

ISE 3.2 MDM Compliance Query Fails Due to Client Suppression and Software Defect

Contents

Issue

Some endpoints authenticated via EAP-TLS on Cisco Identity Services Engine (ISE) are intermittently not receiving a compliance status from Microsoft Intune, even though they are shown as compliant in the Intune dashboard. As a result, those endpoints hit a default wireless authorization policy instead of the expected Posture Compliant or Posture Non-Compliant policy. The affected endpoints do not show mobile device management (MDM) compliance attributes in ISE live logs or External MDM reports, and the issue affects only a subset of clients in the deployment.

Specific symptoms observed include:

- Abnormal clients do not have logs in ISE Report at External Mobile Device Management Report.
- Abnormal clients do not have attributes like MDM compliant status or device compliant status in live log details.
- Abnormal clients hit the wireless 802.1x_EAP-TLS_toyotawifi authorize policy instead of the Posture Compliant policy.
- Error messages in logs are showing "Failed to connect to MDM Server : 404 Not Found".

Environment

- Cisco ISE multi-node cluster version 3.2 patch 6
- 8 ISE nodes in the cluster, all showing green status
- 11,000 wireless/wired clients integrated with Microsoft Intune
- Clients use EAP-TLS (Machine Certificate) authentication
- ISE uses MAC address of the client for queries to Intune
- All clients have compliant status on Microsoft Intune dashboard

- Issue affects some clients but not all of them

Resolution

The issue was resolved through these steps.

Step 1: Identify Root Cause

Analysis of the ISE logs revealed that affected endpoints have stale MDM server ID preventing MDM queries from being executed.

The logs showed:

```
2026-06-15 13:35:14,343 DEBUG [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.util.MDMUtil -:::- M
2026-06-15 13:35:14,343 DEBUG [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.util.MdmServersCache -
2026-06-15 13:35:14,344 ERROR [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.pip.MdmPartnerPIPHandl
```

Additionally, the deployment was found to be hitting Cisco bug ID CSCwv51917, which affects MDM compliance lookups when using MAC address has stale MDM server ID.

Step 2: Temporary Workaround

As a temporary workaround:

- 1.- Delete the endpoint from Context Visibility and re-authenticate. This was observed to fix the issue of querying to the MDM server and getting compliance status.
- 2.- Navigate to **Context Visibility**.
- 3.- Select the endpoint mac-address and delete it.
- 4.- Re-authenticate the endpoint.

Step 3: Permanent Resolution - Software Upgrade

The permanent resolution is being tracked under Cisco bug ID CSCwv51917.

Cause

During authentication, ISE attempts to query the stale MDM server reference, but the corresponding MDM server object no longer exists or is inactive. Consequently, ISE does not retrieve MDM compliance attributes from Intune.

Related Content

- [Cisco bug ID CSCwv519173134](#)
- [ISE 3.2 Release Notes - Resolved Caveats](#)
- [ISE 3.2 End of Life Notice](#)
- [Cisco Technical Support & Downloads](#)