

メッセージ ヘッダーをログに記録するにはどうすればよいですか

目次

[はじめに](#)

[メッセージ ヘッダーをログに記録するにはどうすればよいですか](#)

[関連情報](#)

概要

このドキュメントでは、Cisco E メール セキュリティ アプライアンス (ESA) で処理されるメッセージ ヘッダーの記録方法を説明します。

メッセージ ヘッダーをログに記録するにはどうすればよいですか

場合によっては、メッセージがアプライアンスを通過するときに、メッセージのヘッダーの存在と内容を記録すると便利です。記録するヘッダーは、[logconfig] > [logheaders] で指定します。ESA は、指定されたメッセージ ヘッダーを IronPort テキスト メール ログ、IronPort 配信ログ、および IronPort バウンス ログに記録します。ヘッダーが存在する場合、システムはヘッダーの名前と値を記録します。ヘッダー情報は、配信情報の後に記録されます。

ロギングをイネーブルにし、ヘッダー X-IPAS-Result および X-IronPort-AV を含むすべてのメッセージを記録する方法を次の例に示します。

```
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**

メイン CLI プロンプトに戻り、すべての変更をコミットします。

mail\_logs を確認すると、設定されているとおりにヘッダーの結果がログに挿入されていることがわかります。

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. sblbd\_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**

受信メールでそのヘッダーを直接確認すると、最初の受信ホップよりも前の元のヘッダーで、次で強調表示されている X-IPAS-Result ヘッダーと X-IronPort-AV ヘッダーを確認できます。

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. sblbd\_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**

注: SMTP プロトコルに関する RFC は、<http://www.faqs.org/rfcs/rfc2821.html> にあります。  
この RFC には、ユーザ定義のヘッダーが規定されています。

## 関連情報

- [Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)