Troubleshoot ISE Agentless Posture Not Triggering after Session Reauthentication

Contents

Issue

Agentless posture functionality in Identity Services Engine (ISE) 3.3 fails to trigger after session reauthentication events. During initial authentication, agentless posture works correctly and endpoints become compliant. However, when reauthentication occurs, endpoints receive RADIUS Accounting Interim Update events instead of Accounting Start events, causing the agentless posture flow not to be invoked. As a result, endpoints match an unknown posture policy and remain in an unknown posture state, impacting network access for affected devices.

The issue manifests with endpoints stuck in "Posture Pending" or "Unknown" status after reauthentication, with approximately 800 out of 1200 endpoints affected in the reported environment. Log analysis shows that during reauthentication, ISE receives ACCOUNTING_UPDATE events with agentlessEnabled=true but the posture flow is not re-invoked for the existing session ID.

Environment

- Identity Services Engine (ISE) version 3.3 Patch 4
- Wired 802.1X authentication with MAC Authentication Bypass (MAB)
- Agentless posture configuration enabled
- Session reauthentication timers configured (420 seconds timeout)
- Cisco Catalyst switches as network access devices
- Approximately 1200 endpoints in the environment

Resolution

This behavior is expected and by design in ISE. Agentless posture is only triggered by RADIUS Accounting Start events and is not to be re-invoked by Accounting Interim Update events during session reauthentication when the Framed IP address remains unchanged.

Technical Analysis

The ISE NetAccessEventHandler code path only re-arms the agentless posture flow on fresh RADIUS Accounting-Start packets. During reauthentication, network devices typically send Accounting Interim-Update packets with the same Acct-Session-Id, which causes the shouldInvokePostureFlow() function to return false, preventing posture re-evaluation.

Log evidence showing the behavior:

Initial Authentication (Agentless Posture Triggered):

```
2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle

2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

Reauthentication (Agentless Posture Not Triggered):

```
2026-04-01 11:35:37,669 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

Recommended Workaround

To mitigate the impact of this behavior, configure posture lease settings to maintain endpoint compliance during reauthentication scenarios:

Step 1: Configure **appropriate posture lease duration** in ISE posture policies to ensure endpoints do not lose network access between posture evaluations.

Step 2: Monitor **endpoint posture status** and adjust lease timers based on your organization's security requirements and reauthentication frequency.

Cause

This is expected behavior documented in Cisco Bug ID CSCwu48086. Agentless posture in ISE is designed to trigger only on RADIUS Accounting Start events and is not triggered by Interim Accounting Update events. During session reauthentication, network access devices send Accounting Interim Updates with the

same Framed IP address and session ID, which do not re-invoke the agentless posture evaluation process. The ISE code specifically checks for new sessions (ACCOUNTING_START events) before initiating agentless posture flows.

Related Content

- Cisco Bug ID CSCwu48086
- Cisco Technical Support & Downloads