Como arquivar email na ferramenta de segurança e na nuvem do email envie por correio eletrónico a Segurança?

Índice

Introdução

Este documento descreve as etapas a ser seguidas a fim arquivar email na Segurança do email da ferramenta de segurança (ESA) e da nuvem do email (CES) para a recuperação e a revisão.

Informações de Apoio

Quando você arquiva email no ESA e no CES, pode ser usado para cumprir as exigências regulamentares ou para fornecer meios adicionais dos dados para um diagnóstico e uma revisão mais adicionais do correio. Arquivar envia por correio eletrónico atua como um armazenamento secundário dos email em um formato de registro do mbox nela é fonte original para administradores a fim recuperar e validar.

- Recomenda-se manter os ajustes aos valores padrão se você decide permitir a arquivística dos email. Os valores padrão são 10MB pelo máximo do log e dos logs 10 retido. Os logs continuarão a ser adicionados e rolado baseado sobre no tamanho do arquivo de registro próprio. Os arquivos de registro do mbox do arquivo são enchidos basearam na taxa do tráfego do email que passa embora o dispositivo. Enquanto mais logs são criados, uns logs mais velhos do mbox do arquivo estão removidos ao espaço livre para a criação do log novo.
- Assegure-se de que seu dispositivo tenha o espaço de disco suficiente antes que você aumente os tamanhos do arquivo de registro do mbox do arquivo e os arquivos de registro máximos retidos.
- A fim parar os logs do mbox do arquivo da geração, você terá que desabilitar a função do arquivo pela política.

Note: Os logs do mbox do arquivo ESA e CES não podem ser recuperados pelo S A e são

armazenados localmente por cada ESA e CES com a característica permitida.

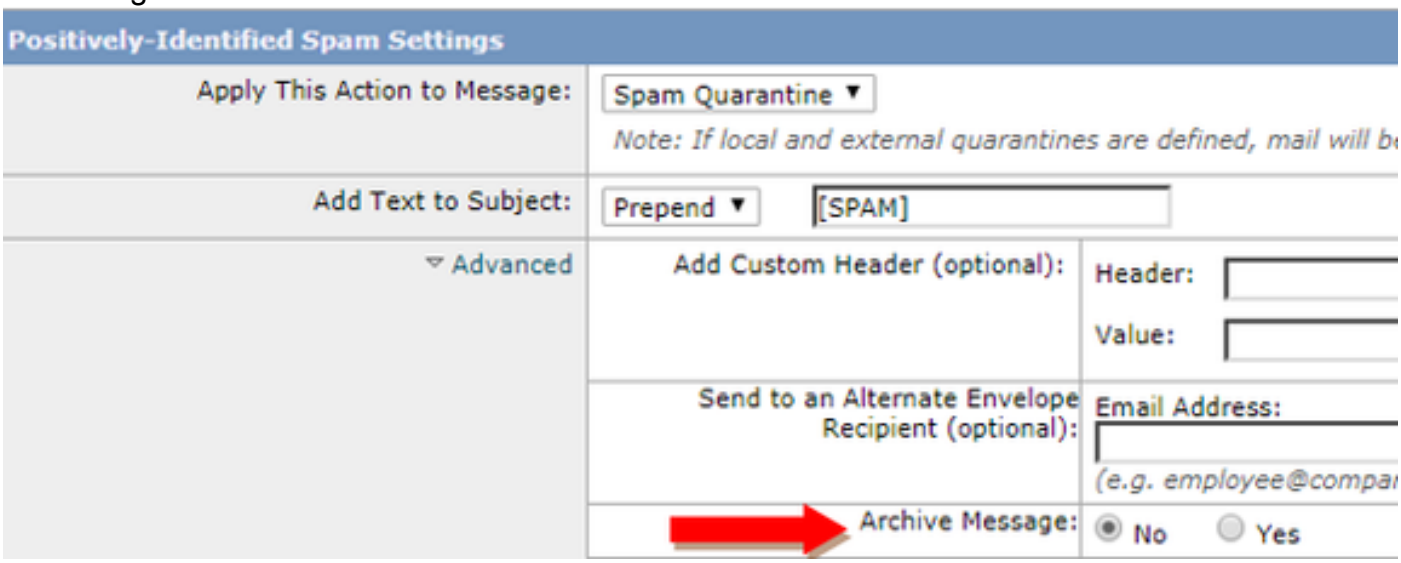
Como arquivar email no ESA e no CES?

A arquivística do email está disponível com os filtros do Anti-Spam, os anti-vírus, os avançados do malware da proteção, do Graymail e da mensagem. A ação do arquivo pode ser configurada no GUI e no CLI para o Anti-Spam, a proteção anti-vírus, avançada do malware e o Graymail.

A ação do arquivo pode ser configurada no CLI somente para filtros da mensagem.

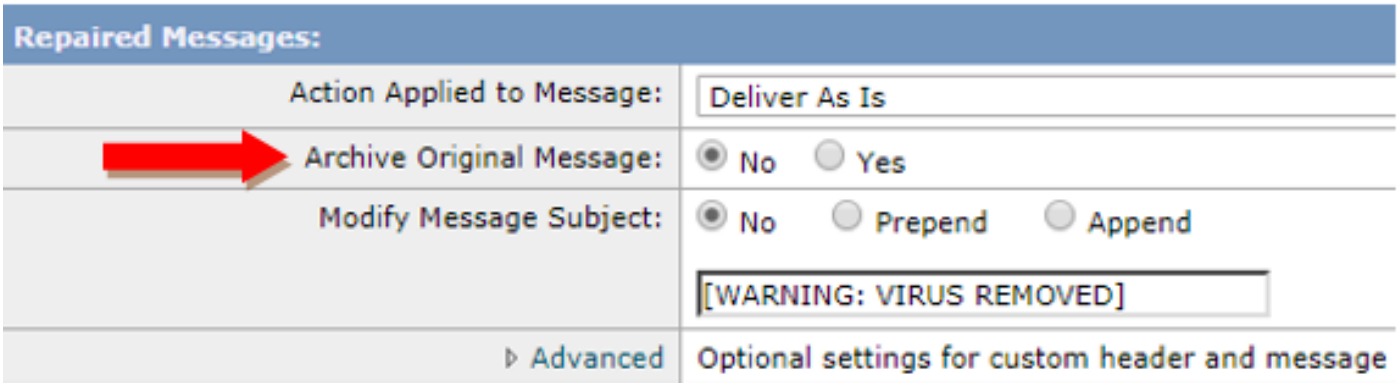
Configurar o arquivo do Anti-Spam

1. Navegue ao **GUI > políticas do correio > políticas entrantes/que parte do correio**.
2. Clique sobre os ajustes do Anti-Spam na política respectiva a fim configurar a arquivística do email.
3. Clique **avançado nos** ajustes disponíveis para ajustes positivamente identificados do Spam, ajustes suspeitados do Spam.
4. Pressione o botão de rádio ao lado do Yes a fim arquivar email com a sentença respectiva do Anti-Spam.
5. A configuração de Submitthe, e compromete estas mudanças segundo as indicações da imagem.



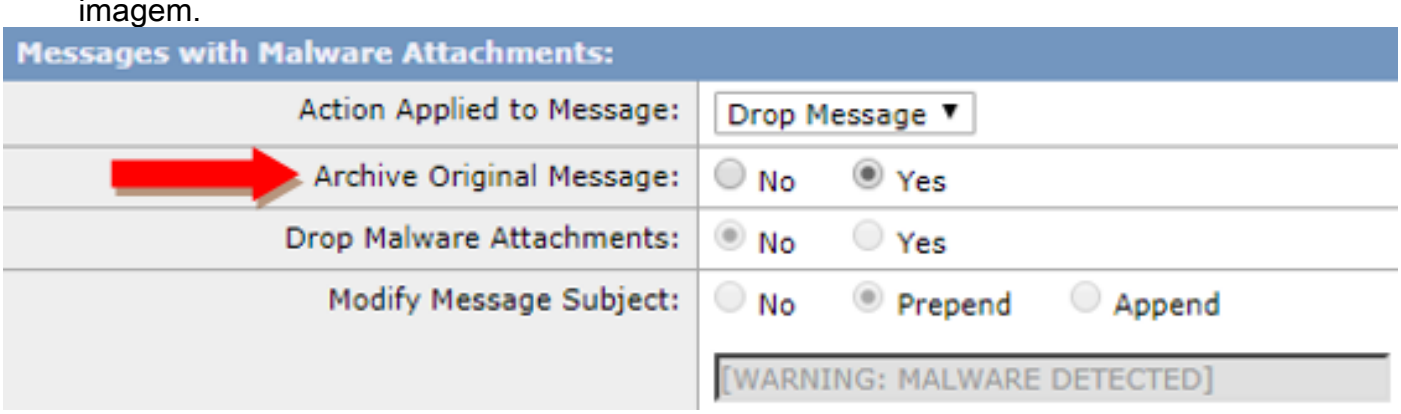
Configurar o arquivo anti-vírus

1. Navegue ao **GUI > políticas do correio > políticas entrantes/que parte do correio**.
2. Clique sobre os ajustes anti-vírus na política respectiva a fim configurar a arquivística do email.
3. Em cada um da exploração as sentenças que você deseja arquivar o mensagem original, pressionam o botão de rádio ao lado do Yes no arquivo do orderto.
4. A configuração de Submitthe, e compromete estas mudanças segundo as indicações da imagem.



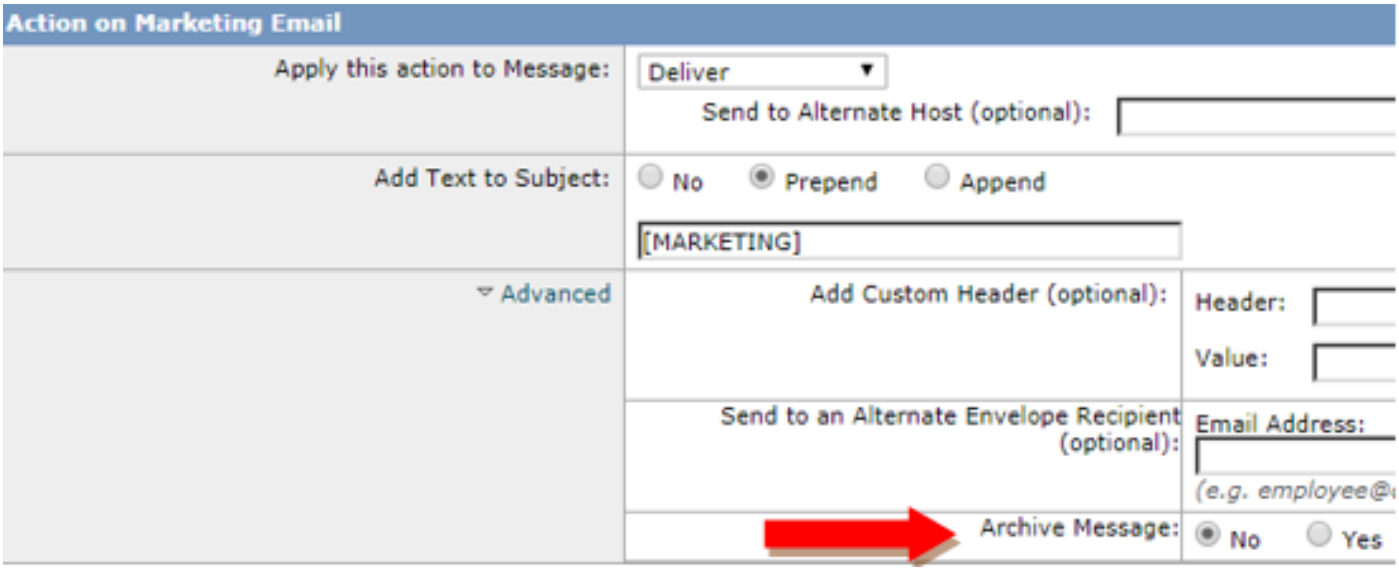
Configurar arquivo avançado da proteção do malware

1. Navegue ao **GUI > políticas do correio > políticas entrantes/que parte do correio**.
2. Clique sobre o malware avançado Protectionsettings na política respectiva a fim configurar a arquivística do email.
3. Em cada um da exploração as sentenças que você deseja a fim arquivar o mensagem original, pressionam o botão de rádio ao lado do Yes a fim arquivar.
4. A configuração de Submitthe, e compromete estas mudanças segundo as indicações da imagem.



Configurar o arquivo de Graymail

1. Navegue ao **GUI > políticas do correio > políticas entrantes/que parte do correio**.
2. Clique sobre os ajustes de Graymail na política respectiva a fim configurar a arquivística do email.
3. Clique **Advancedon os** ajustes disponíveis para introduzir no mercado, Social, volume.
4. Pressione o botão de rádio ao lado do Yes a fim arquivar email com a sentença respectiva de Graymail.
5. Submeta a configuração, e comprometa estas mudanças.



Configurar o arquivo do filtro da mensagem

> **Note**: Um filtro da mensagem com ação do arquivo é exigido a fim ver logs arquivados. Os filtros da mensagem podem somente ser criados dentro do CLI.

Filtro da amostra:

```
Test_Archive:
if (mail-from == "test1@cisco.com")
{
archive("Test");
}
```

1. Início de uma sessão ao dispositivo no CLI.
2. Crie um filtro da mensagem como visto no filtro da amostra fornecido.
3. Submeta este filtro e comprometa suas mudanças.

Valide a Disponibilidade dos logs de Mbox do arquivo

Quando a configuração para o arquivo é comprometida para os serviços respectivos, os email arquivados estão armazenados em um arquivo de registro do formato do mbox. A fim verificar se os log de arquivo estão disponíveis para a recuperação, navegue ao **GUI > assinaturas da administração do sistema > do log**.

Os arquivos dos Serviços de segurança criam um log separado com um tipo do log de arquivo segundo as indicações da imagem:

Configured Log Subscriptions

Add Log Subscription...

Log Settings	Type ▲	Log Files	Rollover Interval
amp	AMP Engine Logs	amp/	None
amparchive	AMP Archive	amparchive/	None
antispam	Anti-Spam Logs	antispam/	None
antivirus	Anti-Virus Logs	antivirus/	None
asarchive	Anti-Spam Archive	asarchive/	None
authentication	Authentication Logs	authentication/	None
avarchive	Anti-Virus Archive	avarchive/	None

Para a mensagem filtra a configuração do arquivo é visto do **CLI somente**:

- **filtros > logconfig**

```
demigod.cisco.com> filters

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> logconfig

Currently configured logs:
    Log Name          Log Type                    Retrieval          Interval
 ------------------------------------------------------------------------------
 1. Test              Filter Archive Logs         Manual Download    None
```

Recupere os logs de Mbox

Para dispositivos autônomos estes logs do mbox podem ser recuperados diretamente do GUI. Navegue ao theGUI **> à administração do sistema > ao log Subscriptionsand** clicam sobre os **arquivos de registro** para o log de arquivo que respectivo você recuperará.

Para dispositivos aglomerados, os logs do mbox podem ser recuperados com o uso da cópia FTP/Secure (SCP) como descrito no [thisarticle](https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00....). (https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00....)

Informações Relacionadas

- [Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final]
- [Que é formato do mbox de UNIX (caixa postal)?]
- [Onde estão os logs armazenados na ferramenta de segurança do email de Cisco (ESA) e como I os alcança]
- [Como extrair um email dos logs do mbox do arquivo]

- Suporte Técnico e Documentação - Cisco Systems