

ISE RCM Feature Causing Endpoint Deletion During Certificate-Based Authentication

Contents

Issue

During a migration from JAMF to Intune MDM for macOS devices, Cisco ISE unexpectedly deletes or merges endpoint records and changes endpoint identity group assignments during EAP-TLS authentication.

The affected endpoints are moved from the **DB_Authorized_Devices** identity group to **Profiled** triggering CoA events with the reason "Deletion of Endpoint." This results in endpoints being removed from the ISE internal database and causes authentication outages for affected devices. The issue occurs when devices switch between wireless and wired connections using the same certificate containing Subject Alternative Name (SAN) URI fields that ISE interprets as a GUID for the Random and Changing MAC (RCM) feature.

Environment

- Cisco Identity Services Engine (ISE) version 3.2
- macOS endpoints using EAP-TLS authentication
- Certificate-based authentication with SAN URI fields containing device identifiers
- Devices switching between wireless and wired network connections
- MDM migration from JAMF to Microsoft Intune
- RCM (Random and Changing MAC) feature enabled by default in ISE 3.2
- Endpoints managed via REST API with custom attributes

Resolution

The issue is caused by the RCM feature in ISE 3.2, which merges endpoint records based on certificate SAN URI fields. Two resolution options are available.

Option 1: Disable RCM Feature (Recommended with Caution)

Step 1: Access the ISE Swagger API Interface

Navigate to **Administration > Settings > API Settings** and click on the **/swagger-ui** link.

Step 2: Check Current LSD Settings

In the Swagger interface, find **LSD Settings** and execute a GET request to view current configuration:

```
GET /api/v1/lsd/settings
```

Step 3: Modify RCM Settings

Execute a PUT request with this request body to disable RCM:

```
{
  "enableEPO": true,
  "enableRCM": false
}
```

Step 4: Verify the Configuration Change

Execute the GET request again to confirm RCM is disabled and LSD remains enabled.

Step 5: Execute Cleanup Scripts

Run the recommended script operation to fix attribute discrepancies after RCM disabling. Monitor the infrastructure for any corner cases during this process.



Caution: Possible. The details mentioned here appears to contain procedures or commands that could cause significant impact if executed. Please ensure the procedures or commands have been evaluated by an SME or Business Unit before executing or recommending.

Option 2: Modify Authorization Policies

Adjust policy sets to account for RCM behavior by creating separate authorization logic for wired and wireless authentication flows, ensuring that merged endpoints receive appropriate access decisions based on connection type rather than identity group membership alone.

Certificate SAN URI Processing

ISE processes certificate SAN URI fields using specific logic to extract GUIDs. For certificates containing Microsoft Entra ID segments, ISE strips transient identity segments using the regex pattern:

```
tag:[a-zA-Z0-9.,-]+:sid:S-[0-9-]+[: ,]?
```

Examples of SAN URI processing:

- Input: "ID:Meraki:GUID:673288144292101809:tag:microsoft.com,2022-09-14:sid:S-1-5-21-2942795583-2590601415-1333022741-66482"
- Stored in session: "ID:Meraki:GUID:673288144292101809"

Cause

The RCM (Random and Changing MAC) feature enabled by default in ISE 3.2 interprets certificate SAN URI fields as GUIDs for endpoint identification. When devices using the same certificate connect via both wireless and wired interfaces, RCM merges the endpoint records based on the shared GUID. During this merge process, attributes from the wireless endpoint are migrated to the wired endpoint, and the wireless MAC entry is deleted from the endpoint database. This behavior occurs before CoA or DHCP probes and results in the loss of custom attributes and identity group assignments that were originally configured via

REST API. The merge process does not preserve custom attributes that are not part of profiling policies, leading to endpoint identity reset and subsequent authentication failures.

Related Content

- [Cisco Technical Support & Downloads](#)