Configure Anyconnect PerApp VPN for iOS with Meraki System Manager

Contents

Introduction Prerequisites Requirements Components Used Background Information Configure Step 1. Register iOS Device to Meraki Systems Manager Step 2. Setup Managed Apps Step 3. Configure PerApp VPN profile Step 4. App Selector Configuration Step 5. ASA Sample Per App VPN Configuration Verify 6. Verify Profile Installation on AnyConnect Application Troubleshoot

Introduction

This document describes how to configure PerApp VPN on Apple iOS devices managed by Meraki Mobile Device Manager (MDM), System Manager (SM).

Prerequisites

Requirements

- AnyConnect v4.0 Plus or Apex license.
- ASA 9.3.1 or later to support Per App VPN.
- Cisco Enterprise Application Selector tool available on Cisco.com

Components Used

The information in this document is based on these software versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document does not include the listed processes:

- SCEP CA Configuration on Systems Manager for client certificate generation
- PKCS12 client certificate generation for the iOS clients

Configure

Step 1. Register iOS Device to Meraki Systems Manager

1.1. Navigate to 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 bers
Systems Manager 🛛 👻	•	Networks		Network tags		C	Devices
	Tag - Co	mbine - Delete Search	✓ 1 network	Over the last week: 0 SM device	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 / (4
	Мар	VPP	Tags	e Togo Nigeria	Sur E	Sudán	Etiopía
	Remote desktop		Policies	oLagos			
	Event log	Add devices	Geofencing	Golfo de Guinea	- VA -	mind	Somalia
	Software		Alerts	Uganda	Kenia		
				ca Ruanda	Nairobi		
	PIAII	ARAÍBA			1. 1. 1.	Tan	zania o

1.2. Click on the **iOS** option to start the enrollment.



1.3. Enroll the device via internet browser or scan the QR code with the camera. In this document, the camera was used for the enrollment process.



1.4. When the QR code is recognized by the camera, select the **Open "meraki.com" in Safari** notification that pops up.

WEBSITE OR CODE Open "meraki.com" in Safari APNS* (required)	Z Add De	vices
Add Devices Time to add some devices! There are a few different enrollment options for	r iOS - for more information, see <u>this article</u> .	0
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 iOS app of Scan the following QR code in the iOS at	
© 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.

1.5. When prompted, select Register.



a meraki.com



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-	
Register	0

1.6. Select **Allow** in order to allow the device to download the MDM profile.

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

1.7. Select **Close** to complete the download.

<	m	n12.meraki.com	Ç	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. Navigate to the iOS Settings App and locate the **Profile Downloaded** option in the left pane and select the **Meraki Management** section.

		General	Profile	
Settings		DOWNLOADED PROFILE		
		Meraki Mana Meraki Inc.	agement	>
Apple ID, iCloud	d, iTunes & App Store			
Desfile Devenies de d				
Profile Downloaded	>			
E Airplane Mode	\bigcirc			
ᅙ Wi-Fi	Marshall			
Bluetooth	On			
	\bigcirc			

1.9. Select the Install option to install the MDM profile.

Settings	Cancel Install Profile	stall
	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	>
Airplane Mode		
🛜 Wi-Fi Marshall	Remove Downloaded Profile	

1.10. You must grant the access to **Install** the SM application.



1.11. Open the recently downloaded application called Meraki MDM located in the home screen.



1.12. Verify all the statuses have a green tick that confirms the enrollment is in complete.

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

Step 2. Setup Managed Apps

In order to setup the Tunneled Apps for PerApp later in this document, you need to manage those same applications via SM. In this configuration example, Firefox is intended to be tunneled via Per App, hence it is added to the managed Apps.

2.1. Navigate to **Systems Manager > Manage > Apps** in order to add the managed apps.

uluulu cisco Meraki	Q Search Dashboard					¶⊂ Anno	uncements + 🔿	Help -	
NETWORK	New in Dashboard: Intro	ducing upcoming Meraki health	feature - Guided CRC Troub	leshooting Flow and 4 otl	her features. <u>Rei</u>	id more.			×
noiguins-network +									
	Meraki has recently upda	ated our list of subprocessors. S	ee the Meraki subprocessor	s page to learn more.					×
Systems Manager	MONITOR	MANAGE	CONFIGURE						
Organization	Overview Devices	Apps Settings	Constal Owners	contact support to rec	over access to th	is organization.			×
	Trusted Access Map Remote desktop	VPP DEP Add devices	Tags Policies Geofencing	and the second	2 Solt	Croacia Serbia	Mar Negro	Georgia	Hide table
	Event log		Alerts	Ne	twork tags			Devices	
	Software		Software installer	er the last week: 1 SM	1 device				CSV - +
	Command line			Clients	Tags	Network tune	Devices	Offline devices	
	Summary			1		MDM	0	0	
1	1 total								

2.2. Select the **Add app** option.



2.3. Select the type of application (App Store app, Custom, B2B) based on where the app is stored. Select **Next** once it is selected.

In this example the app is stored publicly in the App Store.

ululu Meraki	Q Search Dashboard		Anno	ouncements -	⑦ Help *		
NETWORK		Add an app	×				
holguins-network -	Apps list	App platform				+ Add app	e e Help
	Select - Edit - Pust	ios s macOS s tvOS + Android Windows				Import +	Accounts -
Systems Manager	🗆 # Icon	App type		Scope	Tags		¥
Organization	II ()	 App Store app Search for an app from the IOS App Store. Custom (Enterprise) app 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	All devices			

2.4. When prompted, search for the desired application and select the region from where the application is downloaded from. Select **Save** once the app is selected.

Note: If the country does not match the Apple account's region, the user may experience problems with the application.

cisco Meraki	Q Search Dashboard TO Announcements * @ Help	o∗ hol	guins@cisco.c	om • 🌲
NETWORK				
holguins-network 👻	Apps list / New app	<	+ Add app	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) (Bease allow 1/2 minutes for choose to take affect 1			
	Microsoft Edge: Web Browser (commicrosoft.msedge)			
	Microsoft Bing Search (com.microsoft.bing)			

2.5. Click Save once you select all the desired applications.

Step 3. Configure PerApp VPN profile

3.1. Navigate to Systems Manager > Manage > Settings



3.2. Select the Add profile option.

NETWORK	Profiles list					>	+ Add profile O Help
Systems Manager 🛛 👻	Q Search profiles	or select to edit					×
	Nomo -	Daulaada	Saana	Togo	Torontod	lectalized as	*
Systems Manager	default	Payloads	No devices	Tags	0	0	
Organization	1 result						
				Cancel Save	o take effect.)		

3.3. Select Device profile (default) and click Continue.

	Add new profile		ж				
Profiles list	Orested				+ Add profile	O He	elp
Q Search profiles, or select	Standard						×
	 Device profile (default) 	Supported on all	device types				
Name • Pa	Copy an existing profile			Installed on			-
default	Advanced (1)			0			
1 105 dat	O User profile (Apple)	Supported on 🗯 iOS	🗯 macOS				
	O User profile (Chrome)	Supported on	Chrome				
	O Upload custom Apple profile	Supported on 🗯 iOS	🗯 macOS				
		Cancel	Continue				

3.4. Once the **Profile Configuration** menu is displayed, write the **Name** and select the target devices under **Scope**.

ξ္လၖၴ Profile configuration	Profile Configuration				
+ Add settings	Туре	Device profile			
	Name	PerAppVPN-Profile			
		The name that will be shown to users			
	Description				
		Optional			
	Profile Removal Policy				
	Removal Policy	Allow users to remove this profile			
	Targets				
	Group type	Manual Named Configure tag	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. Select **Add settings** and filter the types of profile by **iOS Per App VPN**, select the option as seen below.

PerAppVPN-Profile	×
Image: Specifie configuration Add new settings payload Image: Add settings Device type All types IOS Image: Add new settings payload Image: Add new settings payload Image: Device type All types Image: Image: Device type Image: Image: Device type Image: Image: Image: Device type Image: Image: Image: Image: Device type Image: Ima	×
iOS Per App VPN	×
Supported on 🗯 IOS	>

3.6. Once the menu is displayed, write the connection information based on the example below.

Systems Manager supports two certificate enrollments for these connections, SCEP and manual enrollment. In this example manual enrollment was used.

Note: Select **Add credential** once you filled the text-boxes since this option takes you to a new menu to add a certificate file.

allalla Manada	Profiles list / New profile / iOS Per Ap	p VPN	+ Add profile O Help
cisco Meraki	New profile		
NETWORK			
holguins-network -	र्दुई Profile configuration	iOS Per App VPN dia	Help
	R 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 (IIPv6) for server
		Proxy Setup	None v Configures proxies 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
		Machine Authentication	Certificate ~
			New credential Add credential Credential for authenticating the connection
		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. Once you clicked on **Add credential** and you got redirected to the Certificate menu, write the **Name** of the Certificate, browse in your computer and look for the the **Password** that protects the .pfx file (encrypted certificate file).

cisco Meraki	Q Search Dashboard			🕫 Announcements 👻	⑦ Help *		۰
NETWORK							
holguins-network 👻	Profiles list / New profile / Certificate					+ Add profile	Ø Help
	New profile						
Systems Manager	دم Profile configuration	Certificate					O Help
Organization	All machine-auth × VPN-Corp × + Add settings	Name Password Certificate	machine-auth Name or description of the credential	io ningún archivo. Istalled into a shared keychain and Into the Android Keystore system a sy to uninstall a private key once in	can be used across a nd can be used acros stalled unless you re	oplications. s applications, move the work profil	e from the
		(P1	Cancel Save				

3.8. After the certificate is selected, the certificate filename is displayed.

cisco Meraki	Q Search Dashboard			¶3 Announcements * ⑦ Help *		۰
NETWORK						
holguins-network 👻	Profiles list / New profile / Certificate				+ Add profile	Help
	New profile					
Systems Manager	د المعام الم	Certificate				e Help
Organization	Am machine-auth x Im VPN-Corp x + Add settings	Name Password Certificate	machine-auth Name or description of the credential name or description of the credential machine of the credential Password protecting the certificate file Password protecting the certificate file Filename: pfxbin.pfx Issuer: Subject/CN: Expiration: Select new certificate On iOS and macOS this certificate will be installed in Please note that on Android there is no way device.	talled into a shared keychain and can be used across a to the Android Keystore system and can be used acro to uninstall a private key once installed unless you r	applications. ss applications. remove the work profile	from the
		,	Cancel Save Please allow 1-2 minutes for changes to take effect.)			

3.9. Once you selected the certificate, navigate to the VPN profile you were previously on and select the recently imported credential and Select the tunneled App (Firefox in this case).

Click **Save** once this is completed.

disco Meraki	ද්ථ Profile configuration	iOS Per App VPN 🔹	2	Help
NETWORK	요코 machine-auth ×	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	
		Connection Type	Cisco AnyConnect v	
		Account	User account for authenticating the connection	
		Group	perapp AnyConnect Group Name	
		Machine Authentication	Certificate ~	
		Auto Connect	machine-auth ✓ Add credential Credential for authenticating the connection Disabled ✓ 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.appie.mobilesafari)	
			Firefox: Private, Safe Browser (org.mozila.jos.Firefox)	

3.10. Verify the profile is installed on the target devices.

Profiles list						+ Add profile	0 H	ielp
Q Search profiles, or select to ed	lit							×
Name *	Payloads	Scope	Tags	Targeted	Installed on			r
PerAppVPN-Profile	RE W	All devices		1	1			
default		No devices		0	0			
2 results								

Step 4. App Selector Configuration

4.1. Download app selector from cisco website https://software.cisco.com/download/home/286281283/type/282364313/release/AppSelector-2.0

Caution: Run the application on a Windows machine. The results displayed are not be the expected when the tool is used on MacOS devices.

4.2. Open the java application. Select **iOS** from the dropdown menu, add a friendly name and ensure you type ***.*** in the **App ID**.

실 Cisco AnyConnect Enterprise Application	on Selector		_		Х
File Policy About					
iOS		Ad	d Rule Imp	oort from (Disk
wildcard	Friendly Name:	wildcard			
	App ID:	**			
	Match Thumbprint:				
			Calculate Th	umbprint	
	Delete				

4.3. Navigate to Policy and select View Policy

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

4.4. Copy the string displayed. (This is later used in the VPN headend configuration).



Step 5. ASA Sample Per App VPN Configuration

```
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
```

Х

Verify

6. Verify Profile Installation on AnyConnect Application

6.1. Open the AnyConnect Application and select **Connections** in the left pane. The PerApp VPN profile must be displayed under a new section called **PER-APP VPN**.

Select the i to display the advanced settings.

3:10 Fri 18 Mar		•••• 4 *	? 39% 🗲
AnyCo	nnect	VPN Connections	
	RIVATE NETWORK		
AnyConnect VPN		Add VPN Connection	
Connections	VPN-Corp >	PER-APP VPN	
Details	Disconnected >	VPN-Corp	(i)
		Enabled	
GENERAL			
Settings	>		
Diagnostics	>		
About	>		
111	111		
CIS	CO		

6.2. Select the Advanced option.



6.3. Select the App Rules option.

3:09 Fri 18 Mar				•••		1 🗢 39% 🗲
AnyCor	nnect			VPN C	Connections	
	RIVATE NET		Corp	Advanced		
AnyConnect VPN			corp	Advanced		
Connections	VPN	A				
Details	Disconn	Certifica	ate	h	iolguins-scep >	0
		App Rul	es		>	(i)
CENEDAL		Connec	t On Demand			
Settings		TUNNEL F	PROTOCOL			
Settings		Connect	t with IPsec			
Diagnostics						
About		Only ena the serve	ble 'Connect with IPse er is not configured for	c' if instructed to do so by yo IPsec, you will not be able to	our administrator. If connect.	
					í	
CIS	CO					

6.4. Lastly, confirm the App Rule is installed. (Mozilla is the tunneled App desired in this document, so the app installation was successful).

3:09 Fri 18 Mar			•••			1 🗢 39% 🗲
AnyConnect			VPN Connections			
		Advar	aced	Ann Pules		
AnyConnect VPN		Auvai	iceu	App Rules		
Connections	VPN	oramoz	illa iga Eirofov			
Details	Disconn	org.moz	IIIa.IOS.FITeTOX			(j)
GENERAL						
Settings						
Diagnostics						
About						
il li						
CIS						

Troubleshoot

There are currently no specific troubleshooting steps for this document.