使用Meraki系統管理器配置iOS的Anyconnect PerApp VPN

目錄

箇介
 必要條件
 需求
 採用元件
 背景資訊
 設定
 步驟1.將iOS裝置註冊到Meraki系統管理器
 步驟2.設定託管應用
 步驟3.配置PerApp VPN配置檔案
 步驟4.應用選擇器配置
 步驟5.每個應用VPN配置的ASA示例
 驗證
 6.驗證AnyConnect應用程式上的配置檔案安裝
 疑難排解

簡介

本文檔介紹如何在由Meraki流動裝置管理器(MDM)和系統管理器(SM)管理的Apple iOS裝置上配置 PerApp VPN。

必要條件

需求

- AnyConnect v4.0 Plus或Apex許可證。
- ASA 9.3.1或更高版本,支援每應用VPN。
- Cisco.com上提供了思科企業應用選擇器工具

採用元件

本檔案中的資訊是根據以下軟體版本:

- ASA 5506W-X版本9.15(1)10
- iPad iOS版本15.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔不包括列出的進程:

- Systems Manager上的SCEP CA配置,用於生成客戶端證書
- •為iOS客戶端生成PKCS12客戶端證書

設定

步驟1.將iOS裝置註冊到Meraki系統管理器

1.1. 導航到Systems Manager > Add Devices

cisco Meraki	Q Search Dashboard				¶⊂ Announcem	ents * 🛞 Help	*	
NETWORK	+ Map Satellite +	Address, zip code, etc.	Go	Argelia	Libia	Egipto	Hide table Derse	
Systems Manager 🛛 👻	•	Networks		Network tags		D	evices	
	Tag - Co	mbine - Delete Search	✓ 1 network O	wer the last week: 0 SM device	es		CSV - +	
Systems Manager				Clients Tags	Network type	Devices	Offline devices	
Organization	Overview	Apps	General	0	MDM	0	0	
Organization	Devices	Settings	Owners	Benin	1 2		4	
	Мар	VPP	Tags	e Togo Nigeria	15-5-5	Sudán	Etiopía	
	Remote desktop		Policies	OLagos	Camerún Centroafricana	del Sur		
	Event log	Add devices	Geofencing	Acra Golfo de Guinea	-Vi-	me	Somalia	
	Software		Alerts	Ecuat	orial Congo	Uganda	Kenia	
				Cabon Congo República Ruanda Nairobi Democrática				
					@Kinsasa del Congo Bur		3	
	PIAUL	ARAIBA			the the the	Tanz	Dar es-Salam	

1.2.按一下iOS選項開始註冊。

Let's get started!

Select the device type to be enrolled.



1.3.通過網際網路瀏覽器註冊裝置或使用監視器掃描QR碼。在本文檔中,使用監視器進行註冊過程 。



1.4.當監視器識別QR代碼時,請在彈出的Safari通知中選擇**Open** "meraki.com"。

WEBSITE QR CODE Open "meraki.com" in Safari APNS* (required)	Add Devices
Add Devices Time to add some devices! There are a few different enrollment options for	or iOS - for more information, see <u>this article</u> .
A Mobile Browser	B iOS App
Open <u>m.meraki.com</u> on the device and enter this network ID : 012 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 iOS app C. Scan the following QR code in the iOS app:
© Apple Configurator	D Send enrollment link
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. E-mail SMS

^{1.5.}出現提示時,選擇Register。





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> <u>Policy</u>.

012	
012-	
Register	ø

1.6.選擇Allow以允許裝置下載MDM配置檔案。

<	m	■ n12.meraki.com	Ç	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.選擇Close以完成下載。

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

1.8.導航到iOS設定應用,在左窗格中找到**Profile Downloaded**選項,然後選擇**Meraki** Management部分。

Se	ettinas		Ceneral Profile	
•••	linge		DOWNLOADED PROFILE	
			Meraki Management	>
	Apple ID iCloud iTun	es & Ann Store		
	rappe to, releas, run			
D (
Profi	le Downloaded	>		
≁	Airplane Mode	\bigcirc		
?	Wi-Fi	Marshall		
*	Bluetooth	On		
VPN	VPN	\bigcirc		

1.9.選擇Install選項以安裝MDM配置檔案。

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

1.10.您必須授予訪問**安裝SM**應用程式的許可權。

App Ins "ios.meraki.com" is manage the app Manager" from Your iTunes act charged fr Cancel	stallation s about to install and "Meraki Systems in the App Store, count will not be or this app.		
	• • •		

1.11.開啟位於主螢幕中的最近下載的應用程式Meraki MDM。



1.12.檢驗所有狀態是否都有一個綠色勾選標籤,以確認登記已完成。

	Home	
STATUS		
Connected		>
Enrolled		>
Compliant		>
Contraction		>
RECENT ACTIVITY		
• Meraki Systems Manager A managed app was added on Apr 14, 2020, 10:27:06 PM		888 10:27 PM >
Home	Backpack	Apps

步驟2.設定託管應用

為了稍後在本文檔中設定PerApp的隧道應用,您需要通過SM管理這些相同的應用。在此配置示例 中,Firefox旨在通過Per App進行隧道化,因此會將其新增到託管應用中。

2.1. 導航到Systems Manager > Manage > Apps以新增託管應用。

disult. cisco Meraki	Q Search Dashboard					¶⊄ Announ	cements - 💿	Help -	
NETWORK	New in Dashboard: Introduc	ing upcoming Meraki health fe	eature - Guided CRC Trouble	shooting Flow and 4 oth	ner features. <u>Re</u>	ead 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	Apps Settings VPP	Conoral Owners Tags	contact support to rec	over access to 1	this organization.			×
	Map Remote desktop	DEP Add devices	Policies Geofencing	and	135	Croacia Serbia Italia	Mar Negro	Georgia	Hide table
	Event log		Alerts	Net	twork tags			Devices	
	Software		Software installer	er the last week: 1 SM	I device				CSV - +
	Command line			Clients	Tags	Network type	Devices	Offline devices	
	Summary			1		MDM	0	0	
	1 total								

2.2.選擇Add app 選項。



2.3.根據應用程式的儲存位置選擇應用程式的型別(App Store應用程式、自定義應用程式、 B2B)。選擇後選擇**Next**。

在此示例中,應用會公開儲存在App Store中。

ululu Meraki	Q Search Dashboard		🖘 Anne	ouncements -	⑦ Help +		
NETWORK		Add an app	×				
holguins-network 👻	Apps list Select - Edit - Pust	App platform				+ Add app	Help Accounts -
Systems Manager Organization	# icon 1	 App type App Store app Search for an app from the IOS App Store. Custom (Enterprise) app Upload an .jpa file, provide a manifest URL, or upload a manifest plist. B2B app Provide the ITunes ID for a custom B2B app. 	Next	Scope All devices	Tags		*

2.4.出現提示時,搜尋所需的應用程式,並選擇從中下載應用程式的區域。選擇應用後選擇Save。

注意:如果國家/地區與Apple帳戶的區域不匹配,則使用者可能會遇到應用程式問題。

cisco Meraki	Q Search Dashboard T Announcements * T Hel)Help • holguins@cisco.com • 🌲					
NETWORK							
holguins-network 👻	Apps list / New app	< 🔘	+ Add app	O Help			
	Add new iOS app						
Systems Manager	firefox United States						
Organization	(org.mozilla.los.Firefox)						
	Firefox Focus: Privacy browser Cancel Save (org.mozilla.los.Focus) (manual data for channel in the difference in the d						
	Microsoft Edge: Web Browser (com.microsoft.msedge) vrease allow *2 minutes for changes to case effect.						
	Microsoft Bing Search (com.microsoft.bing)						

2.5.選擇所有所需的應用程式後,按一下Save。

步驟3.配置PerApp VPN配置檔案

3.1.導航到Systems Manager > Manage > Settings

disco Meraki	Q Search Dashboard			τ⊂j Announcements ▼
NETWORK Systems Manager 🔹 👻		APNS* (required)		2 Add Devices
Systems Manager	MONITOR	MANAGE	CONFIGURE	
Organization	Overview Devices Map Remote desktop Event log Software Command line Summary	Apps Settings VPP DEP Add devices	General Tags Policies Geofencing Alerts	ns for iOS - for more information, see <u>this article</u> . B iOS App For easier enrollment, use the iOS app C. Scan the following QR code in the iOS app:
Set up a <u>network enrollment string</u> to use <u>m.meraki.com</u>		use as an enrollment code gement profile on a large or. Below is a link to the	e at Image: Second end end proliment link Alternatively, send an enrollment link via SMS or e-mail. E-mail SMS	

3.2.選擇Add profile 選項。

NETWORK	Profiles list					+ A	dd profile Ø Help	
Systems Manager 🛛 👻	Q Search profiles, o	Search profiles, or select to edit						
	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.選擇Device profile (預設) 並按一下Continue。

	Add new profile	×		
Profiles list			-	+ Add profile Ø 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	
1 result	User profile (Apple)	Supported on # IOS # macOS		
	User profile (Chrome)	Supported on O Chrome		
	 Upload custom Apple profile 	Supported on iOS macOS		
			-	
		Cancel Continue		

3.4.顯示Profile Configuration選單後,寫入Name,然後在Scope下選擇目標裝置。

<ြို Profile configuration	Profile Configuration				
+ Add settings	Туре	Device profile			
	Name	PerAppVPN-Profile			
		The name that will be shown to users			
	Description				
		Optional	lic		
	Profile Removal Policy				
	Removal Policy ()	Allow users to remove this profile			
	Targets				
	Group type	Manual Named Configure tage	S		
	Scope	All devices	*	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. 選擇Add settings並按iOS Per App VPN過濾配置檔案型別,選擇如下所示的選項。

Profiles list / PerAppVPN-Profile		+ Add profile	Ø Help
PerAppVPN-Profile			
રస్ట్ర Profile configuration	Add new settings payload Device type All types & IOS & macOS & tvOS & Android & Chrome # Windows		
	Q per app		×
	iOS Per App VPN Supported on is IOS		>
	Cancel Save		

3.6.顯示選單後,根據以下示例編寫連線資訊。

Systems Manager支援這些連線的兩個證書註冊:SCEP和手動註冊。在此示例中,使用手動註冊。

注意:一旦填滿文本框,請選擇Add credential,因為此選項會將您帶到一個新選單以新增證 書檔案。

allalla Manala	Profiles list / New profile / IOS Per Ap	p VPN		+ Add profile O Help
cisco Meraki	New profile			
NETWORK				
holguins-network 👻	දිංි ? Profile configuration	iOS Per App VPN dia	25	• Help
	Rew certificate ×	Connection Name	VPN-Corp Displayed Connection Profile of	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 F	QDN
			Hostname or IP address (IPv4 or IPv6) for server	
		Proxy Setup	Configures proxies to be used with this VPN connection	
		Connection Type	Cisco AnyConnect 🗸	
		Account		
			User account for authenticating the connection	
		Group	Group-URL configured in the AnyConnect Group Name	VPN headend
		Machine Authentication	Certificate v	
			New credential Add credential Credential for authenticating the connection	t
		Auto Connect	〔Disabled	
			Send All Traffic Routes all network traffic through the VPN connection	
		Safari domains	Domain Add Safari domain	

3.7.按一下Add credential並重定向到「證書」選單後,請寫入證書的Name,在電腦中瀏覽並查詢 保護.pfx檔案(加密證書檔案)的Password。

cisco Meraki	Q Search Dashboard			¶⊂ Announcements - ③ Help -		۰
NETWORK holguins-network 👻	Profiles list / New profile / Certificate New profile				+ Add profile	e Help
Systems Manager	Mr. Duffic and Sumaline	Cartificante				
Organization	Imachine-auth × Imachine-auth ×	Name Password Certificate	machine-auth Name or description of the credential Password protecting the certificate file ExaminarNo se ha seleccionadu On IOS and macOS this certificate will be intailed i Please note that on Android there is no war device.	o ningún archivo. stalled into a shared keychain and can be used across nto the Android Keystore system and can be used acro y to uninstall a private key once installed unless you	applications. ss applications. remove the work profi	ie from the
			Cancel Save (Please allow 1-2 minutes for changes to take effect.)			

'dışılı' Meraki	Q Search Dashboard		¶J Announcements * → ⑦ Help *	
NETWORK				
holguins-network 👻	Profiles list / New profile / Certificate	t.		+ Add profile
	New profile			
Systems Manager	Carl Drafile configuration	Cartifianta		0.111
Organization	 ↓ Provide Grange Balanting ↓ Add settings 	Name Password Certificate	machine-auth Name or description of the credential	applications. ss applications. remove the work profile from the
		(Pi	Cancel Save	

3.9.選擇證書後,導航到您先前使用的VPN配置檔案,選擇最近匯入的憑證並選擇隧道應用(本例 中為Firefox)。

完成此操作後,按一下**Save**。

disco Meraki	ද්ථ Profile configuration	iOS Per App VPN 🔹 io	S	e Help
NETWORK	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 proxies 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 v Automatically control the VPN connection	
			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.mozilla.jos.Firefox)	

3.10.驗證目標裝置上是否已安裝配置檔案。

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

步驟4.應用選擇器配置

4.1.從思科網站下載應用選擇器

https://software.cisco.com/download/home/286281283/type/282364313/release/AppSelector-2.0

注意:在Windows電腦上運行應用程式。在MacOS裝置上使用該工具時,顯示的結果不符合 預期。

4.2. 開啟java應用程式。從下拉選單中選擇iOS,新增一個友好名稱,並確保在App ID中鍵入*.*。

Sisco AnyConnect Enterprise Application Selector						×
File Policy About						
iOS		A	dd Rule	Impo	rt from [Disk
wildcard	Friendly Name: App ID: Match Thumbprint:	wildcard *.*				
	Delete		Calculat	te Thur	nbprint	

4.3.導航到Policy,然後選擇View Policy

🕌 Cisco AnyConnect Enterprise Applicatio	on Selector		_		×
File Policy About					
iO: View Policy		A	dd Rule	mport from	Disk
wildcard	Friendly Name: App ID: Match Thumbprint:	wildcard *.*			
	Delete		Calculate	Fhumbprint	

4.4.複製顯示的字串。(稍後將在VPN頭端配置中使用此功能)。



步驟5.每個應用VPN配置的ASA示例

conf t webvpn anyconnect-custom-attr perapp description PerAppVPN anyconnect-custom-data perapp wildcard eJyrVnL0LE70d84vqCzKTM8oUbJSgrMVNJI1FYwMDEwUwGoUgiuLS1Jzi3UUPPOS9ZR01FxSyzKTU30yi4G6oquh3JDKglSg 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 vpn-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

驗證

6.驗證AnyConnect應用程式上的配置檔案安裝

6.1.開啟AnyConnect應用程式,然後在左側窗格中選擇**Connections**。PerApp VPN配置檔案必須顯 示在名為**PER-APP VPN**的新部分下。

選擇i以顯示高級設定。

3:10 Fri 18 Mar		•••	🗢 39% 🗲
AnyCo	nnect	VPN Connections	
PRIMARY VIRTUAL PI	RIVATE NETWORK		
AnyConnect VPN		Add VPN Connection	
Connections	VPN-Corp >	PER-APP VPN	
Details	Disconnected >	VPN-Corp	(i)
		Enabled	-
GENERAL			
Settings	>		
Diagnostics	>		
About	>		
.1 1.1 1. CISCO			

6.2.選擇Advanced選項。

3:09 Fri 18 Mar			•••		
AnyConnect			VPN Connections		
		Canaal			Davia
AnyConnect VPN		Cancel		VPN-Corp	Save
Connections	VPN	This conr Not all fie	This connection has been imported from an AnyConnect VPN Profile. Not all fields can be edited.		
Details	Disconn	Descriptio	n	VPN-Corp	
		Server Ad	dress	vpn.cisco.com	
GENERAL		Advanced			>
Settings					
Diagnostics					
About					
About	_				
					(i)
CIS					

6.3.選擇App Rules選項。

3:09 Fri 18 Mar						A 🗢 39% 🗲	
AnyConnect			VPN Connections				
		VPN-Corp Advanced					
AnyConnect VPN		Avanced					
Connections	VPN	0			the last free second		
Details	Disconn	Certifica	ite		holguins-sce	ep >	0
		App Rul	es			>	(<u>i</u>)
GENERAL		Connec	t On Demand				
Settings		TUNNEL F	ROTOCOL				
Diagnostics		Connect	t with IPsec				
About		Only ena	ble 'Connect with IPs	ec' if instructed to do so	by your administra	tor. If	
		the serve	n is not comigured to	n resec, you will not be a	ible to connect.		
1111						í	
CIS	CO						

6.4.最後,確認已安裝應用規則。(Mozilla是本文檔中所需的隧道化應用,因此應用安裝成功)。

3:09 Fri 18 Mar				•••		ଏ 🗢 39% 🗲
AnyConnect			VPN Connections			
	RIVATE NETV	Advar	nced	App Rules		
AnyConnect VPN		X Marvar				
Connections	VPN	oramoz	illa ios Eirofox			
Details	Disconn	org.moz	IIIa.IOS.FITeTOX			(j)
GENERAL						
Settings						
Diagnostics						
About						
1111	111					
CIS	CO					

疑難排解

目前沒有適用於本文的具體疑難排解步驟。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。