Microsoft Endpoint Manager Intune の統合

Microsoft Intune と Cisco ISE の統合の概要

Cisco ISE は、エンドポイント管理ソリューションである Microsoft Intune を MDM 統合としてサポートします。Microsoft Intune は、ネットワーク アクセス コントロール（NAC）サービスとして Cisco ISE をサポートし、2 つのシステム間の通信は、『Network access control (NAC) integration with Intune』[英語] で詳しく説明されているように、Microsoft の NAC 統合設計によって管理されます。

2024 年 3 月 24 日以降、Microsoft は MAC アドレスと UDID ベースのクエリをサポートする Intune NAC サービス API のサポートを終了します。Microsoft Compliance Retrieval API または NAC 2.0 API のみがサポートされます。NAC 2.0 API は、2023 年 7 月 31 日以降、GUID および MAC アドレスベースのクエリをサポートしています。

2024 年 3 月 24 日以降、Microsoft Intune 統合を引き続き使用するには、次のいずれかの Cisco ISE リリースにアップグレードする必要があります。

- Cisco ISE リリース 3.1 パッチ 8
- Cisco ISE リリース 3.2 パッチ 4

これらのリリース以前のパッチ、および Cisco ISE リリース 3.0 以前では、2024 年 3 月 24 日以降、接続されている Microsoft Intune サーバーからデバイス登録およびコンプライアンス情報を取得できません。

Microsoft の NAC 2.0 API を使用した場合、Cisco ISE は次のエンドポイント属性情報のみを取得できます。

- コンプライアンスステータス

- Intune による管理
- MAC アドレス（MAC Address）
- 登録済みステータス

Microsoft Endpoint Manager Intune の設定

ここでは、Microsoft Endpoint Manager Intune で通常実行する設定手順の一覧を記載します。組織のニーズに応じて、導入する必要のあるステップを選択してください。Cisco ISE リリース 3.1 以降のリリースを使用している場合は、Cisco ISE MDM API v3 のサポートを有効にして、Microsoft Intune から GUID を受信できます。このサポートを有効にするには、ステップ 2 およびステップ 3 で指定したように、証明書プロファイルでサブジェクト代替名（SAN）を設定します。SAN の設定では、Cisco ISE が Intune サーバーからエンドポイントの一意の GUID を受信し、ランダムに変化する MAC アドレスが原因で発生する問題を処理できるようにします。

標準の商用 Microsoft Azure 環境を使用していない場合は、Microsoft が運用するさまざまな国内のクラウドに対応する Graph API エンドポイントのリストについて、Microsoft の『National Cloud Deployments』のドキュメントを参照してください。

ステップ 1 Microsoft Intune でエンドポイント認証用の証明書を設定します。

ステップ 2 組織のニーズに応じて、次のいずれかの証明書管理プロトコルと対応する証明書プロファイルを設定します。

- Simple Certificate Enrollment Protocol（SCEP）

1. Microsoft Intune で SCEP をサポートするようにインフラストラクチャを設定します。
2. Microsoft Intune で SCEP 証明書プロファイルを作成して割り当てます。

- プライベートおよびパブリック キー インフラストラクチャ（PKI）

1. Microsoft Intune で PKCS 証明書を設定して使用します。
2. PKCS 証明書プロファイルを作成します。

（注） SCEP または PKI プロファイルを設定するには、[サブジェクト代替名（Subject Alternative Name）] エリアで [属性（Attribute）] として [URI] を選択し、[値（Value）] として **ID:Microsoft Endpoint Manager:GUID:{{DeviceId}}** を選択します。

ステップ 3 Wi-Fi および有線エンドポイントでは、プロファイルを作成し、[Subject Alternative Name] フィールドで前に GUID 値を含めて指定した SCEP または PKI 証明書プロファイルを選択します。

Microsoft Intune での Wi-Fi 設定の詳細については、『Add and use Wi-Fi settings on your devices in Microsoft Intune』を参照してください。

Intune で VPN プロファイルを作成して VPN サーバーに接続するには、証明書ベースの認証タイプを選択して、GUID 値を Cisco ISE と共有する必要があります。

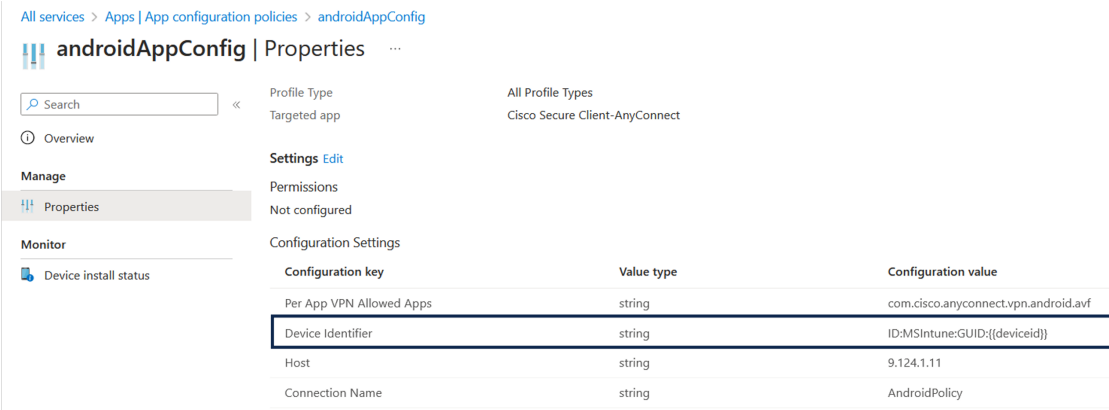
Microsoft Intune を使用した VPN 接続モバイルデバイスの管理

VPN 接続されたモバイルデバイスを管理するには、Microsoft Intune で次の設定が必要になります。

- **Microsoft Intune での VPN 接続された Android デバイスの設定**

  1. 『Android Enterprise device settings to configure VPN in Intune』[英語] に記載されている要件に従って、VPN 接続された Android エンドポイントの設定を行います。
  2. Cisco Secure Client-AnyConnect アプリを介して接続するエンドポイント向けに、Microsoft Intune でアプリ設定ポリシーを作成します。このポリシーでは、デバイス識別子設定キーを [Configuration Settings] に含める必要があります。

     図 *1 : Microsoft Intune* でのアプリケーション設定ポリシーの設定



- **Microsoft Intune での VPN 接続された iOS デバイスの設定**

  VPN 接続された iOS デバイスの場合、Microsoft Intune で必要な VPN 設定については、『Add VPN Settings on iOS and iPadOS devices in Microsoft Intune』[英語] を参照してください。

  iOS または iPadOS デバイスの VPN プロファイルを作成する際は、[Enable network access control (NAC)] 設定を選択して、Microsoft Intune がエンドポイントのデバイス ID を含めることができるようにする必要があることに注意してください。

設定が実行されると、Cisco AnyConnect ログに **ID:Intune:DeviceID:<*device id*>** の形式でデバイス識別子が記録されます。Cisco ISE API はエンドポイントのこのデバイス ID を取得し、エン

ドポイントのコンプライアンス情報を取得する場合はエンドポイントの MAC アドレスよりもデバイス ID を優先します。

Cisco ISE へのモバイルデバイス管理サーバーとしての Microsoft Intune の接続

Microsoft Intune は、2023 年 6 月 30 日に Azure AD Graph アプリケーションのサポートを終了しました。Azure AD Graph を使用するすべての統合を Microsoft Graph に移行する必要があります。Cisco ISE は通常、エンドポイント管理ソリューションである Microsoft Intune との統合に Azure AD Graph を使用しています。

Microsoft Intune との統合を成功させるには、Microsoft Graph アプリケーションをサポートする次の Cisco ISE リリースのいずれかにアップグレードする必要があります。

- Cisco ISE リリース 2.7 パッチ 7 以降
- Cisco ISE リリース 3.0 パッチ 5 以降
- Cisco ISE リリース 3.1 パッチ 3 以降
- Cisco ISE リリース 3.2 以降のリリース

Azure AD Graph から Microsoft Graph への移行の詳細については、次のリソースを参照してください。

- Azure AD Graph アプリの Microsoft Graph への移行
- Azure AD Graph から Microsoft Graph への移行に関するよくある質問
- アプリケーションを Microsoft Authentication Library と Microsoft Graph API を使用するように更新する

Cisco ISE をサポートされているバージョンのいずれかに更新した後、Cisco ISE の各 Microsoft Intune サーバーの統合で、[自動検出URL（Auto Discovery URL）] フィールドを手動で更新します（ステップ 32）。

https://graph.windows.net<*Directory (tenant) ID*> を **https://graph.microsoft.com** に置き換えます。

ステップ 1 Microsoft Azure ポータルにログインし、[Azure Active Directory] に移動します。

ステップ 2 **[管理（Manage）] > [アプリの登録（App registrations）]**を選択します。

ステップ 3 [新規登録（New Registration）] をクリックします。

ステップ 4 表示される [アプリケーションの登録（Register An Application）] ウィンドウで、[名前（Name）] フィールドに値を入力します。

ステップ 5 [サポートされているアカウントタイプ（Supported Account Types）] 領域で、[この組織ディレクトリ内のみのアカウント（Accounts in this organization directory only）] オプションボタンをクリックします。

ステップ 6 [Register] をクリックします。

新しく登録されたアプリケーションの [概要（Overview）] ウィンドウが表示されます。このウィンドウを開いた状態で、Cisco ISE 管理ポータルにログインします。

ステップ 7 Cisco ISE の GUI で、[Menu] アイコン（☰）をクリックし、次のように選択します。**[Administration]** > **[System]** > **[Certificates]** > **[System]** > **[Certificates]**

ステップ 8 表示される証明書のリストから、[デフォルトの自己署名サーバー証明書（Default self-signed server certificate）] チェックボックスまたは隣接するチェックボックスまたは [管理者（Admin）] 用に設定したその他の証明書を選択します。

ステップ 9 [エクスポート（Export）] をクリックします。

ステップ 10 表示されるダイアログボックスで、[証明書のみをエクスポート（Export Certificate Only）] オプションボタンをクリックし、[エクスポート（Export）] をクリックします。

ステップ 11 [表示（View）] をクリックして、この証明書の詳細を表示します。表示される [証明書の階層（Certificate Hierarchy）] ダイアログボックスで [フィンガープリント（Fingerprints）] 領域まで下方向にスクロールします。（これらの値は、後の手順で参照します。）

ステップ 12 Microsoft Azure Active Directory ポータルで、左側ペインの [Certificates & secrets] をクリックします。

ステップ 13 [証明書のアップロード（Upload Certificate）] をクリックし、Cisco ISE からエクスポートした証明書をアップロードします。

ステップ 14 証明書がアップロードされたら、ウィンドウに表示される [サムプリント（Thumbprint）] の値が Cisco ISE 証明書の [フィンガープリント（Fingerprint）] の値と一致することを確認します（ステップ 11）。

ステップ 15 左ペインで [マニフェスト（Manifest）] をクリックします。

ステップ 16 表示される内容で、[表示名（displayName）] の値を確認します。この値は、Cisco ISE 証明書に記載されている共通名と一致する必要があります。

ステップ 17 左側のペインで [API権限] をクリックします。

ステップ 18 [権限を追加（Add a permission）] をクリックし、次の権限を追加します。

API/権限名	タイプ	説明
Intune		
get_device_compliance	[アプリケーション（Application）]	Microsoft Intune からデバイスの状態とコンプライアンス情報を取得します。
Microsoft Graph		
Application.Read.All	Application	すべてのアプリケーションを読み取ります。

ステップ 19 **<テナント名>** の [管理者の同意を付与する（Grant admin consent）] をクリックします。

ステップ 20 アプリケーションの [概要（Overview）] ウィンドウの次の詳細をメモします。

- **アプリケーション（クライアント）ID**
- **ディレクトリ（テナント）ID**

ステップ 21 [概要（Overview）] ウィンドウで [エンドポイント（Endpoints）] をクリックし、[Oauth 2.0 トークンのエンドポイント（V2）（Oauth 2.0 Token Endpoint（V2））] フィールドに値をメモします。

ステップ 22 PEM（チェーン）形式で https://www.digicert.com/kb/digicert-root-certificates.htm から Microsoft Intune 証明書をダウンロードします。

Microsoft は、新しい証明書を定期的にリリースしています。「Connection Failed to the MDM server: There is a problem with the server Certificates or ISE trust store」というエラーが表示されて統合が失敗した場合は、Cisco ISE PAN でパケットキャプチャを実行して、MDM サーバーによって送信された正確な証明書を確認することを推奨します。使用中の証明書がわかっている場合は、Microsoft PKI リポジトリから証明書をダウンロードできます。Cisco ISE と Microsoft Intune 間の信頼された通信のために必要な証明書をダウンロードしてください。

（注） Microsoft Intune と Cisco ISE 間の正常な接続を有効にするには、新しいルート証明書をインポートする必要があります。「Intune 証明書の更新：継続的な接続にはアクションが必要な場合があります」を参照してください。

ステップ 23 Cisco ISE 管理ポータルで、**[Menu]** アイコン（≡）をクリックし、**[Administration]** > **[System]** > **[Certificates]** > **[Trusted Certificates]** を選択します。

ステップ 24 ダウンロードした 4 つの証明書のそれぞれについて次の手順を実行します。

1. [インポート（Import）] をクリックします。
2. [ファイルの選択（Choose File）] をクリックし、システムから対応するダウンロードした証明書を選択します。
3. 証明書をインフラストラクチャとシスコサービスで使用するために信頼できるようにします。[使用目的（Usage）] 領域で、[ISE 内の認証用に信頼する（Trust for authentication within ISE）] と [シスコサービスの認証用に信頼する（Trust for authentication of Cisco Services）] のチェックボックスをオンにします。
4. [Save] をクリックします。

ステップ 25 [Menu] アイコン（≡）をクリックし、次のように選択します。 **[Administration]** > **[Network Resources]** > **[External MDM]**

ステップ 26 [Add] をクリックします。

ステップ 27 [名前（Name）] フィールドに値を入力します。

ステップ 28 [認証タイプ（Authentication Type）] ドロップダウンリストから [OAuth：クライアントクレデンシャル（OAuth – Client Credentials）] を選択します。

ステップ 29 次のフィールドには、Microsoft Azure Active Directory の Microsoft Intune アプリケーションからの情報が必要です。

- [Auto Discovery URL] フィールドに **https://graph.microsoft.com** と入力します。

（注） Microsoft Intune が Azure AD Graph アプリケーションをサポートしていたときは、URL **https://graph.windows.net<*Directory (tenant) ID*>** が使用されていました。 しかしながら、Microsoft Intune は、2023 年 6 月 30 日に Azure AD Graph アプリケーションのサポートを終了しました。統合を成功させるには、Microsoft Graph をサポートする Cisco ISE リリースにアップグレードしてください。

次の Cisco ISE リリースは、Microsoft Graph アプリケーションをサポートしています。

- Cisco ISE リリース 2.7 パッチ 7 以降
- Cisco ISE リリース 3.0 パッチ 5 以降
- Cisco ISE リリース 3.1 パッチ 3 以降
- Cisco ISE リリース 3.2 以降のリリース

- [クライアント ID（Client ID）] フィールドに、Microsoft Intune アプリケーションの [アプリケーション（クライアント）ID（Client ID）] の値を入力します。
- [トークン発行URL（Token Issuing URL）] フィールドに、[Oauth 2.0 トークンのエンドポイント（V2）（Oauth 2.0 Token Endpoint (V2)）] の値を入力します。
- Cisco ISE の次のリリースを使用する場合は、[Token Audience] フィールドに **https://api.manage.microsoft.com//.default** と入力します。
  - Cisco ISE リリース 3.0 パッチ 8 以降のリリース
  - Cisco ISE リリース 3.1 パッチ 8 以降のリリース
  - Cisco ISE リリース 3.2 パッチ 3 以降のリリース
  - Cisco ISE リリース 3.3 以降のリリース

（注） 上記の Cisco ISE リリースでは、新しい統合を作成する場合、ステップ 31 で [OAuth – Client Credentials] を選択すると、新しいトークン対象者の値が自動的に入力されます。既存の統合を使用してこれらのリリースにアップグレードする場合、統合サーバーから更新を受信し続けるには、[Token Audience] フィールドを手動で更新する必要があります。

これは、Microsoft が、認証と認可に Azure Active Directory Authentication Library（ADAL）を使用するアプリケーションを Microsoft Authentication Library（MSAL）に移行することを義務付けているためです。詳細については、「Microsoft Authentication Library（MSAL）へのアプリケーションの移行」を参照してください。

Cisco ISE の他のリリースでは、**https://api.manage.microsoft.com/** と入力します。

ステップ 30 [ポーリング間隔（Polling Interval）] フィールドと [準拠デバイス再認証クエリの間隔（Time Interval For Compliance Device ReAuth Query）] フィールドに必要な値を入力します。

ステップ 31 [テスト接続（Test Connection）] をクリックして、Cisco ISE が Microsoft サーバーに接続できることを確認します。

ステップ 32 テスト接続が成功したら、[ステータス（Status）] ドロップダウンリストから [有効（Enabled）] を選択します。

ステップ 33 [Save] をクリックします。

ステップ 34 Cisco ISE の管理ポータルで、[Menu] アイコン（☰）をクリックして、**[Administration]** > **[Network Resources]** > **[External MDM]**を選択します。追加された Microsoft Intune サーバーは、表示される [MDM サーバー（MDM Servers）] のリストに表示される必要があります。

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。