

Wie können E-Mails auf der E-Mail Security Appliance und Cloud E-Mail Security archiviert werden?

Inhalt

[Einführung](#)

[Hintergrundinformationen](#)

[Wie können E-Mails auf der ESA und CES archiviert werden?](#)

[Anti-Spam-Archiv konfigurieren](#)

[Konfigurieren des Anti-Virus-Archivs](#)

[Advanced Malware Protection-Archiv konfigurieren](#)

[Graymail-Archiv konfigurieren](#)

[Nachrichtenfilterarchiv konfigurieren](#)

[Validieren der Verfügbarkeit von Archive Mbox-Protokollen](#)

[Abrufen der Mbox-Protokolle](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt die Schritte zur Archivierung von E-Mails auf der E-Mail Security Appliance (ESA) und Cloud Email Security (CES) zum Abrufen und Überprüfen.

Hintergrundinformationen

Wenn Sie E-Mails auf der ESA und CES archivieren, können Sie damit gesetzliche Auflagen erfüllen oder zusätzliche Datenquellen für die weitere E-Mail-Diagnose und -Überprüfung bereitstellen. Das Archivieren von E-Mails dient als sekundäre Speicherung der E-Mails in einem Posteingang-Protokollformat in der ursprünglichen Quelle für Administratoren, um diese abzurufen und zu validieren.

- Es wird empfohlen, die Standardwerte für die Einstellungen beizubehalten, wenn Sie die Archivierung von E-Mails aktivieren möchten. Die Standardwerte sind 10 MB pro Protokoll und maximal 10 Protokolle. Die Protokolle werden basierend auf der Größe der Protokolldatei selbst hinzugefügt und weitergeleitet. Archiv-mbox-Protokolldateien werden basierend auf der Geschwindigkeit des E-Mail-Datenverkehrs gefüllt, der durch die Appliance geleitet wird. Wenn mehr Protokolle erstellt werden, werden ältere Archiv-Postfachprotokolle zur Erstellung des neuen Protokolls in freien Speicherplatz entfernt.
- Stellen Sie sicher, dass Ihr Gerät über ausreichend Speicherplatz verfügt, bevor Sie die Größe der Archiv-mbox-Protokolldateien und die maximale Anzahl der gespeicherten Protokolldateien erhöhen.
- Um zu verhindern, dass die Archiv-mbox-Protokolle generiert werden, müssen Sie die Archivfunktion pro Richtlinie deaktivieren.

Hinweis: Die Protokolle der ESA- und CES-Archivboxen können nicht von der Security Management Appliance (SMA) abgerufen werden und werden lokal pro ESA und CES gespeichert, wobei die Funktion aktiviert ist.

Wie können E-Mails auf der ESA und CES archiviert werden?

E-Mail-Archivierung ist mit Anti-Spam, Anti-Virus, Advanced Malware Protection, Graymail und Message Filtern verfügbar. Die Archivaktion kann über die grafische Benutzeroberfläche (GUI) oder Kommandozeile (CLI) für Anti-Spam, Anti-Virus, Advanced Malware Protection und Graymail konfiguriert werden.

Bei Nachrichtenfiltern kann die Archivaktion nur über die CLI konfiguriert werden.

Anti-Spam-Archiv konfigurieren

1. Navigieren Sie zu **GUI > Mail Policies > Incoming/Outgoing Mail Policies**.
2. Klicken Sie auf die Anti-Spam-Einstellungen für die jeweilige Richtlinie, um die E-Mail-Archivierung zu konfigurieren.
3. Klicken Sie auf **Erweitert** in den verfügbaren Einstellungen für Einstellungen für positiv identifizierte Spam und/oder verdächtige Spam.
4. Drücken Sie das Optionsfeld neben "Ja", um E-Mails mit dem entsprechenden Anti-Spam-Urteil zu archivieren.
5. Senden Sie die Konfiguration, und bestätigen Sie diese Änderungen, wie im Bild gezeigt.

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 ▼	<input type="text" value="[[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"/> (e.g. employee@compai
	Archive Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes

Konfigurieren des Anti-Virus-Archivs

1. Navigieren Sie zu **GUI > Mail Policies > Incoming/Outgoing Mail Policies**.
2. Klicken Sie auf die Anti-Virus-Einstellungen in der jeweiligen Richtlinie, um die E-Mail-Archivierung zu konfigurieren.
3. Klicken Sie in jedem der Scanverdicts, in dem die Originalnachricht archiviert werden soll, auf das Optionsfeld neben Yes (Ja), um die Originalnachricht zu archivieren.
4. Senden Sie die Konfiguration, und bestätigen Sie diese Änderungen, wie im Bild gezeigt.

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
	[WARNING: VIRUS REMOVED]
▶ Advanced	Optional settings for custom header and message

Advanced Malware Protection-Archiv konfigurieren

1. Navigieren Sie zu **GUI > Mail Policies > Incoming/Outgoing Mail Policies**.
2. Klicken Sie auf Advanced Malware Protection (Erweiterte Malware-Schutzeinstellungen) in der entsprechenden Richtlinie, um die E-Mail-Archivierung zu konfigurieren.
3. Um die Originalnachricht zu archivieren, aktivieren Sie in jedem der Scanverdicts, die Sie speichern möchten, das Optionsfeld neben Ja, um die Originalnachricht zu archivieren.
4. Senden Sie die Konfiguration, und bestätigen Sie diese Änderungen, wie im Bild gezeigt.

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]

Graymail-Archiv konfigurieren

1. Navigieren Sie zu **GUI > Mail Policies > Incoming/Outgoing Mail Policies**.
2. Klicken Sie auf die Graymail-Einstellungen in der jeweiligen Richtlinie, um die E-Mail-Archivierung zu konfigurieren.
3. Klicken Sie auf Erweitert, um die verfügbaren Einstellungen für Marketing, Social, Bulk anzuzeigen.
4. Drücken Sie das Optionsfeld neben Yes (Ja), um E-Mails mit dem entsprechenden Graymail-Urteil zu archivieren.
5. Senden Sie die Konfiguration, und bestätigen Sie diese Änderungen.

Action on Marketing Email					
Apply this action to Message:	<input type="text" value="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): <table border="1" style="float: right; margin-left: 10px;"> <tr> <td>Header:</td> <td><input type="text"/></td> </tr> <tr> <td>Value:</td> <td><input type="text"/></td> </tr> </table>	Header:	<input type="text"/>	Value:	<input type="text"/>
	Header:	<input type="text"/>			
	Value:	<input type="text"/>			
Send to an Alternate Envelope Recipient (optional): <table border="1" style="float: right; margin-left: 10px;"> <tr> <td>Email Address:</td> <td><input type="text"/></td> </tr> <tr> <td colspan="2"><small>(e.g. employee@)</small></td> </tr> </table>	Email Address:	<input type="text"/>	<small>(e.g. employee@)</small>		
Email Address:	<input type="text"/>				
<small>(e.g. employee@)</small>					
	Archive Message: <input checked="" type="radio"/> No <input type="radio"/> Yes <div style="text-align: center; margin-top: 5px;"> </div>				

Nachrichtenfilterarchiv konfigurieren

Hinweis: Zum Anzeigen archivierter Protokolle ist ein Nachrichtenfilter mit Archivaktion erforderlich. Nachrichtenfilter können nur innerhalb der CLI erstellt werden.

Probenfilter:

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

1. Melden Sie sich am Gerät in der CLI an.
2. Erstellen Sie einen Nachrichtenfilter, wie im bereitgestellten Beispielfilter beschrieben.
3. Senden Sie diesen Filter, und bestätigen Sie Ihre Änderungen.

Validieren der Verfügbarkeit von Archive Mbox-Protokollen

Wenn die Konfiguration für das Archiv für die entsprechenden Dienste reserviert ist, werden die archivierten E-Mails in einer Protokolldatei im mbox-Format gespeichert. Um zu überprüfen, ob die Archivprotokolle zum Abruf verfügbar sind, navigieren Sie zu **GUI > System Administration > Log Subscriptions**.

Sicherheitsdienstarchive erstellen ein separates Protokoll mit einem Archivprotokolltyp, wie im Bild gezeigt:

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

Für Nachrichtenfilter wird die Archivkonfiguration **nur** über die CLI angezeigt:

- filter > 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
```

Abrufen der Mbox-Protokolle

Bei eigenständigen Appliances können diese mbox-Protokolle direkt von der GUI abgerufen werden. Navigieren Sie zu **GUI > System Administration > Log Subscriptions**, und klicken Sie auf die **Protokolldateien** für das entsprechende Archivprotokoll, das Sie abrufen möchten.

Bei geclusterten Appliances können die mbox-Protokolle mit FTP/Secure Copy (SCP) abgerufen werden, wie in [diesem Artikel](#) beschrieben.

(<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00>.)

Zugehörige Informationen

- [Cisco Email Security Appliance - Benutzerhandbücher](#)
- [Was ist das UNIX-mbox-Format \(Mailbox\)?](#)
- [Wo werden Protokolle auf der Cisco E-Mail Security Appliance \(ESA\) gespeichert, und wie kann ich darauf zugreifen?](#)
- [Extrahieren einer E-Mail aus Archiv-Postfachprotokollen](#)

- [Technischer Support und Dokumentation - Cisco Systems](#)