

Hoe u e-mails kunt archiveren op de e-mail security applicatie en cloude-mail security

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Hoe archiveer je e-mails op de ESA en CES?](#)

[Archief van anti-Spam configureren](#)

[Archief tegen virussen configureren](#)

[Geavanceerd Malware Protection-archiefbestand configureren](#)

[Graymail-archiefbestand configureren](#)

[Archief van berichtfilter configureren](#)

[Beschikbaarheid archiefvak wissen](#)

[Logs van box ophalen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document worden de stappen beschreven die moeten worden gevolgd om e-mails te archiveren over de e-mail security applicatie (ESA) en Cloud Email Security (CES) voor ophalen en bekijken.

Achtergrondinformatie

Wanneer u e-mails over de ESA en de CES archiveert, kan deze worden gebruikt om aan de vereisten van de regelgeving te voldoen of om een extra gegevensmiddel te bieden voor de verdere diagnose en beoordeling van de post. Het archiveren van e-mails werkt als een secundaire opslag van de e-mails in een logformaat van het vakje in de oorspronkelijke bron van het bestand voor beheerders om deze op te halen en te valideren.

- Als u wilt dat e-mails kunnen worden gearhiveerd, wordt u aangeraden om de standaardinstellingen te handhaven. De standaardwaarden zijn 10 MB per log en maximaal 10 logs behouden. De logbestanden worden toegevoegd en overgedragen op basis van de grootte van het logbestand zelf. Logbestanden van het archiefvak worden ingevuld op basis van het aantal e-mailberichten dat door het apparaat wordt doorgegeven. Aangezien er meer logbestanden worden gemaakt, worden de oudere logbestanden van het archief naar vrije ruimte verwijderd om het nieuwe logbestand te maken.
- Zorg ervoor dat uw apparaat voldoende schijfruimte heeft voordat u de logbestandsgrootte van het archiefvak verhoogt en de maximale logbestanden die behouden blijven.
- Om te voorkomen dat de logbestanden van het archief worden gegenereerd, moet u de archieffunctie per beleid uitschakelen.

Opmerking: De logbestanden van het ESR- en CES-archief kunnen niet worden opgeroepen door de Security Management-applicatie (SMA) en worden lokaal opgeslagen per ESA en

CES met de functie ingeschakeld.

Hoe archiveer je e-mails op de ESA en CES?

E-mailarchivering is beschikbaar met anti-spam, anti-virus, Advanced Malware Protection, Graymail en Berichtfilters. De archiefactie kan worden geconfigureerd via de grafische gebruikersinterface (GUI) of opdrachtregel interface (CLI) voor anti-spam, anti-virus, Advanced Malware Protection en Graymail.

Voor berichtfilters kan de archiefactie worden ingesteld met alleen de CLI.


Archief van anti-Spam configureren

1. Navigeer naar de **GUI > Mail-beleidslijnen > inkomend/uitgaand postbeleid**.
2. Klik op de anti-spaminstellingen voor het desbetreffende beleid om e-mailarchivering te configureren.
3. Klik op **Advanced** in de beschikbare instellingen voor positief geïdentificeerde spam-instellingen en/of verdachte spam-instellingen.
4. Druk op de radioknop naast Ja om e-mails te archiveren met de respectieve anti-spam uitspraak.
5. Stel de configuratie in en geef deze wijzigingen aan zoals in de afbeelding.

| 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@compa</i> |
| | Archive Message: <input checked="" type="radio"/> No <input type="radio"/> Yes |

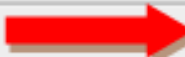
Archief tegen virussen configureren

1. Navigeer naar de **GUI > Mail-beleidslijnen > inkomend/uitgaand postbeleid**.
2. Klik in het betreffende beleid op de anti-virusinstellingen om e-mailarchivering te configureren.
3. Druk op de radioknop naast Ja om het oorspronkelijke bericht te archiveren op elk van de scanvonnissen die u wilt archiveren.
4. Stel de configuratie in en geef deze wijzigingen aan zoals in de afbeelding.

| 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 |

Geavanceerd Malware Protection-archiefbestand configureren

1. Navigeer naar de **GUI > Mail-beleidslijnen > inkomend/uitgaand postbeleid**.
2. Klik in het betreffende beleid op de instellingen voor geavanceerde Malware Protection om het e-mailarchiveren te configureren.
3. Druk op elk van de scanuitspraken die u wilt doen om het oorspronkelijke bericht te archiveren, naast Ja, op de radioknop om het te archiveren.
4. Stel de configuratie in en geef deze wijzigingen aan zoals in de afbeelding.

| 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-archiefbestand configureren

1. Navigeer naar de **GUI > Mail-beleidslijnen > inkomend/uitgaand postbeleid**.
2. Klik op de instellingen voor Graymail in het betreffende beleid om het e-mailarchiveren te configureren.
3. Klik op Advanced om de beschikbare instellingen voor marketing, sociaal, bulk te selecteren.
4. Druk op de radioknop naast Ja om e-mails te archiveren met de betreffende Graymail-uitspraak.
5. Zet de configuratie voor en schrijf deze veranderingen aan.

| Action on Marketing Email | |
|-------------------------------|--|
| Apply this action to Message: | Deliver <input type="button" value="v"/> 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 |

Archief van berichtfilter configureren

Opmerking: Er is een berichtfilter met archiefactie vereist om de gearchiveerde bestanden te kunnen bekijken. Berichtfilters kunnen alleen binnen de CLI worden gemaakt.

Monsterfilter:

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

1. Meld u aan bij het apparaat op de CLI.
2. Maak een berichtfilter zoals in het meegeleverde voorbeeldfilter.
3. Plaats dit filter in en wijk aan de wijzigingen.

Beschikbaarheid archiefvak wissen

Wanneer de configuratie voor het archief is vastgelegd voor de respectieve services, worden de gearchiveerde e-mails opgeslagen in een logbestand met veldindeling. Om te controleren of de archiefbestanden beschikbaar zijn voor het ophalen, navigeer dan naar de **GUI > Systembeheer > Log abonnementen**.

In de beveiligingsservices wordt een afzonderlijk logbestand gemaakt met een archieflogtype zoals in de afbeelding wordt getoond:

| 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 |

Voor berichtfilters wordt de archiefconfiguratie **alleen** vanuit CLI bekeken:

- filters > logbestand

```
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
```

Logs van box ophalen

Voor zelfstandige apparaten kunnen deze kistblogs rechtstreeks worden opgevraagd bij GUI. Navigeer naar **de GUI > Systeembeheer > Log abonnementen** en klik op in de **logbestanden** voor het betreffende archieflogbestand dat u wilt ophalen.

Voor geclusterde apparatuur kunnen de logboeken van de box worden opgehaald met het gebruik van FTP/Secure Copy (SCP), zoals beschreven in [dit artikel](#).
(leaving <https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00...>)

Gerelateerde informatie

- [Cisco e-mail security applicatie - eindgebruikershandleidingen](#)
- [Wat is UNIX mbox \(postvak\) formaat?](#)
- [Waar worden blogs opgeslagen op Cisco Email Security Appliance \(ESA\) en hoe kan ik ze benaderen](#)
- [Hoe een e-mail uit de logbestanden van het archiefvak wordt geëxtraheerd](#)

- [Technische ondersteuning en documentatie – Cisco Systems](#)