

¿Cómo hacen las encabezados de mensaje del registro I?

Contenido

[Introducción](#)

[¿Cómo hacen las encabezados de mensaje del registro I?](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo registrar las encabezados de mensajes procesadas a través del dispositivo de seguridad del correo electrónico de Cisco (ESA).

¿Cómo hacen las encabezados de mensaje del registro I?

En algunos casos, es útil registrar la presencia y el contenido de las encabezados de un mensaje pues pasan a través del dispositivo. Usted especifica las encabezados para registrar vía el **logconfig > los logheaders**. El ESA registrará los encabezados del mensaje especificados en los registros del correo de texto de IronPort, los registros de la salida de IronPort, y los registros de la despedida de IronPort. Si la encabezado está presente, el sistema registra el nombre de la encabezado y del valor. La información de encabezado recored después de la información de entrega.

Abajo está un ejemplo de cómo permitir al registro para registrar cualquier mensaje con el X-IPA-resultado de las encabezados y el X-IronPort-AV:

```
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. avarchive 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**

Vuelva al prompt principal CLI, y **confie** ningunos/todos los cambios.

Quando usted revisa los mail_logs, usted verá el resultado de las encabezados ahora inyectadas en los registros según lo configurado:

```
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
```

Del correo electrónico recibido, si usted mirara las encabezados en ese correo electrónico directamente, usted verá el X-IPA-resultado y las encabezados resaltados X-IronPort-AV en los encabezados originales antes del primer salto recibido:

```
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 ESMTTP; 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

Note: El RFC para el protocolo S TP está situado en <http://www.faqs.org/rfcs/rfc2821.html> y define las encabezados definidas por el usuario.

Información Relacionada

- [Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)