# Meraki System Managerを使用したiOS用 Anyconnect PerApp VPNの設定

# 内容

概要 前提条件 要件 使用するコンポーネント 背景説明 設定 ステップ1: Cisco Meraki Systems ManagerへのiOSデバイスの登録 ステップ2: 管理対象アプリのセットアップ ステップ3: PerApp VPNプロファイルの設定 ステップ4: アプリケーションセレクタの設定 ステップ5: アプリケーションごとのASAのVPN設定例 確認 6. AnyConnectアプリケーションでのプロファイルインストールの確認 トラブルシュート

### 概要

このドキュメントでは、Meraki Mobile Device Manager(MDM)、System Manager(SM)で管理され ているApple iOSデバイスでPerApp VPNを設定する方法について説明します。

# 前提条件

### 要件

- AnyConnect v4.0 PlusまたはApexライセンス。
- Per App VPNをサポートするためのASA 9.3.1以降。
- Cisco Enterprise Application SelectorツールはCisco.comから入手できます。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- ASA 5506W-Xバージョン9.15(1)10
- iPad iOSバージョン15.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

# 背景説明

このドキュメントには、次に示すプロセスは含まれません。

- ・クライアント証明書を生成するためのシステムマネージャでのSCEP CAの設定
- ・iOSクライアント用のPKCS12クライアント証明書の生成

### 設定

### ステップ1: Cisco Meraki Systems ManagerへのiOSデバイスの登録

1.1. [Systems Manager] > [Add Devices] に移動します。

ululu cisco Meraki	Q Search Dashboard			€ Announcements * ① Help *				
	+ Map Satellite #	Address, zip code, etc.	Go	Argelia	Libia	Egipto	Hide table Pers	
Systems Manager 🛛 👻	E E	Networks		Network tags		c.	Devices	
	Tag - Con	nbine - Delete Search	✓ 1 network O	over the last week: 0 SM devic	ces		CSV - +	
Systems Manager				Clients Tags	Network type	Devices	Offline devices	
Organization	Overview	Apps	General	0	MDM	0	0	
Organization	Devices	Settings	Owners	Benin	A A	2 / (		
	Мар	VPP	Tags	e Togo Nigeria	15-5-5	Sudán	Etiopía	
	Remote desktop		Policies	OLagos	Camerún Centroafricana	del Sur		
	Event log	Add devices	Geofencing	Golfo de Guinea	- VA -	mind	Somalia	
	Software		Alerts	Ecuatorial		Uganda	Kenia	
					Repúbli Democrá	ca Ruanda	Nairobi	
Summary Skinasa del Congo					go Burundi			
	PIAUL PJ	ARAÍBA			1. 1. 15	Tan	zania o	

1.2. [iOS] オプションをクリックして登録を開始します。



1.3.インターネットブラウザ経由でデバイスを登録するか、カメラでQRコードをスキャンします 。このドキュメントでは、登録プロセスにカメラを使用しました。



1.4.カメラがQRコードを認識したら、ポップアップ表示される**Safariで「meraki.com」を開く**通 知を選択します。

WEBSITE QR CODE Open "meraki.com" in Safari APNS* (required) Add Devices Time to add some devices! There are a few different enrollment options for	Add Dev	Arices
A Mobile Browser	B iOS App	
Open <u>m.meraki.com</u> on the device and enter this network ID : O12 OR Set up a <u>network enrollment string</u> to use as an enrollment code at <u>m.meraki.com</u>	For easier enrollment, use the <u>iOS app</u> C Scan the following QR code in the iOS ap <b>I I I I I I I I I I</b>	
© Apple Configurator	D Send enrollment link	SQUARE
Another option for installing the management profile on a large number of devices is <u>Apple Configurator</u> . Below is a link to the	Alternatively, send an enrollment link via	SMS or e-mail. SMS

1.5.プロンプトが表示されたら、**Register**を選択します。



a meraki.com

c 🕆 +

#### Meraki SM Setup

#### Step 1: Enter your Network ID

The Network ID is either a 10-digit code or a combination of letters, numbers, or characters (e.g. <u>123-456-7890</u> or network-id).

By installing Systems Manager on your device you acknowledge that you have read and understood the terms of our <u>Privacy</u> Policy.

012-	
UTE	
Register	

### 1.6. [Allow] を選択して、デバイスがMDMプロファイルをダウンロードできるようにします。

<	m	■ n12.meraki.com	C	Û	+	D
		Meraki SM Setup				
		Registration complete!				
		Waiting for your device to check in				
		Click here to try enrolling again.				
		This website is trying to download a configuration profile. Do you want to allow this? Ignore Allow				

#### 1.7. [Close] を選択してダウンロードを完了します。

<	×	🔒 n12.meraki.com	C	Û	+	
		Meraki SM Setup				
		Registration complete!				
		Waiting for your device to check in				
		Click here to try enrolling again.				
		Profile Downloaded Review the profile in Settings app if you want to install it.				
		Close				

1.8. iOS Settings Appに移動し、左側のペインで**Profile Downloaded**オプションを見つけて、 **Meraki Management**セクションを選択します。

Sottingo	General	Profile	
Settings	DOWNLOADED PROFILE		
	Meraki Mana Meraki Inc.	agement	>
Apple ID, iCloud, iTunes & App Store			
Profile Downloaded			
Profile Downloaded			
Airplane Mode	D		
ᅙ Wi-Fi Mars	hall		
Bluetooth	On		

1.9. [Install] オプションを選択して、MDMプロファイルをインストールします。

	Cancel Install Profile	tall
Settings		
	Meraki Management Meraki Inc.	
Apple ID, iCloud, iTunes & App Store	Signed by *.meraki.com Verified ✓	
Profile Downloaded	Description Meraki Systems Manager Contains Device Enrollment Challenge	
	More Details	>
> Airplane Mode		
🛜 Wi-Fi Marshall	Remove Downloaded Profile	

1.10. SMアプリケーションを**インストール**するためのアクセス権を付与する必要があります。



1.11.ホーム画面にある最近ダウンロードしたMeraki MDMというアプリケーションを開きます。



1.12.すべてのステータスに、登録が完了したことを示す緑色のチェックマークが付いていること を確認します。

Home	
STATUS	
Connected	>
Enrolled	>
Compliant	>
Contraction	>
RECENT ACTIVITY	
<ul> <li>Meraki Systems Manager</li> <li>A managed app was added on Apr 14, 2020, 10:27:06 PM</li> </ul>	器 10:27 PM >

### ステップ2:管理対象アプリのセットアップ

Home

o

このドキュメントの後半でPerApp用のトンネルアプリをセットアップするには、SMを介してこ れらの同じアプリケーションを管理する必要があります。この設定例では、FirefoxはPer Appを 介してトンネリングされることを意図しているため、管理対象アプリに追加されます。

Backpack

Apps

2.1. [Systems Manager] > [Manage] > [Apps] に移動し、管理対象アプリケーションを追加します

dialiti cisco Meraki	Q Search Dashboard v3 Announcements * () Help *								
NETWORK	New in Dashboard: Introduc	ing upcoming Meraki health fe	aature - Guided CRC Trouble	shooting Flow and 4 oth	her features. <u>Re</u>	ad more.			×
	Meraki has recently update	d our list of subprocessors. Se	e the Meraki subprocessors	page to learn more.					×
Systems Manager	MONITOR	MANAGE	CONFIGURE						
Organization	Overview Devices Trusted Access Map Remote desktop	Apps Settings VPP DEP Add devices	Conners Owners Tags Policies Geofencing	contact support to rec	cover access to t	talia Croacia Serbia Butor	Mar Negro	Georgia	X Hide table
	Event log Software Command line		Alerts Software installer	Net er the last week: 1 SM	twork tags I device			Devices	CSV - +
	Summary			Clients	Tags	Network type	Devices 0	Offline devices	

2.2. [Add app] オプションを選択します。



2.3.アプリケーションの種類(App Storeアプリ、カスタム、B2B)をアプリの保存場所に基づい て選択します。選択したら、[Next] を選択します。

この例では、アプリケーションはApp Storeにパブリックに保存されます。

ululu uso Meraki	Q Search Dashboard		🕫 Anno	ouncements -	⑦ Help +		
NETWORK		Add an app	×				
holguins-network -	Apps list	App platform				+ Add app	Help
Systems Manager	Belect + Edit + Pusr	App type		Scope	Tags	Import + A	Accounts +
" Organization	1	<ul> <li>App Store app Search for an app from the IOS App Store.</li> <li>Custom (Enterprise) app Upload an .ipa file, provide a manifest URL, or upload a manifest plist.</li> <li>B2B app Provide the ITunes ID for a custom B2B app.</li> </ul>	Next	All devices			
			Next				

2.4.プロンプトが表示されたら、目的のアプリケーションを検索し、アプリケーションのダウン ロード元のリージョンを選択します。アプリを選択したら、[Save] を選択します。

**注**:国がAppleアカウントの地域と一致しない場合は、アプリケーションで問題が発生する 可能性があります。

cisco Meraki	Q Search Dashboard	⑦ Help * hol	guins@cisco.com + 🦺
NETWORK			
holguins-network 👻	Apps list / New app	< 🔘	+ Add app O Help
	Add new iOS app		
Systems Manager	firefox   United States		
Organization	Firefox: Private, Safe Browser       (org.mozilia.los.Firefox)		
	Firefox Focus: Privacy browser Cancel Save (org.mozilla.los.Focus) (Please allow 1-2 minutes for changes to take effect.)		
	Microsoft Edge: Web Browser     (com.microsoft.msedge)		
	Microsoft Bing Search (com.microsoft.bing)		

2.5.目的のアプリケーションをすべて選択したら、[Save] をクリックします。

## ステップ 3: PerApp VPNプロファイルの設定

3.1. [システムマネージャ(Systems Manager)] > [管理(Manage)] > [設定(Settings)] に移動します



3.2. [Add profile] オプションを選択します。

NETWORK	Profiles list						+ Add profile		
Systems Manager 👻	Q Search profiles,	Q Search profiles, or select to edit							
Sustama Managar	Name •	Payloads	Scope	Tags	Targeted	Installed on	×		
Systems Manager	default		No devices		0	0			
Organization	1 result								
		Cancel Save							
		(Please allow 1-2 minutes for changes to take effect.)							

3.3. [Device profile (default)] を選択し、[Continue]をクリックします。

	Add new profile		×			
Profiles list					+ Add profile	Help
Q Search profiles, or selec	Standard					×
	O Device profile (default)	Supported on all	device types			
Name • Pay	O Copy an existing profile			Installed on		×
default	Advanced 0			0		
1 result	O User profile (Apple)	Supported on iOS	t macOS			
		Supported on	Chromo			
	O user profile (Chrome)	Supported on	© Chrome			
	<ul> <li>Upload custom Apple profile</li> </ul>	Supported on iOS	🗯 macOS			
		Cancel	Continue			

3.4. [Profile Configuration] メニューが表示されたら、[Name] を入力し、[Scope] でターゲットデ バイスを選択します。

දිරිූි Profile configuration	Profile Configuration				
+ Add settings	Туре	Device profile			
	Name	PerAppVPN-Profile			
		The name that will be shown to users			
	Description				
			ĥ		
		Optional			
	Profile Removal Policy				
	Removal Policy ()	Allow users to remove this profile			
	Targets				
	Group type	Manual Named Configure tage	S		
	Scope	All devices	Ŧ	Convert to target group	
	Installation target	All devices			
	Status				
	Device in scope: 1 device				
	# Name	System type	Install status	Tags	×
	1 iPad	iPad (6th Gen.)	Not installed		

3.5. [Add settings] を選択し、プロファイルのタイプを[iOS Per App VPN] でフィルタリングして 、次に示すオプションを選択します。

Profiles list / PerAppVPN-Profile		+ Add profile	@ Help
PerAppVPN-Profile			
<ul><li>♀ Profile configuration</li><li>♦ Add settings</li></ul>	Add new settings payload Device type All types & iOS & macOS & tvOS & Android & Chrome # Windows		
	Q per app		×
	iOS Per App VPN Supported on iOS		>
	Cancel Save		

#### 3.6.メニューが表示されたら、次の例に基づいて接続情報を書き込みます。

Systems Managerでは、これらの接続に対して、SCEPと手動登録という2つの証明書登録がサポートされています。この例では、手動登録が使用されています。

**注**:このオプションでは証明書ファイルを追加するための新しいメニューが表示されるため、テキストボックスに入力したら[Add credential] を選択します。

alah sa sa	Profiles list / New profile / iOS Per Ap	p VPN	+ Add profile	Help
cisco Meraki	New profile			
NETWORK				
holguins-network -	နိုင္လ်ို Profile configuration	iOS Per App VPN dia	O He	elp
	A≡ New certificate x	Connection Name	VPN-Corp Displayed Connection Profile on AnyConnect	
Systems Manager	VPN-Corp ×		Display name of the connection (displayed on the device)	
Organization	+ Add settings	Server	Vpn.cisco.com ASA IP address or FQDN	
		Proxy Setup	None  Configures provies to be used with this VPN connection	
		Connection Type	Cisco AnyConnect	
		Account		
			User account for authenticating the connection	
		Group	Perapp Group-URL configured in the VPN headend AnyConnect Group Name	
		Machine Authentication	Certificate v	
			New credential  Add credential Credential for authenticating the connection Select this at last	
		Auto Connect	[Disabled Automatically control the VPN connection ⊕	
			Send All Traffic Routes all network traffic through the VPN connection	
		Safari domains	Domain Add Safari domain	

3.7. [クレデンシャルの追加(Add credential)] をクリックして[証明書(Certificate)]メニューにリダイ レクトされたら、証明書の[名前(Name)] を入力し、コンピュータを参照して、.pfxファイル(暗 号化された証明書ファイル)を保護する[パスワード(Password)] を探します。

cisco Meraki	Q Search Dashboard			¶⊄ Announcements • ⑦ Help •	
NETWORK					
holguins-network 👻	Profiles list / New profile / Certificate				+ Add profile
	New profile				
Systems Manager	M. B. G. M.	0			
Organization	Image: Second comparation       Image: Second comparation	Name Password Certificate	machine-auth Name or description of the credential	io ningún archivo. Istalled into a shared keychain and can be used across a Into the Android Keystore system and can be used acros Iy to uninstall a private key once installed unless you re	pplications. s applications, move the work profile from the
		0	Cancel Save		

#### 3.8.証明書が選択されると、証明書ファイル名が表示されます。

cisco Meraki	Q Search Dashboard		¶⊂ Announcements * ③ H	elp •	ł
NETWORK					
holguins-network 👻	Profiles list / New profile / Certificate	t.		+ Add profile	
	New profile				
Systems Manager	دمان المعالم ال	Certificate		<b>Q</b> Help	
Organization	All machine-auth     x       VPN-Corp     x       + Add settings	Name Password Certificate	machine-auth         Name or description of the credential         image: selecting the credificate file         Password protecting the certificate file         Filename: pfxbln.pfx         Issuer:         Subject/CN:         Expiration:         Select new certificate will be installed into a shared keychain and can be u on Android this certificate will be installed into the Android Keystore system and can b Please note that on Android there is no way to uninstall a private key once installed into evice.	sed across applications. e used across applications. anless you remove the work profile from the	
			Cancel Save Please allow 1-2 minutes for changes to take effect.)		

3.9.証明書を選択したら、以前使用していたVPNプロファイルに移動し、最近インポートしたクレデンシャルを選択し、トンネリングされたアプリを選択します(この場合はFirefox)。

これが完了したら、Saveをクリックします。

'disdo' Meraki	နိုင္ရဲ့ Profile configuration	iOS Per App VPN 🗉 🛙	2	Help
	A machine-auth x	Connection Name	VPN-Corp	
holguins-network 🗸	VPN-Corp ×		Display name of the connection (displayed on the device)	
Systems Manager	+ Add settings	Server	Vpn.cisco.com Hostname or IP address (IPv4 or IPv6) for server	
Organization		Proxy Setup	None →     Configures provides to be used with this VPN connection	
		Connection Type	Cisco AnyConnect v	
		Account		
			User account for authenticating the connection	
		Group	Perapp AnyConnect Group Name	
		Machine Authentication	Certificate v	
			machine-auth  Add credential Credential for authenticating the connection	
		Auto Connect	Disabled ~ Automatically control the VPN connection (9	
			Send All Traffic Routes all network traffic through the VPN connection	
		Safari domains	Domain	
			Add Safari domain	
		Apps	Select apps	
			Safari (com.apple.mobilesafari)	
			Firefox: Private, Safe Browser (org.mozilia.jos.Firefox)	

3.10.プロファイルがターゲットデバイスにインストールされていることを確認する。

Profiles list						+ Add profile	Ø Help
Q Search profiles, or select to edit							×
Name •	Payloads	Scope	Tags	Targeted	Installed on		×
PerAppVPN-Profile		All devices		1	1		
default		No devices		0	0		
2 results							

### ステップ4:アプリケーションセレクタの設定

4.1.シスコのWebサイト

https://software.cisco.com/download/home/286281283/type/282364313/release/AppSelector-2.0からapp selectorをダウンロード<u>する</u>

**注意**:Windowsマシンでアプリケーションを実行してください。表示される結果は、 MacOSデバイスでツールを使用した場合に予想されるものではありません。

4.2. Javaアプリケーションを開きます。ドロップダウンメニューからiOSを選択し、わかりやす い名前を追加して、App IDに\*.\*と入力します。

Gisco AnyConnect Enterprise Applicatio	n Selector			-		×
File Policy About						
iOS		A	dd Rule	Impo	ort from [	Disk
wildcard	Friendly Name: App ID: Match Thumbprint:	wildcard *.*				
	Delete		Calcula	te Thur	mbprint	

4.3. [Policy] に移動し、[View Policy] を選択します

🕌 Cisco AnyConnect Enterprise Applicatio	on Selector		_		$\times$
File Policy About					
iOs View Policy		A	dd Rule Im	port from I	Disk
wildcard	Friendly Name: App ID: Match Thumbprint:	wildcard *.*	Calculate Th	umbprint	

4.4.表示された文字列をコピーする。(これは後でVPNヘッドエンド設定で使用されます)。



### ステップ5:アプリケーションごとのASAのVPN設定例

conf t
webvpn
anyconnect-custom-attr perapp description PerAppVPN
anyconnect-custom-data perapp wildcard
eJyrVnLOLE70d84vqCzKTM8oUbJSgrMVNJI1FYwMDEwUwGoUgiuLS1Jzi3UUPPOS9ZR01FxSyzKTU30yi4G6oquh3JDKglSg
IYkFBTmpupn5xUB1jgUFcEVA8cwUoLyWnhZQJi0vMRekujwzJyU5sShFqTYWCAFHcjDB
ip local pool vpnpool 10.204.201.20-10.204.201.30 mask 255.255.255.0
access-list split standard permit 172.168.0.0 255.255.0.0
access-list split standard permit 172.16.0.0 255.255.0.0
group-policy GP-perapp internal
group-policy GP-perapp attributes

ypn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
split-tunnel-all-dns disable
anyconnect-custom perapp value wildcard

tunnel-group perapp type remote-access tunnel-group perapp general-attributes address-pool vpnpool default-group-policy GP-perapp tunnel-group perapp webvpn-attributes authentication certificate group-alias perapp enable

### 確認

### 6. AnyConnectアプリケーションでのプロファイルインストールの確認

6.1. AnyConnectアプリケーションを開き、左側のペインで**Connections**を選択します。PerApp VPNプロファイルは、**PER-APP VPN**という名前の新しいセクションに表示される必要がありま す。

#### iを選択すると、詳細設定が表示されます。

3:10 Fri 18 Mar		•••	1 🗢 39% 🗲
AnyCo	onnect	VPN Connections	
PRIMARY VIRTUAL F	PRIVATE NETWORK		
AnyConnect VPN		Add VPN Connection	
Connections	VPN-Corp >	PER-APP VPN	
Details	Disconnected >	VPN-Corp Enabled	i
GENERAL			
Settings	>		
Diagnostics	>		
About	>		
۱۱ ۱ CIS			

6.2. [Advanced] オプションを選択します。

3:09 Fri 18 Mar				•••	
AnyC	onnect		VPN Connections		
	PRIVATE NET	Canaal			Cours
AnyConnect VPN		Cancel		VPN-Corp	Save
Connections	VPN	This cor Not all fi	nection has b elds can be eo	een imported from an AnyC dited.	Connect VPN Profile.
Details	Disconn	Descripti	on	VPN-Corp	
		Server A	ddress	vpn.cisco.com	
GENERAL		Advance	d		>
Settings					
Diagnostics					
About					
	uli.				
					i
CIS					

6.3. [App Rules] オプションを選択します。

3:09 Fri 18 Mar			•••	A 🗢 39% 🗲
AnyConnect			VPN Connections	
		< VPN-	Corp Advanced	
AnyConnect VPN				-
Connections	VPN	0		
Details	Disconn	Certifica	te holguins-scep	>
		App Rul	25	> (1)
GENERAL		Connec	On Demand	
Settings		TUNNEL F	ROTOCOL	
Diagnostics		Connec	with IPsec	
About		Only ena the serve	ole 'Connect with IPsec' if instructed to do so by your administrator r is not configured for IPsec, you will not be able to connect.	. If
· 1 1. CIS	ו וי co	_	(	D

6.4.最後に、App Ruleがインストールされていることを確認します。(このドキュメントでは Mozillaが望ましいトンネル化されたAppであるため、Appのインストールは成功しました)。

3:09 Fri 18 Mar						1 🗢 39% 🗲
AnyConnect					VPN Connections	
		Advar	red Ann Pules			
AnyConnect VPN						
Connections	VPN					
Details	Disconn	org.moz	IIIa.Ios.Firefox			
						(1)
GENERAL						
Settings						
Diagnostics						
About						
111						
CIS	CO					

# トラブルシュート

現在のところ、このドキュメントに固有のトラブルシューティング手順はありません。

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。