Understand Posture Lease in ISE

Contents

Introduction

This document describes the configuration and working of posture lease in Cisco ISE.

Prerequisites

Requirements

- Knowledge of Posture flow in Cisco ISE
- Knowledge of AAA Policies in Cisco ISE

Components Used

The information in this document is based on these software and hardware versions:

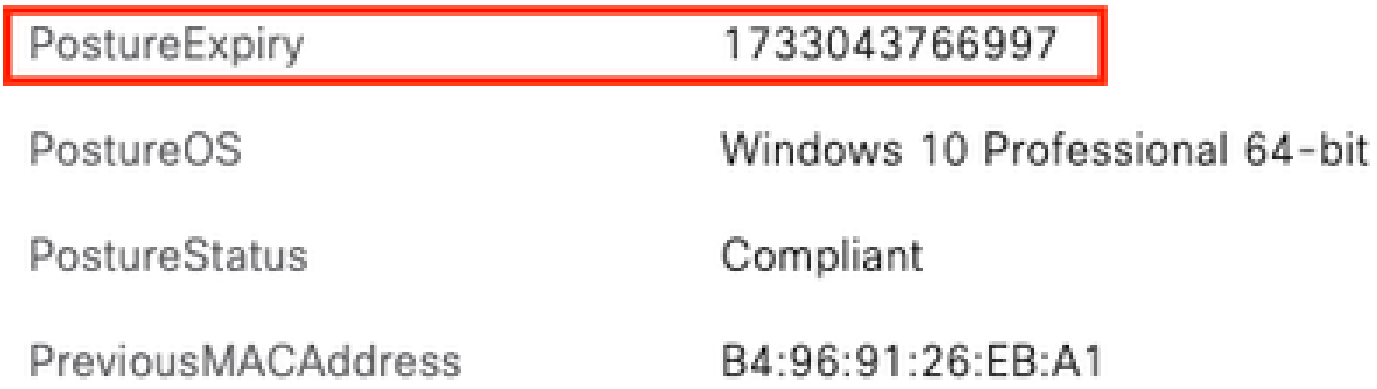
- Cat9300 switch Version 17.9.5
- Identity Service Engine (ISE) v3.2
- PC Windows 10 Enterprise with ISE posture module 5.1.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Posture lease is a feature in Cisco ISE which stores the last known compliance status up to 365 Days in DB and does not reach out to the endpoint to check for compliance. But when the posture lease expires, Cisco ISE does not automatically trigger a re-authentication or a posture reassessment for the endpoint. The endpoint stays in the same compliance state since the same session is being used. When the endpoint re-authenticates, the posture is run and the posture lease time is reset.

Posture lease is an endpoint attribute which stores in the Oracle DB, and stores the time in EPOCH time. The same can be validated from Context visibility and Oracle DB.



Along with the posture lease, there is one more feature in ISE which caches the last known compliance status for configurable amount of time (max 200 days / 4800 hours / 288000 minutes) configured in Last Known Posture Compliant State. This feature allows Cisco ISE to cache the last compliance status, and if an endpoint becomes non-compliant within the Last Known Posture Compliant State, ISE marks the endpoint as compliant until the grace period configured in posture policy.

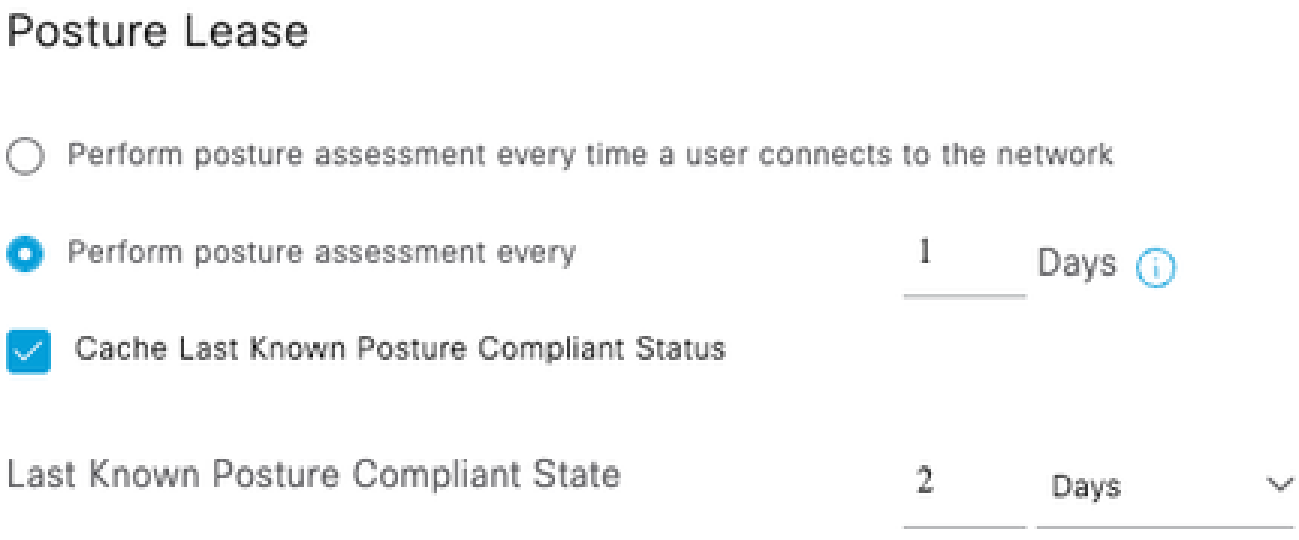
Last Known Posture Compliant State value stores in the Oracle DB. It also stores in EPOCH time.

Configuration

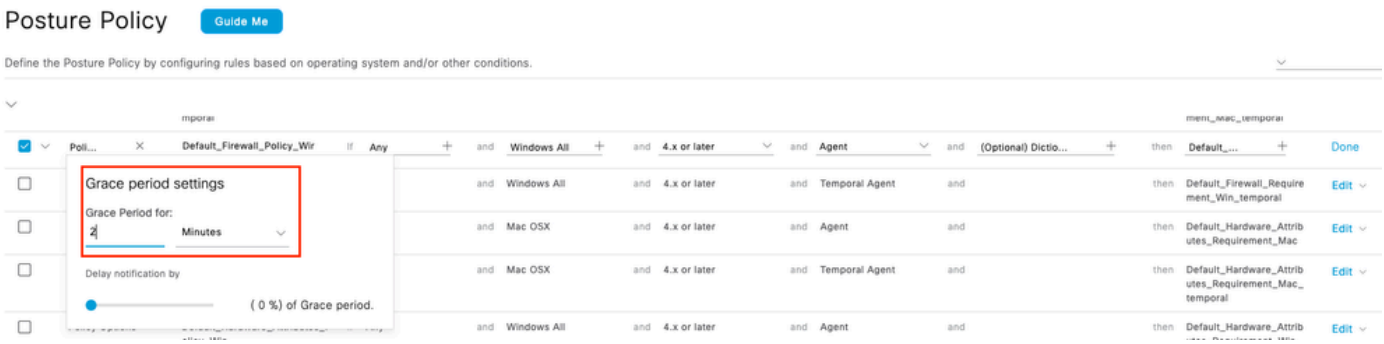
To configure the posture lease in Cisco ISE:

Navigate to **Work Centers > Posture > Settings > Posture Lease**. Check **Perform posture assessment** every and configure number of Day(s)(1-365 Days). Here it is set to 1 Day.

Check the Cache Last Known Posture Compliant Status and configure Last Known Posture Compliant State time (max 200 days / 4800 hours / 288000 minutes). Here it is configured for 2 Days.

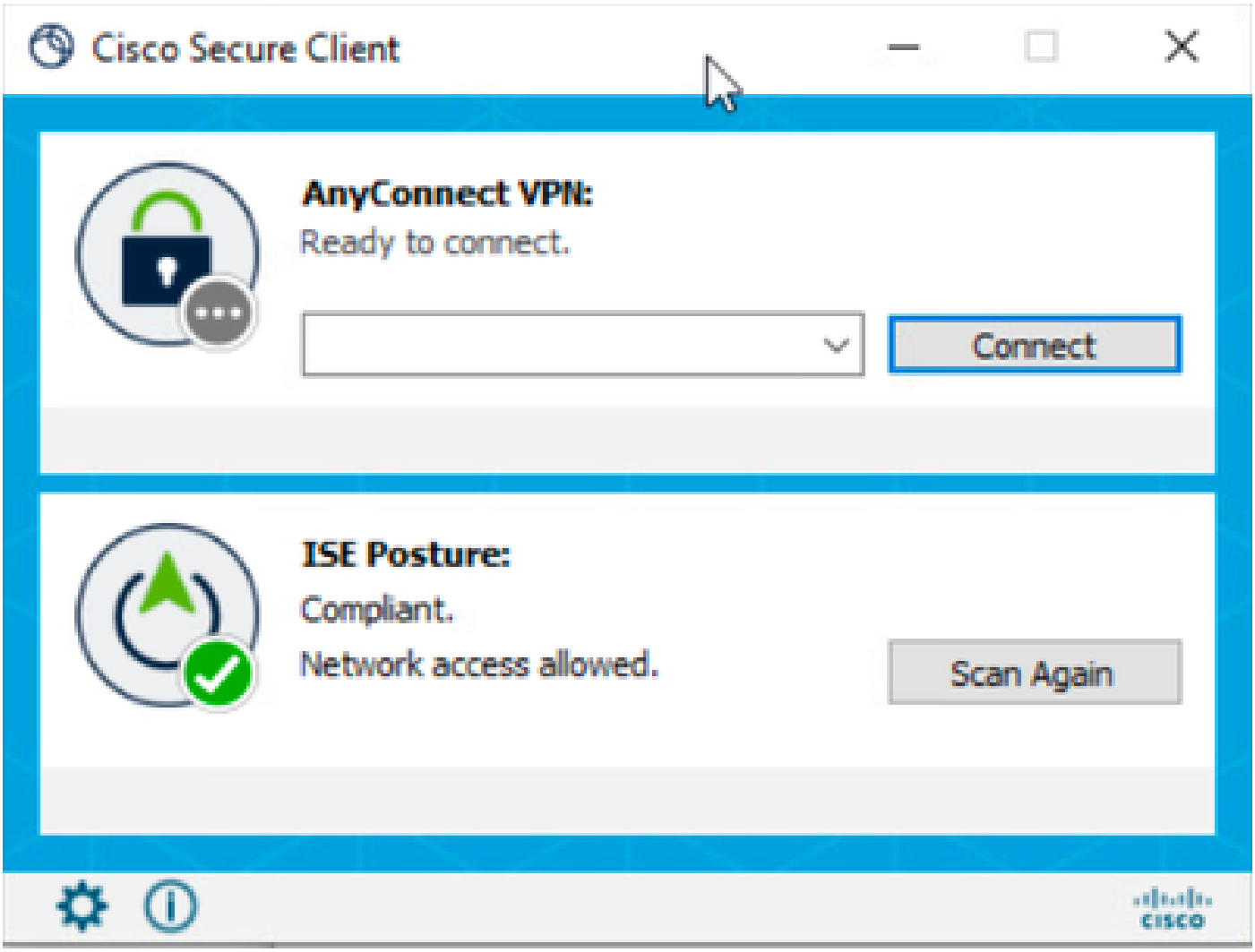


For simplicity, only one posture policy (Windows FW check) has been enabled with Grace period of 2 Mins.



Verify

The Endpoint connects for the first time and is compliant.



ISE-PSC.log (Posture in DEBUG)

In the ise-psc.log, you can see that there is no expiry time in the DB as the EP is connecting for the first time.

```
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
```

The EP goes through the posture check process and becomes compliant. Once the EP becomes compliant, ISE updates the DB with expiry time as 1 Day (1733073953816).

```
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
```

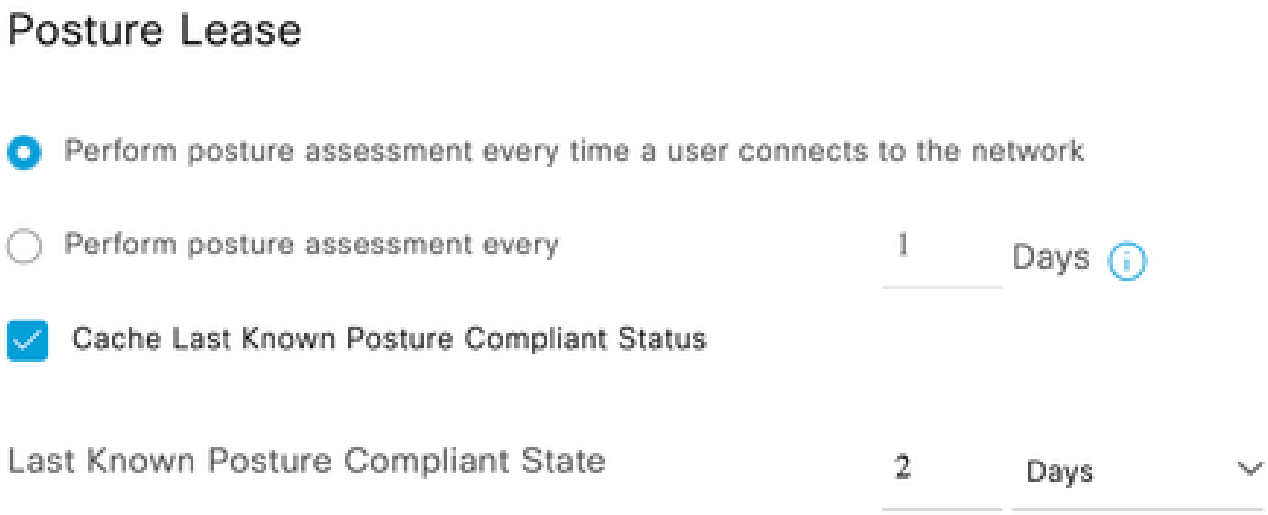
Also, ISE updates the DB with the grace period expiry time 1733160354306 (2 Days).

```
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
```

After reconnecting the EP, the session directly become Complaint. As the posture lease is enabled, ISE retrieved the posture expiry time form the DB and marked the session as 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.PosturePol
2024-11-30 23:04:17,680 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
```

Scenario 1 : Disable **Posture lease** and enable C**ache Last Known Posture Compliant Status** with **Last Known Posture Compliant State** is 2 Days. (This scenario is also valid in case posture lease expires and EP connects after that.)



After EP authenticates, as posture lease is not enabled, ISE performs the posture check.

```
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
```

After the EP becomes compliant, ISE updates the DB within the grace period expiry time 1733231423117 (2 Days).

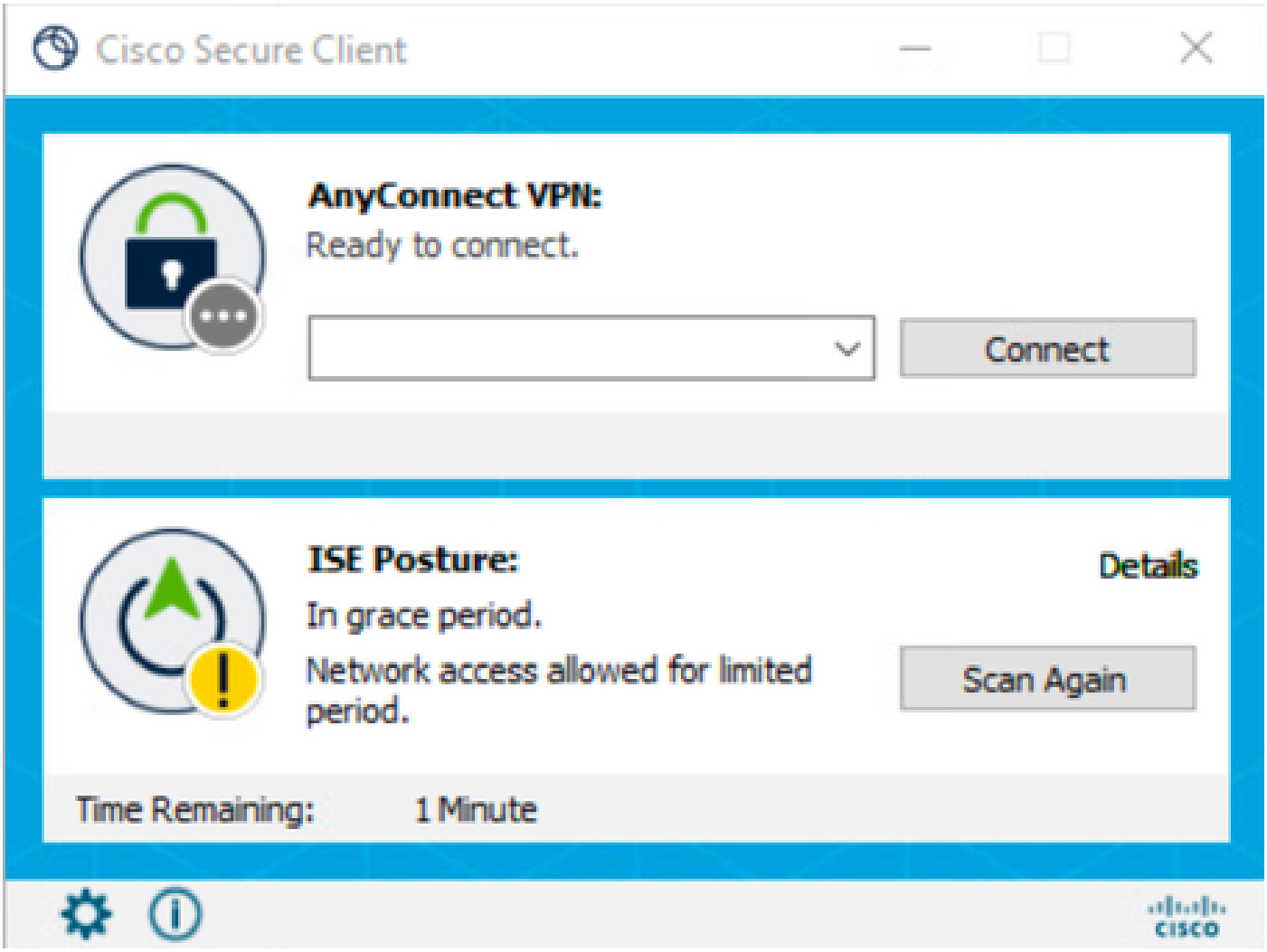
```
2024-12-01 18:40:23,116 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-3][[]] cisco.cpm.posture.edf.Pos
2024-12-01 18:40:23,117 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-3][[]] cisco.cpm.posture.runtime
2024-12-01 18:40:23,117 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-3][[]] cisco.cpm.posture.runtime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

Now, the EP becomes non-complaint.

As in the posture policy, only windows FW is getting checked. Disable the **Windows FW** and re-connect the **EP**.

The EP becomes non-complaint but, 2 Mins grace period is configured in the posture policy. Due to this, the AC posture module is showing the status as In grace period.



In the RADIUS live log, you can see the EP is marked as complaint, even though the posture check failed. After the grace period expired, the session became Non-Compliant.

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

In the ise-psc.log, you can see that when the EP connects, as the lease is not enabled, it checked the LSD to retrieve the posture status.

```
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
```

Posture check happen and it fails for the EP. After that ISE checked the DB to retrieve the lastCompliantExpiry value which is 1733160354306 (2 Days).

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

As the lastCompliantExpiry is still valid, it further checks the grace period configured on the posture policy which is configured as 2 Mins.

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

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

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

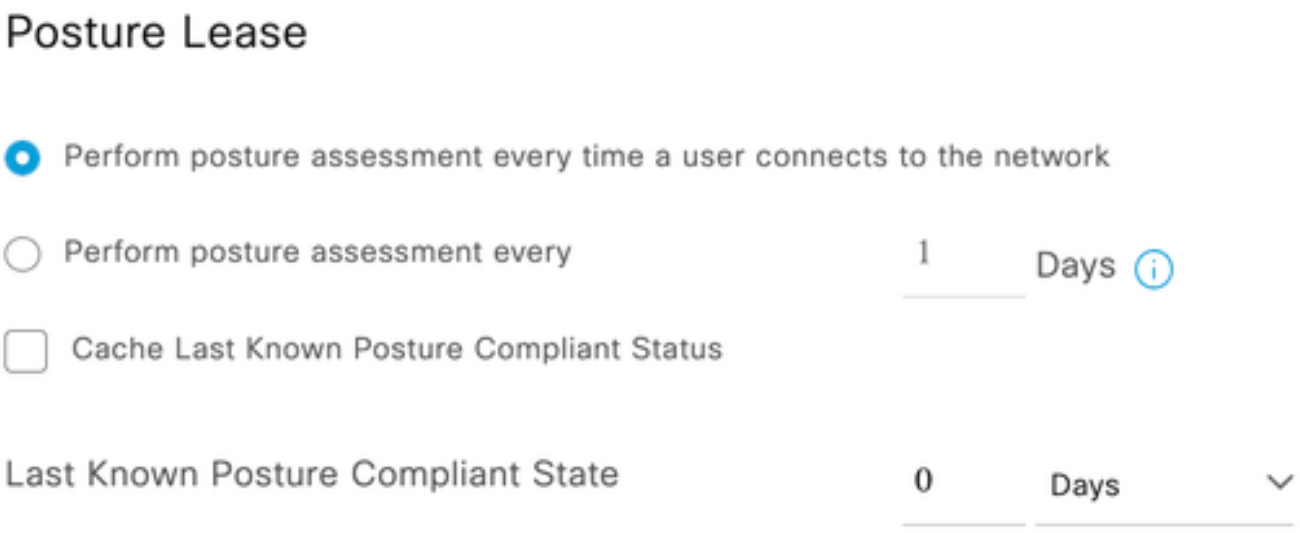
After the grace period is over, AC module sends the failed report to ISE. ISE checks the grace period in DB and finds that it has been expired, then it marked the session as non-complaint and removes the LastCompExpiryTime and GracePeriodTime from DB.

```
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
```

If the EP re-connects again and becomes non-complaint, ISE does not honor the grace period of posture policy, as the Last compliant period is already expired and the session is directly updated as Non-Complaint.

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

Scenario 2 : Disable **Posture lease** along with **Cache Last Known Posture Compliant Status**.



In this case, by default, ISE updates lastCompliantexpiry time to 365 Days in DB.

As the Posture lease is not enabled, posture check happens and EP becomes complaint after that ISE updates the lastCompliant expiry time to 365 Days in DB.

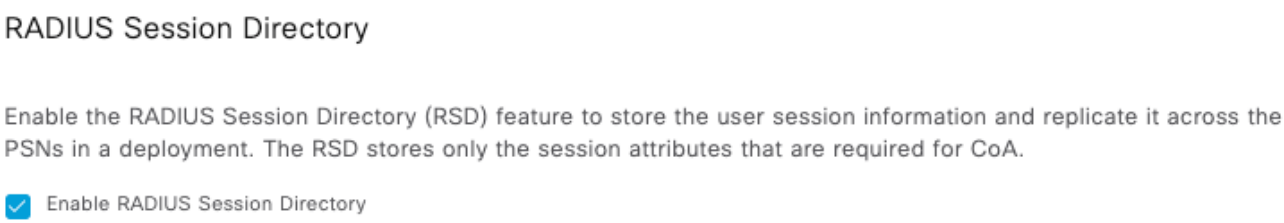
```
2024-12-01 00:58:17,191 DEBUG [PolicyEngineEvaluationThread-12][[]] cisco.cpm.posture.pip.PostureStatus
2024-12-01 00:58:17,191 DEBUG [PolicyEngineEvaluationThread-12][[]] cisco.cpm.posture.pip.PostureStatus
2024-12-01 00:58:17,191 DEBUG [PolicyEngineEvaluationThread-12][[]] cisco.cpm.posture.pip.PostureStatus

2024-12-01 00:58:56,722 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.runtim

2024-12-01 00:58:56,723 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.runtim
2024-12-01 00:58:56,723 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.runtim
2024-12-01 00:58:56,723 DEBUG [https-jsse-nio-10.127.197.170-8445-exec-10][[]] cisco.cpm.posture.edf.Po
```

Scenario 3 : Effect of Light Session Directory (LSD) on Posture Lease.

Enabling or disabling LSD does not affect the posture lease and last compliance status because both of these attributes are stored in Oracle DB and replicated across the deployment. Whereas, LSD stores limited EP attributes in the memory and replicates to other PSNs.

When LSD is enabled:

To enable LSD, navigate to **Administration > System > Settings > Light Data Distribution > Check RADIUS Session Directory**.



EP connects for the first time and goes through the posture check. Once the EP becomes compliant, it updates the Posture lease and last known compliance attributes in DB.

```
2024-12-02 19:36:43,274 DEBUG [PolicyEngineEvaluationThread-11][[]] cisco.cpm.posture.pip.PostureStatus
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
```

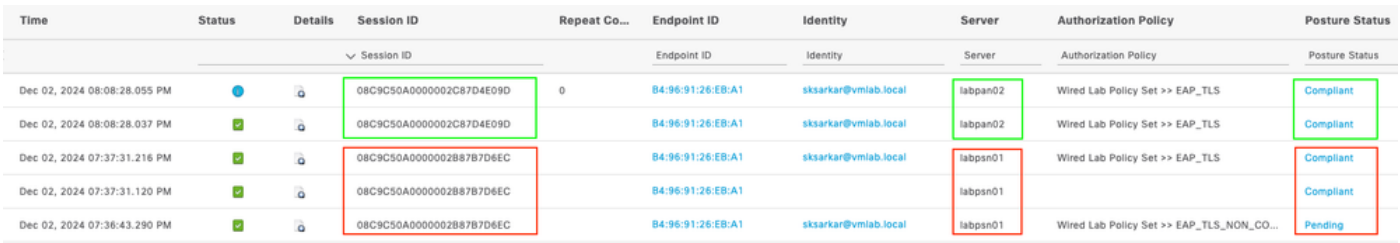
These are the attributes in LSD which are distributed across the PSN. You can see neither posture lease nor last compliance status is in the attributes.

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

Now, authenticate the EP with another PSN in the deployment.

After the authentication request lands on an another PSN, you can see the PSN retrieve the posture lease time from DB and mark the session directly as compliant. The same can be verified from the live logs.

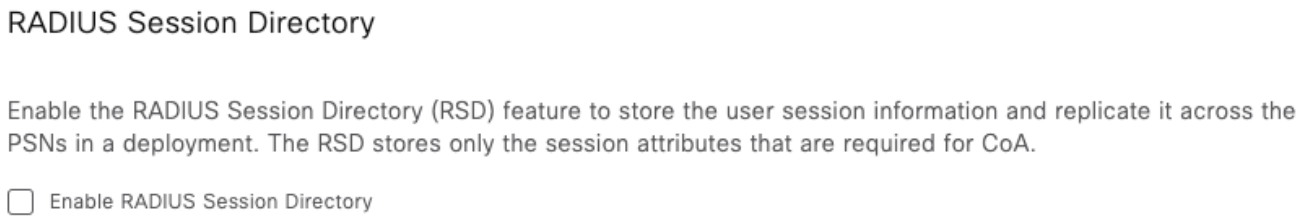
```
2024-12-02 20:08:27,449 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
2024-12-02 20:08:27,449 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
2024-12-02 20:08:27,468 DEBUG [PolicyEngineEvaluationThread-5][[]] cisco.cpm.posture.pip.PostureStatusP
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		Endpoint ID	Identity	Server	Authorization Policy	Posture Status
Dec 02, 2024 08:08:28.055 PM			08C9C50A0000002C87D4E09D	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			08C9C50A0000002C87D4E09D		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			08C9C50A0000002B87B7D6EC		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			08C9C50A0000002B87B7D6EC		B4:96:91:26:EB:A1		labpsn01		Compliant
Dec 02, 2024 07:36:43.290 PM			08C9C50A0000002B87B7D6EC		B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS_NON_CO...	Pending

When LSD is Disabled:

To disable LSD, navigate to **Administration > System > Settings > Light Data Distribution > Uncheck RADIUS Session Directory**.



EP Connects for the first time and goes through the posture process. Once the EP becomes compliant, it updates the Posture lease and last known compliance attributes in DB.

```
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
```

Now, authenticate the EP with another PSN in the deployment.

After the authentication request lands on an another PSN, you can see the PSN retrieve the posture lease time from DB and marks the session directly as compliant. The same can be verified from the live logs.

```
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			08C9C50A0000003187FADE13	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			08C9C50A0000003187FADE13		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			08C9C50A0000003087F1EE30		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			08C9C50A0000003087F1EE30		B4:96:91:26:EB:A1		labpsn01		Compliant
Dec 02, 2024 08:40:10.436 PM			08C9C50A0000003087F1EE30		B4:96:91:26:EB:A1	sksarkar@vmlab.local	labpsn01	Wired Lab Policy Set >> EAP_TLS_NON_CO...	Pending

From these two scenarios, you can confirm that LSD does not affect the Posture Lease.

Frequently Asked Questions

1. Is Posture Lease and Cached last known posture is independent of each other?

Yes, Posture Lease can be enabled without enabling the Cached last known posture and vice versa. Posture Lease saves the Endpoint Compliance statue as an endpoint attribute for the configured amount of time. Cached last known posture is the time saved in DB during which the Grace period is given if the Endpoint becomes non-compliant. This is not an endpoint attribute.

2. Is Posture Lease and Cached last known posture both replicated across the nodes?

Posture Lease is an endpoint attribute and is replicated across all the nodes. Cached last known posture is not an endpoint attribute but, as the value is in Oracle DB, it is also replicated to all the nodes.

3. Does reboot of the node remove these values?

No, as both of them are saved in the Oracle DB, reloading of nodes does not remove the values.

4. Does Posture Lease cause any Security issue?

When the posture lease is enable, ISE does not check for the posture status of the Endpoint. It can cause a security issue because if the Endpoint is not compliant, ISE can treat it as Complaint. It is recommended to use Posture Reassessment along with the Posture lease to minimize this risk.

Known Defects

Cisco bug ID CSCwk07454 PSN does not update the DB with the correct Posture Lease Expiry time.

Cisco bug ID CSCwi58421 PSN node not updating the DB with correct Posture expiry time when Posture lease is enabled.