

# Advanced Flow Collector Engine 사용자 지정 보안 이벤트 발생 동작 구성

## 목차

---

[소개](#)

[배경](#)

[기본 플로우 컬렉터 동작](#)

[cse\\_exec\\_interval\\_secs 고급 설정](#)

[성능에 미치는 영향](#)

[classify\\_flows 스레드의 기간 측정](#)

[성능 기간 동안의 엔진 상태](#)

[SFI - 정적 흐름 색인](#)

[구성](#)

[변경 확인](#)

[축하합니다!](#)

---

## 소개

이 문서에서는 SNA Flow Collector에서 CSE(Custom Security Events)를 실행하는 방법을 변경할 수 있는 두 가지 플로우 컬렉터 고급 설정에 대해 설명합니다.

## 배경

레거시 early\_check\_age 플로우 컬렉터 고급 설정과 새로운 cse\_exec\_interval\_secs 플로우 컬렉터 고급 설정은 플로우 컬렉터 엔진이 사용자 정의 보안 이벤트를 실행하는 방식을 결정합니다. Flow Collector는 SNA 시스템 아키텍처의 첫 번째 어플라이언스로, 네트워크의 흐름을 확인하므로, Flow Collector 엔진은 Flow Cache에 있는 동안 흐름의 특성을 모니터링하고, 흐름이 지정된 Custom Security Event의 구성된 기준을 충족하는지 확인합니다. 그러나 이러한 플로우 컬렉터 고급 설정은 기본 제공 코어 보안 이벤트의 발생 특성을 변경하지 않습니다.

## 기본 플로우 컬렉터 동작

기본적으로 flow collector early\_check\_age advanced 설정은 160초로 구성됩니다. 즉, flow collector engine은 플로우가 구성된 Custom Security Event와 일치하는지 확인하기 전에 플로우에 대해 최소 160초 동안 대기합니다. 기본적으로 이 확인은 흐름이 끝날 때까지 다시 수행되지 않습니다.

이 160초 조기 확인 값은 모범 사례를 사용하는 경우 60초마다 텔레메트리를 전송하도록 텔레메트리 내보내기를 구성해야 하기 때문에 특별히 선택되었습니다. 이 기본값을 사용하면 일반적인 환경에서 흐름 컬렉터가 특정 대화/흐름의 양쪽에 관련된 흐름 정보를 충분히 볼 수 있습니다. 따라서 early\_check\_age는 고급 설정 목록에 미리 정의되어 있지 않습니다. 이는 설계에 따른 것이며, 지

원/엔지니어링과 먼저 협의하지 않고 이 값을 변경해서는 안 됩니다. 그러나 이 초기 설계는 바이트 또는 패킷 수의 축적을 포함하는 사용자 지정 보안 이벤트 컨피그레이션과 결합된 다소 조용한 흐름 특성을 고려할 때 효과적이지 않습니다. 이는 `cse_exec_interval_secs` 고급 설정 매개변수를 생성하기 위한 이유입니다.

## cse\_exec\_interval\_secs 고급 설정

7.4.2에서 사용할 수 있도록 `cse_exec_interval_secs` 흐름 컬렉터 고급 설정을 추가하면 이제 구성된 사용자 지정 보안 이벤트에 대해 흐름 캐시의 흐름을 주기적으로 검사하도록 엔진에 지시할 수 있습니다. 이 고급 설정은 지정된 플로우가 기본 160초 `early_check_age`의 CSE 기준에 부합하지 않지만 플로우의 나중에 해당 임계값을 초과하는 긴 플로우의 경우 특히 유용합니다. 이 고급 설정이 없으면 흐름이 끝날 때까지 사용자 지정 보안 이벤트가 실행되지 않으며, 경우에 따라 며칠 후가 될 수도 있습니다.

## 성능에 미치는 영향

이 간격 CSE 기준을 실행하면 기본값이 정의하는 것보다 더 많은 CPU가 필요한 플로우가 플로우 수명 동안 더 많이 확인됩니다. 이 지침은 `cse_exec_interval_secs` 매개변수를 활성화하기 전에 플로우 수집기 엔진의 `sw.log` 파일 내용을 조사하는 과정을 안내합니다. 이 고급 설정을 활성화하는 것을 고려하고 있고 TAC에서 이 변경에 대비하여 플로우 컬렉터 상태를 확인하는 데 도움이 되도록 하려면 지원 케이스를 열고 플로우 컬렉터 진단 팩을 SR에 연결하면 됩니다.

## classify\_flows 스레드의 기간 측정

한 가지 빠른 성능 영향 측정을 수행하면 오늘부터 `sw.log`를 조사하고 설정이 활성화되기 전에 "cf-" 로그 항목 다음에 나열된 숫자를 설정이 적용된 후의 숫자와 비교합니다.

```
/lancope/var/sw/today/logs/grep "cf-" sw.log
```

```
20:43:21 l-flo-f0: classify_flows: flows n-1744317 ns-178613 ne-188095 nq-0 nd-0 nx-0 to-300 cf-21 ft-126473/792802/940383/14216
```

```
20:44:20 l-flo-f4: classify_flows: flows n-1754296 ns-191100 ne-167913 nq-0 nd-0 nx-0 to-300 cf-20 ft-122830/783378/949392/14928
```

```
20:44:21 l-flo-f2: classify_flows: flows n-1773175 ns-191930 ne-169039 nq-0 nd-0 nx-0 to-300 cf-20 ft-123055/788507/962264/15431
```

```
20:44:21 l-flo-f3: classify_flows: flows n-1750066 ns-189197 ne-165940 nq-0 nd-0 nx-0 to-300 cf-20 ft-122563/779792/944192/15154
```

```
20:44:21 l-flo-f5: classify_flows: flows n-1753899 ns-190477 ne-168004 nq-0 nd-0 nx-0 to-300 cf-20 ft-122261/783375/946651/15423
```

```
20:44:21 l-flo-f1: classify_flows: flows n-1763952 ns-191342 ne-169518 nq-0 nd-0 nx-0 to-300 cf-20 ft-122782/786822/955997/15175
```

20:44:21 l-flo-f7: classify\_flows: flows n-1757535 ns-188154 ne-166221 nq-0 nd-0 nx-0 to-300 cf-20 ft-122808/781388/951528/14363

20:44:21 l-flo-f6: classify\_flows: flows n-1764211 ns-190964 ne-169013 nq-0 nd-0 nx-0 to-300 cf-21 ft-122713/784446/954149/16320

20:44:21 l-flo-f0: classify\_flows: flows n-1764197 ns-189780 ne-168784 nq-0 nd-0 nx-0 to-300 cf-21 ft-123290/787327/952186/14352

20:45:22 l-flo-f4: classify\_flows: flows n-1780277 ns-177512 ne-149843 nq-0 nd-0 nx-0 to-300 cf-21 ft-129553/766777/964933/14864

20:45:22 l-flo-f2: classify\_flows: flows n-1789285 ns-175763 ne-155809 nq-0 nd-0 nx-0 to-300 cf-21 ft-129685/772482/976850/15289

20:45:22 l-flo-f3: classify\_flows: flows n-1774883 ns-177085 ne-149715 nq-0 nd-0 nx-0 to-300 cf-22 ft-129067/764272/962000/15090

20:45:22 l-flo-f5: classify\_flows: flows n-1775998 ns-176898 ne-150682 nq-0 nd-0 nx-0 to-300 cf-22 ft-128835/768374/963353/15347

20:45:22 l-flo-f1: classify\_flows: flows n-1786441 ns-175776 ne-151846 nq-0 nd-0 nx-0 to-300 cf-22 ft-129255/770212/970360/15129

cf 항목은 "Classify Flows(플로우 분류)"를 나타냅니다. 스레드가 책임 있는 플로우 캐시 섹션을 통과하는 데 걸린 시간(초)을 나타냅니다. CSE가 흐름에 적용되는 "Classify Flows" 스레드에 있습니다. 기능을 활성화한 후 이러한 수치가 증가하면 성능에 미치는 전반적인 영향을 효과적으로 측정할 수 있습니다.

이 고급 간격 설정을 추가한 후 상승이 예상되지만 이 수가 60에 가까우면 영향이 너무 크므로 설정을 제거하십시오. 몇 초의 증가가 예상되고 합리적이라고 여겨진다.

## 성능 기간 동안의 엔진 상태

"이전 및 이후" 측정에서 수행할 수 있는 다른 성능 중 하나는 sw.log 파일의 "성능 기간" 섹션을 보면 흐름 처리에 대한 설정의 영향을 측정하기 위해 5분마다 기록됩니다. grep를 사용하여 이러한 블록을 찾을 수도 있습니다. 엔진이 오버되면 이 고급 설정 간격 검사를 비활성화해야 합니다.

```
/lancope/var/sw/today/logs/ grep -A3 "Performance Period" sw.log
```

"Engine status Normal(엔진 상태 정상)" 이외의 다른 상태에 주의하십시오.

"Engine status Input rate too high(엔진 상태 입력 속도가 너무 높음)"와 같은 상태는 classify\_flows 스레드가 CPU를 너무 많이 사용하고 있음을 나타냅니다.

## SFI - 정적 흐름 색인


분류 스레드가 흐름 캐시를 통과하는 통과를 완료할 수 없었음을 의미합니다. 분류 스레드는 "Static Flow Index"를 나타내며 분류 스레드에서 고전을 겪고 있음을 나타냅니다. 그 자체로는 재해가 아니

지만, 엔진이 한계에 도달하기 시작하고 있으며 현재 cf 레벨에서 성능이 저하되기 시작하고 있음을 나타냅니다.

```
sw.log:16:09:49 I-flow-f1: classify_flows: sfi:base(8388608) (10522745 -> 11014427)
max(16777215) cod(1) (491681/8388608)----->(5%)
sw.log:16:09:49 I-flow-f3: classify_flows: sfi:base(25165824) (27269277 -> 27754304)
max(33554431) cod(1) (485026/8388608)----->(5%)
sw.log:16:09:49 I-flow-f4: classify_flows: sfi:base(33554432) (35652656 -> 36138422)
max(41943039) cod(1) (485765/8388608)----->(5%)
sw.log:16:09:49 I-flow-f2: classify_flows: sfi:base(16777216) (18985626 -> 19499308)
max(25165823) cod(1) (513681/8388608)----->(6%)
sw.log:16:09:54 I-flo-f0: classify_flows: sfi:base(0) (1786480 -> 421161) max(8388607) cod(1)
(7023288/8388608)----->(83%)
sw.log:16:10:49 I-flo-f0: classify_flows: sfi:base(0) (421161 -> 1402189) max(8388607) cod(0)
(981027/8388608)----->(11%)
sw.log:16:10:49 I-flow-f2: classify_flows: sfi:base(16777216) (19499308 -> 17522620)
max(25165823) cod(0) (6411919/8388608)----->(76%)
sw.log:16:10:49 I-flow-f1: classify_flows: sfi:base(8388608) (11014427 -> 8976309)
max(16777215) cod(0) (6350489/8388608)----->(75%)
sw.log:16:10:49 I-flow-f3: classify_flows: sfi:base(25165824) (27754304 -> 25702968)
max(33554431) cod(0) (6337271/8388608)----->(75%)
sw.log:16:10:49 I-flow-f7: classify_flows: sfi:base(58720256) (58848913 -> 59630528)
max(67108863) cod(0) (781614/8388608)----->(9%)
sw.log:16:10:49 I-flow-f4: classify_flows: sfi:base(33554432) (36138422 -> 34064015)
max(41943039) cod(1) (6314200/8388608)----->(75%)
sw.log:16:10:49 I-flow-f5: classify_flows: sfi:base(41943040) (43310891 -> 44059251)
max(50331647) cod(1) (748359/8388608)----->(8%)
sw.log:16:10:49 I-flow-f6: classify_flows: sfi:base(50331648) (51714170 -> 52444661)
max(58720255) cod(1) (730490/8388608)----->(8%)
sw.log:16:11:49 I-flow-f5: classify_flows: sfi:base(41943040) (44059251 -> 42121104)
max(50331647) cod(0) (6450460/8388608)----->(76%)
sw.log:16:11:49 I-flo-f0: classify_flows: sfi:base(0) (1402189 -> 2373792) max(8388607) cod(1)
(971602/8388608)----->(11%)
sw.log:16:11:49 I-flow-f6: classify_flows: sfi:base(50331648) (52444661 -> 50483491)
max(58720255) cod(1) (6427437/8388608)----->(76%)
sw.log:16:11:49 I-flow-f3: classify_flows: sfi:base(25165824) (25702968 -> 26385879)
max(33554431) cod(1) (682910/8388608)----->(8%)
sw.log:16:11:49 I-flow-f1: classify_flows: sfi:base(8388608) (8976309 -> 9662167) max(16777215)
cod(1) (685857/8388608)----->(8%)
sw.log:16:11:49 I-flow-f4: classify_flows: sfi:base(33554432) (34064015 -> 34742593)
max(41943039) cod(1) (678577/8388608)----->(8%)
sw.log:16:11:50 I-flow-f7: classify_flows: sfi:base(58720256) (59630528 -> 60298366)
max(67108863) cod(1) (667837/8388608)----->(7%)
sw.log:16:11:50 I-flow-f2: classify_flows: sfi:base(16777216) (17522620 -> 18202249)
max(25165823) cod(1) (679628/8388608)----->(8%)
```

## 구성

웹 브라우저를 열고 Flow Collector Appliance IP로 직접 이동합니다. 로컬 관리자 사용자로 로그인합니다.



The image shows the login page for Cisco Secure Network Analytics. At the top, there is the Cisco logo (a stylized bridge) followed by the word "SECURE" in large green letters and "Network Analytics" in black. Below this, it says "Flow Collector NetFlow VE" and "7.4.2". There are two input fields: "Username:" and "Password:". A blue button labeled "Login >>" is located at the bottom right of the form area.

Support(지원) -> Advanced Settings(고급 설정)로 이동합니다.

Advanced Setting(고급 설정) 화면을 아래로 스크롤하여 목록 하단의 "Add New Option(새 옵션 추가)" 컨피그레이션 상자를 표시합니다

새 옵션 추가: 편집 상자에 cse\_exec\_interval\_secs를 입력하고 옵션 값: 편집 상자에 119를 입력합니다. 이러한 상자를 편집하면 추가 단추가 활성화됩니다. Add(추가) New Option(새 옵션 추가): edit(편집) 상자에 cse\_exec\_interval\_secs를 입력한 후 Add(추가) 버튼을 누르고 Option Value(옵션 값):edit(수정) 상자에 119를 입력합니다.

새 옵션 추가: 및 옵션 값: 편집 상자는 여러 개의 새 고급 설정이 입력될 경우에 대비해 지워집니다. 새로 추가된 Advanced Settings(고급 설정)는 추가되는 동안 목록의 맨 아래에 추가됩니다. 이렇게 하면 사용자가 항목을 검사할 수 있습니다. 고급 설정의 정확한 철자는 대/소문자도 중요합니다. 모든 고급 설정은 소문자로 표시됩니다.

zmq_high_water_mark	<input type="text" value="1048576"/>	<input type="checkbox"/>
cse_exec_interval_secs	<input type="text" value="119"/>	<input type="checkbox"/>

Add New Option:  Option value:

Advanced Setting(고급 설정)이 올바르게 입력되었으므로 Apply(적용) 버튼을 누릅니다. Apply(적용) 버튼이 활성화되지 않은 경우도 있습니다. 이 기능을 활성화하려면 Add New Option: 편집 상자를 클릭한 다음 Apply(적용) 버튼을 클릭하여 클릭합니다. 이 팝업이 표시되면 확인 단추를 눌러 새 고급 설정 및 값을 제출합니다.

**[2001:420:3044:2010::a00:4c82] says**

**Warning:**  
 These settings should only be changed under direct instruction from Cisco Support.  
 Misconfiguration may seriously impact the performance of this Secure Network Analytics appliance and/or the loss of monitoring capabilities.

Are you sure you want to continue?

## 변경 확인

이 최종 검증이 가장 중요합니다. Support(지원) 메뉴를 다시 클릭하고 Browse Files(파일 찾아보기)를 선택합니다.

그러면 FC의 파일 시스템으로 이동합니다. sw(소프트웨어)를 클릭합니다.



- Home
- Configuration
- Manage Users
- Support
- Audit Log
- Operations
- Logout
- Help

### Browse Files

Name	Size	Last Modified
admin	-	Jan 26, 2024 7:51:47 PM UTC
containers	-	Jan 26, 2024 7:34:52 PM UTC
database	-	Jan 26, 2024 7:31:03 PM UTC
endpoint	-	Jan 25, 2024 3:58:39 PM UTC
etc	-	Jan 26, 2024 7:51:53 PM UTC
fc	-	Jan 26, 2024 7:33:33 PM UTC
imgstore	-	Nov 6, 2023 9:08:15 PM UTC
lib	-	Jan 26, 2024 7:31:54 PM UTC
logs	-	Feb 1, 2024 7:01:01 PM UTC
lost+found	-	Jan 26, 2024 7:29:37 PM UTC
manual-set-time	-	Nov 6, 2023 6:07:55 PM UTC
nginx	-	Jan 26, 2024 7:33:33 PM UTC
services	-	Jan 26, 2024 7:34:52 PM UTC
sw	-	Feb 1, 2024 4:00:01 AM UTC
sw-flow-proxyparser	-	Jan 25, 2024 3:59:01 PM UTC
swa-agent	-	Jan 25, 2024 3:58:39 PM UTC
sysimage	-	Jan 26, 2024 7:31:41 PM UTC
tcpdump	-	Jan 31, 2024 2:00:05 AM UTC
tomcat	-	Jan 26, 2024 7:31:47 PM UTC

오늘 클릭



The screenshot shows the 'Browse Files (/sw)' page. The left sidebar contains navigation options: Home, Configuration, Manage Users, Support, Audit Log, Operations, Logout, and Help. The main content area displays a table of files in the /sw directory.

Name	Size	Last Modified
26	-	Jan 27, 2024 4:00:00 AM UTC
27	-	Jan 28, 2024 4:00:01 AM UTC
28	-	Jan 29, 2024 4:00:00 AM UTC
29	-	Jan 30, 2024 4:00:00 AM UTC
30	-	Jan 31, 2024 4:00:00 AM UTC
31	-	Feb 1, 2024 4:00:01 AM UTC
data	-	Feb 1, 2024 7:36:49 PM UTC
tmp	-	Feb 1, 2024 8:23:00 PM UTC
tmp_db	-	Feb 1, 2024 6:12:45 AM UTC
today	-	Jan 25, 2024 3:58:00 PM UTC

로그를 클릭합니다.

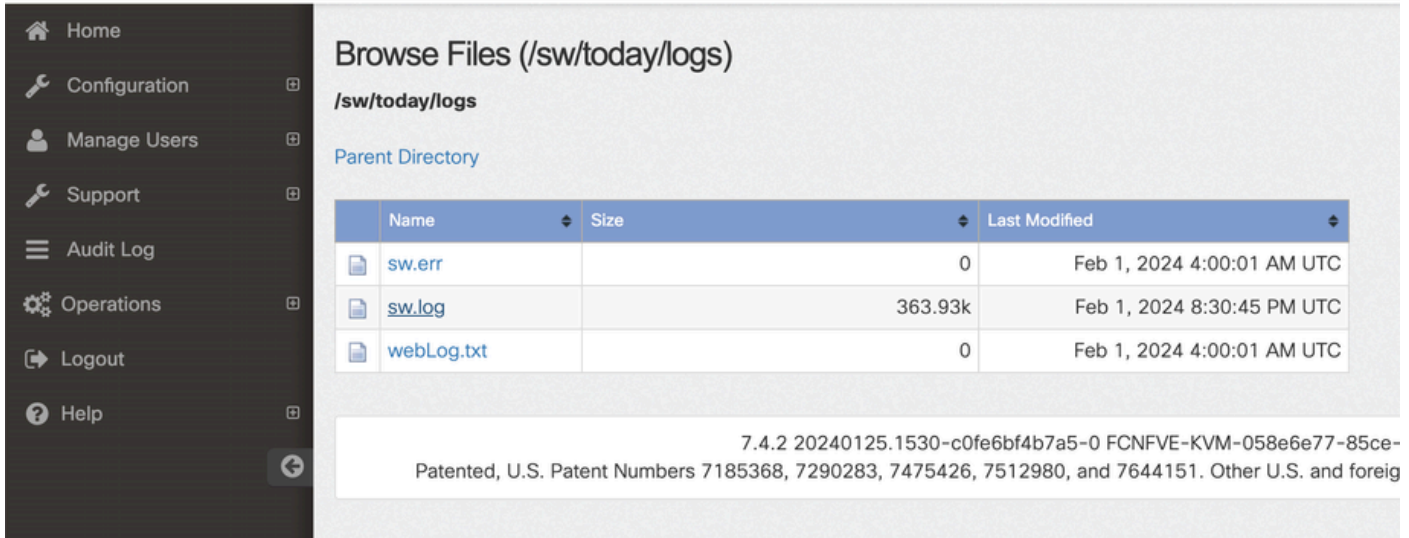
The browser address bar shows the URL: [https://\[2001:420:3044:2010::a00:4c82\]/swa/files/sw/today](https://[2001:420:3044:2010::a00:4c82]/swa/files/sw/today). The browser is identified as Mozilla Firefox.

The screenshot shows the 'Browse Files (/sw/today)' page. The left sidebar is the same as in the previous screenshot. The main content area displays a table of files in the /sw/today directory.

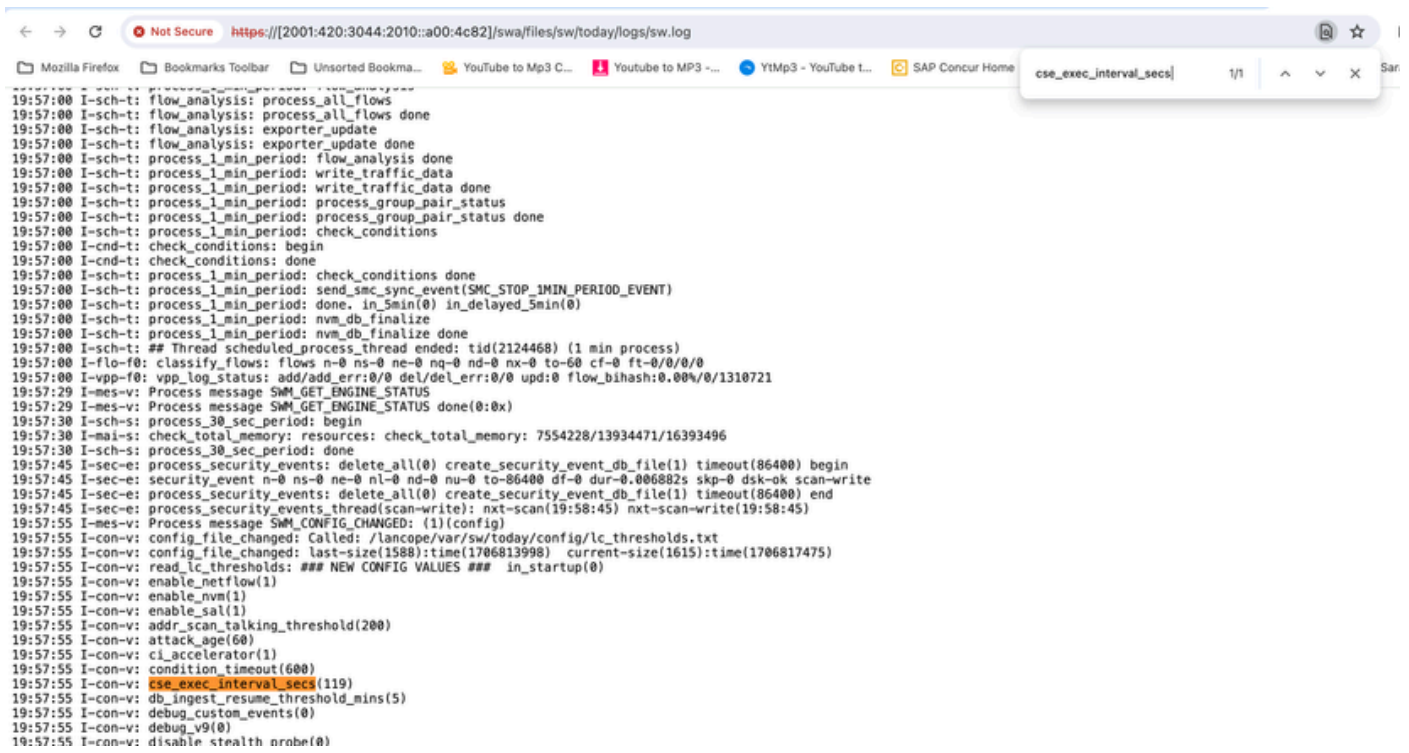
Name	Size	Last Modified
config	-	Feb 1, 2024 8:27:00 PM UTC
data	-	Feb 1, 2024 4:00:01 AM UTC
logs	-	Feb 1, 2024 7:36:36 PM UTC

At the bottom of the page, there is a footer with the following text: 7.4.2 20240125.1530-c0fe6bf4b7a5-0 FCNFVE-KVM-058e6e77-85 Patented, U.S. Patent Numbers 7185368, 7290283, 7475426, 7512980, and 7644151. Other U.S. and for

sw.log를 클릭합니다.



브라우저 페이지에서 검색을 수행하고 검색 상자에 cse\_exec\_interval\_secs를 입력하여 고급 설정을 찾습니다



승인된 고급 설정이 스크린샷과 같이 나열됩니다.

허용되지 않는 항목은 "입력 컨피그레이션에 포함되지 않음"으로 표시되며, 이 경우 사용자가 설정을 잘못 입력했기 때문입니다. 따라서 이러한 컨피그레이션을 변경한 후 로그를 확인하는 것이 중요합니다.

```
-----  
20:41:52 I-con-v: read_lc_thresholds: ### NEW CONFIG VALUES ### in_startup(0)  
20:41:52 I-con-v: enable_netflow(1)  
20:41:52 I-con-v: enable_nvm(1)  
20:41:52 I-con-v: enable_sal(1)  
20:41:52 I-con-v: addr_scan_talking_threshold(200)  
20:41:52 I-con-v: attack_age(60)  
20:41:52 I-con-v: ci_accelerator(1)  
20:41:52 I-con-v: condition_timeout(600)  
20:41:52 I-con-v: (cse_exec_interval_sec) not part of input configuration  
20:41:52 I-con-v: cse_exec_interval_secs(119)  
-----
```

## 축하합니다!

방금 새 고급 설정을 입력하고 엔진에서 해당 설정을 승인했습니다.

이제 이 기능은 플로우가 `early_check_age`에 도달하면 약 2분마다 플로우에 대해 CSE 논리를 실행할 수 있습니다. 기본값은 160초입니다.

CSE 규칙에서 시간의 경과에 따른 바이트 수 누적이 포함된 경우, 이 기능은 CSE가 정의한 기준과 일치하는 플로우에서 트리거되는 타이밍을 개선합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.