

ESA ي ف CEF س ووو CEF ل ج س ل ا خ د ا ن ي و ك ت

ت ا ي و ت ح م ل ا

[ق م د ق م ل ا](#)

[ق ي س ا س ا ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[ق م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ق ي س ا س ا ت ا م و ل ع م](#)

[ن ي و ك ت ل ا](#)

[C E F ل ج س ل ا خ د ا](#)

[ر د ا ص ل ا / د ر ا و ل ا ي و ت ح م ل ا ق ي ف ص ت ل م ا ع ق ف ا ض ا](#)

[ع م ج م ل ا ث ا د ح ا ل ا ل ج س ي ف ك ا ر ت ش ا ل ا ي ف C E F ل ج س ل ا خ د ا ق ف ا ض ا](#)

[C E F ن ي و ا ن ع](#)

[ل ج س ل ا ي ل ا C E F س و و ر ق ف ا ض ا](#)

[ع م ج م ل ا ث ا د ح ا ل ا ل ج س ي ف ك ا ر ت ش ا ل ا ي ف C E F ل ج س ل ا خ د ا ق ف ا ض ا](#)

[ق ل ص ت ا ذ ت ا م و ل ع م](#)

ق م د ق م ل ا

د ي ر ب ل ا ق ر ا ب ع س و و ر و (C E F) ك ر ت ش م ل ا ث د ح ل ا ق ي س ن ت ل ج س ل ا خ د ا ن ي و ك ت د ن ت س م ل ا ا ذ ه ق ص ي
Cisco ن م (S E G) ق ن م ا ل ا ي ن و ر ت ك ل ل ا ل ا

ق ي س ا س ا ل ا ت ا ب ل ط ت م ل ا

ت ا ب ل ط ت م ل ا

ق ي ل ل ا ت ل ا ت ا ع و و م ل ا ق ف ر ع م ب Cisco ي ص و ت

- (S E G / E S A) ي ن و ر ت ك ل ل ا ل ا د ي ر ب ل ا ن ا م ا ز ا ه ج / Cisco ن م ق ن م ا ل ا ي ن و ر ت ك ل ل ا ل ا د ي ر ب ل ا ق ر ا ب ع
- ي و ت ح م ل ا ق ي ف ص ت ل م ا و ع ق ف ر ع م
- ك ا ر ت ش ا ل ا ق ف ر ع م ل ي ج س ت

ق م د خ ت س م ل ا ت ا ن و ك م ل ا

ق ي ل ل ا ت ل ا ق ي د ا م ل ا ت ا ن و ك م ل ا و ج م ا ر ب ل ا ت ا ر ا د ص ا ي ل ا د ن ت س م ل ا ا ذ ه ي ف ق ر ا و ل ا ت ا م و ل ع م ل ا د ن ت س ت

- 14.3 ر ا د ص ا ل ا ، Email Security Appliance ز ا ه ج
- ق ص ا خ ق ي ل م ع م ق ي ي ف ق د و ج و م ل ا ق ز ه ج ا ل ا ن م د ن ت س م ل ا ا ذ ه ي ف ق ر ا و ل ا ت ا م و ل ع م ل ا ا ش ن ا م ت
ت ن ا ك ا ذ ا . (ي ض ا ر ت ف ا) ح و س م م ن ي و ك ت ب د ن ت س م ل ا ا ذ ه ي ف ق م د خ ت س م ل ا ق ز ه ج ا ل ا ع ي م ج ت ا د ب
ر م ا ي ا ل ل م ت ح م ل ا ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ل ي غ ش ت ل ا د ي ق ك ت ك ب ش

ق ي س ا س ا ت ا م و ل ع م

اذه لجسلا عون مدختسا. دحاو لجس رطس يف ةلاسر شح لك "ةجمدملا ثادحالا تالجس" زجوت نامألا تامولعم" دروم ىلا ةلسررملا (لجسلا تامولعم) تانايبلل تيابلل تادحو ددع ليلقتل CEF لجس لئاسر قيسنتب تالجسلا دجوت. ليلحتلل قيبطتلا و (SIEM) "ثادحالا ةرادو SIEM. يدروم مظعم لبق نم عساو لكشب همادختسا متي يذلا

ديربلا ثادحاً بقعتل ةيفاضا تامولعم ريفوتل CEF س وؤرو CEF لجس لاخدا ةفاضلا متت اهميظنتو.

نيوكتلا

CEP لجس لاخدا

رداصل/دراولا يوتحمل ةيفصت لماع ةفاضلا

ESA: ىلع يوتحمل احشرم عاشناب مق، الوأ

1. Mail Policies > Incoming/Outgoing content filters للاقنالا
2. Add Filter يف رقنا
3. ةيفصتلا لماع ةيمست
4. بوغرم طرش ةفاضلا
5. Add Action يف رقنا
6. Add CEF Log Entry ديدحت
7. ةميقلا عبرم Action Variables اهمادختساو ةيمستلا ةيمستب مق
8. Submit and Commit

ةروصللا يف حضورم وه امك، عارجالا ريغتم \$MatchedContent همادختسن يذلا اذه قيثوتلا لاثم:

لجس لاخدا عارجا

يوتحمل ةيفصت لماع يف CEF

عمحمل ثادحالا لجس يف كارتشالا يف CEF لجس لاخدا ةفاضلا

CEP لجس لاخدا ةفاضلا دحوملا ثادحالا لجس يف كارتشالا ليدعت و عاشناب مق، كلذ دعب

اقبس م هؤاشن ا مت ي ذلا:

1. System Administration > Log Subscriptions ل ل ا ق ت ن ا ل ا
2. اه د ي د ح ت و ا ة د ح و م ث ا د ح ا ت ا ل ج س ة ف ا ض ا
3. Add ق و ف ر ق ن ا و Custom Log Entries د ي د ح ت
4. Submit and Commit

Log Subscription

Log Type: Consolidated Event Logs

Log Name: CEF_test
(will be used to name the log directory)

Log Fields:

Available Log Fields:

- AV Verdict
- Content Filters Verdict
- Custom Log Headers
- DANE Host
- DANE Status
- DCID Timestamp
- DMA IP
- DKIM Verdict
- DLP Verdict
- DMARC Verdict
- Data IP
- File(s) Details
- Friendly From
- Graymail Verdict
- SCID Timestamp
- Listener Name
- Mail Direction

Selected Log Fields:

- Serial Number
- MID
- SCID
- DCID
- Custom Log Entries

Buttons: Add, Remove, Move Up, Move Down

لجس ل ا ت ا ل ا خ د ا

لجس ل ا ت ا ل ا خ د ا ي ف ة ص ص خ م ل ا

CEP ن ي و ا ن ع

لجس ل ا ي ل ل CEP س و و ر ة ف ا ض ا

ESA ي ف CEP س و و ر ة ف ا ض ا ب ا ل و ا م ق

1. System Administration > Logs Subscription ل ل ا ق ت ن ا ل ا
2. ة ي م و م ع ل ا ت ا د ا د ع ا ل ا ن م ض Edit Settings ي ف ر ق ن ا
3. اه ل ي ج س ت م ت ي س ي ت ل ا س و و ر ل ا د ر س ب م ق ، CEP س و و ر ت ح ت
4. Submit and Commit

Log Subscriptions Global Settings

Mode -- Cluster: Hosted_Cluster

Change Mode...

Centralized Management Options

Edit Global Settings

System metrics frequency: 60 seconds

Logging Options:

- Message-ID headers in Mail Logs
- Original subject header of each message
- Remote response text in Mail Logs

Headers (Optional): List any headers you want to record in the log files:

- X-IronPort-Anti-Spam-Result, To, From, Reply-To, Sender, X-IronPort-Anti-Spam-Result

CEF Headers (Optional): List any headers you want to record in the CEF log files:

- Message-ID, Mime-version, Content-type, Content-disposition, Content-transfer-encoding, Thread-Topic, Thread-Index, X-IronPort-Anti-Spam-Result, To, From, Reply-To, Sender

Buttons: Cancel, Submit

CEP س و و ر ن ي و ك ت

ع م ج م ل ا ث ا د ح ا ل ا ل ج س ي ف ك ا ر ت ش ا ل ا ي ف CEP ل ج س ل ا خ د ا ة ف ا ض ا

CEF سوؤر ةفاضل جمدملا ثادحالا لجس يف كارتشالا ليدعت وء عاشناب مق ،كلذ دعب اقبس م ةلجس مالا

1. للاقنالا System Administration > Logs Subscription
2. اهديدجت وء ةدوم ثادحالا لجس ةفاضلا
3. قوف رقناو Custom Log Entries ديدجت
4. Submit and Commit

Log Subscription

Log Type: Consolidated Event Logs

Log Name: cef_test
(will be used to name the log directory)

Log Fields:

Available Log Fields:

- AMP Verdict
- AS Verdict
- AV Verdict
- Content Filters Verdict
- DANE Host
- DANE Status
- DCID Timestamp
- DHA IP
- DKIM Verdict
- DLP Verdict
- DMARC Verdict
- Data IP
- File(s) Details
- Friendly From
- Graymail Verdict
- ICID Timestamp

Selected Log Fields:

- Serial Number
- MD
- ICID
- DCID
- Custom Log Entries
- Custom Log Headers

Buttons: Add, Remove, Move Up, Move Down

CEF لجس كارتشا

يف CEF لجس سوؤر

ةلص تاذ تامولعم

- [ESA 14.3 يئاهنلا مدختسملا ليلد](#)
- [14.3 رادصالا ، ESA رادصالا تاطحالم](#)
- [Cisco Systems - ينفالام عدلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة م ادخت ساب دن تسمل اذة Cisco ت مچرت
ملاعلاء انء مچ م ف ن م دخت سمل م عد ى وت م م يدقت ل ة يرش ب ل و
امك ة قيق د نوك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م ى چر ى . ة صا ل م هت ب
Cisco ي لخت . فرت م مچرت م ا م دقي ي ت ل ة ي فارت حال ة مچرت ل م لاعل و
ى ل أمئ اد عوچر ل اب ي ص و ت و ت امچرت ل هذه ة ق د ن ع اهت ي ل وئ س م
Systems (رفو تم ط بارل ا) ي ل ص أل ا ي زي ل چ ن إل ا دن تسمل ا