

# 証明書ベースの認証中にエンドポイントが削除される原因となるISE RCM機能

## 内容

---

## 問題

MacOSデバイスのJAMFからIntune MDMへの移行中に、Cisco ISEが予期せずエンドポイントレコードを削除またはマージし、EAP-TLS認証中にエンドポイントIDグループの割り当てを変更します。

影響を受けるエンドポイントは、DB\_Authorized\_Devices IDグループからProfiledに移動され、「エンドポイントの削除」という理由でCoAイベントがトリガーされます。その結果、エンドポイントがISE内部データベースから削除され、該当するデバイスの認証が停止します。この問題は、ISEがRandom and Changing MAC(RCM)機能のGUIDとして解釈するSubject Alternative Name(SAN)URIフィールドを含む同じ証明書を使用して、デバイスがワイヤレス接続と有線接続を切り替えた場合に発生します。

## 環境

- Cisco Identity Services Engine(ISE)バージョン3.2
- eap-TLS認証を使用するMacOSエンドポイント
- デバイスIDを含むSAN URIフィールドによる証明書ベースの認証
- ワイヤレスネットワーク接続と有線ネットワーク接続を切り替えるデバイス
- JAMFからMicrosoft IntuneへのMDM移行
- ISE 3.2では、RCM(Random and Changing MAC)機能がデフォルトで有効になっている
- カスタム属性を使用してREST APIで管理されるエンドポイント

## 解決方法

この問題は、証明書SAN URIフィールドに基づいてエンドポイントレコードをマージするISE 3.2のRCM機能が原因で発生します。2つの解像度オプションを使用できます。

### オプション1:RCM機能を無効にする ( 注意して推奨 )

ステップ1:ISE Swagger APIインターフェイスにアクセスします。

Administration > Settings > API Settingsの順に移動し、/swagger-uiリンクをクリックします。

ステップ2：現在のLSD設定の確認

Swaggerインターフェイスで、LSD Settingsを探し、GETリクエストを実行して現在の設定を表示します。

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

ステップ3:RCM設定の変更

RCMを無効にするには、この要求本文でPUT要求を実行します。

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

## ステップ4：設定変更の確認

GET要求を再実行して、RCMが無効になっており、LSDが有効になっていることを確認します。

## ステップ5：クリーンアップスクリプトの実行

RCMを無効にした後、推奨されるスクリプト操作を実行して、属性の不一致を修正します。このプロセスの間に起こったコーナーケースについて、インフラストラクチャを監視します。



注意：可能です。ここで説明する詳細には、実行すると重大な影響を与える可能性のあるプロシージャまたはコマンドが含まれています。実行または推奨を行う前に、SMEまたはビジネスユニットによって手順またはコマンドが評価されていることを確認してください。

---

## オプション2：許可ポリシーの変更

有線とワイヤレスの認証フローに対して個別の許可ロジックを作成することで、RCMの動作に合わせてポリシーセットを調整します。これにより、マージされたエンドポイントは、IDグループメンバーシップだけではなく、接続タイプに基づいて適切なアクセス決定を受け取ることができます。

## 証明書SAN URIの処理

ISEは、特定のロジックを使用して証明書SAN URIフィールドを処理し、GUIDを抽出します。Microsoft Entra IDセグメントを含む証明書の場合、ISEは正規表現パターンを使用して一時的なIDセグメントを削除します。

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

SAN URI処理の例：

- 入力 : 「ID:Meraki:GUID:673288144292101809:tag:microsoft.com,2022-09-14:sid:S-1-5-21-2942795583-2590601415-1333022741-66482」
- セッション「ID:Meraki:GUID:673288144292101809」に保存

## 原因

ISE 3.2でデフォルトで有効になっているRCM(Random and Changing MAC)機能は、証明書のSAN URIフィールドをエンドポイント識別用のGUIDとして解釈します。同じ証明書を使用するデバイスが無線インターフェイスと有線インターフェイスの両方を介して接続する場合、RCMは共有GUIDに基づいてエンドポイントレコードをマージします。このマージプロセスでは、ワイヤレスエンドポイントの属性が有線エンドポイントに移行され、ワイヤレスMACエントリがエンドポイントデータベースから削除されます。この動作は、CoAまたはDHCPプローブの前に発生し、REST APIを使用して最初に設定されたカスタム属性とアイデンティティグループ割り当てが失われます。マージプロセスでは、プロファイリングポリシーの一部ではないカスタム属性は保持されず、エンドポイントIDのリセットとそれに続く認証の失敗につながります。

## 関連コンテンツ

- [シスコのテクニカルサポートとダウンロード](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。