

# Hoe log ik berichtkoppen?

## Inhoud

[Inleiding](#)

[Hoe log ik berichtkoppen?](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft hoe u berichten kunt opnemen die via Cisco e-mail security applicatie (ESA) zijn verwerkt.

## Hoe log ik berichtkoppen?

In bepaalde gevallen is het handig om de aanwezigheid en de inhoud van de kopregels van het bericht op te nemen terwijl deze door het apparaat gaan. U specificeert de headers om te registreren via **logbestand > logheaders**. ESA zal de gespecificeerde berichtkopregels in de Logs van de Tekst van de Strijkmachine Strijkdroog, de Logs van de Levering van de IJzerenPort en de Stemmen van de Startprijs registreren. Als de header aanwezig is, registreert het systeem de naam van de header en de waarde. De headerinformatie wordt geregistreerd na de bezorgingsinformatie.

Hieronder staat een voorbeeld van hoe u loggen kunt toestaan om een bericht met de kopregels X-IPAS-Resultaat en X-IronPort-AV op te nemen:

```
my_esa.local> logconfig
```

```
Currently configured logs:
```

```
Log Name Log Type Retrieval Interval
```

```
-----  
1. amp AMP Engine Logs Manual Download None  
2. amparchive AMP Archive Manual Download None  
3. antispam Anti-Spam Logs Manual Download None  
4. antivirus Anti-Virus Logs Manual Download None  
5. asarchive Anti-Spam Archive Manual Download None  
6. authentication Authentication Logs Manual Download None  
7. aarchive Anti-Virus Archive Manual Download None  
8. bounces Bounce Logs Manual Download None  
9. cli_logs CLI Audit Logs Manual Download None  
10. encryption Encryption Logs Manual Download None  
11. error_logs IronPort Text Mail Logs Manual Download None  
12. euq_logs Spam Quarantine Logs Manual Download None  
13. euqgui_logs Spam Quarantine GUI Logs Manual Download None  
14. ftpd_logs FTP Server Logs Manual Download None  
15. gui_logs HTTP Logs Manual Download None  
16. mail_logs IronPort Text Mail Logs Manual Download None
```

17. mail\_logs\_copy IronPort Text Mail Logs SCP Push - Host  
192.168.0.200: Port 22None
18. repeng Reputation Engine Logs Manual Download None
19. reportd\_logs Reporting Logs Manual Download None
20. reportqueryd\_logs Reporting Query Logs Manual Download None
21. scanning Scanning Logs Manual Download None
22. slbld\_logs Safe/Block Lists Logs Manual Download None
23. snmp\_logs SNMP Logs Manual Download None
24. sntpd\_logs NTP logs Manual Download None
25. status Status Logs Manual Download None
26. system\_logs System Logs Manual Download None
27. trackerd\_logs Tracking Logs Manual Download None
28. updater\_logs Updater Logs Manual Download None
29. upgrade\_logs Upgrade Logs Manual Download None

Choose the operation you want to perform:

- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.

[> **logheaders**

Please enter the list of headers you wish to record in the log files.

Separate multiple headers with commas.

[> **X-IPAS-Result, X-IronPort-AV**

Ga terug naar de hoofdprompt van CLI en voer alle wijzigingen in.

Wanneer u de mail\_logs bekijkt, ziet u het resultaat van de kopregels die nu in de logbestanden zijn geïnjecteerd zoals ingesteld:

```
Thu Aug 14 08:40:18 2014 Info: New SMTP ICID 10282 interface Management
(192.168.0.199) address 192.168.0.200 reverse dns host ns.domain.com verified no
Thu Aug 14 08:40:18 2014 Info: ICID 10282 RELAY SG RELAY_SG match 192.168.0.200
SBRS not enabled
Thu Aug 14 08:40:18 2014 Info: Start MID 1403 ICID 10282
Thu Aug 14 08:40:18 2014 Info: MID 1403 ICID 10282 From: <orig_user@domain.com>
Thu Aug 14 08:40:18 2014 Info: MID 1403 ICID 10282 RID 0 To: <end_user@example.com>
Thu Aug 14 08:40:18 2014 Info: MID 1403 using engine: SPF Verdict Cache using
cached verdict
Thu Aug 14 08:40:18 2014 Info: SPF Verdict Cache cache status: hits = 7, misses = 12,
expires = 0, adds = 12, seconds saved = 0.06, total seconds = 0.56
Thu Aug 14 08:40:18 2014 Info: MID 1403 SPF: helo identity postmaster@domain.com None
Thu Aug 14 08:40:18 2014 Info: MID 1403 using engine: SPF Verdict Cache using
cached verdict
Thu Aug 14 08:40:18 2014 Info: MID 1403 SPF: mailfrom identity orig_user@domain.com
Pass (v=spf1)
Thu Aug 14 08:40:18 2014 Info: MID 1403 using engine: SPF Verdict Cache using
cached verdict
Thu Aug 14 08:40:18 2014 Info: MID 1403 SPF: pra identity orig_user@domain.com None
headers from
Thu Aug 14 08:40:18 2014 Info: MID 1403 Message-ID '<20140814124103.GC6764@domain.com>'
Thu Aug 14 08:40:18 2014 Info: MID 1403 Subject 'Hello - this is the morning report...'
Thu Aug 14 08:40:18 2014 Info: MID 1403 ready 611 bytes from <orig_user@domain.com>
Thu Aug 14 08:40:18 2014 Info: MID 1403 matched all recipients for per-recipient policy
DEFAULT in the outbound table
Thu Aug 14 08:40:18 2014 Info: ICID 10282 close
```

```
Thu Aug 14 08:40:20 2014 Info: MID 1403 interim verdict using engine: CASE spam negative
Thu Aug 14 08:40:20 2014 Info: MID 1403 using engine: CASE spam negative
Thu Aug 14 08:40:20 2014 Info: MID 1403 interim AV verdict using Sophos CLEAN
Thu Aug 14 08:40:20 2014 Info: MID 1403 antivirus negative
Thu Aug 14 08:40:20 2014 Info: MID 1403 Outbreak Filters: verdict negative
Thu Aug 14 08:40:20 2014 Info: MID 1403 DLP no violation
Thu Aug 14 08:40:20 2014 Info: MID 1403 queued for delivery
Thu Aug 14 08:40:20 2014 Info: New SMTP DCID 173 interface 192.168.0.199 address
111.22.111.22 port 25
Thu Aug 14 08:40:20 2014 Info: DCID 173 STARTTLS command not supported
Thu Aug 14 08:40:20 2014 Info: Delivery start DCID 173 MID 1403 to RID [0]
Thu Aug 14 08:40:20 2014 Info: Message done DCID 173 MID 1403 to RID [0]
[('X-IPAS-Result', 'AmYGAMSt7FPAqADI/2dsb2JhbABahBuNU6VQAZpbiQV3hCMhYxg0BRi
JC8VuF4wKg1+DGYEDAQSPCoMniiEBmHaDHwEBAQ'), ('X-IronPort-AV', 'E=Sophos;i=
"5.01,863,1400040000"; \r\n d="scan\'208";a="1403"')]
Thu Aug 14 08:40:20 2014 Info: MID 1403 RID [0] Response '2.0.0 OK
F6/FE-18769-93EACE35'
Thu Aug 14 08:40:20 2014 Info: Message finished MID 1403 done
Thu Aug 14 08:40:25 2014 Info: DCID 173 close
```

Als u de kopregels in die e-mail rechtstreeks wilt bekijken, dan ziet u in de ontvangen e-mail de gemarkeerde X-IPAS-Resultaat en X-IronPort-AV-headers in de oorspronkelijke headers voordat de eerste ontvangen hop:

```
X-IronPort-Anti-Spam-Filtered: true
X-IPAS-Result: AmYGAMSt7FPAqADI/2dsb2JhbABahBuNU6VQAZpbiQV3hCMhYxg0BRiJC8VuF4wKg1+
DGYEDAQSPCoMniiEBmHaDHwEBAQ
X-IronPort-AV: E=Sophos;i="5.01,863,1400040000";
d="scan\'208";a="1403"
Received: from ns.domain.com (HELO mail.domain.com) ([192.168.0.200]) by
myesa_local.domain.com with ESMTP; 14 Aug 2014 08:40:18 -0400
Received: by mail.domain.com (Postfix, from userid 1000)id 29F4E8033E; Thu,
14 Aug 2014 08:41:03 -0400 (EDT)
Date: Thu, 14 Aug 2014 08:41:03 -0400
From: robert <orig_user@domain.com.com>
To: <end_user@example.com>
Subject: Hello - this is the morning report...
Message-ID: <20140814124103.GC6764@domain.com>
MIME-Version: 1.0
User-Agent: Mutt/1.5.21 (2010-09-15)
X-RR-Connecting-IP: 111.22.111.222:25
X-Cloudmark-Score: 0
Return-Path: orig_user@domain.com.com
X-MS-Exchange-Organization-AuthSource: xhc-aln-x10.example.com
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 10
Content-type: text/plain;
charset="US-ASCII"
Content-transfer-encoding: 7bit
```

No info this morning.

-Joe

**Opmerking:** de RFC voor het TCP-protocol bevindt zich op <http://www.faqs.org/rfcs/rfc2821.html> en definieert gebruikersgedefinieerde headers.

## Gerelateerde informatie

- [Cisco e-mail security applicatie - eindgebruikershandleidingen](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)