使用Meraki系统管理器为iOS配置Anyconnect PerApp VPN

目录

简介 先决条件 要求 使用的组件 背景信息 配置 步骤1:将iOS设备注册到Meraki系统管理器 步骤1:将iOS设备注册到Meraki系统管理器 步骤1:将iOS设备注册到Meraki系统管理器 第二步:设置托管应用 第三步:设置托管应用 第三步:配置PerApp VPN配置文件 第四步:应用选择器配置 第五步:每个应用VPN配置的ASA示例 验证 6.验证AnyConnect应用程序上的配置文件安装 故障排除

简介

本文档介绍如何在Meraki移动设备管理器(MDM)和系统管理器(SM)管理的Apple iOS设备上配置 PerApp VPN。

先决条件

要求

- AnyConnect v4.0 Plus或Apex许可证。
- ASA 9.3.1或更高版本,可支持Per App VPN。
- Cisco Enterprise Application Selector工具可在Cisco.com上获取

使用的组件

本文档中的信息基于以下软件版本:

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

本文档不包括列出的流程:

- Systems Manager上的SCEP CA配置,用于生成客户端证书
- iOS客户端的PKCS12客户端证书生成

配置

步骤1:将iOS设备注册到Meraki系统管理器

1.1.导航到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	ver the last week: 0 SM devic	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	Sudán	Etiopía
	Remote desktop		Policies	oLagos	Camerún Centroafricana	del Sur	
	Event log	Add devices	Geofencing	Golfo de Guinea	-VA-	mind	Somalia
	Software		Alerts	Ecuat	orial Congo	Uganda	Kenia
				República Ruanda Nairol		Nairobi	
					WKinsasa del Con	go Burundi	3
	PIAUL	ARAIBA			1. 1. 1.	Tanz	Dar es-Salam

1.2.单击iOS选项开始注册。

Let's get started!

Select the device type to be enrolled.



1.3.通过互联网浏览器注册设备或使用摄像头扫描QR码。在本文档中,摄像头用于注册过程。



1.4.当摄像头识别QR代码时,选择弹出的Safari通知中的打开"meraki.com"。

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

^{1.5.}出现提示时,选择**Register**。



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> <u>Policy</u>.

010	
012-	J
Register	Ø

1.6.选择Allow以允许设备下载MDM配置文件。

< > m	n12.meraki.com	¢	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?				

1.7.选择**关闭**以完成下载。

<	>	m	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.导航到iOS设置应用,在左侧窗格中找到Profile Downloaded选项,然后选择Meraki Management部分。

Se	ttings	-	Ceneral	Profile	
	Apple ID, iCloud, iTune	es & App Store	Meraki M Meraki Inc	lanagement	>
Profil	e Downloaded	>			
≁	Airplane Mode	\bigcirc			
?	Wi-Fi	Marshall			
*	Bluetooth	On			
VPN	VPN	\bigcirc			

1.9.选择**安装**选项以安装MDM配置文件。

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

1.10.您必须授予访问**安装**SM应用程序。



1.11.打开位于主屏幕中的最近下载的应用程序Meraki MDM。



1.12.检验所有状态是否都有一个绿色勾选标记,以确认登记已完成。

Home	
STATUS	
Connected	>
S Enrolled	>
Compliant	>
Control Location	>
RECENT ACTIVITY	
 Meraki Systems Manager A managed app was added on Apr 14, 2020, 10:27:06 PM 	闘 10:27 PM >

第二步:设置托管应用

为了稍后在本文档中设置PerApp的隧道应用,您需要通过SM管理这些相同的应用。在此配置示例中,Firefox旨在通过Per App进行隧道传输,因此会将其添加到托管应用中。

Backpack

Apps

2.1.导航到Systems Manager > Manage > Apps以添加托管应用。

Home

പ്പ

disdis cisco Meraki	Q Search Dashboard						📢 Announ	cements - 💿	Help -	
NETWORK										~
holguins-network -	New in Dashboard: Introdu	cing upcoming Meraki health fe	eature - Guided CRC Troubles	shooting F	low and 4 othe	r features. <u>Re</u>	ad more.			^
	Meraki has recently update	d our list of subprocessors. Se	e the Meraki subprocessors (page to lea	arn more.					×
Systems Manager	MONITOR	MANAGE	CONFIGURE							
Organization	Overview Devices	Apps -	Constal Owners	contact s	upport to recov	ver access to t	his organization.			×
	Trusted Access Map Remote desktop	VPP DEP Add devices	Tags Policies Geofencing	0	Part .		Croacia Serbia	Mar Negro	Georgia	Hide table
	Event log		Alerts		Netw	ork tags			Devices	
	Software		Software installer	er the la	st week: 1 SM d	levice				CSV - +
	Command line			c	lients	Tags	Network type	Devices	Offline devices	
	Summary			1			MDM	0	0	
	1 total									

2.2.选择Add app选项。



2.3.根据应用的存储位置选择应用的类型(应用商店应用、自定义、B2B)。选择**Next**后,选择它 。

在本示例中,应用公开存储在App Store中。

ululu Meraki	Q Search Dashboard		Anno	ouncements -	⑦ Help *		
NETWORK		Add an app	×				
holguins-network -	Apps list	App platform				+ Add app	O Help
	Select - Edit - Pust	🔹 iOS 🔹 macOS 🔹 tvOS 🗣 Android 🗱 Windows				Import - A	ccounts +
Systems Manager	🗆 # Icon	App type		Scope	Tags		¥
Organization	🗆 1 🔘	App Store app Search for an app from the IOS App Store.		All devices			
		Upload an .ipa file, provide a manifest URL, or upload a manifest plist.					
		B2B app Provide the iTunes ID for a custom B2B app.					
			Next				

2.4.出现提示时,搜索所需的应用程序,并选择从中下载该应用程序的区域。选择应用后选择 **Save**。

注:如果国家/地区与Apple帐户所在区域不匹配,用户可能会遇到应用程序问题。

cisco Meraki	Q Search Dashboard TS Announcements - @ Help	> • holguins@cisco.com • 🌲
NETWORK		
holguins-network 👻	Apps list / New app	< 🗃 🕂 Add app 🛛 Help
	Add new iOS app	
Systems Manager	firefox	
Organization	Firefox: Private, Safe Browser	
	Firefox Focus: Privacy browser Cancel Save (org.mozilla.ios.Focus) (Prease allow 1-2 minutes for changes to take effect.)	
	Com.microsoft Edge: Web Browser (com.microsoft.msedge)	
	Microsoft Bing Search (com.microsoft.bing)	

2.5.选择所有所需的应用程序后,单击Save。

第三步:配置PerApp VPN配置文件

3.1.导航到Systems Manager > Manage > Settings

cisco Meraki	Q Search Dashboard			tr⊂ Announcements ~ ⑦ Help ~			
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 Set up a <u>networ</u> <u>m.meraki.com</u>	Apps General Apps General Settings General VPP Tags tesktop DEP Policies Add devices Geofencing Alerts d line Set up a <u>network enrollment string</u> to use as an enrollment code m.meraki.com		ns for iOS - for more information, see <u>this article</u> . Image: Bios App For easier enrollment, use the iOS app C. Scan the following QR code in the iOS app: Image: Bios App Image: Bios App For easier enrollment, use the iOS app C. Scan the following QR code in the iOS app: Image: Bios App Imap			
	© Apple 0	Configurator		D Send enrollment link			
	Another option for installing the management number of devices is <u>Apple Configurator</u> .		ement profile on a large or. Below is a link to the	Alternatively, send an enrollment link via SMS or e-mail. E-mail SMS			

3.2.选择Add profile选项。

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

3.3.选择Device profile (默认),然后点击Continue。

	Add new profile		х			
Profiles list				+ Add profile	0 He	elp
Q Search profiles, or select	Standard					×
	O Device profile (default)	Supported on all device ty	/pes			
Name • Pa	O Copy an existing profile		Installed on			¢
default	Advanced (1)		0			
1 result	O User profile (Apple)	Supported on iOS imac	os			
	O Liser profile (Chrome)	Supported on @ Chron				
	O oser prolie (Chrome)	Supported on Section				
	 Upload custom Apple profile 	Supported on SiOS Simon	OS			
			_			
		Cancel Contin	nue			

3.4.显示Profile Configuration菜单后,在Scope下写入Name并选择目标设备。

နိုင်္သိ Profile configuration	Profile Configuration				
+ Add settings	Туре	Device profile			
	Name				
		PerAppVPN-Profile			
		The name that will be shown to users			
	Description				
		Optional	Al.		
	Profile Removal Policy				
	Removal Policy (1)	Allow users to remove this profile			
	Targets				
	Group type	Manual Named Configure tag	S		
	Scope	All devices		Convert to target group	
	Installation toront	All devices			
	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.选择Add settings并按iOS Per App VPN过滤配置文件类型,选择如下所示的选项。

Profiles list / PerAppVPN-Profile		+ Add profile	Ø Help
PerAppVPN-Profile			
ర్షస్టై? Profile configuration + Add settings	Add new settings payload Device type All types & iOS & macOS & tvOS & Android & Chrome Windows		
	C per app iOS Per App VPN Supported on 10S		×
	Cancel Save		

3.6.显示菜单后,根据以下示例编写连接信息。

Systems Manager支持这些连接的两个证书注册:SCEP和手动注册。在本示例中,使用手动注册。

注意:填写文本框后,请选择Add credential,因为此选项会将您引导至新菜单以添加证书文件。

ululu xa	Profiles list / New profile / iOS Per Ap	P VPN	+ Add profile O Help
cisco Meraki	New profile		
NETWORK			
holguins-network 👻	ද်္ဂ်ို Profile configuration	iOS Per App VPN dia	Help
	Re New certificate	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
			Hostname or IP address (IPv4 or IPv6) for server
		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 Group-URL configured in the VPN headend AnyConnect Group Name
		Machine Authentication	Certificate
			New credential 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

3.7.单击Add credential并重定向到Certificate菜单后,请写入Name证书,在计算机中浏览并查找保 护.pfx文件(加密证书文件)的Password。

cisco Meraki	Q Search Dashboard			¶⊄ Announcements - ③ Help -	
NETWORK	Profiles list / New profile / Certificate				+ Add profile
	New profile				
Systems Manager	M. C.				
Organization	Image: Around coming and additional and the set of the set	Name Password Certificate	machine-auth Name or description of the credential name or description of the credential Password protecting the certificate file Examinar No se ha seleccionad On IOS and macOS this certificate will be in the or Android this certificate will be in the or Android there is no ward device.	lo ningún archivo. stalled into a shared keychain and can be used across a into the Android Keystore system and can be used acror ny to uninstall a private key once installed unless you n	applications. ss applications. emove the work profile from the
		(Cancel Save Please allow 1-2 minutes for changes to take effect.)		

3.8.选择证书后,将显示证书文件名。

cisco Meraki	Q Search Dashboard		¶S Announcements × → ③ Help ×	٠
NETWORK				
holguins-network -	Profiles list / New profile / Certificate		+	Add profile
	New profile			
Systems Manager	M. C. C. C.	0		
Organization	Imachine-auth × Imachine-auth ×	Password Certificate	machine-auth Name or description of the credential	Une Peop
			On Android this certificate will be installed into the Android Keystore system and can be used across appli Please note that on Android there is no way to uninstall a private key once installed unless you remove device.	cations. the work profile from the

3.9.选择证书后,导航到您之前使用的VPN配置文件,然后选择最近导入的凭证并选择隧道应用 (本例中为Firefox)。

完成此操作后,单击Save。

disco Meraki	ද်္ဂ်္ဘဲ Profile configuration	iOS Per App VPN 🗉 io	S	Ø Help
NETWORK	Is 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 V 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 ~	
			machine-auth Add credential Credential for authenticating the connection Image: 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.验证配置文件是否已安装在目标设备上。

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

第四步:应用选择器配置

4.1.从思科网站下载应用选择器

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

注意:在Windows计算机上运行应用程序。在MacOS设备上使用工具时,显示的结果不是预 期结果。

4.2.打开java应用程序。从下拉菜单中选择iOS,添加一个友好名称,并确保在应用ID中键入*.*。

🕌 Cisco AnyConnect Enterprise Applicatio	on Selector			_		Х
File Policy About						
iOS			Add Rule	Impo	ort from I	Disk
wildcard	Friendly Name: App ID: Match Thumbprint:	wildcard *.*				
	Delete		Calcula	ate Thur	mbprint	

4.3.导航到Policy并选择View Policy

🕌 Cisco AnyConnect Enterprise Applicati	on Selector		-	- C	x c
File Policy About					
iO: View Policy		Ad	d Rule	Import f	rom Disk
wildcard	Friendly Name: App ID: Match Thumbprint:	wildcard *.*	Calculate	e Thumb	print

4.4.复制显示的字符串。(这稍后将在VPN头端配置中使用)。



第五步:每个应用VPN配置的ASA示例

authentication certificate group-alias perapp enable

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

 \times

验证

6.验证AnyConnect应用程序上的配置文件安装

6.1.打开AnyConnect应用程序,然后在左侧窗格中选择**Connections**。PerApp VPN配置文件必须显 示在名为**PER-APP VPN**的新部分下。

选择i以显示高级设置。

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 , CIS	и и СО		

6.2.选择Advanced选项。

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.选择App Rules选项。

3:09 Fri 18 Mar			•••				1 🗢 39% 🗲
AnyConnect			VPN Connections				
AnyConnect VPN							
Connections	VPN	A					
Details	Disconn	Certifica	ate		holguins-scep	>	
		App Rules				>	(i)
GENERAL		Connec	t On Demand				
Settings		TUNNEL F	ROTOCOL				
Diagnostica		Connec	t with IPsec				
Diagnostics		Only ena	ble 'Connect with IPse	ec' if instructed to do	so by your administrate	or. If	
About		the serve	er is not configured fo				
						- 1	
						- 1	
						- 1	
						- 1	
						- 1	
	111					6	
CIS	CO						

6.4.最后,确认已安装应用规则。(Mozilla是本文档中所需的隧道应用,因此应用安装成功)。

3:09 Fri 18 Mar				•••		1 🗢 39% 🗲	
AnyConnect			VPN Connections				
		Advar	oced	App Pules			
AnyConnect VPN		Auvai	iceu	App Rules			
Connections	VPN	oramoz	illa ios Eirofox				
Details	Disconn	org.moz	IIId.IUS.FITETUX			(j)	
GENERAL							
Settings							
Diagnostics							
About							
CIS	CO						

故障排除

本文档目前没有具体的故障排除步骤。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。