



UEM および MDM サーバーと Cisco ISE の統合

- [Cisco ISE の統合エンドポイント管理の概要 \(1 ページ\)](#)
- [VPN 接続エンドポイントの MAC アドレス \(3 ページ\)](#)
- [その他の参考資料 \(3 ページ\)](#)
- [通信、サービス、およびその他の情報 \(4 ページ\)](#)

Cisco ISE の統合エンドポイント管理の概要

統合エンドポイント管理 (UEM) またはモバイルデバイス管理 (MDM) サーバーを使用して、ネットワークに配置されているエンドポイントを保護、監視、管理、およびサポートする場合は、これらのサーバーと相互運用するように Cisco ISE を設定できます。Cisco ISE とエンドポイント管理サーバーを統合して、API を介してこれらのサーバーからデバイス属性情報にアクセスします。その後、デバイス属性を使用してアクセスコントロールリスト (ACL) と許可ポリシーを作成し、ネットワーク アクセス コントロールを有効にできます。

Cisco ISE PSN は、設定されたポーリング間隔で、接続されている UEM または MDM サーバーから非準拠デバイスのリストを取得するための API も送信します。ポーリング時にアクティブなセッションを持つ非準拠エンドポイントは隔離され、取得された情報に基づいて Cisco ISE で CoA が発行されます。

このドキュメントでは、これらのサーバーを Cisco ISE と統合するためにエンドポイント管理サーバーで実行する必要がある設定について詳しく説明します。このドキュメントでは、現在、次の MDM または UEM ベンダーに必要な設定について詳しく説明しています。

- Cisco Meraki Systems Manager
- Ivanti (以前の MobileIron UEM) 、コアおよびクラウド UEM サービス
- Microsoft Endpoint Manager Intune

Cisco ISE は、次のエンドポイント管理サーバーもサポートしています。

- 42 ギア

- 絶対値 (Absolute)
- Blackberry : BES
- Blackberry : Good Secure EMM
- Citrix XenMobile 10.x (オンプレミス)
- Globo
- IBM MaaS360
- JAMF Casper Suite
- Microsoft Endpoint Configuration Manager
- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE (以前の AirWatch)



(注) Cisco ISE 3.0 以前のリリースは、Jamf Pro 10.42.0 以降と統合できません。

Cisco ISE に接続する MDM または UEM サーバーで必要な設定を実行した後、サーバーを Cisco ISE に参加させる必要があります。ご使用のリリースの『[Cisco ISE Administrator Guide](#)』の「Secure Access」の章にある「Configure Mobile Device Management Servers in Cisco ISE」を参照してください。

GUID の Cisco ISE MDM API バージョン 3

Cisco ISE リリース 3.1 では、エンドポイントの MAC アドレスをランダムに変更する機能が導入されています。Cisco ISE MDM API バージョン 3 を使用して、接続された MDM および UEM サーバーから GUID という名前の一意のエンドポイント識別子を受信できます。次に、Cisco ISE は MAC アドレスではなく GUID を使用してエンドポイントを識別します。ご使用のリリースの『[Cisco ISE Administrator Guide](#)』の「Secure Access」の章にある「Handle Random and Change MAC Addresses With Mobile Device Management Servers」を参照してください。

UEM または MDM サーバーから GUID を受信するには、次の条件を満たす必要があります。

- MDM または UEM サーバーが Cisco ISE MDM API バージョン 3 をサポートしている。
- UEM または MDM で、[サブジェクト代替名 (Subject Alternative Name)] フィールドまたは [共通名 (Common Name)] フィールド、あるいはその両方が GUID を Cisco ISE にプッシュするように、Cisco ISE の証明書の使用が設定されている。

次の UEM または MDM サーバーは現在、Cisco ISE MDM API バージョン 3 をサポートしています。

- Cisco Meraki Systems Manager
- Ivanti（以前の MobileIron UEM）、コアおよびクラウド UEM サービス
- Microsoft Endpoint Manager Intune
- JAMF Casper Suite
- VMware Workspace ONE（以前の AirWatch）



(注) VMware Workspace ONE の設定については、次を参照してください。

VPN 接続エンドポイントの MAC アドレス

Cisco ISE は、エンドポイントの MAC アドレスを使用して、データベースでエンドポイントデータを保存および管理し、コンテキストの可視性の情報を表示し、承認のワークフローを可能にします。

VPN 接続エンドポイントの場合、VPN ヘッドエンドは通常、エンドポイントの MAC アドレスまたは固有のデバイス ID (UDID)、またはその両方を Cisco Secure Client (旧称 Cisco AnyConnect) から受信し、RADIUS 通信経由で情報を Cisco ISE に送信します。

Cisco ISE を MDM サーバーと統合すると、Cisco ISE はエンドポイントの MAC アドレスまたは UDID のいずれかを使用して、エンドポイントの登録とコンプライアンスステータス、およびその他の MDM 属性値について MDM サーバーにクエリを実行します。

Cisco ISE がエンドポイントの UDID を使用して MDM サーバーにクエリを実行する場合、MDM サーバーからのコンプライアンス応答には、通常、エンドポイントの MAC アドレスが含まれます。Cisco Secure Client または MDM サーバーのいずれかからエンドポイントの MAC アドレスを受信することは、Cisco ISE にとって重要です。Cisco ISE は、MAC アドレスを使用して、データベース内のエンドポイントデータを保存および管理します。

その他の参考資料

Cisco ISE を使用するとき活用できるその他のリソースについては、『[Cisco ISE End-User Resources](#)』 [英語] を参照してください。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[Cisco Services](#) [英語] にアクセスしてください。
- サービス リクエストを送信するには、[Cisco Support](#) [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet](#) にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

シスコバグ検索ツール

[シスコバグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。