

ISE에서 포스처 리스 이해

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[설정](#)

[다음을 확인합니다.](#)

[자주 묻는 질문\(FAQ\)](#)

[알려진 결함](#)

소개

이 문서에서는 Cisco ISE에서 포스처 리스의 컨피그레이션 및 작업에 대해 설명합니다.

사전 요구 사항

요구 사항

- Cisco ISE의 상태 흐름에 대한 지식
- Cisco ISE의 AAA 정책에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cat9300 스위치 버전 17.9.5
- ISE(Identity Service Engine) v3.2
- ISE Posture Module 5.1.60이 포함된 PC Windows 10 Enterprise

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

포스처 리스는 마지막으로 알려진 컴플라이언스 상태를 DB에 최대 365일까지 저장하는 Cisco ISE의 기능으로, 컴플라이언스를 확인하기 위해 엔드포인트에 도달하지 않습니다. 그러나 포스처 리스가 만료되면 Cisco ISE는 엔드포인트에 대한 재인증 또는 포스처 재평가를 자동으로 트리거하지 않습니다. 동일한 세션이 사용되고 있으므로 엔드포인트는 동일한 규정 준수 상태를 유지합니다.

. 엔드포인트가 재인증되면 포스처가 실행되고 포스처 임대 시간이 재설정됩니다.

포스처 리스는 Oracle DB에 저장되며 시간을 EPOCH 시간으로 저장하는 엔드포인트 속성입니다. Context visibility 및 Oracle DB에서도 동일한 내용을 검증할 수 있습니다.

PostureExpiry	1733043766997
PostureOS	Windows 10 Professional 64-bit
PostureStatus	Compliant
PreviousMACAddress	B4:96:91:26:EB:A1

포스처 리스와 함께 ISE에는 Last Known Posture Compliant State에서 구성된 구성 가능한 시간(최대 200일/4800시간/288000분)에 대해 마지막으로 알려진 컴플라이언스 상태를 캐시하는 기능이 하나 더 있습니다. 이 기능을 통해 Cisco ISE는 마지막 규정 준수 상태를 캐시할 수 있으며, 엔드포인트가 Last Known Posture Compliant State(마지막으로 알려진 포스처 규정 준수 상태) 내에서 규정준수가 되지 않을 경우 ISE는 포스처 정책에 구성된 유예 기간까지 엔드포인트를 규정준수로 표시합니다.

마지막으로 알려진 포스처 호환 상태 값은 Oracle DB에 저장됩니다. 또한 EPOCH 시간에 저장합니다.

설정

Cisco ISE에서 포스처 리스를 구성하려면

Work Centers(작업 센터) > Posture(포스처) > Settings(설정) > Posture Lease(포스처 임대)로 이동합니다. Perform posture assessment every(포스처 평가 수행)를 선택하고 일 수(1-365일)를 구성합니다. 여기에서는 1일로 설정되어 있습니다.

Cache Last Known Posture Compliant Status(캐시 최종 알려진 포스처 규정 준수 상태)를 확인하고 최종 알려진 포스처 규정 준수 상태 시간(최대 200일/4800시간/288000분)을 구성합니다. 여기서는 2일로 구성됩니다.

Posture Lease

- ☐ Perform posture assessment every time a user connects to the network
- ☒ Perform posture assessment every 1 Days ⓘ
- ☒ Cache Last Known Posture Compliant Status

Last Known Posture Compliant State 2 Days ▾

간소화를 위해 단 하나의 포스처 정책(Windows FW 검사)만 2분의 유예 기간 동안 활성화되었습니다.

Posture Policy [Guide Me](#)

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

	Policy	Condition	Action
☒	Default_Firewall_Policy_Win	If Any + and Windows All + and 4.x or later ▾ and Agent ▾ and (Optional) Dictio... +	then Default_... + Done
☐		and Windows All and 4.x or later and Temporal Agent and	then Default_Firewall_Require...ment_Win_temporal Edit ▾
☐		and Mac OSX and 4.x or later and Agent and	then Default_Hardware_Attrib...utes_Requirement_Mac Edit ▾
☐		and Mac OSX and 4.x or later and Temporal Agent and	then Default_Hardware_Attrib...utes_Requirement_Mac...temporal Edit ▾
☐		and Windows All and 4.x or later and Agent and	then Default_Hardware_Attrib... Edit ▾

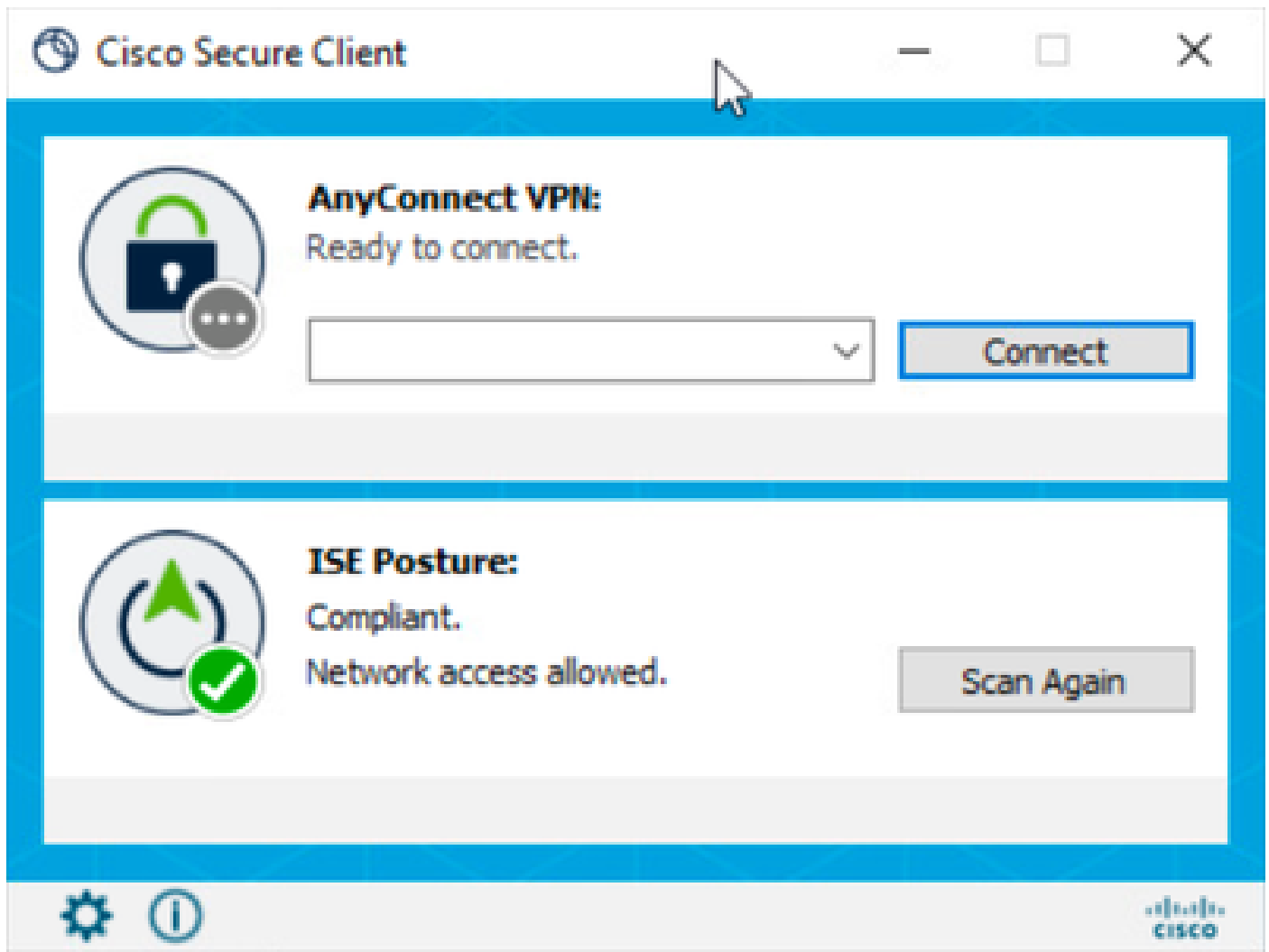
Grace period settings

Grace Period for: 2 Minutes ▾

Delay notification by (0 %) of Grace period.

다음을 확인합니다.

엔드포인트는 처음으로 연결되며 규정을 준수합니다.



Nov 30, 2024 10:55:55.910 PM	✓	🔒	B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS	Compliant
Nov 30, 2024 10:55:55.822 PM	✓	🔒	B4:96:91:26:EB:A1		labpsn01		Compliant
Nov 30, 2024 10:55:08.085 PM	✓	🔒	B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS_NON_CO...	Pending

ISE-PSC.log(Posture in DEBUG)

ise-psc.log에서 EP가 처음 연결되므로 DB에 만료 시간이 없음을 확인할 수 있습니다.

```
2024-11-30 22:55:08,485 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-8][[]] cisco.cpm.posture.runtime
2024-11-30 22:55:08,485 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-8][[]] cisco.cpm.posture.runtime
```

EP는 포스처 확인 프로세스를 거치고 규정을 준수하게 됩니다. EP가 규정을 준수하면 ISE는 만료 시간을 1일(1733073953816)로 하여 DB를 업데이트합니다.

```
2024-11-30 22:55:55,306 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-1][[]] cisco.cpm.posture.runtime
2024-11-30 22:55:55,307 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-1][[]] cisco.cpm.posture.runtime
2024-11-30 22:55:55,307 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-1][[]] cisco.cpm.posture.runtime
```

또한 ISE는 유예 기간 만료 시간 1733160354306(2일)로 DB를 업데이트합니다.

```
2024-11-30 22:55:55,306 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-1][[]] cisco.cpm.posture.edf.Pos
2024-11-30 22:55:55,306 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-1][[]] cisco.cpm.posture.runtime
2024-11-30 22:55:54,306 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-1][[]] cisco.cpm.posture.runtime
```

EP를 다시 연결한 후에는 세션이 직접 Complaint가 됩니다. 포스처 리스가 활성화되면 ISE는 DB에서 포스처 만료 시간을 검색하고 세션을 Compliant로 표시했습니다.

Nov 30, 2024 11:04:17.689 PM			B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS	Compliant
------------------------------	--	--	-------------------	----------------------	----------	---------------------------------	-----------

```
2024-11-30 23:04:17,673 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
2024-11-30 23:04:17,673 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
2024-11-30 23:04:17,677 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
2024-11-30 23:04:17,679 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.runtime.PostureMan
2024-11-30 23:04:17,679 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.runtime.PostureMan
2024-11-30 23:04:17,679 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
2024-11-30 23:04:17,679 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
2024-11-30 23:04:17,680 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.runtime.PosturePo
2024-11-30 23:04:17,680 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
```

시나리오 1: 상태 임대를 비활성화하고 캐시 마지막 알려진 상태 호환 상태를 활성화하십시오. 마지막으로 알려진 상태 호환 상태는 2일입니다. (이 시나리오는 상태 임대가 만료되고 그 이후에 EP가 연결되는 경우에도 유효합니다.)

Posture Lease

☒ Perform posture assessment every time a user connects to the network

☐ Perform posture assessment every

1

Days

☒ Cache Last Known Posture Compliant Status

Last Known Posture Compliant State

2

Days

EP가 인증되면 포스처 리스가 활성화되지 않으므로 ISE는 포스처 확인을 수행합니다.

```
2024-12-01 18:39:50,901 DEBUG [PolicyEngineEvaluationThread-3][[]] cisco.cpm.posture.pip.PostureStatusP
2024-12-01 18:39:50,901 DEBUG [PolicyEngineEvaluationThread-3][[]] cisco.cpm.posture.pip.PostureStatusP
```

2024-12-01 18:39:50,901 DEBUG [PolicyEngineEvaluationThread-3][[]] cisco.cpm.posture.pip.PostureStatusP

EP가 규정 준수가 되면 ISE는 유예 기간 만료 시간 1733231423117(2일) 내에 DB를 업데이트합니
다.

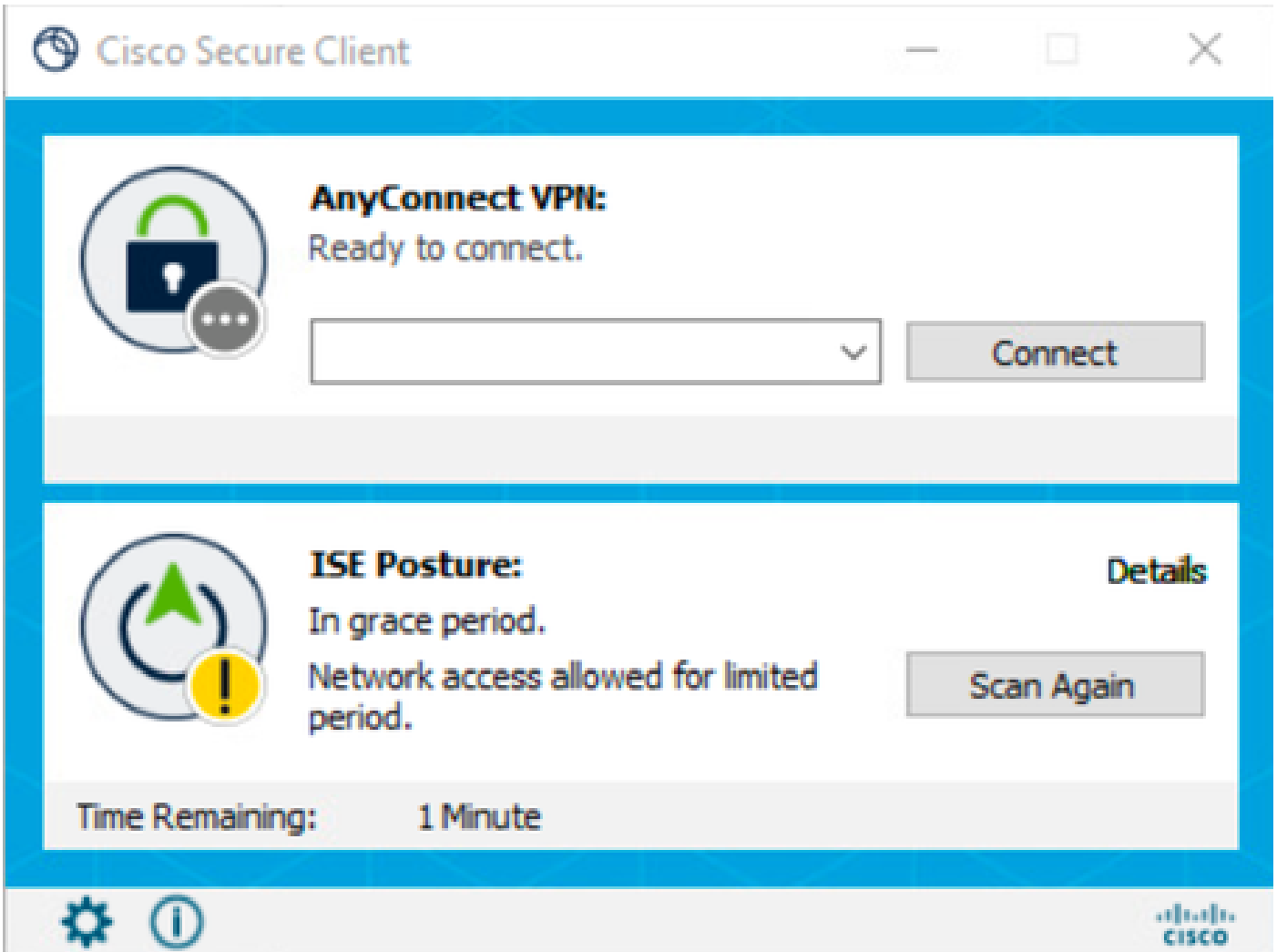
2024-12-01 18:40:23,116 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-3][[]] cisco.cpm.posture.edf.Pos
2024-12-01 18:40:23,117 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-3][[]] cisco.cpm.posture.runtime
2024-12-01 18:40:23,117 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-3][[]] cisco.cpm.posture.runtime
2024-12-01 18:40:23,117 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-3][[]] cisco.cpm.posture.edf.Pos

Time	Status	Details	Repeat Cou...	Endpoint ID	Identity	Server	Authorization Policy	Posture Status
				Endpoint ID	Identity	Server	Authorization Policy	Posture Status
Dec 01, 2024 06:40:25.217 PM			0	B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS	Compliant
Dec 01, 2024 06:40:25.202 PM				B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS	Compliant
Dec 01, 2024 06:40:25.126 PM				B4:96:91:26:EB:A1		labpsn01		Compliant
Dec 01, 2024 06:39:50.911 PM				B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS_NON_CO...	Pending

이제 EP는 불만 사항이 됩니다.

포스처 정책에서처럼 windows FW만 확인됩니다. Windows FW를 비활성화하고 EP를 다시 연결합
니다.

EP는 Non-Complaint가 되지만 포스처 정책에서 2분 유예 기간이 구성됩니다. 이로 인해 AC
Posture 모듈은 In grace period(유예 기간 중)로 상태를 표시합니다.



RADIUS 라이브 로그에서 상태 검사가 실패했더라도 EP가 불만 신고로 표시되는 것을 볼 수 있습니다. 유예 기간이 만료된 후 세션이 Non-Compliant가 되었습니다.

Time	Status	Details	Repeat Cou...	Endpoint ID	Identity	Server	Authorization Policy	Posture Status
		▼		Endpoint ID	Identity	Server	Authorization Policy	Posture Status
Nov 30, 2024 11:29:25.424 PM	●	🔒	0	B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS_NON_CO...	NonCompliant
Nov 30, 2024 11:29:25.402 PM	✓	🔒		B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS_NON_CO...	NonCompliant
Nov 30, 2024 11:29:25.301 PM	✓	🔒		B4:96:91:26:EB:A1		labpsn01		NonCompliant
Nov 30, 2024 11:27:21.642 PM	✓	🔒		B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS	Compliant
Nov 30, 2024 11:27:21.554 PM	✓	🔒		B4:96:91:26:EB:A1		labpsn01		Compliant
Nov 30, 2024 11:26:16.491 PM	✓	🔒		B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS_NON_CO...	Pending

ise-psc.log에서 EP가 연결될 때 임대가 활성화되지 않았기 때문에 LSD를 확인하여 포스터 상태를 검색했음을 확인할 수 있습니다.

```
2024-11-30 23:26:16,482 DEBUG [PolicyEngineEvaluationThread-16][[]] cisco.cpm.posture.pip.PostureStatus
2024-11-30 23:26:16,482 DEBUG [PolicyEngineEvaluationThread-16][[]] cisco.cpm.posture.pip.PostureStatus
2024-11-30 23:26:16,483 DEBUG [PolicyEngineEvaluationThread-16][[]] cisco.cpm.posture.pip.PostureStatus
```

상태 확인은 EP에 대해 실패 합니다. 그 후 ISE는 DB를 검사하여 1733160354306(2일)인

lastCompliantExpiry 값을 검색했습니다.

```
2024-11-30 23:27:19,123 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.runtime
```

lastCompliantExpiry가 여전히 유효하므로 2분으로 구성된 포스처 정책에 구성된 유예 기간을 추가로 확인합니다.

```
2024-11-30 23:27:19,123 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.runtime
```

```
2024-11-30 23:27:19,544 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.runtime
```

```
2024-11-30 23:27:19,544 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.runtime
```

```
2024-11-30 23:27:19,546 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.runtime
```

```
2024-11-30 23:27:19,546 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.runtime
```

```
2024-11-30 23:27:19,546 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.runtime
```

유예 기간이 끝나면 AC 모듈은 실패한 보고서를 ISE로 전송합니다. ISE는 DB에서 유예 기간을 확인하고 만료되었음을 확인한 다음 해당 세션을 불만사항으로 표시하고 DB에서 LastCompExpiryTime 및 GracePeriodTime을 제거합니다.

```
2024-11-30 23:29:23,289 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-4][[]] cisco.cpm.posture.runtime
```

```
2024-11-30 23:29:23,289 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-4][[]] cisco.cpm.posture.runtime
```

```
2024-11-30 23:29:23,289 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-4][[]] cisco.cpm.posture.runtime
```

```
2024-11-30 23:29:23,289 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-4][[]] cisco.cpm.posture.runtime
```

```
2024-11-30 23:29:23,289 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-4][[]] cisco.cpm.posture.edf.Pos
```

```
2024-11-30 23:29:23,289 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-4][[]] cisco.cpm.posture.runtime
```

```
2024-11-30 23:29:23,289 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-4][[]] cisco.cpm.posture.edf.Pos
```

```
2024-11-30 23:29:23,289 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-4][[]] cisco.cpm.posture.edf.Pos
```

EP가 다시 연결되고 불만사항이 되면 Last compliant 기간이 이미 만료되었고 세션이 Non-Complaint로 직접 업데이트되었으므로 ISE는 포스처 정책의 유예 기간을 준수하지 않습니다.

```
2024-12-01 00:49:40,004 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-6][[]] cisco.cpm.posture.runtime
```

시나리오 2: 캐시 마지막으로 알려진 포스처 규정 준수 상태와 함께 포스처 임대를 비활성화합니다.

Posture Lease

- ☒ Perform posture assessment every time a user connects to the network
- ☐ Perform posture assessment every Days 
- ☐ Cache Last Known Posture Compliant Status

Last Known Posture Compliant State Days 

이 경우 기본적으로 ISE는 lastCompliantexpiry 시간을 365일(DB)로 업데이트합니다.

포스처 리스가 활성화되지 않으면 포스처 검사가 수행되고 ISE가 lastCompliant 만료 시간을 DB에서 365일로 업데이트한 후 EP가 불만사항이 됩니다.

```
2024-12-01 00:58:17,191 DEBUG [PolicyEngineEvaluationThread-12][[]] cisco.cpm.posture.pip.PostureStatus
2024-12-01 00:58:17,191 DEBUG [PolicyEngineEvaluationThread-12][[]] cisco.cpm.posture.pip.PostureStatus
2024-12-01 00:58:17,191 DEBUG [PolicyEngineEvaluationThread-12][[]] cisco.cpm.posture.pip.PostureStatus
2024-12-01 00:58:56,722 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.runtime
2024-12-01 00:58:56,723 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.runtime
2024-12-01 00:58:56,723 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.runtime
2024-12-01 00:58:56,723 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.edf.Po
```

시나리오 3: 상태 임대 LSD(Light Session Directory)의 영향.

LSD를 활성화하거나 비활성화해도 상태 임대 및 최종 규정 준수 상태에는 영향을 주지 않습니다. 이러한 두 속성은 모두 Oracle DB에 저장되고 구축 전반에 복제되기 때문입니다. 반면 LSD는 제한된 EP 특성을 메모리에 저장하고 다른 PSN에 복제합니다.

LSD가 활성화된 경우

LSD를 활성화하려면 Administration > System > Settings > Light Data Distribution > Check RADIUS Session Directory로 이동합니다.

RADIUS Session Directory

Enable the RADIUS Session Directory (RSD) feature to store the user session information and replicate it across the PSNs in a deployment. The RSD stores only the session attributes that are required for CoA.

☒ Enable RADIUS Session Directory

EP는 처음 연결하여 포스처 확인을 거칩니다. EP가 규정 준수가 되면 DB에서 포스처 임대 및 마지막으로 알려진 규정 준수 특성을 업데이트합니다.

```
2024-12-02 19:36:43,274 DEBUG [PolicyEngineEvaluationThread-11][[]] cisco.cpm.posture.pip.PostureStatusP
2024-12-02 19:36:43,276 WARN [PolicyEngineEvaluationThread-11][[]] cisco.cpm.posture.runtime.PostureMan
2024-12-02 19:36:43,276 INFO [PolicyEngineEvaluationThread-11][[]] cisco.cpm.posture.pip.PostureStatusP
```

```
2024-12-02 19:37:27,164 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-5][[]] cisco.cpm.posture.runtime
```

```
2024-12-02 19:37:29,110 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-6][[]] cisco.cpm.posture.runtime
```

```
2024-12-02 19:37:29,113 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-6][[]] cisco.cpm.posture.runtime
2024-12-02 19:37:29,113 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-6][[]] cisco.cpm.posture.runtime
```

이는 PSN에 분산된 LSD의 특성입니다. 속성에서 포스처 리스 상태 또는 마지막 규정준수 상태를 확인할 수 없습니다.

```
2024-12-02 19:37:32,221 DEBUG [LSD-consumers-pool-28][[]] cisco.cpm.lsd.service.SessionDirectory -:::
```

이제 구축에서 다른 PSN으로 EP를 인증합니다.

인증 요청이 다른 PSN에 랜딩한 후 PSN이 DB에서 포스처 리스 시간을 검색하고 세션을 규정 준수로 직접 표시하는 것을 볼 수 있습니다. 라이브 로그에서도 확인할 수 있습니다.

```
2024-12-02 20:08:27,449 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
2024-12-02 20:08:27,449 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
2024-12-02 20:08:27,468 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
2024-12-02 20:08:27,471 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.runtime.PostureMan
2024-12-02 20:08:27,471 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.runtime.PostureMan
2024-12-02 20:08:27,472 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
2024-12-02 20:08:27,472 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
```

Time	Status	Details	Session ID	Repeat Co...	Endpoint ID	Identity	Server	Authorization Policy	Posture Status
			Session ID			Identity	Server	Authorization Policy	Posture Status
Dec 02, 2024 08:08:28.055 PM			08C9C50A000002C87D4E09D	0	B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpan02	Wired Lab Policy Set >> EAP_TLS	Compliant
Dec 02, 2024 08:08:28.037 PM			08C9C50A000002C87D4E09D		B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpan02	Wired Lab Policy Set >> EAP_TLS	Compliant
Dec 02, 2024 07:37:31.216 PM			08C9C50A000002B87B7D6EC		B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS	Compliant
Dec 02, 2024 07:37:31.120 PM			08C9C50A000002B87B7D6EC		B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS	Compliant
Dec 02, 2024 07:36:43.290 PM			08C9C50A000002B87B7D6EC		B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS_NON_CO...	Pending

LSD가 비활성화된 경우:

LSD를 비활성화하려면 Administration > System > Settings > Light Data Distribution > Uncheck RADIUS Session Directory로 이동합니다.

RADIUS Session Directory

Enable the RADIUS Session Directory (RSD) feature to store the user session information and replicate it across the PSNs in a deployment. The RSD stores only the session attributes that are required for CoA.

☐ Enable RADIUS Session Directory

EP는 처음 연결 포스처 프로세스를 거칩니다. EP가 규정 준수가 되면 DB에서 포스처 임대 및 마지막으로 알려진 규정 준수 특성을 업데이트합니다.

```
2024-12-02 20:40:10,417 DEBUG [PolicyEngineEvaluationThread-9][[]] cisco.cpm.posture.pip.PostureStatusP
2024-12-02 20:40:10,423 WARN [PolicyEngineEvaluationThread-9][[]] cisco.cpm.posture.runtime.PostureMana
2024-12-02 20:40:10,423 INFO [PolicyEngineEvaluationThread-9][[]] cisco.cpm.posture.pip.PostureStatusPI
```

```
2024-12-02 20:40:45,679 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-1][[]] cisco.cpm.posture.runtime
```

```
2024-12-02 20:40:45,682 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-1][[]] cisco.cpm.posture.runtime
2024-12-02 20:40:45,682 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-1][[]] cisco.cpm.posture.runtime
```

이제 구축에서 다른 PSN으로 EP를 인증합니다.

인증 요청이 다른 PSN에 랜딩한 후 PSN이 DB에서 포스처 리스 시간을 검색하고 세션을 규정 준수로 직접 표시하는 것을 볼 수 있습니다. 라이브 로그에서도 확인할 수 있습니다.

```
2024-12-02 20:49:56,115 DEBUG [PolicyEngineEvaluationThread-10][[]] cisco.cpm.posture.pip.PostureStatus
2024-12-02 20:49:56,115 DEBUG [PolicyEngineEvaluationThread-10][[]] cisco.cpm.posture.pip.PostureStatus
2024-12-02 20:49:56,119 DEBUG [PolicyEngineEvaluationThread-10][[]] cisco.cpm.posture.pip.PostureStatus
```

2024-12-02 20:49:56,123 DEBUG [PolicyEngineEvaluationThread-10][[]] cisco.cpm.posture.runtime.PostureMa
2024-12-02 20:49:56,123 DEBUG [PolicyEngineEvaluationThread-10][[]] cisco.cpm.posture.runtime.PostureMa
2024-12-02 20:49:56,123 DEBUG [PolicyEngineEvaluationThread-10][[]] cisco.cpm.posture.pip.PostureStatus
2024-12-02 20:49:56,123 DEBUG [PolicyEngineEvaluationThread-10][[]] cisco.cpm.posture.pip.PostureStatus

Time	Status	Details	Session ID	Repeat Co...	Endpoint ID	Identity	Server	Authorization Policy	Posture Status
			Session ID		Endpoint ID	Identity	Server	Authorization Policy	Posture Status
Dec 02, 2024 08:50:26.305 PM			08C9C50A000003187FADE13	0	B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpan02	Wired Lab Policy Set >> EAP_TLS	Compliant
Dec 02, 2024 08:49:56.133 PM			08C9C50A000003187FADE13		B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpan02	Wired Lab Policy Set >> EAP_TLS	Compliant
Dec 02, 2024 08:40:47.777 PM			08C9C50A000003087F1EE30		B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS	Compliant
Dec 02, 2024 08:40:47.692 PM			08C9C50A000003087F1EE30		B4:96:91:26:EB:A1		labpsn01		Compliant
Dec 02, 2024 08:40:10.436 PM			08C9C50A000003087F1EE30		B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS_NON_CO...	Pending

이 두 시나리오에서 LSD가 포스처 리스에 영향을 주지 않음을 확인할 수 있습니다.

자주 묻는 질문(FAQ)

1. Posture Lease 및 Cached 마지막으로 알려진 상태는 서로 독립적입니까?

예, 캐시된 마지막으로 알려진 상태를 활성화하지 않고 포스처 임대를 활성화할 수 있으며 그 반대
의 경우도 가능합니다. 상태 임대는 엔드포인트 규정 준수 상태를 구성된 시간 동안 엔드포인트 특
성으로 저장합니다. 마지막으로 알려진 캐시된 상태는 엔드포인트가 규정을 준수하지 않는 경우 유
예 기간이 주어지는 동안 DB에 저장된 시간입니다. 이는 엔드포인트 특성이 아닙니다.

2. Posture Lease와 Cached last known posture가 둘 다 노드에 복제됩니까?

포스처 리스는 엔드포인트 특성이며 모든 노드에 복제됩니다. 캐시된 마지막으로 알려진 상태는 엔
드포인트 속성이 아니지만 Oracle DB에 있는 값이므로 모든 노드에 복제됩니다.

3. 노드를 재부팅하면 이러한 값이 제거됩니까?

아니요. 두 노드 모두 Oracle DB에 저장되므로 노드를 다시 로드해도 값이 제거되지 않습니다.

4. 포스처 임대로 인해 보안 문제가 발생합니까?

포스처 리스가 활성화된 경우 ISE는 엔드포인트의 포스처 상태를 확인하지 않습니다. 엔드포인트
가 규정을 준수하지 않으면 ISE에서 이를 Complaint로 처리할 수 있으므로 보안 문제가 발생할 수
있습니다. 이 위험을 최소화하기 위해 Posture Reassessment를 Posture Lease와 함께 사용하는 것
이 좋습니다.

알려진 결함

Cisco 버그 ID [CSCwk07454](#) PSN은 올바른 상태 임대 만료 시간으로 DB를 업데이트하지 않습니다
.

Cisco 버그 ID [CSCwi58421](#) PSN 노드가 포스처 리스가 활성화된 경우 올바른 포스처 만료 시간으
로 DB를 업데이트하지 않습니다.

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.