

# Cisco Meraki Systems Manager の統合

• Cisco Meraki Systems Manager の設定 (1ページ)

## 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。

"disdi" Meraki	Q Search Dashboard			Demo networks	Demo Admin 👻	¶\$ Announcements ▼	⊗ Help ¥	🚔 example@cisco.com 👻 🧲
NETWORK	Profiles list / CiscolSEMDM							+ Add profile O Help
Network SSID -	CiscolSEMDM							
	နိုင်ငံ Profile configuration	Profile Configuration						3
Network-wide	SEEP Certificate	Туре	Device profile					
Security & SD-WAN		Name	CiscolSEMDM		7.	6		
Switch	+ Add settings		The name that will be shown to users			0		
Wireless	🔾	Description						
Systems Manager	2		Optional		.le			
Cameras		Profile Removal Policy						
Environmental		Removal Policy 🕲	Allow users to remove this profile	v				
Insight		Targets					7	
Organization		Group type	Manual Named Configure	e tags				
		Scope	All devices		*	Convert to target group		
		Installation target	All devices					
Organization		Scope Installation target	All devices	a tags	¥	Convert to target group	•	(16)

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。

ululu useo Meraki	ද်္ဂ်ွဲ? Profile configuration	SCEP Certificate					
NETWORK	A dd athres	Name	ISE_SCEP Name or description of the certificate				
Meraki San Francisco 🖕 SFO12	Add settings     ■	Subject name	Text to be used for the certificate subject name				
Network-wide			CN=0wner email				
Security & SD-WAN		Subject alternative name	Text to be used as certificate SubjectAltName @				
Switch			uri=ID:MerakiSM:DeviceID:SM device ID				
Wireless Systems Manager		Key size	0 1024				
			0 2048				
Cameras			4096				
Environmental		Key usage	Signing				
Insight			C Encryption				
Organization			Some certificate authorities, such as Microsoft CA, support only encryption or signing, but not both at the same time.				
		Key extractability	Key is extractable If false, the private key cannot be exported from the keychain				
		CA Provider	Meraki PKi *				
		Validity period	1 year 🔹				
		Auto renewal	Disable •				

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。 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。