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

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

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
- 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

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。

Cisco Meraki Systems Manager の設定

Cisco Meraki Systems Manager はさまざまなプラットフォームをサポートし、一般的となっている多様なデバイスエコシステムを実現します。Systems Manager は成長している組織に向け、広範囲に及ぶ拡張性を備えたエンドポイント管理用の一元化されたクラウドベースのツールを提供します。Cisco Meraki Systems Manager を Cisco ISE の MDM サーバーとして統合し、コンプライアンスチェックとエンドポイントポリシー管理のために Cisco Meraki Systems Manager によって収集されたエンドポイント情報を活用します。

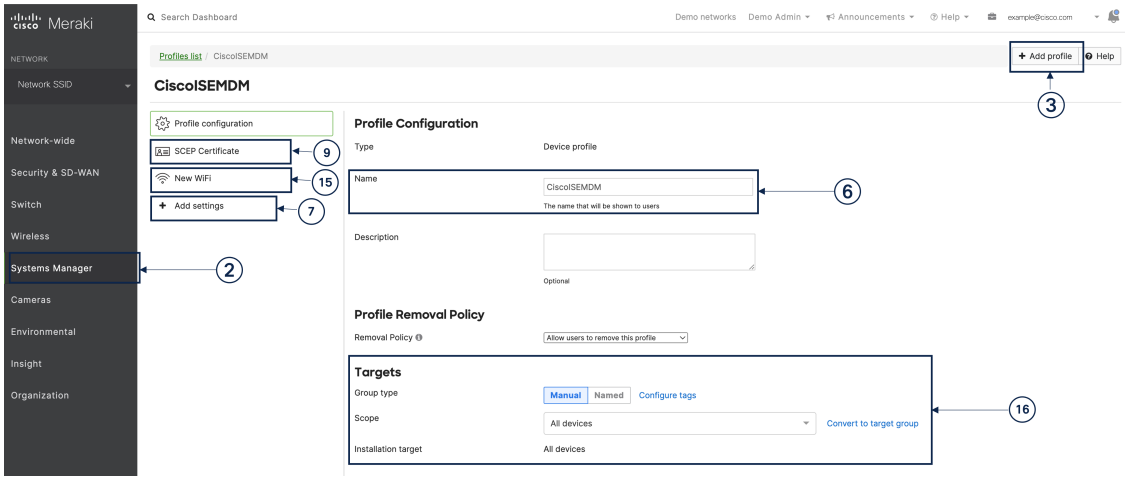
Cisco Meraki Systems Manager の詳細については、データシートを参照してください。

Cisco Meraki Systems Manager は、MDM API バージョン 3 をサポートし、接続されたエンドポイントの一意のデバイス識別子を Cisco ISE に提供できるようになりました。Cisco ISE でアクティブな Cisco Meraki Systems Manager 統合がすでにある場合は、Cisco Meraki Systems Manager で Cisco ISE 関連のデバイスプロファイルに対してステップ 8 ～ 15 を実行します。

Cisco Meraki Systems Manager を MDM または UEM サーバーとして設定する

このセクションの画像は、このタスク中に操作する必要がある Cisco Meraki Systems Manager の GUI フィールドを示しています。画像中の番号は、タスクのステップの番号に対応しています。

図 *1 : Cisco Meraki Systems Manager* を設定するためのステップ



始める前に

Cisco ISE で、管理者用に設定されたシステム証明書を作成してエクスポートします。この証明書は、次のタスクのステップ 12 で使用します。

システム証明書を作成およびエクスポートする方法については、ご使用のリリースの『Cisco ISE Administrator Guide』の「Basic Setup」の章の「System Certificates」のトピックを参照してください。

ステップ 1 Cisco Meraki Systems Manager ポータルにログインします。

ステップ 2 メインメニューから、**[システムマネージャ（Systems Manager）]>[管理（Manage）]>[設定（Settings）]** に移動します。

ステップ 3 [+プロファイルの追加（+ Add Profile）] をクリックします。

ステップ 4 表示される [新しいプロファイルの追加（Add New Profile dialog）] ダイアログボックスで、[デバイスプロファイル（デフォルト）（Device profile（Default））] ラジオボタンをクリックします。

ステップ 5 [続行（Continue）] をクリックします。

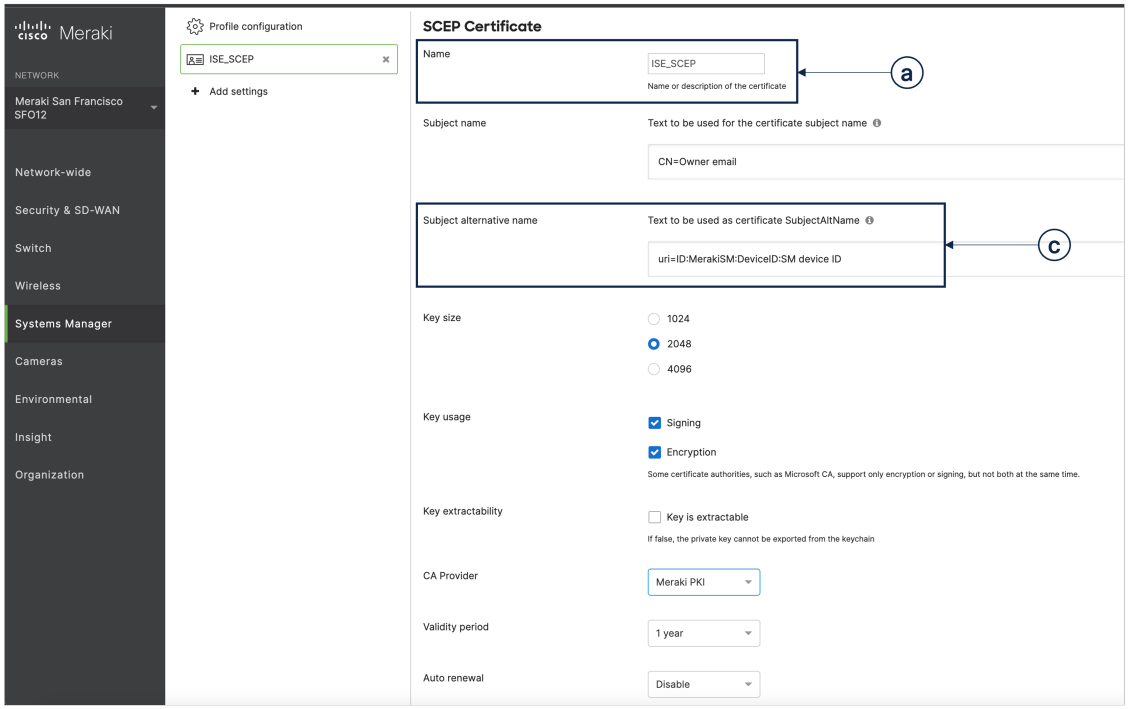
ステップ 6 [名前（Name）] フィールドおよび [説明（Description）] フィールドに必要な値を入力します。

ステップ 7 [+設定の追加（+Add Setting）] をクリックします。

ステップ 8 表示される [新しい設定ペイロードの追加（Add New Settings Payload）] ウィンドウで、[SCEP証明書（SCEP Certificate）] をクリックします。

ステップ 9 表示される [SCEP証明書（SCEP Certificate）] ウィンドウで以下のステップを実行します。

図 *2 : Cisco Meraki Systems Manager* の *[SCEP*証明書の設定（*SCEP Certificate Configuration*）*]* ウィンドウ



a) [名前（Name）] フィールドに、SCEP 証明書の名前を入力します。たとえば、**ISE_SCEP** などです。
b) [サブジェクト名（Subject name）] フィールドに、証明書の共通名の値を入力します。
c) [サブジェクト代替名（Subject alternative name）] フィールドに、**uri=ID:MerakiSM:DeviceID:$SM Device ID** と入力します。

   $ を入力すると、変数のドロップダウンリストが表示されます。リストから [SMデバイスID（SM Device ID）] を選択します。

d) [キーサイズ（Key Size）] エリアで、[2048] ラジオボタンをクリックします。
e) [キーの用途（Key Usage）] エリアで、[署名（Signing）] と [暗号化（Encryption）] チェックボックスをオンにします。
f) [CAプロバイダー（CA Provider）] エリアで、ドロップダウンリストから [CAプロバイダー（CA Provider）] を選択します。
g) [保存（Save）] をクリックします。

ステップ 10 [+設定の追加（+Add Setting）] をクリックします。

ステップ 11 表示される [新しい設定ペイロードの追加（Add New Settings Payload）] ウィンドウで、[証明書（Certificate）] をクリックします。

ステップ 12 表示される [証明書（Certificate）] ウィンドウで以下のステップを実行します。

a) [名前（Name）] フィールドに、証明書の名前を入力します。
b) [CertStore] ドロップダウンリストから、[システム（System）] を選択します。
c) [証明書（Certificate）] フィールドで、[ファイルの選択（Choose File）] をクリックし、このタスクの前提条件としてダウンロードした Cisco ISE のシステム証明書をアップロードします。

d) [保存（Save）] をクリックします。

ステップ 13 [+設定の追加（+Add Setting）] をクリックします。

ステップ 14 表示される [新しい設定ペイロードの追加（Add New Settings Payload）] ウィンドウで、[Wi-Fi設定（WiFi Settings）] をクリックします。

ステップ 15 表示される [Wi-Fi設定（WiFi Settings）] ウィンドウで以下のステップを実行します。

a) [SSID] フィールドに、参加する Wi-Fi ネットワークの名前を入力します。

b) [セキュリティ（Security）] ドロップダウンリストから、Wi-Fi Protected Access（WPA）オプションのいずれかを選択します。

c) [セキュリティ（Security）] ドロップダウンリストからエンタープライズオプションを選択すると表示される [エンタープライズ設定（Enterprise Settings）] エリアで、以下のステップを実行します。

1. [プロトコル（Protocol）] タブで、TLS などの証明書ベースのプロトコルのチェックボックスをオンにします。
2. [認証（Authentication）] タブの [ID証明書（Identity Certificate）] エリアで、ドロップダウンリストから、ステップ 10 で Cisco ISE のユースケースで作成した SCEP 証明書を選択します。
3. [トラスト（Trust）] タブの [信頼できる証明書（Trusted Certificates）] エリアで、ステップ 12 でアップロードした Cisco ISE 証明書の横にあるチェックボックスをオンにします。
4. [保存（Save）] をクリックします。

ステップ 16 [プロファイル設定（Profile Configuration）] タブの [ターゲット（Targets）] エリアで、ISE のユースケースのタグを追加します。Meraki Systems Manager でタグを作成および管理する方法については、『Manage Tags』を参照してください。タグを適用することで、関連するデバイスに証明書と Wi-Fi 設定を含む ISE プロファイルが適用されます。

ステップ 17 [保存されていない変更があります（You have unsaved changes）] ダイアログボックスで、[保存（Save）] をクリックします。

ステップ 18 左側のメニューペインから、[組織（Organization）] > [設定（Configure）] > [MDM] を選択します。

ステップ 19 [ISE設定（ISE Settings）] エリアから以下のステップを実行します。

a) Cisco ISE に入力する必要があるユーザー名とパスワードの詳細を書き留めます。

b) Cisco ISE で使用する必要がある SCEP 証明書をダウンロードするには、[ダウンロード（Download）] ボタンをクリックします。

次のタスク

次に、Cisco Meraki Systems Manager を Cisco ISE の MDM サーバーとして接続します。このタスクの実行方法についての詳細は、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。

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 を使用し、Cisco ISE MDM API v3 のサポートを有効にして Microsoft Intune から GUID を受信する場合は、ステップ 2 およびステップ 3 で示されているように、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 プロファイルを作成し、[サブジェクト代替名（Subject Alternative Name）] フィールドには、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。

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 は Azure Active Directory（Azure AD）Graph を廃止しており、2022 年 6 月 30 日以降、Azure AD Graph 対応の統合をサポートしません。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 Microsoft Intune との統合に Azure AD Graph を使用します。Cisco ISE と、Azure AD Graph アプリケーション（https://graph.windows.net/<*Directory (tenant) ID*>）をまだ使用している Microsoft Intune 間の統合は、2022 年 6 月 30 日以降は機能しません。

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

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
- Cisco ISE リリース 3.0 パッチ 5
- Cisco ISE リリース 3.1 パッチ 2

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 [登録（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、[メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム（System）] > [証明書（Certificates）]** をクリックします。

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、左側のウィンドウの [証明書とシークレット（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		
Directory.Read.All	[委任（Delegated）]	ディレクトリデータを読み取ります。
Directory.Read.All	[アプリケーション（Application）]	ディレクトリデータを読み取ります。
offline_access	[委任（Delegated）]	アクセス権が付与されたデータへのアクセスを維持します。
openid	[委任（Delegated）]	ユーザーにサインインします。
User.Read	[委任（Delegated）]	ユーザーにサインインし、ユーザープロファイルを読み取ります。

API/権限名	タイプ	説明
User.Read.All	[委任（Delegated）]	すべてのユーザーの完全なプロファイルを読み取ります。
User.Read.All	[アプリケーション（Application）]	すべてのユーザーの完全なプロファイルを読み取ります。

ステップ 19 左側のペインから、**[API権限（API permissions）]** > **[権限を追加（Add a permission）]** > **[組織で使用されるAPI（APIs my organization uses）]**の順に選択します。

ステップ 20 **Windows Azure Active Directory** を検索し、検索結果から同じものを選択します。

ステップ 21 次の権限を追加します：

API/権限名	タイプ	説明
Azure Active Directory Graph		
Directory.Read.All	[委任（Delegated）]	ディレクトリデータを読み取ります
Directory.Read.All	[アプリケーション（Application）]	ディレクトリデータを読み取ります
User.Read.All	[委任（Delegated）]	すべてのユーザの完全なプロファイルを読む取ります。

権限を追加した後の最終的なテーブルは、次のようになります。

図 *3 : Microsoft Intune* で設定する必要のある *API* と権限

API / Permissions name	Type	Description	Admin consent requ...	Status
Azure Active Directory Graph (3)				
Directory.Read.All	Delegated	Read directory data	Yes	Granted
Directory.Read.All	Application	Read directory data	Yes	Granted
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted
Intune (1)				
get_device_compliance	Application	Get device state and compliance information from Micros...	Yes	Granted
Microsoft Graph (7)				
Directory.Read.All	Delegated	Read directory data	Yes	Granted
Directory.Read.All	Application	Read directory data	Yes	Granted
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted
openid	Delegated	Sign users in	No	Granted
User.Read	Delegated	Sign in and read user profile	No	Granted
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted
User.Read.All	Application	Read all users' full profiles	Yes	Granted

ステップ 22 **<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 23 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 24 [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 25 PEM（チェーン）形式で https://fef.manage.microsoft.com/ から次の証明書をダウンロードします。

- Baltimore CyberTrust Root
- DigiCert SHA2 Secure Server CA
- DigiCert Global Root CA
- DigiCert Global Root G2
- CA 01 発行の Microsoft Azure TLS
- CA 02 発行の Microsoft Azure TLS
- CA 05 発行の Microsoft Azure TLS
- CA 06 発行の Microsoft Azure TLS

Microsoft PKI リポジトリから CA 証明書の発行の Microsoft Azure TLS をダウンロードできます。

（注） Microsoft Intune 証明書が更新されました。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 26 Cisco ISE 管理ポータルで、click the **Menu** icon (☰) をクリックし、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 27 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. [保存（Save）] をクリックします。

ステップ 28 [メニュー（Menu）] アイコン（☰）をクリックし、**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [外部MDM（External MDM）]**の順に選択します。

ステップ 29 [追加（Add）] をクリックします。

ステップ 30 [名前（Name）] フィールドに値を入力します。

ステップ 31 [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 32 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。

- [自動検出URL（Auto Discovery URL）] フィールドに **https://graph.microsoft.com/<*Directory (tenant) ID*>** と入力します。
- [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。
- [トークンの対象者（Token Audience）] フィールドに、https://api.manage.microsoft.com/ と入力します。

.

ステップ 33 [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 34 [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 35 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 36 [保存（Save）] をクリックします。

ステップ 37 Cisco ISE の管理ポータルで、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [ネットワークリソース（Network Resources）] > [外部 MDM（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。

Ivanti（以前の MobileIron）統合エンドポイント管理サーバーの設定

（注） MobileIron は Ivanti に買収されました。MobileIron は、このドキュメントの執筆時点で、MobileIron Core（オンプレミス）や MobileIron Cloud などの統合エンドポイント管理（UEM）ソリューションを引き続き提供しています。

Cisco ISE リリース 3.1 は、BasicAuth フレームワークを介して API を利用して MobileIron Core または MobileIron Cloud サーバーに接続し、これらのサーバーから GUID 値を受信します。次

に Cisco ISE は MAC アドレスの代わりに GUID 値を使用してエンドポイントを識別し、MAC アドレスのランダム化が使用されている場合でも信頼できる認証を可能にします。

GUIDベースの認証は、X509またはアイデンティティ証明書とも呼ばれるクライアント証明書を使用して行われます。次のタスクを実行して、MobileIron CloudまたはMobileIron Core サーバーから Cisco ISE に送信される証明書を設定し、GUID 値を含めます。

MobileIron Core 11.3.0.0 ビルド 24 以降のリリースでは、Cisco ISE への GUID のプロビジョニングがサポートされています。

MobileIron Cloud または MobileIron Core の管理者ポータルでは次が実行されます：

1. ユーザーアカウントを作成し、必要な API 権限を割り当てます。
2. 認証局を設定します。
3. GUID 情報を含めるようにアイデンティティ証明書を設定します。
4. 必要に応じて、ルート証明書または信頼できる証明書をアップロードします。
5. Wi-Fi プロファイルを設定します。

（注） MobileIron Cloud または MobileIron Core サーバーをすでに CiscoI SE リリース 3.1 に接続していて、接続されたサーバから GUID を受信する場合は、必要に応じてステップ 3、4、および 5 を実行します。

既存のアイデンティティ証明書または Wi-Fi 設定、あるいはその両方を編集すると、MobileIron は更新された設定を接続された管理対象デバイスに再公開します。MobileIron は、自己署名証明書またはローカル CA の使用を推奨していません。このガイドでは、自己署名証明書とローカル CA の手順を例として説明し、CiscoI SE リリース 3.1 でランダムおよび変更された MAC アドレスを処理するために必要なサブジェクトおよびサブジェクト代替名属性の設定を強調します。

Cisco ISE で、次の手順を実行します。

1. Cisco ISE の MobileIron ポータルで生成された証明書をアップロードします。
2. MobileIron UEM サーバーを Cisco ISE に接続します。

MobileIron Cloud UEM サーバーの設定

ここでは、大規模な MobileIron Cloud UEM サーバーを設定するためのさまざまな手順について説明します。

MobileIron Cloud のユーザーアカウントの作成と Cisco ISE の運用ロールの割り当て

ステップ 1 MobileIron Cloud ポータルにログインします。

ステップ 2 トップメニューから [ユーザー（Users）] を選択します。

ステップ 3 [Add（追加）] ドロップダウンリストから、[APIユーザーを追加（Add API User）] を選択します。

ステップ 4 [APIユーザーを追加（Add API User）] ウィンドウで、次のフィールドに値を入力します。

- **[ユーザー名（Username）]**
- **電子メール アドレス（Email Address）**
- **[名（First Name）]**
- **[姓（Last Name）]**
- **Password**
- **Confirm Password**

ステップ 5 ユーザーが Cisco ISE の統合に必要な API を起動できるようにするには、[ロールの割り当て（Assign Roles）] 領域で [Cisco ISE の運用（Cisco ISE Operations）] チェックボックスをオンにします。

ステップ 6 [完了（Done）] をクリックします。

MobileIron Cloud での認証局の設定

この手順では、ローカル CA を設定する方法について説明します。ただし、MobileIron Cloud では、より広範な CA 設定から選択できます。組織の要件に最適なオプションを選択してください。

MobileIron Cloud でサポートされているさまざまなタイプの証明書管理については、http://mi.extendedhelp.mobileiron.com/75/all/en/Welcome.htm#LocalCertificates.htmを参照してください。

ステップ 1 MobileIron Cloud ポータルで、**[管理（Admin）]** > **[証明書の管理（Certificate Management）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [スタンドアロン認証局の作成（Create a Standalone Certificate Authority）] をクリックします。

ステップ 4 表示されたダイアログボックスで、次のフィールドに詳細情報を入力します。

1. **Name**
2. [サブジェクトパラメータ（Subject Parameters）] 領域で、次のフィールドの少なくとも 1 つに値を入力します。
   - **Common Name**
   - **Email**
   - **組織単位（Organisation Unit）**
   - **Organisation**
   - **Street Address**

- 市区町村郡（City）
- リージョン（Region）
- 国

3. [キー生成パラメータ（Key Generation Parameters）] 領域で、次の手順を実行します。
   - [キータイプ（Key Type）] ドロップダウンリストから [RSA] を選択します。
   - [署名アルゴリズム（Signature Algorithm）] ドロップダウンリストから [SHA256withRSA] を選択します。
   - [キーの長さ（Key Length）] ドロップダウンリストから [2048] を選択します。

MobileIron Cloud でのルート証明書または信頼できる証明書のアップロード

信頼できるサードパーティ CA を使用してアイデンティティ証明書を生成する場合は、このタスクを無視できます。

ローカルの MobileIron Cloud CA または社内や組織にプライベートな内部 CA を使用する場合は、CA のルート証明書をアップロードして、接続先のデバイスに配布する必要があります。これにより、デバイスは認証に使用されるアイデンティティ証明書の送信元または発行元を信頼できるようになります。

ステップ 1 [MobileIron Cloud] メニューから [設定（Configurations）] を選択します。

ステップ 2 [追加（Add）] をクリックし、[証明書（Certificates）] を選択します。

ステップ 3 [名前（Name）] フィールドに、信頼できる証明書の名前を入力します。

ステップ 4 [設定のセットアップ（Configuration Setup）] エリアで、[ファイルの選択（Choose File）] をクリックし、CA の信頼できる証明書またはルート証明書を選択します。

ステップ 5 [次へ（Next）] をクリックします。

MobileIron Cloud でのアイデンティティ証明書の設定

MobileIron Cloud でアイデンティティ証明書を設定し、モバイルデバイスの証明書認証メカニズムを定義します。アイデンティティ証明書は、X.509 証明書（.p12 または .pfx ファイル）です。認証局をソースとして使用して、アイデンティティ証明書を動的に生成することもできます。

（注） Cisco ISE MDM の使用例用に設定された既存のアイデンティティ証明書が MobileIron Cloud にある場合は、この手順のステップ 5 に従って証明書を変更し、MobileIron サーバーから GUID 情報を受信します。

ステップ 1 MobileIron Cloud のトップメニューから [設定（Configurations）] を選択し、[アイデンティティ証明書（Identity Certificate）] をクリックします。

ステップ 2 [名前（Name）] フィールドに値を入力します。

ステップ 3 [設定のセットアップ（Configuration Setup）] 領域で、ドロップダウンリストから [動的に設定（Dynamically Generated）] を選択します。

ステップ 4 [送信元（Source）] ドロップダウンリストから、「MobileIron Cloud での認証局の設定」の手順で設定した CA を選択します。

ステップ 5 [サブジェクト代替名タイプ（Subject Alternative Name Type）] ドロップダウンリストから、[ユニフォームリソース識別子（Uniform Resource Identifier）] を選択します。

ステップ 6 [サブジェクト代替名の値（Subject Alternative Name Value）] フィールドに、**ID:Mobileiron:${deviceGUID}** と入力します。GUID の [サブジェクト代替名（Subject Alternative Name）] フィールドを設定することをお勧めします。

ステップ 7 （任意） または、[共通名（Common Name）] フィールドを使用して GUID をCisco ISE にプッシュするには、[件名（Subject）] フィールドに **CN=ID:Mobileiron:${deviceGUID}** と入力します。

ステップ 8 [設定をテストし続行（Test Configuration and Continue）] をクリックします。
[設定テストが正常に完了しました（Configuration Test Successful）] ダイアログボックスに、作成したアイデンティティ証明書の詳細が表示されます。

ステップ 9 [配布（Distribute）] ウィンドウで [カスタム（Custom）] をクリックします。

ステップ 10 [デバイスグループの配布の定義（Define Device Group Distribution）] 領域で、この設定で配布するデバイスグループのチェックボックスをオンにします。

ステップ 11 [完了（Done）] をクリックします。

ステップ 12 Cisco ISE MDM の使用例で既存のアイデンティティ証明書の SAN フィールドまたは CN フィールドを更新した場合は、更新された証明書をネットワークに接続されているエンドユーザーに送信する必要があります。更新された証明書をエンドユーザーに送信するには、**[設定（Configurations）]**>**[コンフィグを選択（Choose Config）** > **[編集（Edit）]** ウィンドウで、[キャッシュされた証明書をクリアし、最新の更新を使用して新しい証明書を発行します（Clear cached certificates and issue new ones with recent updates）] チェックボックスをオンにします。

MobileIron Cloud での Wi-Fi プロファイルの設定

すでに管理対象の iOS や Android デバイスに Wi-Fi プロファイルを展開している場合は、Wi-Fi プロファイルを編集して最新のアイデンティティ証明書を設定します。これでコネクティッドデバイスでは、サブジェクト名またはサブジェクト代替名の属性に GUID が設定された、新しいアイデンティティ証明書が受信されるようになります。

ステップ 1 [MobileIron Cloud] メニューから [設定（Configurations）] を選択し、[Wi-Fi] をクリックします。

ステップ 2 [名前（Name）] フィールドに値を入力します。

ステップ 3 [サービスセット識別子（SSID）（Service Set Identifier (SSID)）] フィールドにネットワークの名前を入力します。

ステップ 4 デフォルトでは、[自動参加（Auto Join）] チェックボックスはオンになっています。変更しないでください。

ステップ 5 [セキュリティタイプ（Security Type）] ドロップダウンリストから必要なオプションを選択します。

ステップ 6 [エンタープライズ設定（Enterprise Settings）] 領域の [プロトコル（Protocols）] タブで、[TLS] チェックボックスをオンにします。

ステップ 7 [認証（Authentication）] タブで、[ユーザー名（Username）] フィールドと [パスワード（Password）] フィールドに必要な値を入力します。

ステップ 8 [アイデンティティ証明書（Identity Certificate）] ドロップダウンリストから、手順内で作成したアイデンティティ証明書を選択しますMobileIron Cloud でのアイデンティティ証明書の設定 （15 ページ）。

ステップ 9 （任意） [信頼（Trust）] タブで、使用する信頼できる証明書のチェックボックスをオンにします。

ステップ 10 [すべてのバージョン（All Versions）] 領域で、[ネットワークタイプ（Network Type）] ドロップダウンリストから [標準（Standard）] を選択します。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 [配布（Distribute）] ウィンドウで、必要なオプションをクリックします。

ステップ 13 [デバイスグループの配布の定義（Define Device Group Distribution）] エリアで、この設定に含めるデバイスグループに隣接するチェックボックスをオンにします。

ステップ 14 [完了（Done）] をクリックします。

MobileIron Core UEM サーバーの設定

ここでは、大規模な MobileIron CORE UEM サーバーを設定するためのさまざまな手順について説明します。

MobileIron Core ユーザーの作成と API 権限の割り当て

ステップ 1 MobileIron Core 管理者ポータルにログインします。

ステップ 2 **[デバイスとユーザー（Devices and Users）]** > **[ユーザー（Users）]**の順に選択します。

ステップ 3 [Add（追加）] ドロップダウンリストから、[ローカルユーザーを追加（Add Local User）] を選択します。

ステップ 4 次のフィールドに必要な値を入力します：

- **ユーザー ID（User ID）**
- **[名（First Name）]**
- **[姓（Last Name）]**
- **Password**
- **Confirm Password**
- **Email**

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 新しく作成したユーザーにAPIロールを割り当てるには、[管理者（Admin）]をクリックし、対応するユーザー名の横にあるチェックボックスをオンにします。

ステップ 7 [アクション（Actions）] ドロップダウンリストから、[ポッドへの割り当て（Assign to Pod）] を選択します。

ステップ 8 [スペースを選択（Select Space）] ドロップダウンリストからユーザーの定義済みスペースを選択するか、表示されたオプションからユーザーに割り当てるロールを選択します。作成したユーザーにはテナント管理者権限が必要です。また、このユーザーに対して **API ロール**を有効にする必要があります。

ステップ 9 [保存（Save）] をクリックします。

MobileIron Core での認証局の設定

MobileIron Core では、より広範な CA 設定から選択できます。組織の要件に最適なオプションを選択してください。この手順では、例として自己署名証明書のステップを詳しく説明します。

ステップ 1 MobileIron Core 管理者ポータルで、**[サービス（Services）]** > **[ローカルCA（Local CA）]** の順に選択します。

ステップ 2 [追加（Add）]ドロップダウンリストから、[自己署名証明書の生成（Generate Self-Signed Cert）] を選択します。

ステップ 3 [自己署名証明書の生成（Generate Self-Signed Cert）]ダイアログボックスで次のフィールドに必要な詳細情報を入力します：

- **ローカル CA 名**
- **キーの長さ（Key Length）**
- **CSR 署名アルゴリズム**
- **キーライフタイム（日数）**
- **発行元名**

ステップ 4 [生成（Generate）] をクリックします。

ステップ 5 後で CA 証明書を Cisco ISE にアップロードする必要があるため、CA 証明書をダウンロードします。ダウンロードする証明書の横にある [証明書を表示（View Certificate）] をクリックし、表示されるダイアログボックスにすべての内容をコピーします。このコンテンツを任意のテキストエディタに貼り付け、ドキュメントを .cer ファイルとして保存します。

MobileIron Core でのルート証明書または信頼できる証明書のアップロード

ステップ 1 MobileIron Core 管理者ポータルで、**[ポリシーと設定（Policies and Configs）]** > **[設定（Configurations）]**の順に選択します。

ステップ 2 [新規を追加（Add New）] ドロップダウンリストで [証明書（Certificates）] を選択します。

ステップ 3 表示される [新規証明書の設定（New Certificate Setting）] ダイアログボックスで、対応するフィールドに証明書の名前と説明を入力します。

ステップ 4 [ファイル名（File Name）] 領域で、[参照（Browse）] をクリックし、以前に設定した CA にアップロードする必要があるルートまたは信頼できる証明書を選択します。

使用できるファイルタイプは、.cer、.crt、.pem、および .der です。

ステップ 5 [保存（Save）] をクリックします。

MobileIron Core での証明書登録の設定

この手順では、例としてのみローカル CA を接続する手順について詳しく説明し、Cisco ISE リリース 3.1 でランダムおよび変更された MAC アドレスを処理するために必要なサブジェクトおよびサジェクト代替名属性の設定に重点を置きます。MobileIron は、自己署名証明書またはローカル CA の使用を推奨していません。

ステップ 1 MobileIron Core 管理者ポータルで、**[ポリシーと設定（Policies and Configs）]** > **[設定（Configurations）]**の順に選択します。

ステップ 2 [新規を追加（Add New）] をクリックし、[証明書の登録（Certificate Enrollment）] を選択して、設定した CA に適切なコネクタを選択します。ローカル CA を設定する場合は、[ローカル（Local）] を選択します。

この手順では、ローカル CA のステップについて説明します。MobileIron Core サーバーを Cisco ISE に接続するために設定した CA に応じて、証明書の登録オプションを選択する必要があります。

ステップ 3 表示される [新規ローカル証明書の登録設定（New Local Certificate Enrollment Setting）] ダイアログボックスで、次のフィールドに値を入力します。

- **Name**
- **ローカル CA**
- **キー タイプ**
- [件名（Subject）] : [件名（Subject）] フィールドを使用して UUID（Cisco ISE では GUID と呼ばれる）を Cisco ISE 3.1 以降のリリースと共有するには、**CN=ID:Mobileiron:$DEVICE_UUID$** と入力します。
- **キーの長さ（Key Length）**
- **CSR 署名アルゴリズム**
- [サブジェクト代替名タイプ（Subject Alternative Name Type）] エリアでは、[追加（Add）] をクリックし、[ユニフォームリソース識別子（Uniform Resource Identifier）] を [タイプ（Type）] ドロップダウンリストから選択します。[値（Value）] 列に **ID:Mobileiron:$DEVICE_UUID$** と入力し、このフィールドを使用して UUID（Cisco ISE では GUID と呼ばれる）を Cisco ISE 3.1 以降のリリースと共有します。

ステップ 4 [テスト証明書を発行する（Issue Test Certificate）] をクリックします。

MobileIron Core での Wi-Fi プロファイルの設定

ステップ 1 MobileIron Core 管理者ポータルで、**[ポリシーと設定（Policies and Configs）]** > **[設定（Configurations）]**の順に選択します。

ステップ 2 [新規を追加（Add New）] ドロップダウンリストから [Wi-Fi] を選択します。

ステップ 3 [新規のWi-Fi設定（New Wi-Fi Setting）] ダイアログボックスで、次のフィールドに必要な値を入力します。

- [EAPタイプ（EAP Type）] 領域で、[TLS] チェックボックスをオンにします。
- [アイデンティティ証明書（Identity Certificate）] ドロップダウンリストから、手順 MobileIron Core での証明書登録の設定 （19 ページ） で設定した証明書の登録を選択します。
- [保存（Save）] をクリックします。

MobileIron Core のラベルへのリソースのマッピング

エンドポイントとデバイスのグループに適用する必要がある設定、ルール、およびプロファイルを定義するラベルを設定します。ラベルを使用して、組織単位、デバイスタイプ、エンドポイントで実行されているオペレーティングシステムなど、さまざまな基準に基づいてエンドポイントとデバイスをグループ化できます。ラベルを作成したら、[ポリシーと設定（Policies & Configs）] ウィンドウでこのラベルをさまざまなリソースに割り当て、設定、ポリシー、およびデバイスまたはユーザーグループを相互にマッピングします。

Cisco ISE の使用例の設定とポリシーをマッピングおよび配布するには、適切なラベルを設定し、証明書登録、Wi-Fi プロファイル、およびこの使用例用に作成するその他の設定をラベルに適用します。

ステップ 1 ラベルを作成するには：

1. MobileIron Core 管理者ポータルで、**[デバイスおよびユーザー（Devices & Users）]** > **[ラベル（Labels）]** の順に選択します。
2. [ラベルの追加（Add Label）] をクリックします。
3. [ラベルの追加（Add Label）] ダイアログボックスでは、[名前（Name）] フィールドのラベル名を入力します。
4. [基準（Criteria）] 領域で、[フィールド（Field）]、[演算子（Operator）]、および [値（Value）] フィールドに適切な値を選択して、このラベルのパラメータを定義します。
5. [保存（Save）] をクリックします。

ステップ 2 [ポリシーと設定（Policies & Configs）] リソースにラベルを割り当てます。

1. MobileIron Core 管理者ポータルで、[ポリシーと設定（Policies & Configs）]をクリックし、選択したリソースメニューを選択します。

2. 作成したラベルを割り当てる設定またはポリシーのチェックボックスをオンにします。
3. [アクション（Actions）] ドロップダウンリストから、[ラベルへ適用（Apply To Label）] を選択します。
4. [ラベルに適用（Apply To Label）] ダイアログボックスで、適用するラベルの横にあるチェックボックスをオンにし、[適用（Apply）] をクリックします。

その他の参考資料

次のリンクには、Cisco ISE で作業するときに使用できる追加のリソースが含まれています。
https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

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、シスコサービス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、シスコサポート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。

Cisco 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。