

如何归档在电子邮件安全工具和Cloud的电子邮件给安全发电子邮件？

目录

[简介](#)

[背景信息](#)

[如何归档在ESA和CES的电子邮件？](#)

[配置反垃圾邮件存档](#)

[配置抗病毒存档](#)

[配置先进的恶意软件保护存档](#)

[配置Graymail存档](#)

[配置消息过滤器存档](#)

[验证存档Mbox日志可用性](#)

[检索Mbox日志](#)

[相关信息](#)

简介

本文描述将被跟随的步骤为了归档在电子邮件安全工具(ESA)和Cloud电子邮件安全(CES)的电子邮件检索和复核的。

背景信息

当您归档在ESA和CES时的电子邮件，可以用于符合章程要求或为进一步邮件诊断和复核提供数据另外的平均值。归档发电子邮件作为电子邮件的间接储藏在mbox日志格式的在它是管理员的初始源为了获取和验证。

- 如果决定启用电子邮件，存档推荐保持设置到默认值。默认值是10MB每保留的日志和10本日志最大数量。日志将继续被添加和滚动基于日志文件的大小。存档mbox日志文件被填充根据虽则通过设备的电子邮件流量的速率。当更多日志创建，更旧的存档mbox日志删除对新的日志的创建的可用空间。
- 保证您的设备有充足的磁盘空间，在您增加保留前的存档mbox日志文件大小和最大日志文件。
- 为了从生成终止存档mbox日志，您将必须禁用存档功能每项策略。

Note:ESA和CES存档mbox日志不可能由SMA检索和每个每个ESA和CES存储本地与启用的功能。


如何归档在ESA和CES的电子邮件？

电子邮件存档用反垃圾邮件、防病毒，先进的恶意软件保护、Graymail和消息过滤器是可用的。存档操作在GUI和CLI可以配置反垃圾邮件、防病毒、先进的恶意软件保护和Graymail的。

存档操作在仅CLI可以配置消息过滤器的。

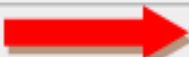
配置反垃圾邮件存档

1. 导航对GUI >邮件策略>流入/流出的邮件策略。
2. 点击在各自策略的反垃圾邮件设置为了配置电子邮件存档。
3. 点击先进在确实地已确定垃圾邮件设置的可用的设置，怀疑的垃圾邮件设置。
4. 在是旁边按单选按钮为了归档与各自反垃圾邮件判决的电子邮件。
5. 如镜像所显示， Submitthe配置， 和确认这些更改。

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine ▼ <i>Note: If local and external quarantines are defined, mail will be</i>
Add Text to Subject:	Prepend ▼ [SPAM]
▼ Advanced	
Add Custom Header (optional):	Header: <input type="text"/> Value: <input type="text"/>
Send to an Alternate Envelope Recipient (optional):	Email Address: <input type="text"/> <i>(e.g. employee@company.com)</i>
	Archive Message: <input checked="" type="radio"/> No <input type="radio"/> Yes

配置抗病毒存档

1. 导航对GUI >邮件策略>流入/流出的邮件策略。
2. 点击在各自策略的抗病毒设置为了配置电子邮件存档。
3. 在其中每一扫描您希望归档原始消息的判决，在是旁边按单选按钮在orderto存档。
4. 如镜像所显示， Submitthe配置， 和确认这些更改。

Repaired Messages:	
Action Applied to Message:	Deliver As Is
	Archive Original Message: <input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[WARNING: VIRUS REMOVED]"/>
▶ Advanced	Optional settings for custom header and message

配置先进的恶意软件保护存档

1. 导航对GUI >邮件策略>流入/流出的邮件策略。
2. 点击在各自策略的先进的恶意软件Protectionsettings为了配置电子邮件存档。
3. 在其中每一扫描您希望为了归档原始消息的判决，在是旁边按单选按钮为了归档。
4. 如镜像所显示， Submitthe配置， 和确认这些更改。

Messages with Malware Attachments:	
Action Applied to Message:	Drop Message ▾
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Malware Attachments:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
[WARNING: MALWARE DETECTED]	

配置Graymail存档

1. 导航对GUI > 邮件策略 > 流入/流出的邮件策略。
2. 点击在各自策略的Graymail设置为了配置电子邮件存档。
3. 点击Advanced on 销售的可用的设置，社交，容量。
4. 在是旁边按单选按钮为了归档与各自Graymail判决的电子邮件。
5. 提交配置，并且确认这些更改。

Action on Marketing Email	
Apply this action to Message:	Deliver ▾ Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[MARKETING]"/>
Advanced	Add Custom Header (optional): Header: <input type="text"/> Value: <input type="text"/>
	Send to an Alternate Envelope Recipient (optional): Email Address: <input type="text"/> (e.g. employee@)
	Archive Message: <input checked="" type="radio"/> No <input type="radio"/> Yes

配置消息过滤器存档

Note: 有存档操作的一个消息过滤器要求为了查看归档日志。消息过滤器可能在CLI内只创建。

示例过滤器：

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

1. 设备的洛金在CLI。
2. 如在提供的示例过滤器中看到创建消息过滤器。
3. 提交此过滤器并且确认您的更改。

验证存档Mbox日志可用性

当存档的配置为各自服务时被提交，归档的电子邮件在mbox格式日志文件存储。为了验证，如果归档日志为检索是可用的，请导航对GUI >System Administration >日志订阅。

如镜像所显示，安全服务存档创建与归档日志类型的一本单独的日志：

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

对于消息过滤存档配置从CLI只查看：

• 过滤器> 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
```

检索Mbox日志

对于独立设备这些mbox日志可以直接地从GUI被检索。导航对theGUI >System Administration >日志Subscriptionsand点击您将检索的各自归档日志的日志文件。

对于集群设备，mbox日志可以检索与使用FTP/Secure复制(SCP)正如[this article 所描述](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....>)

相关信息

- [思科电子邮件安全工具-最终用户指南](#)
- [什么是UNIX mbox \(邮箱\)格式？](#)
- [那里在思科电子邮件安全工具存储的日志\(ESA\)，并且我如何访问他们](#)
- [如何解压缩从存档mbox日志的一电子邮件](#)
- [技术支持和文档 - Cisco Systems](#)