seu ambiente: • **Notação CIDR /21**: contém dois blocos de IP /21. • **Notação CIDR /24**: contém uma lista de blocos de IP /24. • **IPs individuais**: contém uma lista de endereços IP individuais. • **Otimizado para o Microsoft Office 365**: para os usuários do Microsoft Office 365, este arquivo contém uma lista de endereços IP que são formatados para serem usados ao criar um conector de entrada no Forefront Online Protection for Exchange (FOPE).

Página Configurações da criação de usuário

A página de configurações da criação de usuário configura o método que será usado para criar contas de usuários (endereços de e-mail) no Email Protection e designa uma ação a ser tomada quando o endereço de e-mail do destinatário for inválido.

Tabela 6-6 Definições das opções das configurações da criação de usuário

Opção	Definição
Modo de criação do usuário	• **Descoberta de SMTP**: especifica que os usuários são criados automaticamente com base em transações de SMTP. Neste modo, uma conta de usuário é criada automaticamente quando diversas mensagens tiverem sido entregues com êxito a um destinatário que ainda não possui uma conta de usuário. O número de mensagens entregues necessário para desencadear um evento de criação de usuário varia devido aos fatores relacionados ao sistema. Somente as mensagens entregues a endereços de e-mail de destinatário em um domínio primário são contadas com o propósito de criação de usuário. As mensagens enviadas a endereços de e-mail de destinatário em aliases de domínios não são contadas. • **Explícito**: especifica que somente os métodos de criação e exclusão manuais estão ativos no Email Protection. Se o Email Protection receber um e-mail que não possui uma conta de usuário existente, ele executará a ação designada na área **Quando um destinatário for inválido**. Quando a ação for **Negar entrega**, o e-mail será rejeitado e uma mensagem de erro será exibida ao remetente. • **Processamento inválido do destinatário** (limitado aos usuários selecionados): especifica que os usuários devem definir explicitamente os endereços de e-mail e aliases usando as configurações do gerenciamento de contas. Após essas configurações serem definidas, os usuários podem usar o link para forçar os usuários a definir explicitamente os endereços de e-mail e aliases.
Quando um destinatário é inválido	• **Aceitar e descartar silenciosamente a mensagem**: o e-mail é aceito, porém é descartado sem notificação. • **Negar entrega**: a entrega do e-mail é negada. • **Nenhuma ação**: a entrega do e-mail será negada se o MTA do cliente tiver classificado o e-mail como destinatário inválido e o método de criação de usuário estiver definido como **Explícito**.

Documentos registrados

O recurso de documentos registrados impede que seus documentos internos confidenciais sejam enviados como anexos de e-mail.

Conteúdo

- *Como o registro de documentos impede a distribuição de documentos de propriedade*
- *Fazer upload de um documento registrado*
- *Página Documentos Registrados*

Como o registro de documentos impede a distribuição de documentos de propriedade

Para impedir seus documentos importantes de serem enviados em e-mails, é necessário registrar esses documentos com o Email Protection. Ao registrar o documento, será criado uma impressão

digital que poderá ser usada pelo sistema para identificar o texto e filtrar o e-mail antes que seja enviado ao seu destino.

Ao fazer upload de um arquivo para registrá-lo, o documento é dividido em pequenas partes. Cada parte individual cria uma impressão digital única. Um documento registrado poderá resultar em centenas ou até mesmo em milhares de impressões digitais.

Quando um documento é enviado no e-mail de saída por um usuário, ele também é dividido da mesma forma. Em seguida, as impressões digitais do e-mail de saída são comparadas com as que estão armazenadas no sistema. Se um número suficiente de impressões digitais corresponder, a ação da política especificada por você será aplicada.

- Para que o registro entre em vigor, o sistema precisa conter uma quantidade substancial de conteúdo de texto que ele possa receber uma impressão digital e ser armazenado. Portanto, documentos muito curtos podem ser rejeitados durante o processo de registro porque não haverá conteúdo suficiente que o sistema possa usar.
- O registro de formatos compactados, como arquivos zip, pode não produzir correspondências precisas.

Fazer upload de um documento registrado

Registre seus documentos confidenciais e crie uma impressão digital.

Antes de iniciar
Ative o Email Encryption antes de fazer upload de seus documentos.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1. No Email Protection, selecione **Instalação** | **Documentos registrados**.
2. Clique em **Novo** para exibir a interface de upload e adicionar um arquivo.
3. Clique em **Procurar** e selecione um arquivo.
4. Digite uma **Descrição** para o documento.
5. Clique em **Salvar**.

Após o upload do arquivo, o documento terá um status pendente. Após alguns minutos, clique em **Atualizar** para verificar se o documento foi registrado.

Página Documentos Registrados

A página **Documentos registrados** permite gerenciar os documentos que você não deseja que sejam distribuídos fora de sua empresa.

Tabela 6-7 Definições das opções da página Documentos registrados

Opção	Definição
Novo	Clique para registrar um novo documento.
Editar	Clique para editar a descrição de um documento existente.
Excluir	Clique para excluir o documento selecionado.
Atualizar	Clique para atualizar a página e o status de um documento.

Tabela 6-7 Definições das opções da página Documentos registrados *(continuação)*

Opção	Definição
Lista de documentos registrados	• **Nome do arquivo**: o nome do documento. • **Descrição**: o resumo do documento. • **Tamanho**: o tamanho do documento. • **Data de registro**: a data em que o documento foi registrado. • **Data de vencimento**: a data em que o documento expira.
Opções Novo/Editar	• **Documento registrado**: especifica o nome do documento. • **Procurar**: clique para selecionar o documento na máquina local que deseja registrar. • **Descrição**: especifica um resumo do documento. Insira qualquer detalhe relativo na descrição. • **Salvar**: clique para salvar a descrição e fazer upload do arquivo se estiver registrando um novo documento. • **Cancelar**: clique para fechar as opções sem salvar as alterações.

Instalação do DKIM

O DKIM (DomainKeys Identified Mail) permite que você associe o nome do seu domínio a suas mensagens de e-mail, adicionando uma assinatura DKIM ao cabeçalho da mensagem. Isso permite identificar facilmente um e-mail legitimo e pode facilitar a detecção de ataques de phishing.

Conteúdo

- *Configurar DKIM*
- *Página Configuração de DKIM*

Configurar DKIM

Para configurar um DKIM para seu e-mail de saída, é necessário adicionar chaves DKIM ao DNS.

Antes de iniciar

O DKIM estará disponível somente se um pacote de saída tiver sido associado a um domínio.

Configure seus servidores de saída.

Tarefa

Para obter definições de opções, clique em **Ajuda** na interface.

1. No Email Protection, selecione **Configuração** | **Configuração do DKIM**.
2. Se necessário, clique no link do domínio para alterar os domínios.
3. Clique em **Gerar chaves**.
4. Antes de continuar, crie um registro txt de DNS para o nome de host especificado.
5. Copie e cole as chaves DKIM no novo arquivo.

6 Assim que as chaves DKIM tiverem sido adicionadas ao DNS, clique em **Validar**.

7 Quando o registro validar com êxito, clique em **Ativar**.

Uma assinatura DKIM é incluída no cabeçalho da mensagem de todos os e-mails de saída.

Página Configuração de DKIM

A página **Configuração de DKIM** permite adicionar assinaturas DKIM a e-mails de saída.

Tabela 6-8 Definições das opções da página Configuração de DKIM

Opção	Definição
Gerar chaves	Clique para gerar um par de chaves. Esta é a primeira etapa no processo.
Validar	Clique para certificar-se de que a entrada de DNS está correta. Se a entrada de DNS não validar, volte e certifique-se de ter inserido o valor corretamente.
Ativar	Clique para ativar sua assinatura DKIM.
Desativar	Clique para excluir sua assinatura DKIM.

7 Auditoria de mensagens

A auditoria de mensagens fornece um recurso de auditoria de mensagens autônomo que permite que você pesquise informações de disposição de mensagem, bem como endereços IP bloqueados.

Conteúdo

- *Exibição de informações de disposição de mensagem*
- *Visualizando os endereços de IP bloqueados*
- *Exibição do histórico de pesquisa*

Exibição de informações de disposição de mensagem

A auditoria de mensagens fornece um recurso de auditoria de mensagens autônomo que permite que você pesquise informações de disposição de mensagem.

As informações de disposição de mensagem descrevem a *disposição* e uma mensagem que pode incluir os itens a seguir.

- Se a mensagem foi ou não entregue com êxito.
- Se ela foi lida.
- Se ela foi bloqueada ou colocada em quarentena.

Pesquisar por detalhes da mensagem

Use a opção de detalhes da mensagem para exibir as informações de disposição de mensagem com base em partes específicas da mensagem (por exemplo, o remetente ou a linha de assunto).

Tarefa

Para pesquisar por detalhes da mensagem, execute as etapas abaixo.

1. No Email Protection, selecione **Auditoria de mensagens**.
2. Clique em **Pesquisa de mensagens**.

   Essa opção é selecionada por padrão.
3. Selecione **Pesquisar por detalhes da mensagem**.

   Essa opção é selecionada por padrão.
4. Selecione os critérios de pesquisa preenchendo um ou mais dos itens a seguir.

Um e-mail em "para" ou "de" é necessário.

- Na lista suspensa, selecione o **Domínio** correto associado ao cliente escolhido.
- Digite o endereço do domínio no campo **De**.

Você poderá usar caracteres curinga nessa pesquisa. Os exemplos incluem:

- o caractere curinga (*) para representar zero ou qualquer número de valor alfanumérico.
- o caractere curinga (?) para representar uma única instância de um valor alfanumérico. Exemplo: b?b@domain.*.
- Um campo em branco também induzirá uma pesquisa.

- Digite o endereço do domínio no campo **Para**.

Você poderá usar caracteres curinga nessa pesquisa. Os exemplos incluem:

- o caractere curinga (*) para representar zero ou qualquer número de valor alfanumérico.
- o caractere curinga (?) para representar uma única instância de um valor alfanumérico. Exemplo: b?b@domain.*.
- Um campo em branco também induzirá uma pesquisa.

- Digite a data de início.
- Digite a hora de início.
- Digite a data de término.
- Digite a hora de término.
- Digite o texto da linha de assunto.
- Selecione *Todas as palavras*, *Quaisquer das palavras* ou *Frase exata* para restringir a pesquisa de uma linha de assunto.
- Digite o **IP do remetente**.

5 Clique em **Pesquisar**.

Os resultados serão exibidos na janela **Resultados da pesquisa**.

6 Visualizar e fazer download dos resultados da pesquisa.

Para...	Use estas etapas...
Fazer download de todos os resultados	Clique em **Fazer download** na janela **Resultados da pesquisa**.
Visualizar um resultado	Selecione um item para visualizá-lo na janela **Visualizar detalhes da auditoria**.
Visualizar os detalhes do resultado	Clique duas vezes em um item para visualizá-lo em uma nova guia de **Detalhes da auditoria**.
Fazer download de um resultado individual	Clique duas vezes em um item para visualizá-lo em uma nova guia de **Detalhes da auditoria** e clique em **Fazer download**.

Pesquisa por ID da mensagem

Use a pesquisa na opção ID da mensagem para localizar as informações de mensagem com base no ID de mensagem exclusivo de uma mensagem de e-mail.

Tarefa

Para pesquisar por ID da mensagem, execute as etapas abaixo.

1. No Email Protection, selecione **Auditoria de mensagens**.
2. Clique em **Pesquisa de mensagens**.

   Essa opção é selecionada por padrão.
3. Selecione **Pesquisar por ID da mensagem**.
4. Digite a ID exclusiva do e-mail no campo **ID da mensagem**.
5. Clique em **Pesquisar**.

   Os resultados serão exibidos na janela **Resultados da pesquisa**.
6. Visualizar e fazer download dos resultados da pesquisa.

Para...	Use estas etapas...
Fazer download de todos os resultados	Clique em **Fazer download** na janela **Resultados da pesquisa**.
Visualizar um resultado	Selecione um item para visualizá-lo na janela **Visualizar detalhes da auditoria**.
Visualizar os detalhes do resultado	Clique duas vezes em um item para visualizá-lo em uma nova guia de **Detalhes da auditoria**.
Fazer download de um resultado individual	Clique duas vezes em um item para visualizá-lo em uma nova guia de **Detalhes da auditoria** e clique em **Fazer download**.

Pesquisar por cabeçalho

Use a opção Pesquisar por cabeçalho para encontrar as informações de disposição de mensagem com base no cabeçalho de mensagem de uma mensagem de e-mail.

Tarefa

Para pesquisar por cabeçalho, conclua as seguintes etapas.

1. No Email Protection, selecione **Auditoria de mensagens**.
2. Clique em **Pesquisa de mensagens**.

   Essa opção é selecionada por padrão.
3. Selecione **Pesquisar por cabeçalho**.
4. Digite um cabeçalho de e-mail no campo **Cabeçalho**.

   A pesquisa de cabeçalho não suporta caracteres curinga.

5 Clique em **Pesquisar**.

Os resultados serão exibidos na janela **Resultados da pesquisa**.

6 Visualizar e fazer download dos resultados da pesquisa.

Para...	Use estas etapas...
Fazer download de todos os resultados	Clique em **Fazer download** na janela **Resultados da pesquisa**.
Visualizar um resultado	Selecione um item para visualizá-lo na janela **Visualizar detalhes da auditoria**.
Visualizar os detalhes do resultado	Clique duas vezes em um item para visualizá-lo em uma nova guia de **Detalhes da auditoria**.
Fazer download de um resultado individual	Clique duas vezes em um item para visualizá-lo em uma nova guia de **Detalhes da auditoria** e clique em **Fazer download**.

Auditoria de mensagens

A página **Auditoria de mensagens** permite aos administradores parceiros ou superiores pesquisarem informações sobre a disposição da mensagem. Você pode pesquisar com base nos detalhes, na ID ou no cabeçalho da mensagem.

- As informações de entrada não diferenciam maiúsculas e minúsculas.
- As opções **Pesquisa por detalhes da mensagem**, **Pesquisa por ID da mensagem** e **Pesquisar por cabeçalho** são exibidas em painéis recolhíveis. Clique no título para abrir o painel e ver as opções de pesquisa.

Tabela 7-1 Pesquisa por detalhes da mensagem

Opção	Definição
De	Se estiver usando o campo como o seu campo de pesquisa primário, convém usar um caractere curinga para a sua pesquisa. Por exemplo: • o caractere curinga (*) para representar zero ou qualquer número de valor alfanumérico. • o caractere curinga (?) para representar uma única instância de um valor alfanumérico. Exemplo: b?b@domain.* • Um campo em branco também induzirá uma pesquisa.
Para	Se estiver usando o campo como o seu campo de pesquisa primário, convém usar um caractere curinga para a sua pesquisa. Por exemplo: • o caractere curinga (*) para representar zero ou qualquer número de valor alfanumérico. • o caractere curinga (?) para representar uma única instância de um valor alfanumérico. Exemplo: b?b@domain.*
Data de início	Digite uma data de início dentro dos últimos 60 dias. A data é baseada no seu fuso horário. Clique no ícone de calendário para selecionar uma data na janela do calendário.
Hora de início	Selecione a hora de início na data de início para restringir o intervalo de data e hora. O menu suspenso lista a hora do dia em intervalos de 15 minutos.
Data de término	Digite uma data de término dentro dos últimos 60 dias. A data é baseada no seu fuso horário. Clique no ícone de calendário para selecionar uma data na janela do calendário.

Tabela 7-1 Pesquisa por detalhes da mensagem *(continuação)*

Opção	Definição
Hora de término	Selecione a hora de término na data de término para restringir o intervalo de data e hora. O menu suspenso lista a hora do dia em intervalos de 15 minutos.
Assunto	Digite o assunto do e-mail que você está procurando. Selecione *todas as palavras*, *quaisquer das palavras* ou *frase exata* no menu suspenso para restringir a pesquisa. Você pode usar um caractere curinga de asterisco (*) na pesquisa.
IP do remetente	Digite o IP completo do remetente. Pesquisas com caractere curinga não são permitidas.

Tabela 7-2 Pesquisa por ID da mensagem

Opção	Definição
ID da mensagem	Digite a ID completa de mensagem do e-mail.

Tabela 7-3 Pesquisar por cabeçalho

Opção	Definição
Cabeçalho de mensagem	Digite ou copie o cabeçalho da mensagem do e-mail na caixa de texto. Pesquisas com caractere curinga não são permitidas.

Tabela 7-4 Resultados da pesquisa

Opção	Definição
De	O endereço de e-mail em *De*.
Para	O endereço de e-mail em *Para*.
Assunto	A linha de assunto.
Direção	Descreva se o e-mail foi enviado ou recebido: **Entrada** — Um e-mail enviado a um destinatário em um domínio fornecido no serviço de filtragem. **Saída** — Um e-mail proveniente de um domínio fornecido no serviço de filtragem para um destinatário externo.
Recebido em	A data em que o e-mail foi recebido.
Fazer download	Clique para fazer download de todos os resultados da pesquisa em um arquivo csv.

A janela **Visualização de detalhes da auditoria** e as guias em **Detalhes da auditoria** exibem os detalhes do e-mail e o conteúdo de entrega.

Tabela 7-5 Janela de visualização de detalhes da auditoria e detalhes da auditoria

Opção	Descrição
Fazer download	Clique para fazer download dos detalhes da auditoria em um arquivo .csv.
	• **De** — Especifica o endereço de e-mail do remetente. • **Para** — Especifica o endereço de e-mail do destinatário. • **Assunto** — Especifica a linha de assunto. • **Tamanho** — Especifica o tamanho de arquivo do e-mail. • **ID da mensagem** — Especifica a ID de mensagem exclusiva. • **ID de rastreamento** — Especifica a ID de rastreamento exclusiva. • **IP do remetente** — Especifica o endereço IP do remetente. • **Direção** — Especifica se o e-mail foi enviado (saída) ou recebido (entrada). • **Pontuação de spam** — Especifica a probabilidade do e-mail ser um spam.

Tabela 7-6 Detalhes do evento

Opção	Descrição
Data e hora	A data e o horário do evento.

Evento	Fornece detalhes sobre cada evento, incluindo:
	• Um campo em branco também induzirá uma pesquisa.
	• Transport Layer Security (TLS) de front-end/back-end — sim/não.
	• IP de back-end — o destino tentado para o qual o servidor IP foi enviado.
	• Nome do usuário — quem liberou o e-mail da quarentena.
	• As marcas de mensagens em quarentena incluem:
	  • qa — Anexo em quarentena
	  • qh — Em quarentena pelo ClickProtect
	  • qk — Palavra-chave do conteúdo da quarentena
	  • qs — Spam em quarentena
	  • qv — Vírus em quarentena
	
	Se a mensagem tiver sido excluída da quarentena, é possível que você possa ver que a excluiu. Por exemplo: Detalhes: excluída da quarentena por: global@kt2.com.

Definições do evento Visualização de detalhes da auditoria

Use as definições de disposição para entender cada disposição, sua descrição, e as ações sugeridas que você pode tomar em resposta.

Descrições da disposição do destinatário

- Um único e-mail pode ter diversos destinatários.
- A disposição de status de um destinatário registra o status de um destinatário individual de e-mail.
- As seguintes disposições não estão inclusas: Email Continuity (mensagens novas, respondidas, encaminhadas, de saída, ou geradas pelo sistema).

Tabela 7-7 Descrições da disposição do destinatário

Evento	Definição e ações sugeridas
250 back-end; modo: normal	A mensagem foi aceita para a entrega.
250 Backend; (Mode: exempt)	O destinatário está isento de filtragem. Entre em contato com o administrador do cliente se desejar remover a isenção.
250 Deferred; (Mode: normal)	O remetente da mensagem recebe uma confirmação informando que a entrega foi bem-sucedida, mas uma cópia ou notificação da mensagem é enviada a um destinatário designado devido a uma violação de política. Entre em contato com seu administrador de clientes se isso estiver errado.
250 OK	Entregue com êxito. O nome do usuário que removeu o e-mail da quarentena pode ser listado na janela **Detalhes da auditoria**.
250 OK silent discard for recipient shield	Devido à blindagem do destinatário, a mensagem foi descartada silenciosamente, mas o destinatário recebeu uma mensagem de OK. Entre em contato com seu administrador de clientes para permitir a entrega.
521 outbound.logi.com must use TLS (Mode: normal)	O TLS imposto é ativado, mas o servidor nega o e-mail. Entre em contato com o administrador do seu servidor de e-mail. O servidor de e-mail de saída não pode ter o TLS configurado
551 Sender is on domain's block list (Mode: normal)	As configurações de política determinam que a mensagem falhou permanentemente e que não haverá nova tentativa de envio. Para os usuários: efetue logon no Control Console, no Email Protection selecione **Políticas** | **selecionar política** | **Permitir/Negar** para redefinir a lista de bloqueio de domínio. Aguarde até 15 minutos para que as alterações sejam efetuadas.
551 Mailhost is on a global block list	O host de e-mails está enviando uma alta porcentagem de spam. Tente novamente em 2 horas. Se falhar novamente, significa que o endereço IP continua enviando spam. Entre em contato com seu administrador de e-mail se isso estiver errado.
551 Mailhost is on our global block list	Devido ao último abuso, o remetente ou destinatário está sendo bloqueado. Entre em contato com seu administrador de clientes para apelar deste status.
551 Sender is on domain's block list	Este remetente não tem permissão para enviar mensagens de acordo com as configurações de política. Entre em contato com seu administrador de clientes se isso estiver errado.
552 Message size exceeds fixed maximum	Este remetente enviou uma mensagem que excede o máximo da configuração de uma política. Entre em contato com seu administrador de clientes se isso estiver errado.
553 Invalid recipient (Mode: normal)	A mensagem foi rejeitada porque a criação de usuários foi definida para ser negada. Entre em contato com seu administrador de clientes se isso estiver errado.

Tabela 7-7 Descrições da disposição do destinatário *(continuação)*

Evento	Definição e ações sugeridas
553 Mailbox is restricted	A mensagem foi enviada a um endereço rejeitado por uma blindagem de destinatário. Entre em contato com seu administrador de clientes.
553 Sender is on user deny list	O usuário adicionou o remetente à sua lista de negação. Efetue logon no Control Console, e no Email Protection selecione **Políticas** | **Conjunto de políticas** | **Permitir/Negar** para redefinir e remover o remetente da sua lista de negação.
554 Denied IPR	O endereço IP de envio tem apresentado recentemente uma alta porcentagem de spam. Tente novamente em 2 horas. Se falhar novamente, significa que o endereço IP continua enviando spam. Entre em contato com seu administrador de e-mail se isso estiver errado.
554 Denied Spamhaus	Spamhaus é um serviço de listagem de bloqueio de terceiros. Acesse `www.spamhaus.org` para ver a lista de bloqueio ou efetue logon no Control Console, e no Email Protection selecione **Políticas** | **selecione a política de entrada** | **Spam** | **Mais opções** | **desmarque Ativar lista de bloqueio em tempo real**.
592 Recipient does not accept mail	O endereço de e-mail do destinatário é questionável. Informe o seu administrador de clientes.

Descrições da disposição da mensagem

- As disposições do status dos dados registram o status de um e-mail em referência ao corpo do e-mail.
- As seguintes disposições não estão inclusas: Email Continuity (mensagens novas, respondidas, encaminhadas, de saída, ou geradas pelo sistema).

Tabela 7-8 Descrição da disposição da mensagem

Evento	Definição e ações sugeridas
250 Entregue com resposta	Entrega bem-sucedida.
250 Failsafe	A mensagem foi aceita e está armazenada no Failsafe. Notifique o destinatário de que seu servidor de e-mail está inoperante.
250 Na fila	A mensagem está na fila. Cada mensagem é tratada de forma diferente devido à política. As informações da fila podem ser listadas na janela **Detalhes da auditoria**.
250 OK qa	A mensagem foi colocada em quarentena porque continha um anexo rejeitado pela política do seu administrador de clientes. O título do anexo pode ser listado na janela **Detalhes da auditoria**. Entre em contato com seu administrador de clientes, se necessário.
250 OK qh	A mensgaem foi colocada em quarentena pelo ClickProtect.
250 OK qk	A mensagem foi colocada em quarentena porque continha uma palavra-chave rejeitada pela política do seu administrador de clientes. A palavra-chave pode ser listada na janela Detalhes da auditoria. Entre em contato com seu administrador de clientes.

Tabela 7-8 Descrição da disposição da mensagem *(continuação)*

Evento	Definição e ações sugeridas
250 OK qs	A mensagem continha spam. Entre em contato com seu administrador de clientes, se necessário.
250 OK qv	A mensagem pode conter vírus e está sendo colocada em quarentena. O nome do vírus pode ser listado na janela **Detalhes da auditoria**. Entre em contato com seu administrador de clientes, se necessário.
250 OK, Silent Deny	O remetente acredita que a entrega foi bem-sucedida, mas a mensagem foi descartada pela política. Entre em contato com seu administrador de clientes para ativar ou desativar a negação silenciosa.
250 encrypted	A mensagem foi entregue por meio da caixa de entrada de criptografia. Entre em contato com seu administrador de clientes se isso estiver errado.
451 No Recipients	A mensagem é recebida, mas o sistema não consegue verificar se os destinatários podem receber e-mail. O sistema tentará enviar a mensagem, mas, se não obtiver êxito, as tentativas de enviar a mensagem serão interrompidas após um período de tempo especificado (normalmente, cinco dias). Notifique o destinatário.
521 Could not deliver message over TLS for domain	O TLS imposto é ativado, mas o servidor nega o e-mail. Entre em contato com o administrador do seu servidor de e-mail. O servidor de e-mail recebido não pode ter o TLS configurado.
551 Denied IVF	Existe um alto risco de vírus e worms e, por isso, esse tipo de mensagem é automaticamente negado. O nome do vírus pode ser listado na janela **Detalhes da auditoria**. Informe o seu administrador de clientes.
551 Denied SPAM	Este tipo de mensagem é automaticamente negado por conter spam. O título do spam pode ser listado na janela **Detalhes da auditoria**. Informe o seu administrador de clientes.
551 Message contains an encrypted ZIP File	Esta política nega os anexos que não podem ser varridos. Peça a seu administrador de clientes para permitir.
552 message size exceeds fixed maximum message size of {whatever} (Mode: normal)	O remetente acredita que a entrega foi bem-sucedida, mas a mensagem excedeu o tamanho máximo da política e foi descartada. Entre em contato com seu administrador de clientes se isso estiver errado.
554 Denied	Esta política não permite uma palavra-chave específica. A palavra-chave pode ser listada na janela **Detalhes da auditoria**. Peça a seu administrador de clientes para colocar o conteúdo em quarentena ou permiti-lo.
554 Denied SPAM	Esta política determina este tipo de mensagem como spam. O título do spam pode ser listado na janela **Detalhes da auditoria**. Entre em contato com seu administrador de clientes para permitir.
554 Content filter will not allow this message	Esta política contém um grupo de conteúdo de spam que bloqueou esta mensagem. A palavra-chave do spam pode ser listada na janela **Detalhes da auditoria**. Entre em contato com seu administrador de clientes.

Tabela 7-8 Descrição da disposição da mensagem *(continuação)*

Evento	Definição e ações sugeridas
554 This message contains a virus	Esta política nega um anexo que contém este vírus ou o vírus não pode ser limpo. O nome do vírus pode ser listado na janela **Detalhes da auditoria**. Entre em contato com seu administrador de clientes.
554 Message Denied: Restricted attachment	A configuração de política nega estes anexos devido ao tipo ou tamanho. O nome do anexo pode ser listado na janela **Detalhes da auditoria**. Entre em contato com seu administrador para remover o anexo e colocá-lo em quarentena, ou tentar descontaminar o anexo.
554 Denied, restricted attachment (contains two restricted attachments)	A configuração de política nega estes anexos devido ao tipo ou tamanho. O nome do anexo pode ser listado na janela **Detalhes da auditoria**. Entre em contato com seu administrador de clientes para permitir.
554 must use TLS (Mode normal)	O TLS não é imposto. Trabalho em conjunto com o administrador de e-mail do domínio que falhou para garantir que o TLS está ativado em ambos os servidores de e-mail.
554 Error: SPF validation failed because no SPF records available	Negado devido a uma violação da política de SPF imposto. Entre em contato com seu administrador de clientes se esta política estiver errada.

Visualizando os endereços de IP bloqueados

A **Pesquisa de bloqueio de perímetro** permite que o usuário pesquise e analise os IPs que foram bloqueados com base no histórico do IP do remetente.

Se houver um problema com os resultados da sua pesquisa de IP, faça o seguinte.

- Se um IP tiver sido bloqueado por engano, você deve enviar uma solicitação de pesquisa de IP acessando postmaster.mcafee.com e clicando no link que diz **clique aqui para enviar um Solicitação de pesquisa de IP** para preencher o formulário e enviá-lo para análise.
- Se o IP foi permitido, mas a auditoria de mensagens foi incapaz de rastreá-lo, leve essas informações ao seu administrador de clientes para futuras pesquisas.
- Se a auditoria de mensagens for incapaz de rastrear o IP, leve essas informações ao seu administrador de clientes.

Executar uma pesquisa de bloqueio de perímetro

Use o formulário de pesquisa de bloqueio de perímetro para pesquisar e analisar os IPs que foram bloqueados com base no histórico do IP do remetente.

Tarefa

Para executar uma pesquisa de bloqueio de perímetro, realize as etapas abaixo.

1 No Email Protection, selecione **Auditoria de mensagens**.

2 Clique em **Pesquisa de bloqueio de perímetro**.

3 Digite o endereço IP do remetente.

Esse campo é obrigatório. Use um endereço IP totalmente qualificado. Pesquisas com caractere curinga não são permitidas.

4 Digite uma data de início.

5 Digite ou selecione uma data de término.

6 Clique em **Pesquisar**.

Os resultados serão exibidos na janela **Resultados da pesquisa**.

7 Clique em **Fazer download** na janela **Resultados da pesquisa** para fazer download de todos os resultados.

Janela Pesquisa de bloqueio de perímetro

A janela Pesquisa de bloqueio de perímetro permite que você pesquise e analise os IPs que foram bloqueados.

Tabela 7-9 Janela Critérios de pesquisa

Opção	Definição
IP do remetente	Digite o IP completo do remetente. Pesquisas com caractere curinga não são permitidas.
Data de início	Digite uma data de início usando um intervalo dentro dos últimos 14 dias. A data é baseada no seu fuso horário. Clique no ícone de calendário para selecionar uma data na janela do calendário.
Data de início	Digite uma data de término usando um intervalo dentro dos últimos 14 dias. A data é baseada no seu fuso horário. Clique no ícone de calendário para selecionar uma data na janela do calendário.
Pesquisar	Clique para executar a pesquisa.

Tabela 7-10 Janela Resultados da pesquisa

Opção	Definição
Data e hora	A data e a hora em que o endereço IP foi bloqueado ou permitido.
IP do remetente	O endereço IP que está sendo analisado.
Status	Indica se o endereço IP foi bloqueado ou permitido.
Fazer download	Clique para gerar um arquivo csv contendo os detalhes da pesquisa.

Exibição do histórico de pesquisa

O histórico de pesquisa permite que você exiba o histórico dos usuários que realizaram pesquisas na auditoria de mensagens nos últimos 14 dias.

Analisar o histórico de pesquisa

Use o formulário de pesquisa para localizar os resultados do histórico de pesquisa com base em um intervalo de datas.

Tarefa

Para analisar seu histórico de pesquisa, conclua as seguintes etapas.

1 No Email Protection, selecione **Auditoria de mensagens**.

2 Clique em **Histórico de pesquisa**.

3 Digite uma data de início.

4 Digite uma data de término.

5 Clique em **Pesquisar**.

Os resultados serão exibidos na janela **Resultados da pesquisa**.

6 Visualizar e fazer download dos resultados da pesquisa.

Para	Use estas etapas
Fazer download de todos os resultados	Clique em **Fazer download** na janela **Resultados da pesquisa**.
Visualizar um resultado	Selecione um item para visualizar na janela **Visualizar**.
Visualizar os detalhes do resultado	Clique duas vezes em um item para visualizá-lo em uma nova guia de **Detalhes**.
Fazer download de um resultado individual	Clique duas vezes em um item para visualizá-lo em uma nova guia de **Detalhes** e clique em **Fazer download**.

Janela de histórico de pesquisa

A janela de histórico de pesquisa permite que você exiba informações sobre pesquisas realizadas.

Para alterar os domínios, ou se for apropriado, alterar os clientes, você pode clicar no link do seu cliente/domínio atual no canto superior direito da janela. Na janela **Selecionar** que é aberta, comece inserindo o nome da entidade desejada, e selecione essa entidade quando uma lista de entidades for exibida.

As informações de entrada não diferenciam maiúsculas e minúsculas.

A pesquisa por critérios, por ID da mensagem e pelo cabeçalho da mensagem são painéis recolhíveis. Basta clicar no cabeçalho a ser usado para abrir a janela específica.

Tabela 7-11 Critérios de pesquisa

Opção	Definição
Data de início	Digite uma data de início usando um intervalo dentro dos últimos 60 dias. A data é baseada no seu fuso horário. Clique no ícone de calendário para selecionar uma data na janela do calendário.
Data de término	Digite uma data de término usando um intervalo dentro dos últimos 60 dias. A data é baseada no seu fuso horário. Clique no ícone de calendário para selecionar uma data na janela do calendário.
Pesquisar	Clique para executar a pesquisa.

Tabela 7-12 Resultados da pesquisa

Opção	Definição
Data e hora	A data e hora fornecem o registro do endereço IP que foi bloqueado ou permitido com base nos critérios de tempo selecionado.
Usuário	O usuário que realizou a pesquisa.
Tipo de pesquisa	O tipo de pesquisa (de mensagem ou de bloqueio de perímetro)
Critérios de pesquisa	Os campos e critérios de pesquisa usados na pesquisa.
Fazer download	Clique para gerar um arquivo .csv que contenha os detalhes da pesquisa.

A janela de visualização e a guia de detalhes fornecem informações e opções adicionais para um resultado de pesquisa individual.

Tabela 7-13 Janela de visualização e detalhes

Opção	Descrição
IP do usuário	O endereço IP do usuário que realizou a pesquisa.
Contagem de resultados	O número de resultados retornados pela pesquisa.
Fazer download	Na guia **Detalhes**, clique para gerar um arquivo .csv que contenha os detalhes da pesquisa.

8 Relatórios

O Email Protection fornece um grande número de relatórios com os quais monitorar o seu serviço.

Conteúdo

- *Visão geral dos relatórios*
- *Configuração de cliente ou domínio e fuso horário*
- *Relatório Visão geral do tráfego*
- *Relatório* ***Tráfego: TLS***
- *Relatório Tráfego: Criptografia*
- *Relatório Ameaças: Visão geral*
- *Relatório Ameaças: Vírus*
- *Relatório Ameaças: Spam*
- *Relatório Ameaças: Conteúdo*
- *Relatório Ameaças: Anexos*
- *Relatório TLS imposto: Detalhes*
- *Relatório SPF imposto*
- *Relatório DKIM imposto*
- *Relatório ClickProtect: Visão geral*
- *Relatório ClickProtect: Registro de cliques*
- *Relatório Quarentena: Visão geral da liberação*
- *Relatório Quarentena: Registro de liberação*
- *Relatório Atividades do usuário*
- *Relatório* ***Log de eventos***
- *Relatório Trilha de auditoria*
- *Relatório Conexões de servidor de entrada*
- *Relatório Recuperação de desastres: Visão geral*
- *Relatório Recuperação de desastres: Log de eventos*

Visão geral dos relatórios

O Email Protection fornece um grande número de relatórios com os quais monitorar o seu serviço. A tabela a seguir oferece a lista de relatórios disponíveis e uma visão geral de suas funções.

Tabela 8-1 Visão geral dos relatórios

Relatório	Descrição
Visão geral do tráfego	Informações sobre todo o tráfego de e-mail de entrada e saída e a largura de banda para o domínio designado durante a data ou intervalo de datas selecionado.
Ameaça: TLS	Informações sobre todo o tráfego de e-mail de entrada e saída de TLS e a largura de banda para o domínio designado durante a data ou intervalo de datas selecionado.

Tabela 8-1 Visão geral dos relatórios *(continuação)*

Relatório	Descrição
Criptografia do tráfego	Informações sobre todo o tráfego de e-mail de saída, porcentagens e largura de banda, que foram enviados para ser criptografados, para o domínio designado durante a data ou intervalo de datas selecionado.
Ameaças: Visão geral	Informações sobre as violações de e-mail por tipo de política para o domínio designado durante a data ou intervalo de datas selecionado.
Ameaças: Vírus	Informações sobre todos os e-mails de entrada e saída que violaram as políticas de vírus do domínio designado durante a data ou intervalo de datas selecionado.
Ameaças: Spam	Informações sobre os e-mails que violaram as políticas de spam domínio designado durante a data ou intervalo de datas selecionado.
Ameaças: Conteúdo	Informações sobre os e-mails que violaram as políticas de palavra-chave de conteúdo do domínio designado durante a data ou intervalo de datas selecionado.
Ameaças: Anexos	Informações sobre os e-mails que continham anexos que violavam as políticas de anexo do domínio designado durante a data ou intervalo de datas selecionado.
Detalhes do TLS imposto	Informações sobre todo o tráfego de e-mails de entrada e saída de TLS imposto, incluindo o número de mensagens e a largura de banda do domínio designado durante um período determinado. O relatório inclui uma contagem de mensagens de entrada e saída que foram negadas devido à violação de uma política de TLS imposto.
SPF imposto	Informações sobre todo o tráfego de e-mails recebidos de SPF imposto, incluindo o domínio designado durante um período determinado. O relatório também inclui uma contagem de mensagens que foram negadas devido a uma violação da política de SPF imposto.
DKIM imposto	Informações sobre todo o tráfego de e-mails recebidos de DKIM imposto, incluindo o domínio designado durante um período determinado. O relatório também inclui uma contagem de mensagens que foram negadas devido a uma violação da política de DKIM imposto.
ClickProtect: Visão geral	Informações sobre o processamento do ClickProtect. O processamento do ClickProtect monitora os hyperlinks da Web recebidos em e-mails que podem ser clicados e seguidos pelo usuário ou que podem ser bloqueados, dependendo das configurações do ClickProtect para o domínio designado durante a data ou intervalo de datas selecionado.
ClickProtect: Registro de cliques	Informações sobre os hyperlinks da Web em e-mails que foram clicados pelo destinatário para o domínio designado durante a data ou intervalo de datas selecionado.
Quarentena: Visão geral da liberação	Informações sobre os e-mails que foram colocados em quarentena e liberados de todas as áreas de quarentena do Email Protection para o domínio designado durante a data ou intervalo de datas selecionado.
Quarentena: Registro de liberação	Informações sobre os e-mails que foram liberados de todas as áreas de quarentena do Email Protection para o domínio designado durante a data ou intervalo de datas selecionado.
Atividades do usuário	Informações sobre todo o tráfego de e-mail de entrada e saída e a largura de banda para o domínio designado durante a data ou intervalo de datas selecionado.
Registro de eventos	Exibe as mensagens que tiveram ações executadas com base no conteúdo, conteúdo de spam, vírus, ou nas definições da política de anexo. As mensagens podem ser classificadas por domínio e por direção de entrada, direção de saída ou ambas. As mensagens identificadas como ameaças pelo Email Protection também são incluídas.
Trilha de auditoria	Exibe os itens do registro de auditoria para todas as ações executadas pelos usuários no gerenciador de relatórios, ou nível superior, as funções no Control Console para o domínio designado durante a data ou intervalo de datas selecionado, incluindo alterações de conexão e configuração.

Tabela 8-1 Visão geral dos relatórios *(continuação)*

Relatório	Descrição
Conexões de servidor de entrada	Exibe informações sobre as conexões feitas com os servidores de e-mail de entrada durante o processamento.
Recuperação de desastres: Visão geral	Informações sobre os e-mails que foram colocados e retirados do spool pelo serviço de recuperação de desastres para o domínio designado durante a data ou intervalo de datas selecionado.
Recuperação de desastres: Registro de eventos	Exibe os itens do registro de eventos para as ações executadas no serviço de recuperação de desastres. Entre eles estão as ações executadas automaticamente pelo Email Protection e executadas manualmente pelo administrador.

Configuração de cliente ou domínio e fuso horário

Em todos os relatórios, selecione o cliente ou o domínio a ser gerenciado.

Tarefa

1 Selecione o relatório do cliente.

2 Dependendo de como o sistema foi configurado, você poderá executar um relatório para um domínio primário, um alias de domínio ou um domínio público. Um domínio público é um domínio registrado com um registro MX público que é usado para endereços de e-mail uniformes em diversos domínios primários. Um nome de domínio público tem o domínio primário anexado a ele entre colchetes [domínio primário] e um alias de domínio é incluído entre colchetes [alias]. Os exemplos abaixo demonstram esse recurso:

- acme.com [acme-denver.com] é o domínio público [domínio primário], respectivamente.
- acme.com [alias]

Relatório Visão geral do tráfego

O relatório **Visão geral do tráfego** contém diversos gráficos e um texto resumido que fornecem a você uma noção geral das tendências de tráfego e largura de banda para o período de tempo especificado. O botão **Fazer download** na parte superior da janela permite que você faça download de todas as informações do relatório para uma planilha.

Campo	Descrição
Resumo do tráfego	Resume em forma de texto os dados exibidos nos gráficos. Os dados de mensagem incluem mensagens para o domínio especificado para o relatório. Para incluir dados correspondentes à página de **Visão geral do Email Protection**, selecione a opção **Todos os domínios** no menu suspenso **Domínio**. Se você tiver apenas um domínio, as contagens de mensagens enviadas deste relatório podem não corresponder às contagens de mensagens enviadas na página de **Visão geral do Email Protection** porque essa página inclui todas as mensagens enviadas pelos usuários administrados, até mesmo as mensagens de domínios não administrados no Control Console.
Resumo do volume de dados	Resume em forma de texto os dados exibidos nos gráficos.
Solicitações de tráfego permitido	Exibe os agregados das solicitações permitidas pelos usuários em um período de tempo especificado. Esses números incluem uma ou mais correspondências em uma única visita a uma página da Web.

Campo	Descrição
Tendências de tráfego bloqueado	Exibe os agregados das solicitações bloqueadas para o período de tempo especificado. Esses números incluem uma ou mais solicitações de conteúdo em uma única visita a uma página da Web.
Tendências de volume de dados de entrada	Exibe o uso de largura de banda de entrada.
Tendências de volume de dados de saída	Exibe o uso de largura de banda de saída.

Relatório Tráfego: TLS

O relatório Tráfego: TLS exibe informações sobre todo o tráfego de e-mails recebidos e enviados de TLS, as porcentagens e a largura de banda referentes ao domínio determinado durante a data ou o intervalo de datas selecionado.

Todos os dados do relatório do mês atual ou anterior podem ser vistos diariamente, semanalmente ou mensalmente. O botão **Fazer download** na parte superior da janela permite que você faça download de todas as informações do relatório para uma planilha.

Tabela 8-2 Resumo do tráfego

Título	Descrição
Mensagens de entrada TLS	O total de mensagens recebidas de TLS que foram processadas por meio de uma conexão TLS.
% de mensagens de entrada enviadas por TLS	A porcentagem de mensagens de e-mail recebidas processadas por meio de uma conexão TLS.
Mensagens de entrada bloqueadas por TLS imposto	O total de mensagens de e-mail recebidas bloqueadas por uma política de TLS imposto.
Mensagens de saída TLS	O total de mensagens enviadas de TLS que foram processadas por meio de uma conexão TLS.
% de mensagens de saída enviadas por TLS	A porcentagem de mensagens de e-mail enviadas processadas por meio de uma conexão TLS.
Mensagens de saída bloqueadas por TLS imposto	O total de mensagens de e-mail enviadas bloqueadas por uma política de TLS imposto.

Tabela 8-3 Resumo de largura de banda

Título	Descrição
Largura de banda total de entrada TLS	A quantidade de dados transferidos por TLS, medidos em bytes.
% de bytes de entrada enviados por TLS	A porcentagem de e-mails de entrada enviados por TLS, medidos em bytes.
Largura de banda total de saída	A quantidade de dados transferidos por TLS, medidos em bytes.
% de bytes de saída enviados por TLS	A porcentagem de e-mails de saída por TLS, medidos em bytes.

Relatório Tráfego: Criptografia

O relatório **Tráfego: Criptografia** exibe informações sobre todo o **tráfego de e-mail de saída**, as porcentagens e a largura de banda do domínio designado durante a data ou o intervalo de datas selecionado enviado para ser criptografado.

Todos os dados do relatório do mês atual ou anterior podem ser vistos diariamente, semanalmente ou mensalmente.

Tabela 8-4 Resumo do Email Encryption

Título	Descrição
Mensagens criptografadas de saída	O total de mensagens de saída a serem entregues para criptografia.
Porcentagem de mensagens de saída enviadas para criptografia	A porcentagem de mensagens de e-mail de saída enviadas para serem criptografadas.

Tabela 8-5 Resumo de largura de banda do Email Encryption

Título	Descrição
Largura de banda total de saída	A largura de banda total das mensagens de e-mail de saída enviadas para criptografia.
Porcentagem de mensagens de saída enviadas para criptografia	A porcentagem de bytes de mensagens de saída enviadas para serem criptografadas.

Relatório Ameaças: Visão geral

O relatório **Ameaças: Visão geral** fornece uma visão rápida das ameaças recebidas e enviadas, como spam, vírus, beacons de spam, violações de conteúdo e violações de anexo, que estão sendo filtradas pelo Email Protection antes que possam chegar à rede do cliente. Os administradores podem usar os relatórios para avaliar rapidamente a eficácia e o valor do Email Protection.

O relatório **Ameaças: Visão geral** indica o número total de e-mails de entrada e saída que violaram cada tipo de política do domínio e intervalo de datas designados. Os dados de cada tipo de política estão codificados com cores na legenda abaixo do gráfico. Seus tipos e configuração de política determinam o conteúdo deste relatório.

- Total de mensagens recebidas categorizadas como: spam, vírus, conteúdo e anexos.
- Total de mensagens enviadas categorizadas como: vírus, conteúdo e anexos.

Os números contidos no **Resumo das ameaças de entrada** são incluídos para dar a você um panorama geral do que o Email Protection está fazendo para proteger a sua empresa. Os números provavelmente não somarão 100% porque os seguintes utilitários são usados para varrer e-mails:

- Diversos mecanismos diferentes de antivírus
- Software que identifica diversos vírus em um único e-mail
- Software que resolve diversos nomes e aliases de domínio em seu site
- Utilitários que identificam spam e vírus em um único e-mail

Tabela 8-6 Resumo das ameaças de entrada

Título	Descrição
Total de vírus	Todos os e-mails de entrada que continham vírus conhecidos.
Taxa de infecção	O número de e-mails com vírus/todos os e-mails de entrada. Expressado nesta notação: 0/407, neste exemplo, a notação significa "0" e-mails infectados em um total de "407" e-mails recebidos.
Total de spam identificado	Todos os e-mails de entrada que continham spam potencial.
Volume de spam	A porcentagem dos e-mails de entrada que continham spam potencial.
Beacons de spam detectados	Todos os beacons de spam detectados em e-mails de entrada. Cada e-mail pode conter diversos beacons de spam, e todos os beacons são contados. Definição: Os beacons de spam, normalmente um gráfico de 1x1 pixel transparente incorporado no conteúdo HTML, podem revelar a atividade do usuário aos spammers enquanto marcam o endereço do destinatário como ativo.
Violações da palavra-chave de conteúdo	Todos os e-mails de entrada que violaram as políticas de palavra-chave de conteúdo.
Violações da política de anexo	Todos os e-mails de entrada que continham anexos que violavam as políticas de anexo.

Tabela 8-7 Resumo das ameaças de saída

Título	Descrição
Total de vírus	Todos os e-mails de saída que continham vírus conhecidos.
Taxa de infecção	A porcentagem dos e-mails de saída que continham vírus conhecidos.
Violações da palavra-chave de conteúdo	Todos os e-mails de saída que violaram as políticas de palavra-chave de conteúdo.
Violações da política de anexo	Todos os e-mails de saída que continham anexos que violavam as políticas de anexo.

Relatório Ameaças: Vírus

O relatório **Ameaças: Vírus** mede o número de e-mails recebidos e enviados infectados por vírus filtrados pelo serviço e fornece informações sobre terem sido limpos ou removidos conforme a preferência do cliente. O relatório também inclui os nomes dos vírus conhecidos filtrados.

Tabela 8-8 Resumo da detecção de vírus

Campo	Descrição
Total de vírus de entrada	O número total de e-mails de entrada que continham vírus conhecidos ("e-mails infectados").
Taxa de infecção de entrada	A porcentagem dos e-mails de entrada infectados em relação ao número total de e-mails de entrada recebidos.
Total de vírus de saída	O número total de e-mails de saída infectados.
Taxa de infecção de saída	A porcentagem dos e-mails de saída infectados em relação ao número total de e-mails de saída enviados.

Tabela 8-8 Resumo da detecção de vírus *(continuação)*

Campo	Descrição
Descontaminado (limpo)	O número total de e-mails infectados que tiveram seus vírus removidos com êxito e os e-mails que foram encaminhados aos seus destinos.
Removido	O número total de e-mails infectados que tiveram seus anexos infectados removidos e, em seguida, foram encaminhados aos seus destinos.

Tabela 8-9 Ações da política de vírus

Campo	Descrição
Negar	A porcentagem de e-mails que foram infectados e tiveram as ações da política aplicadas a eles. A entrega é negada.
Quarentena	A porcentagem de e-mails que foram infectados e tiveram as ações da política aplicadas a eles. O e-mail é enviado para a área de quarentena do destinatário.

Tabela 8-10 Principais vírus de entrada

Campo	Descrição
{ name }	Os nomes dos vírus encontrados com mais frequência nos e-mails de entrada, na ordem dos mais frequentes para os menos frequentes.
{ number}	A quantidade dos vírus encontrados com mais frequência nos e-mails de entrada, na ordem dos mais frequentes para os menos frequentes.

Tabela 8-11 Principais vírus de saída

Campo	Descrição
{ name }	Os nomes dos vírus encontrados com mais frequência nos e-mails de saída, na ordem dos mais frequentes para os menos frequentes.
{ number}	A quantidade dos vírus encontrados com mais frequência nos e-mails de saída, na ordem dos mais frequentes para os menos frequentes.

Relatório Ameaças: Spam

A janela do relatório **Ameaças: Spam** exibe informações sobre os e-mails que violaram as políticas de spam do domínio designado durante a data ou o intervalo de datas selecionado.

Os administradores podem avaliar facilmente o impacto dos spams de ameaça de e-mail mais comuns com esse relatório, que inclui três importantes medidas:

- Total de spam de entrada identificado
- Volume de spam de entrada
- E-mail inválido detectado

Tabela 8-12 Resumo da detecção de spam

Campo	Descrição
Total de spam de entrada identificado	O número total de e-mails de entrada que violaram políticas de spam.
Volume de spam de entrada	A porcentagem de e-mails de entrada que violaram as políticas de spam X o número total de e-mails de entrada recebidos.
E-mail inválido detectado	Exibe o número de mensagens classificadas como e-mail inválido. Um e-mail inválido é definido como um e-mail enviado por um remetente inválido ou um e-mail enviado a destinatários inválidos.

Tabela 8-12 Resumo da detecção de spam *(continuação)*

Campo	Descrição
Beacons de spam detectados	Todos os beacons de spam detectados em e-mails recebidos. Cada e-mail pode conter diversos beacons de spam, e todos os beacons são contados. DEFINIÇÃO: os beacons de spam, normalmente um gráfico de pixel de 1x1 transparente incorporado ao conteúdo HTML, podem revelar a atividade do usuário aos spammers enquanto marcam o endereço do destinatário como ativo.
Listas de bloqueio em tempo real	Exibe o número de mensagens identificadas como suspeitas pela filtragem DNSBL baseada na reputação.
Mensagens devolvidas negadas	Exibe o número total de mensagens negadas. Esses totais não são incluídos nos totais de volume de spam, nos totais identificados de spam de entrada ou nos gráficos de ações de política de spam.

Tabela 8-13 Ações de política de spam

Campo	Descrição
Negar	A porcentagem de e-mails que violaram as políticas de spam e tiveram as ações da política aplicadas a eles. A entrega é negada.
Quarentena	A porcentagem de e-mails que violaram as políticas de spam e tiveram as ações da política aplicadas a eles. O e-mail é enviado para a área de quarentena do destinatário.
Marcar	A porcentagem de e-mails que violaram as políticas de spam e tiveram as ações da política aplicadas a eles. O e-mail é enviado ao destinatário com a marca [SPAM].
Outros	A porcentagem de e-mails que recaem em todas as outras políticas (por exemplo; Nenhuma ação) e tiveram as ações da política aplicadas a eles. O e-mail é enviado ao destinatário com a ação apropriada aplicada ou então o e-mail é negado.

Relatório Ameaças: Conteúdo

O relatório **Ameaças: Conteúdo** indica o número total de e-mails recebidos e enviados que violaram as políticas de conteúdo de palavra-chave e a porcentagem de ações de política (por exemplo, colocar em quarentena) aplicadas aos e-mails que violaram as políticas de conteúdo de palavra-chave durante a data ou o intervalo de datas selecionado.

Tabela 8-14 Principais violações do grupo de conteúdo de entrada/saída

Campo	Descrição
Cartão de crédito	O número total de e-mails que continham palavras-chaves e frases do grupo de conteúdo predefinido de cartão de crédito.
Linguagem vulgar	O número total de e-mails que continham palavras-chaves e frases do grupo de conteúdo predefinido de linguagem vulgar.
Racismo	O número total de e-mails que continham palavras-chaves e frases do grupo de conteúdo predefinido de racismo.
Conotação sexual	O número total de e-mails que continham palavras-chaves e frases do grupo de conteúdo predefinido de conotação sexual.
Seguro social	O número total de e-mails que continham palavras-chaves e frases do grupo de conteúdo predefinido de seguro social.
Uso aceitável - Linguagem ofensiva	O número total de e-mails que continham palavras-chaves e frases do grupo de conteúdo predefinido de linguagem ofensiva.
Uso aceitável - Discriminação	O número total de e-mails que continham palavras-chaves e frases do grupo de conteúdo predefinido de discriminação.

Tabela 8-14 Principais violações do grupo de conteúdo de entrada/saída *(continuação)*

Campo	Descrição
América do Norte PII - Violações de números de seguro social	O número total de e-mails que continham palavras-chaves e frases do grupo de conteúdo predefinido de violações de números de seguro social.
América do Norte PII - Violações de números de cartões de créditos não criptografados	O número total de e-mails que continham palavras-chaves e frases do grupo de conteúdo predefinido de violações de números de cartão de crédito.
Conteúdo sexual	O número total de e-mails que continham palavras-chaves e frases do grupo de conteúdo predefinido de conteúdo sexual.
{ custom }	O número total de e-mails que continham palavras-chaves e frases de um grupo de conteúdo {custom} criado por você. Você pode ter diversos grupos de conteúdo {custom), cada um com um nome exclusivo.

Tabela 8-15 Ações da política de conteúdo

Campo	Descrição
Negar	A porcentagem de e-mails que violaram as políticas de palavra-chave de conteúdo e tiveram as ações da política aplicadas a eles. A entrega é negada.
Quarentena	A porcentagem de e-mails que violaram as políticas de palavra-chave de conteúdo e tiveram as ações da política aplicadas a eles. O e-mail poderá ser visualizado na área de quarentena de conteúdo/quarentena de mensagem do domínio.
Permitir	A porcentagem dos e-mails que não violaram as políticas de palavra-chave de conteúdo. O e-mail é encaminhado ao endereço de e-mail do destinatário sem nenhum processamento aplicado.
Marcar	A porcentagem de e-mails que violaram as políticas de palavra-chave de conteúdo e tiveram as ações da política aplicadas a eles. O e-mail é enviado ao endereço de e-mail do destinatário com a palavra "[CONTEÚDO]" adicionada à linha de assunto.
Criptografar	A porcentagem dos e-mails de saída que violaram as políticas de criptografia.

Relatório Ameaças: Anexos

Com o relatório **Ameaças: Anexos**, os administradores podem exibir o número de mensagens recebidas e enviadas encontradas que violam as políticas de anexo do cliente. O relatório inclui o total de mensagens por tipo de arquivo bloqueado, incluindo arquivos executáveis, de scripts, de documentos, de áudio, de imagem e compactados.

Tabela 8-16 Resumo do anexo

Campo	Descrição
Tamanho de anexo médio	O tamanho médio (em KB) dos anexos encontrados nos e-mails.
Executáveis	O número total de arquivos executáveis (por exemplo, *.exe) recebidos como anexo.
Scripts	O número total de arquivos de script recebidos como anexo.
Documentos do Office	O número total de documentos do Microsoft Office (por exemplo, arquivos *.doc ou *.xls, etc.) recebidos como anexo.
Áudio	O número total de arquivos de áudio (por exemplo, arquivos *.wav ou *.mp3, etc.) recebidos como anexo.

Tabela 8-16 Resumo do anexo *(continuação)*

Campo	Descrição
Imagens	O número total de arquivos gráficos (por exemplo, arquivos *.gif ou *.bmp, etc.) recebidos como anexo.
Arquivos compactados	O número total de arquivos compactados (por exemplo, arquivos *.zip ou *.tar, etc.) recebidos como anexo.

Tabela 8-17 Ações da política de anexo

Campo	Descrição
Negar	A porcentagem de e-mails que violaram as políticas de anexo e tiveram as ações da política aplicadas a eles. A entrega é negada.
Quarentena	A porcentagem de e-mails que violaram as políticas de anexo e tiveram as ações da política aplicadas a eles. O e-mail poderá ser visualizado na área de quarentena de anexo/quarentena de mensagem do domínio.
Criptografar	A porcentagem dos e-mails de saída que violaram as políticas de criptografia.
Remover	A porcentagem dos e-mails que tiverem o texto removido de um anexo.

Relatório TLS imposto: Detalhes

O relatório **TLS imposto: Detalhes** exibe informações sobre todo o tráfego de e-mails recebidos e enviados de TLS imposto, incluindo o número de mensagens e a largura de banda do domínio designado durante um determinado período. O relatório também inclui uma contagem de mensagens recebidas e enviadas que foram negadas devido à violação de uma política de TLS imposto.

Tabela 8-18 TLS imposto: Detalhes

Campo	Descrição
TLS imposto aceito - Mensagens de entrada	O número total de mensagens recebidas de TLS que foram processadas por meio de uma conexão de TLS imposto em um determinado domínio.
TLS imposto aceito - Mensagens de saída	O número total de mensagens enviadas de TLS que foram processadas por meio de uma conexão de TLS imposto em um determinado domínio.
TLS imposto aceito - Largura de banda de entrada	A quantidade de dados transferidos por meio de TLS imposto para mensagens recebidas, medida em bytes, em um determinado domínio.
TLS imposto aceito - Largura de banda de saída	A quantidade de dados transferidos por meio de TLS imposto para mensagens enviadas, medida em bytes, em um determinado domínio.
TLS imposto negado - Mensagens de entrada	O total de mensagens de e-mail recebidas bloqueadas por uma política de TLS imposto em um determinado domínio.
TLS imposto negado - Mensagens de saída	O total de mensagens de e-mail enviadas bloqueadas por uma política de TLS imposto em um determinado domínio.

Relatório SPF imposto

O relatório **SPF imposto** identifica as mensagens de e-mail recebidas que foram entregues ou negadas devido a uma violação de política de SPF imposto.

Tabela 8-19 Relatório SPF imposto

Campo	Descrição
Dez principais domínios negados de SPF imposto	Mostra os principais domínios e o número total de mensagens de e-mail negadas por uma política de SPF imposto. Para exibir os dados, deve haver uma política de SPF imposto configurada com o conjunto apropriado de domínios e ações de *negação*.
Resumo de mensagens de SPF	Resume os totais e as porcentagens dos e-mails de SPF imposto bem-sucedidos, indisponíveis ou com falhas: • **Validação bem-sucedida** — Especifica o número e a porcentagem de e-mails de SPF imposto validados com êxito. • **Falha na validação** — Especifica o número e a porcentagem de e-mails de SPF imposto com falha na validação. • **SPF indisponível** — Especifica o número e a porcentagem de e-mails de SPF imposto em que o SPF estava indisponível.

Relatório DKIM imposto

O relatório **DKIM imposto** identifica as mensagens de e-mail recebidas que foram entregues ou negadas devido a uma violação de política de DKIM imposto.

Tabela 8-20 Relatório DKIM imposto

Campo	Descrição
Dez principais domínios negados de DKIM impostos	Mostra os principais domínios e o número total de mensagens de e-mail negadas por uma política de DKIM imposto. Para exibir os dados, deve haver uma política de DKIM imposto configurada com o conjunto apropriado de domínios e ações de *negação*.
Resumo de mensagens DKIM	Resume os totais e as porcentagens dos e-mails de DKIM imposto bem-sucedidos, indisponíveis ou com falha: • **Validação bem-sucedida** — Especifica o número e a porcentagem de e-mails de DKIM imposto validados com êxito. • **Falha na validação** — Especifica o número e a porcentagem de e-mails de DKIM imposto com falha na validação. • **DKIM indisponível** — Especifica o número e a porcentagem de e-mails de DKIM imposto em que o DKIM estava indisponível.

Relatório ClickProtect: Visão geral

O relatório **ClickProtect: Visão geral** fornece os resultados de sua implementação do ClickProtect, incluindo a contagem de mensagens afetadas e o número de cliques de usuários que foram permitidos e negados.

Tabela 8-21 Estatísticas do ClickProtect

Campo	Descrição
Mensagens com links	O número total de mensagens de e-mail que continham um link.
Mensagens com vários links	O número total de mensagens de e-mail que continham mais de um link.
Total de cliques	O número total de vezes que os destinatários clicaram em links em seu e-mail.
Total de click-throughs permitidos	O número total de vezes que os destinatários foram autorizados a acessar o site depois de clicar no link.
Total de click-throughs avisa e permite	O número total de vezes que os destinatários foram levados para a página de aviso antes de serem autorizados a acessar o site.
Total de click-throughs negados devido à reputação	O número total de vezes que os destinatários tiveram acesso negado a um site devido à reputação do site.
Total de click-throughs negados devido a malware	O número total de vezes que os destinatários tiveram o acesso negado a um site porque o site continha malware.
Número de usuários individuais que clicaram	O número total de destinatários que tentaram clicar em um link em um e-mail.
Mensagens de spam com click-throughs	O número total de e-mails de spam que continham links clicados pelos destinatários.
Mensagens com links na Lista de permissão do ClickProtect	O número total de e-mails que continham links que estão listados na lista de permissão do ClickProtect.

Relatório ClickProtect: Registro de cliques

O relatório **ClickProtect: Registro de cliques** fornece detalhes sobre cada link de e-mail varrido em relação a possíveis riscos, bem como a ação resultante.

Tabela 8-22 Opções de ClickProtect: Registro de cliques

Campo	Descrição
Data e hora	Exibe a data e a hora.
De	Exibe o endereço de e-mail do remetente.
Para	Exibe o endereço de e-mail do destinatário.
Assunto	Exibe a linha de assunto do e-mail.
URL	Exibe o URL completo do link.

Tabela 8-22 Opções de ClickProtect: Registro de cliques *(continuação)*

Campo	Descrição
Reputação	Exibe a reputação do site da Web. • **Alto risco** — Especifica uma URL que apresenta comportamento prejudicial. Por exemplo, o site é conhecido por hospedar malware. • **Risco médio** — Especifica uma URL que apresenta comportamento questionável que pode ser prejudicial para o usuário. • **Risco mínimo** — Especifica uma URL que exibe comportamento adequado ou que é verificada como confiável. • **Não verificado** — Especifica uma URL de onde nenhuma informação de reputação foi obtida.
Categoria	Quando disponível, exibe a categoria associada ao site.
Malware	Quando encontrado, exibe o nome do software malicioso.
Ação	A ação realizada no momento de clique. • **Malware negado** • **Reputação negada** • **Avisa e permite** • **Permitido**
Pontuação	Exibe a pontuação de probabilidade de spam atribuída ao e-mail como uma barra gráfica. A pontuação de spam varia de 0 a 100% (verde para vermelho), com 100% (ou vermelho) sendo a maior probabilidade de que o e-mail é spam.

Relatório Quarentena: Visão geral da liberação

O relatório **Quarentena: Visão geral da liberação** fornece uma visão geral imediata da atividade de mensagens recebidas dentro da quarentena de mensagens. É possível exibir o número total de mensagens colocadas em quarentena ou liberadas em cada uma das quatro categorias: spam, vírus, violações de conteúdo e violações de anexo.

Tabela 8-23 Detalhes do relatório Quarentena: Visão geral da liberação

Opção	Definição
Inbound Quarantine Release Trends (Tendências de liberação da quarentena de entrada)	Exibe as tendências de liberação das mensagens colocadas em quarentena no período de 24 horas. • Clique nos ícones para alterar o formato do gráfico. • Clique nas categorias para mostrar ou ocultar tendências de **Spam**, **Vírus**, **Anexo** e **conteúdo**.
Resumo da liberação de spam de entrada	• **Total de spam identificado** — O número total de e-mails colocados em quarentena que foram identificados como spam. • **Total de spam liberado** — O número total de e-mails liberados da quarentena de spam. • **Porcentagem de liberação** — A porcentagem de e-mails liberados da quarentena de spam em relação ao número total de e-mails que foram colocados em quarentena como spams em potencial. • **Número total de indivíduos** — O número total de contas de usuário que tiveram e-mails liberados da quarentena de spam.

Tabela 8-23 Detalhes do relatório Quarentena: Visão geral da liberação *(continuação)*

Opção	Definição
Resumo da liberação de vírus de entrada	• **Total de vírus identificados** — O número total de vírus detectados nos e-mails recebidos que foram colocados em quarentena. • **Total de vírus liberados** — O número total de vírus liberados da quarentena de spam. • **Porcentagem de liberação** — A porcentagem de e-mails liberados da quarentena de vírus em relação ao número total de e-mails que foram colocados em quarentena devido a vírus. • **Número total de indivíduos** — O número total de contas de usuário que tiveram e-mails liberados da quarentena de vírus.
Resumo da liberação de conteúdo de entrada	• **Total de conteúdo identificado** — O número total de e-mails colocados em quarentena violaram políticas de conteúdo. • **Total de conteúdo liberado** — O número total de vírus liberados da quarentena de conteúdo. • **Porcentagem de liberação** — A porcentagem de e-mails liberados da quarentena de conteúdo em relação ao número total de e-mails que foram colocados em quarentena devido a seu conteúdo. • **Número total de indivíduos** — O número total de contas de usuário que tiveram e-mails liberados da quarentena de conteúdo.
Resumo da liberação de anexo de entrada	• **Total de violações da política de anexo** — O número total de e-mails colocados em quarentena que violaram as políticas de anexos. • **Total de anexos liberados** — O número total de anexos liberados da quarentena de anexo. • **Porcentagem de liberação** — A porcentagem de e-mails liberados da quarentena de anexo em relação ao número total de e-mails que foram colocados em quarentena devido a anexos. • **Número total de indivíduos** — O número total de contas de usuário que tiveram e-mails liberados da quarentena de anexo.

Relatório Quarentena: Registro de liberação

O relatório **Quarentena: Registro de liberação** inclui uma lista com todas as mensagens liberadas das áreas de quarentena: spam, vírus, anexos e conteúdo. Você pode visualizar o e-mail liberado da quarentena de 1 até 30 dias. Nesse log, você pode pesquisar e-mails liberados por dia, semana ou mês.

Campo Exibir

Use a lista suspensa para designar o tipo de evento de liberação de quarentena a ser exibido:

- **Todos os eventos:** eventos de liberação de todas as quarentenas.
- **Spam:** eventos de liberação da quarentena de spam.
- **Vírus:** eventos de liberação da quarentena de vírus.
- **Anexos:** eventos de liberação da quarentena de anexo.
- **Conteúdo:** eventos de liberação da quarentena de conteúdo.

Janela pop-up de itens do log

Passe o cursor do mouse sobre um item do log para que uma janela pop-up seja exibida com informações adicionais sobre o item, como o endereço do **IP do remetente**.

Tabela 8-24 Resumo Quarentena: Registro de liberação

Campo	Descrição
Tipo	O motivo pelo qual o e-mail foi para quarentena: **spam**: o e-mail violou as políticas de spam, **vírus**: o e-mail continha um vírus conhecido, **anexo**: o anexo do e-mail violou as políticas de anexo, **conteúdo**: o e-mail tinha conteúdo que violava as políticas de conteúdo, incluindo palavras-chave e HTML.
De	O endereço de e-mail que enviou o e-mail.
Para	O endereço de e-mail do destinatário.
Assunto	O texto na linha de assunto do e-mail.
Data de lançamento	A data, a hora e o fuso horário em que o e-mail foi liberado da quarentena pelo Email Protection.
Tamanho	O tamanho total do arquivo do e-mail, incluindo todos os anexos.

Relatório Atividades do usuário

O relatório **Atividades do usuário** exibe uma lista dos principais endereços de e-mail de usuário de entrada e saída por domínio na sua organização. O número total de mensagens recebidas ou enviadas e o tamanho de arquivo total de todas as mensagens do usuário também são exibidos para cada endereço de e-mail de usuário.

Tabela 8-25 Principais usuários de entrada

Campo	Descrição
Endereço de e-mail	Os endereços de e-mail de destinatário que receberam mais e-mails de entrada, em ordem de volume.
Mensagens	O número total de e-mails recebidos por cada endereço de e-mail.
Tamanho	O tamanho total em bytes (KB ou MB) de todos os e-mails, incluindo anexos, recebidos por cada endereço de e-mail.

Tabela 8-26 Principais usuários de saída

Campo	Descrição
Endereço de e-mail	Os endereços de e-mail de remetente que enviaram mais e-mails de saída, em ordem de volume. Se um endereço de e-mail de remetente não tiver sido criado no sistema do Email Protection, você poderá ver um endereço nessa lista formatado como "<unknown>@xyz.com" ou "@xyz.com" onde "xyz.com" pode ser qualquer domínio relacionado à conta do cliente.
Mensagens	O número total de e-mails enviados por cada endereço de e-mail.
Tamanho	O tamanho total em bytes (KB ou MB) de todos os e-mails, incluindo anexos, enviados por cada endereço de e-mail.

Relatório Log de eventos

O relatório **Log de eventos** exibe mensagens que tiveram ações executadas com base em definições específicas de política. Você pode classificar as mensagens por domínio, assim como por direção de

entrada, direção de saída ou ambas. As mensagens identificadas como ameaças também são incluídas.

Tabela 8-27 Relatório Log de eventos

Opção	Definição
Exibir	• **Todos os eventos** — Exibe eventos de imposição de política para vírus, tipos de conteúdo de spam, anexos e conteúdo. • **Conteúdo de spam** — Exibe eventos de imposição de política para tipos de conteúdo de spam. • **Vírus** — Exibe eventos de imposição de política para vírus. • **Anexos** — Exibe eventos de imposição de política para anexos. • **Conteúdo** — Exibe eventos de imposição de política para conteúdo. • **TLS imposto** — Exibe eventos de imposição de política para TLS imposto. • **SPF imposto** — Exibe eventos de imposição de política para SPF imposto (somente para mensagens recebidas).
Direção	• **Somente entrada** — Exibe apenas os e-mails recebidos. • **Somente saída** — Exibe apenas os e-mails enviados. • **Entrada & saída** — Exibe tanto os e-mails recebidos quanto os enviados.

Tabela de log de eventos	• **Tipo** — Especifica o tipo de política que o e-mail filtrado violou.
	• **Data e hora** — Especifica a data, a hora e o fuso horário de execução da ação no e-mail filtrado.
	• **De** — Especifica o endereço de e-mail que enviou a mensagem.
	• **Para** — Especifica o endereço de e-mail do destinatário.
	• **Assunto** — Especifica o texto na linha de assunto do e-mail.
	• **Detalhes** — Especifica o motivo da ação.
	  • Se o e-mail continha um vírus, o "nome do vírus" é mostrado.
	  • Se o e-mail continha uma palavra-chave de spam da política imposta, a "palavra-chave" é mostrada.
	  • Se o e-mail continha conteúdo da política imposta, o "conteúdo" é mostrado.
	  • Se o e-mail continha anexo da política imposta, o "tipo do anexo" é mostrado.
	  • Se o e-mail foi negado para a política de TLS imposta, o "domínio" negado é mostrado.
	• **Ação** — Especifica a ação aplicada ao e-mail (por exemplo, colocado em quarentena, negado ou nenhuma).
	Passe o cursor do mouse sobre um item do log para exibir informações adicionais sobre um item, como o endereço **IP do remetente**.

Relatório Trilha de auditoria

O relatório **Trilha de auditoria** exibe os itens do Log de auditoria para todas as ações executadas por usuários no nível do gerenciador de relatórios ou superior. Esse log apresenta a atividade do domínio

designado durante a data ou o intervalo de datas selecionado, incluindo entradas e alterações de configuração.

Este relatório fornece informações detalhadas sobre a atividade no Control Console, incluindo:

- Uma auditoria das tentativas de entrada bem-sucedidas/malsucedidas.
- Todas as alterações feitas no domínio, como a criação de grupos ou usuários.
- Todas as alterações feitas em configurações do IP de entrada, conjuntos de políticas e filtros.
- Todas as alterações na configuração de clientes.
- Quaisquer outras alterações do nível de usuário até o nível de domínio.

Tabela 8-28 Detalhes da trilha de auditoria

Campo	Descrição
Data e hora	A data, a hora e o fuso horário em que a ação foi realizada no Control Console.
Domínio	O domínio onde a ação foi realizada.
Detalhes	Uma descrição da ação realizada, incluindo a função e a conta de usuário da pessoa.

Relatório Conexões de servidor de entrada

O relatório **Conexões de servidor de entrada** exibe informações sobre as conexões feitas aos servidores de e-mail de entrada (MTAs do cliente) durante o processamento. O relatório inclui dados das tendências de volume do servidor e detalhes sobre êxitos e falhas na conexão. O endereço IP do servidor é resolvido no momento da geração do relatório, para corresponder os dados do evento. Os servidores não configurados também são mostrados, incluindo os servidores inativos ou excluídos.

Este relatório descreve as taxas gerais de êxito e falha das conexões com os servidores de e-mail de entrada dos clientes. Os administradores podem usar este relatório para identificar as falhas de conexão em um servidor específico, visualizando o status da conexão do IP de entrada, a % da taxa de falhas e os êxitos ou falhas.

O administrador do cliente pode exibir rapidamente o status da conexão aqui.

Exibir tendências de volume para

Use a lista suspensa para exibir:

- **Todos os servidores:** informações sobre todos os servidores de entrada configurados para o domínio selecionado.
- **{servidor específico}:** informações apenas sobre o servidor de entrada selecionado.

Taxa de falha geral

A porcentagem de falhas de conexão com o servidor designado.

Total de êxitos

O número total de conexões bem-sucedidas com o servidor designado. Cada mensagem de e-mail entregue é igual a uma conexão bem-sucedida.

Total de falhas

O número total de tentativas malsucedidas de se conectar ao servidor designado.

Tabela 8-29 Detalhes da conexão do servidor de entrada

Campo	Descrição
Servidor: Porta	O endereço do servidor e o número da porta.
Endereço IP	O endereço IP do servidor.
Status	Se o servidor atualmente está ativo, inativo, ou excluído.
Preferência	A preferência do MX para este servidor. Ao entregar o e-mail, o serviço tentará entregá-lo primeiro ao servidor de menor número.
% de taxa de falha	A porcentagem de falha de conexão para este servidor e porta.
Êxito	A porcentagem de êxito de conexão para este servidor e porta. Cada mensagem de e-mail entregue é igual a uma conexão bem-sucedida.
Falha	O número total de tentativas mal-sucedidas de se conectar ao servidor e porta selecionados.

Relatório Recuperação de desastres: Visão geral

A janela de relatório **Recuperação de desastres: Visão geral** exibe informações sobre e-mails colocados ou retirados do spool pelo Serviço de recuperação de desastres do domínio designado durante a data ou o intervalo de datas selecionado. O relatório detalha a atividade das mensagens dentro do **Email Continuity** ou do **Fail Safe Service**, incluindo o número de mensagens colocadas ou retiradas do spool pelos serviços de recuperação de desastres de e-mail.

Tabela 8-30 Resumo da recuperação de desastres - Mensagens

Campo	Descrição
Mensagens no spool	O número de e-mails que foram colocados no spool, de forma automática ou manual.
Mensagens fora do spool	O número de e-mails que foram retirados do spool, de forma automática ou manual.

Tabela 8-31 Resumo da recuperação de desastres - Bytes

Campo	Descrição
Bytes no spool	A quantidade de armazenamento de spool usado pelo spool de e-mails durante uma interrupção.
Bytes fora do spool	A quantidade de armazenamento de spool usado pela remoção de spool de e-mails após uma interrupção.

Relatório Recuperação de desastres: Log de eventos

O relatório **Recuperação de desastres: Log de eventos** exibe os itens do log de eventos das ações executadas dentro do serviço de recuperação de desastres. Entre elas estão as ações executadas automaticamente pelo Email Protection e manualmente pelo administrador. Inclui dados sobre spool e remoção de spool automáticos/manuais de mensagens de e-mail durante uma interrupção no domínio

selecionado. O **Log de eventos de recuperação de desastres** inclui eventos de **Recuperação de desastres** e do **Email Continuity**.

Tabela 8-32 Recuperação de desastres: Log de eventos

Campo	Descrição
Data e hora	A data, a hora e o fuso horário em que a ação foi realizada no modo de recuperação de desastres.
Evento	Os itens de registro de eventos para ações de recuperação de desastres realizadas para o domínio e o intervalo de datas determinados.
Iniciado por	A parte responsável que realizou ação da recuperação de desastres. Se uma ação foi realizada manualmente, indica a função e a conta de usuário da pessoa que realizou a ação. Todas as ações realizadas pelo Email Protection serão listadas nos usuários do *sistema*.

Índice

C

Convenções 7

E

Encontrar a documentação 8

O

O que há neste guia 8

P

Público-alvo 7

S

Sobre este guia 7