# **Configure AnyConnect Management VPN Tunnel** on ASA

## Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Working of Management Tunnel
Limitations
<u>Configure</u>
Configuration on ASA through ASDM/CLI
Creation of AnyConnect Management VPN Profile
Deployment Methods for AnyConnect Management VPN Profile
(Optional) Configure a Custom Attribute to Support Tunnel-All Configuration
<u>Verify</u>
<u>Troubleshoot</u>
Related Information

## Introduction

This document describes configuring ASA as the VPN gateway accepts connections from AnyConnect Secure Mobility Client through Management VPN tunnel.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- VPN configuration through Adaptive Security Device Manager (ASDM)
- Basic Adaptive Security Appliance (ASA) CLI Configuration
- X509 Certificates

### **Components Used**

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

- Cisco ASA software version 9.12(3)9
- Cisco ASDM software version 7.12.2
- Windows 10 with Cisco AnyConnect Secure Mobility Client version 4.8.03036

Note: Download the AnyConnect VPN Web deploy package (anyconnect-win\*.pkg or anyconnect-macos\*.pkg)

from the Cisco <u>Software Download</u> (registered customers only). Copy the AnyConnect VPN client to the flash memory of the ASA that is to be downloaded to the remote user computers to establish the SSL VPN connection with the ASA. Refer to <u>Installing the AnyConnect Client</u> section of the ASA configuration guide for more information.

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**

A management VPN tunnel ensures connectivity to the corporate network whenever the client system is powered up, not just when a VPN connection is established by the end user. You can perform patch management on out-of-the-office endpoints, especially devices that are infrequently connected by the user, via VPN, to the office network. Endpoint OS login scripts that require corporate network connectivity also benefit from this feature.

AnyConnect Management Tunnel allows administrators to have AnyConnect connected without user intervention prior to when the user logs in. AnyConnect Management tunnel can work in conjunction with Trusted Network Detection and therefore is triggered only when the endpoint is off-premise and disconnected from a User-initiated VPN. AnyConnect Management tunnel is transparent to the end user and disconnects automatically when the user initiates VPN.

OS/Application	Minimum Version Requirements
ASA	9.0.1
ASDM	7.10.1
Windows AnyConnect Version	4.7.00136
macOS AnyConnect Version	4.7.01076
Linux	Unsupported

## Working of Management Tunnel

AnyConnect VPN agent service is automatically started upon system boot-up. It detects that the management tunnel feature is enabled (via the management VPN profile), therefore it launches the management client application to initiate a management tunnel connection. The management client application uses the host entry from the management VPN profile to initiate the connection. Then the VPN tunnel is established as usual, with one exception: no software update is performed during a management tunnel connection since the management tunnel is meant to be transparent to the user.

The user initiates a VPN tunnel via the AnyConnect UI, which triggers the management tunnel termination. Upon management tunnel termination, the user tunnel establishment continues as usual.

The user disconnects the VPN tunnel, which triggers the automatic re-establishment of the management tunnel.

## Limitations

- User interaction is not supported
- Certificate-based authentication through Machine Certificate Store (Windows) is only supported

- Strict Server Certificate checking is enforced
- A private proxy is not supported
- A public proxy is not supported (ProxyNative value is supported on platforms where Native Proxy settings are not retrieved from the browser)
- AnyConnect Customization Scripts are not supported

**Note:** For more information, refer to <u>About the Management VPN Tunnel.</u>

### Configure

This section describes how to configure the Cisco ASA as the VPN gateway to accept connections from AnyConnect clients through the Management VPN tunnel.

### Configuration on ASA through ASDM/CLI

Step 1. Create the AnyConnect Group Policy. Navigate to Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Click Add.

**Note:** It is advisable to create a new AnyConnect Group Policy which is used for the AnyConnect Management tunnel only.

🕤 Home 🔏 Configuration 📴 Monitoring 🔚	Save 🔇 Refresh 🔇 Back 🔘 Forw	ard 💡 Help Type topic Go		cisco
COO Remote Access VPN	Configuration > Remote Acc	ess VPN > Network (Client) Access	> Group Policies	
Introduction     Intredition     Intredition     Intredity     Introduction     Introd	Manage VPN group policies.A VPN gr policy information is referenced by V To enforce authorization attributes f Add 2 Edit 2 Delete Ass Name	oup is a collection of user-oriented PN connection profiles and user acc rom an LDAP server you must use an lign	authorization attribute/value pairs that may be stored in ounts. I LDAP attribute map. Tunneling Protocol	Connection Profiles /Users
S Group Policies	AnyConnect	Internal	ssl-client	AnyConnect
IPsec(IKEv1) Connection Profiles	DfltGrpPolicy (System Default)	Internal	ikev1:ikev2:l2tp-ipsec	DefaultRAGroup:DefaultL2LGroup:DefaultADMINGroup:DefaultWE
<ul> <li>Secure Mobility Solution</li> <li>Secure Solution</li> <li>Advanced</li> <li>Secure Desktop Manager</li> <li>Secure Desktop Manager</li> <li>Secure Desktop Manager</li> <li>Secure Desktop Manager</li> <li>Decollazation</li> <li>Language Localization</li> <li>Advanced</li> </ul>				
Site-to-Site VPN	Find:	Match Case		
Device Management				
»			Reset Apply	

Step 2. Provide a Name for the Group Policy. Assign/Create an Address Pool. Choose Tunneling Protocols as SSL VPN Client and/or IPsec IKEv2, as shown in the image.

• • •		Edit Internal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers	Name: AnyConnect_MGMT_	Tunnel	
Advanced	Banner: 🗹 Inherit		
	SCEP forwarding URL: 🗹 Inherit		
	Address Pools: Inherit VPN_Po	lool	Select
	IPv6 Address Pools: 🗹 Inherit		Select
	More Options		*
	Tunneling Protocols:	Inherit Clientless SSL VPN 🗹 SSL VPN Client IPsec IKEv1 🗹 IPsec IKEv2	L2TP/IPsec
	Filter:	✓ Inherit	Manage
	Access Hours:	✓ Inherit	Manage
e	Simultaneous Logins:	✓ Inherit	
	Restrict access to VLAN:	✓ Inherit	0
	Connection Profile (Tunnel Group) Lock:	✓ Inherit	٥
	Maximum Connect Time:	✓ Inherit Unlimited minutes	
	Idle Timeout:	✓ Inherit	
	Security Group Tag (SGT):	✓ Inherit None (2 – 65519)	
	On smart card removal:	☑ Inherit Olisconnect OKeep the connection	
	Timeout Alerts		
	Maximum Connect Time Alert Interval:	✓ Inherit Default minutes	
	Periodic Certificate Authentication Interval	: 🗹 Inherit 🗌 Unlimited hours	
Find:	Next	Previous	
		Help Careel OK	
		neip Cancel OK	

Step 3. Navigate to Advanced > Split Tunneling. Configure the Policy as Tunnel Network List Below and choose the Network List, as shown in the image.

		Edit Internal G	roup Policy: AnyConnect_MGMT_	Tunnel	
General Servers	The VPN client makes split tunneling de fields.	cisions on the	basis of a network list that can	be specified below by providing the proper parameters to 'Policy' an	d 'Networl
Split Tunneling	DNS Names:	🗹 Inherit			
Browser Proxy ► AnyConnect Client ► IPresc(I/Er/1) Client	Send All DNS Lookups Through Tunnel:	🗌 Inherit	🔿 Yes 💿 No		
P IFSec(IKEV1) Client	Policy:	🗌 Inherit	Tunnel Network List Below	<b>C</b>	
	IPv6 Policy:	🗹 Inherit		0	
	Network List:	Inherit	VPN-Split	<b>•</b>	Manag
•	Pressing this button to set up split exlus Set up Split Exclusion for Web Securi Intercept DHCP Configuration Message	sion for Web S ty from Microso	iecurity proxies. ft Clients		
Find:	Next 🔮	Previous			
		Help	Cancel OK	1	

**Note:** If a client address is not pushed for both IP protocols (IPv4 and IPv6), the Client Bypass Protocol setting must be enabled so that the traffic that corresponds is not disrupted by the management tunnel. To configure, refer to <u>Step 4</u>. Step 4. Navigate to Advanced > AnyConnect Client. Set Client Bypass Protocol to Enable. Click OK to Save, as shown in the image.

eneral	Keep Installer on Client System:	🔽 Inherit	O Yes	No	
ervers	Datagram Transport Layer Security (DTLS):	Inherit	C Enable	Disable	
Split Tunneling	DTLS Compression:	Inherit	Enable	Disable	
Browser Proxy	SSL Compression:	Inherit	Deflate	LZS Disable	
IPsec(IKEv1) Client	Ignore Don't Fragment(DF) Bit:	Inherit	Enable	Disable	
	Client Bypass Protocol:	🗌 Inherit	Enable	Disable	
	FQDN of This Device:	🗹 FQDN			
	MTU:	🗹 Inherit			
	Keepalive Messages:	🗹 Inherit	Disable Ir	seconds	
	Optional Client Modules to Download:	🗹 Inherit			
•	Always-On VPN:	🗹 Inherit	O Disable	Use AnyConnect Profile setting 🛛 💿	
	Client Profiles to Download:	🗹 Inherit			
		🕈 Add 📋	Delete		
		Profile Name		Profile Usage/Type	
		L			
	🔘 Next 🔘	Previous			
d:					
	🔘 Next 🔘	Previous			

Step 5. As shown in this image, click Apply to push the configuration to the ASA.

🚮 Hom	e 🦂 Configuration 🔯 Monitoring 🔒	Save 🔇 Refresh 🔇 Back 🔘 Forw	rard <b>? Help</b> Type topic Go		cisco
00	Remote Access VPN	Configuration > Remote Acc	cess VPN > Network (Client) Acces	s > Group Policies	
marks	Pintroduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localizati AnyConnect Client Profile AnyConnect Client Software	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes Add - C Edit Delete As	roup is a collection of user-orientee VPN connection profiles and user ac from an LDAP server you must use a sign	I authorization attribute/value pairs that may be stored in counts. n LDAP attribute map.	Iternally on the device or externally on a RADIUS/LDAP server. The group
ookr	B Dynamic Access Policies	Name	Туре	Tunneling Protocol	Assigned To
aš m	Breck(KEyl) Connection Profiles	AnyConnect	Internal	ssi-client	AnyConnect
	Prec(KEv1) Connection Profiles	DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;DefaultWE
	Secure Mobility Solution	AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel
	BAddress Assignment     Gadvance     Glendess SSLVPN Access     Advanced     Glendess SSLVPN Access     Advanced     Glendess SSLVPN Access     Guest Users     Guest Use				
0	Site-to-Site VPN				
	Bala Harris	Find:	Match Case		
	Device Management			Reset Apply	

CLI Configuration for Group Policy:

```
<#root>
```

ip local pool

#### VPN\_Pool

192.168.10.1-192.168.10.100 mask 255.255.255.0 ! access-list

#### VPN-Split

standard permit 172.16.0.0 255.255.0.0
!
group-policy

#### AnyConnect\_MGMT\_Tunnel

internal group-policy

#### AnyConnect\_MGMT\_Tunnel

attributes vpn-tunnel-protocol

ikev2 ssl-client

```
split-tunnel-network-list value
```

#### VPN-Split

```
client-bypass-protocol enable
```

address-pools value

VPN\_Pool

 $Step \ 6. \ Create \ the \ AnyConnect \ Connection \ Profile. \ Navigate \ to \ Configuration > Remote \ Access \ VPN > Network \ (Client) \ Access > AnyConnect \ Connection \ Profile. \ Click \ Add.$ 

**Note:** It is advisable to create a new AnyConnect Connection Profile which is used for the AnyConnect Management tunnel only.



Step 7. Provide a Name for the Connection Profile, and set Authentication Method as Certificate only. Choose the Group Policy as the one created in <u>Step 1</u>.

Basic	Name:	AnyConnect_MGMT_Tunnel	
Advanced	Aliases:		
	Authentication		
	Method:	Certificate only	
	AAA Server Group:	LOCAL	S Manage
		Use LOCAL if Server Group fails	
	SAML Identity Provider		
	SAML Server :	None	ᅌ Manage
	Client Address Assignment	t	
	DHCP Servers:		
		None DHCP Link DHCP Subnet	
	Client Address Pools:		Select
	Client IPv6 Address Pool	s:	Select
	Default Group Policy		
	Group Policy:	AnyConnect_MGMT_Tunnel	Manage
	(Following fields are link	ed to attribute of the group policy selected above.)	
	🗹 Enable SSL VPN cli	ent protocol	
	Enable IPsec(IKEv2	) client protocol	
	DNS Servers:		
	WINS Servers:		
	Domain Name:		
Finds		A Neutral Descious	
Find:		Vext Previous	

**Note:** Ensure that the Root certificate from Local CA is present on the ASA. Navigate to Configuration > Remote Access VPN > Certificate Management > CA Certificates to add/view the certificate.

**Note:** Ensure that an Identity certificate issued by the same Local CA exists in the Machine Certificate Store (For Windows) and/or in System Keychain (For macOS).

Step 8. Navigate to Advanced > Group Alias/Group URL. Click Add under Group URLs and add an URL. Ensure Enabled is checked. Click OK to Save, as shown in the image.

Add AnyConnect Connection Profile

Basic Advanced General Client Addressing Authentication Secondary Authentication Authorization Accounting Group Alias/Group URL	<ul> <li>Enable the display of Radius Reject-Message on the login screen when authentication is rejected</li> <li>Enable the display of Securld messages on the login screen</li> <li>Connection Aliases</li> <li>This SSL VPN access method will present a list of aliases configured for all connection profiles. You r the Login Page Setting in the main panel to complete the configuration.</li> <li>Add Delete (The table is in-line editable.)</li> <li>Alias</li> </ul>
	Group URLs This SSL VPN access method will automatically select the connection profile, without the need for use Add Delete (The table is in-line editable.) • URL Enabled URL: https://asa.example.com/AnyConnect_MGMT_Tunnel ✓ Enabled Help Cancel OK
Find:	Next Previous      Help Cancel OK

If IKEv2 is used, ensure IPsec (IKEv2) Access is enabled on the interface used for AnyConnect.

O O Remote Access VPN	Config	Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles									
Introduction Network (Client) Access AnyConnect Connection Profiles	The security Client suppo	The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEV2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.									
S AnyConnect Customization/Local	Access Interfa	ces									
anyConnect Client Profile	Enable 0	isco AnyConnect	VPN Client access	on the interfaces	selected in the table below						
AnyConnect Client Software	SSL access r	nust be enabled if	you allow AnyCor	pect client to be l	aunched from a browser (V	leb Launch) .					
Group Policies	Interface SSL Access IPsec (IKEv2) Access Allow Access Enable DTLS Allow Access Enable Client Services Device Contificute										
Psec(IKEv1) Connection Profiles	outside	outside 2 2 2 2 C C Centre Certificate									
Secure Mobility Solution	inside			0	0	Port Settings					
Sp Address Assignment											

Step 9. Click Apply to push the configuration to the ASA.

....



CLI configuration for connection profile (tunnel-group):

```
<#root>
tunnel-group
AnyConnect_MGMT_Tunnel
type remote-access
tunnel-group
AnyConnect_MGMT_Tunnel
general-attributes
default-group-policy AnyConnect_MGMT_Tunnel
tunnel-group AnyConnect_MGMT_Tunnel webvpn-attributes
authentication certificate
group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable
```

Step 10. Ensure that a trusted certificate is installed on the ASA and bound to the interface used for AnyConnect connections. Navigate to Configuration > Remote Access VPN > Advanced > SSL Settings to add/view this setting.



Remote Access VPN	Configuration > Remote Acce	ss VPN > Advanced > SSL Settings				
Introduction						
Network (Client) Access AnyConnect Connection Pr	Configure SSL parameters. These par	ameters affect both ASDM and SSL VPN acc	ess.			
AnyConnect Customization	The minimum SSL version for the sec	urity appliance to negotiate as a "server":	TLS V1	0	O DTLSV1 O DTLSV1.2	
AnyConnect Client Softwar	The minimum SSL version for the sec	urity appliance to negotiate as a "client":	TLS V1	۵		
Group Policies	Diffie-Hellman group to be used wit	n SSL:	Group2 - 1024-bit modulus	0		
IPsec(IKEv1) Connection P IPsec(IKEv2) Connection P	ECDH group to be used with SSL:		Group19 - 256-bit EC	2		
Secure Mobility Solution	Encountion					
Sp Address Assignment	cheryption				An an an Andrea	_
Advanced	Cipher version	Cipher Security Level		Cipher Algorithms/	Custom String	Edit
Clientless SSL VPN Access	Deraut	Medium		DES-CBC3-SHA A	ES128-SHA DHE-KSA-AES128-SHA AES256-SHA DHE-KSA	
AAA/Local Users	TLSVI	Medium		DHE-KSA-AES256	-SHA AES256-SHA DHE-KSA-AES128-SHA AES128-SHA	
AAA Server Groups	TLSV1.1	Medium		DHE-RSA-AES256	-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
Se I DAR Ancibude Man	115V1.2	Medium		ECDHE-ECDSA-AE	S256-GCM-SHA384 ECDHE-KSA-AES256-GCM-SHA384 D.	
	DTLSV1	Medium		DHE-RSA-AES256	-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
g Local Users	DTLSV1.2	Medium		ECDHE-ECDSA-AB	S256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D.	
Secure Desktop Manager						
Certificate Management						
Language Localization						
Load Balancing						
DHCP Server	Server Name Indication (SNI)					
DNS	Domain		Certificate			Add
Advanced						
+2+ Connection Gateway						Edit
SSL Settings						
Reference Identity						Delete
Continents to Am Connect						
Certificate to AnyConnect						
HTTP Redirect						
Maximum VPN Sessions						
💕 Crypto Engine						
	Certificates					
	Specify which certificates, if any, s	hould be used for SSL authentication on ea	ch interface. The fallback certificate	will be used on interface	is not associated with a certificate of their own.	
evice Setup	Interface	Primary Certificate	Load Balancing Certificate		Key-Type	Edit
evice setup	inside					
irewall	management					
	outside	ROOT-CA:hostname=ASA.example	.co		Primary: RSA (2048 bits), Load Balancing: none	
Remote Access VPN						
ite-to-Site VPN						
Device Management						
			Recet Ann	ala c		

CLI Configuration for SSL Trustpoint:

<#root>

ssl trust-point ROOT-CA outside

### **Creation of AnyConnect Management VPN Profile**

Step 1. Create the AnyConnect Client Profile. Navigate to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. Click Add, as shown in the image.

	Home 🍫 Configuration 📴 Monitori	ng 🔚 Save 🔇 Refresh 🔇 Back 🔘 Fo	orward 🍞 Help Type topic Go			cisco
	O O Remote Access VPN	○ ○ ○ Configuration > Remote Access	VPN > Network (Client) Access > AnyCo	nnect Client Profile		
oolmarks	Introduction     Directory Connection Profil     Directory Connect Connection Profil     Directory Connect Clant Profile     Directory Connect Clant Profile     Directory Profile     Directory Profile     Directory Profile     Directory Profile	This panel is used to manage AnyConne button to add a new profile. Pressing the The profile Usage field is introduced wit HostScan configuration can be performe Add Edit 22 Change Group Policy	ct Client Profiles and perform group assign e Import or Export button is for upload and h the Secure Mobility Solution. This field cc ed by going to Secure Desktop Manager/Ho going to Secure Desktop Manager/Ho Delete The Import Secure Construction (Construction)	ment for AnyConnect version 2.5 or later.You can select download of client profiles between local machine and d ontains different profile usage in AnyConnect version 3.0 stScan. If 'HostScan' is not visible under 'Secure Desktop te	a profile to edit, change group or to delete. You can select the 'Add' evice. and later. Manager', you will need to restart ASDM.	
	IPsec(IKEv1) Connection Profil	Profile Name	Profile Usage	Group Policy	Profile Location	
	Prectitiev2) Connection Profil     Secure Mobility Solution     Address Assignment     Signature Mobility Solution     Address Assignment     Signature MAA/Local Users     AAA/Local Users     AAA/Local Users     Control Desktop Manager     Control Desktop Manager     Certificate Management     Language Localization     DHCP Server     OHCP Server     OHCP Server     Contection Gateway     Sis Settings					
	<ul> <li>Reference Identity</li> <li>Certificate to AnyConnect and</li> <li>HTTP Redirect</li> <li>Maximum VPN Sessions</li> <li>Crypto Engine</li> </ul>					
	Device Setup					
	Remote Access VPN					
	Site-to-Site VPN					
	*			Reset Apply		

Step 2. Provide a Profile Name. Choose the Profile Usage as AnyConnect Management VPN profile. Choose the Group Policy created in <u>Step 1</u>. Click OK, as shown in the image.

Profile Name		Profile Usage	Group Policy	Profile Location
	• • •	Add AnyConnect Client	Profile	
	Profile Name	AnyConnect_MGMT_Profile		
	Profile Usage	AnyConnect Management VPN Profile		
	Enter a device f created if it do	file path for an xml file, ie. disk0:/ac_profile. The file es not exist.	e will be automatically	
	Profile Location	n disk0:/anyconnect_mgmt_profile.vpnm	Browse Flash	
			Upload	
	Group Policy	AnyConnect_MGMT_Tunnel		
	_	Enable 'Always On VPN' for selected group		
		Help Cancel	ОК	

Step 3. Choose the Profile created and click **Edit**, as shown in the image.



Step 4. Navigate to Server List. Click Add to add a new Server List Entry, as shown in the image.

• •	Any	Connect Client Profile Ed	itor - AnyConnect_MGI	MT_Profile			
Profile: AnyConnect_MG	MT_Profile					About	
VPN Preferences (Part 1) Preferences (Part 2) Backup Servers Certificate Pinning Certificate Matching Server List	Server List						
	Hostname	Host Address	User Group	Backup Server List	Certificate Pins		
•	Note: at most o	ne server can be defined	d in a management VP	N profile. Add Edit	Delete Details		
	<u></u>	Help	ancel OK				

Step 5. Provide a Display Name. Add the FQDN/IP address of the ASA. Provide the User Group as the tunnel group name. Group URL is automatically populated with the FQDN and User Group. Click OK.

Server	Certificate Pinning
Primary Server Display Name (required) AnyConnect_MGMT_Tunnel FQDN or IP Addr User Group (required)	Connection Information Primary Protocol SSL  ASA gateway Auth Method During IKE Negotiation
Group URL asa.example.com/AnyConnect_MGMT_Tunnel	IKE Identity (IOS gateway only)
Backup Servers Host Address	Add
	Move Up Move Down
	Delete
ОК	Cancel

**Note:** The FQDN/IP Address + User Group must be the same as the Group URL mentioned during the configuration of the AnyConnect Connection Profile in <u>Step 8</u>.

**Note:** AnyConnect with IKEv2 as a protocol can also be used to establish Management VPN to ASA. Ensure Primary Protocol is set to IPsec in <u>Step 5</u>.

Step 6. As shown in the image, click OK to Save.

8 🔘 🖶	AnyC	connect Client Profile Edit	or - AnyConnect_MGM	Γ_Profile	
Profile: AnyConnect_MG	iMT_Profile				Abo
VPN Preferences (Part 1) Preferences (Part 2)	Server List				
Backup Servers	Hostname	Host Address	User Group	Backup Server List	Certificate Pins
Certificate Finning	AnyConnect_MGMT	_T asa.example.com	AnyConnect_MGMT_	T Inherited	J
	Note: at most or	e server can be defined	in a management VPN	profile Add	Delete
	Note. at most of	le server can be denned	in a management vriv	Edit	Details
		Help Ca	ncel OK		

Step 7. Click Apply to push the configuration to the ASA, as shown in the image.



CLI Configuration after the addition of AnyConnect Management VPN Profile.

<#root>

#### webvpn

```
enable outside
hsts
 enable
 max-age 31536000
 include-sub-domains
 no preload
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
I
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-network-list value VPN-Split
 client-bypass-protocol enable
 address-pools value VPN_Pool
```

webvpn

anyconnect profiles value AnyConnect\_MGMT\_Profile type vpn-mgmt

#### AnyConnect Management VPN Profile on AnyConnect Client Machine:

<#root>

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSc
    <ClientInitialization>
        <UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>
        <AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
        <ShowPreConnectMessage>false</ShowPreConnectMessage>
        <CertificateStore>Machine</CertificateStore>
        <CertificateStoreMac>System</CertificateStoreMac>
        <CertificateStoreOverride>true</CertificateStoreOverride>
        <ProxySettings>IgnoreProxy</ProxySettings>
        <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
        <AuthenticationTimeout>30</AuthenticationTimeout>
--- Output Omitted ---
        <CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
        <AllowManualHostInput>false</AllowManualHostInput>
    </ClientInitialization>
<ServerList>
        <HostEntry>
            <HostName>AnyConnect_MGMT_Tunnel</HostName>
            <HostAddress>asa.example.com</HostAddress>
            <UserGroup>AnyConnect_MGMT_Tunnel</UserGroup>
        </HostEntry>
```

</ServerList>

</AnyConnectProfile>

**Note:** If Trusted Network Detection (TND) is used in the User AnyConnect VPN profile, it is advisable to match the same settings in the Management VPN Profile for a consistent user experience. The management VPN tunnel is triggered based on the TND settings applied to the User VPN tunnel profile. Additionally, the TND Connect action in the management VPN profile (enforced only when the management VPN tunnel is active), always applies to the user VPN tunnel, to ensure that the management VPN tunnel is transparent to the end user.

Note: On any end-user PC, if the Management VPN profile has the TND settings enabled and if the user VPN profile is missing, it considers the default preferences settings for the TND (it is disabled on the default preferences in the AC client application) in place of missing user VPN profile. This mismatch can lead to unexpected/undefined behavior.

By default, TND settings are disabled in the default preferences.

To overcome the default preferences hardcoded settings in the AnyConnect Client application, the

end-user PC must have two VPN profiles, a user VPN profile & an AC Management VPN profile, and both of them must have the same TND settings.

The logic behind Management VPN tunnel connection and disconnection is that to establish a Management VPN tunnel, the AC agent uses the user VPN profile TND settings and for disconnection of the Management VPN tunnel, it checks for management VPN profile TND settings.

### **Deployment Methods for AnyConnect Management VPN Profile**

• A successful User VPN connection is completed with the ASA Connection Profile in order to download the AnyConnect Management VPN Profile from the VPN Gateway.

**Note:** If the protocol used for the Management VPN tunnel is IKEv2, the first connection is needed to be established through SSL (In order to download the AnyConnect Management VPN profile from the ASA).

• The AnyConnect Management VPN Profile can be manually uploaded to the client machines either through a GPO push or by manual installation (Ensure the name of the profile is VpnMgmtTunProfile.xml).

Location of Folder where the profile needs to be added: Windows: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun macOS: /opt/cisco/anyconnect/profile/mgmttun/

### (Optional) Configure a Custom Attribute to Support Tunnel-All Configuration

Management VPN tunnel requires a split that includes tunneling configuration, by default, to avoid an impact on the user-initiated network communication. This can be overridden when you configure the custom attribute in the group policy used by the management tunnel connection.

Step 1. Navigate toConfiguration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. Click Add, as shown in the image.



Step 2. Set the custom attribute Type to ManagementTunnelAllAllowed and provide a Description. Click OK, as shown in the image.

_			Des			
			Des	cription		
		Create Custom A	ttribute Type			
	•	Create Custom A	utribute Type			
Тур	e: Managerr	Create Custom A	ttribute Type			
Тур	e: Managen	Create Custom A tentTunnelAllAllowed	ttribute Type			
Тур	Managem	Create Custom A tentTunnelAllAllowed entTunnelAllAllowed	.ttribute Type			
Typ Des	e: Managem Managem :cription:	Create Custom A tentTunnelAllAllowed entTunnelAllAllowed	.ttribute Type			
Typ Des	e: Managem Managem	Create Custom A tentTunnelAllAllowed entTunnelAllAllowed	uttribute Type			
Typ Des	e: Managen Managem :cription:	Create Custom A nentTunnelAllAllowed entTunnelAllAllowed	uttribute Type			

Step 3. Navigate to Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. Click Add, as shown in the image.



Step 4. Choose the Type as ManagementTunnelAllAllowed . Set the Name as true. Click Addto provide a custom attribute value, as shown in the image.

○ ○ ○ Configuration > Remo	ote Access VPN > Network (Client) Acce	ess > Advanced > AnyConnect Custor	n Attribute Names
Declarations of custom attrib	ute names and these attributes are enfor	ced in <u>AnyConnect group policy</u> and <u>Any</u>	Connect dynamic access policy
🕈 Add 🗹 Edit 📋 Delete			
Type Name Values			
	Create Custom At	ttribute Name	
Type:	ManagementTunnelAllAllowed		Manage
.,pe.			
Name:	true		
	Value	Add	
		Edit	
		Delete	
		Delete	
Configure Values			
Configure values:			
	Help Canc	el OK	



		Create Custom Attril	oute Name			
Type:	ManagementTunn	Manage				
Name:	true					
	Value			Add		
		Add	Value	e.e.		
true						
Value:						
Value:						
Value:						
Value:						
Value:						
Value:						

 $Step \ 6. \ Navigate \ to \ Configuration > Remote \ Access \ VPN > Network \ (Client) \ Access > Group \ Policies. \ Choose \ the \ Group \ Policy. \ Click \ Edit \ , as \ shown \ in \ the \ image.$ 

đ	Home 🖓 Configuration 📴 Monitoring	🔜 Save 💽 Refresh 🤇	Back 🔘 Forward	<b>?</b> Help Type topic	Go		cisco
	O O Remote Access VPN	O O O Configuratio	on > Remote Access	VPN > Network (Client	Access > Group Policies		
ks 💼 Device List	Introduction     Introduction     Network (Client) Access     AnyConnect Connection Profiles     AnyConnect Customization/Localization     AnyConnect Client Profile     AnyConnect Client Profile	Manage VPN group server. The group p To enforce authoriz Add C Z Edit	policies.A VPN group olicy information is ration attributes from Delete 🔀 Assign	p is a collection of user-o referenced by VPN conne n an LDAP server you mus	riented authorization attribute/value pairs tha tion profiles and user accounts. t use an LDAP attribute map.	t may be stored internally on the device or externally on a RADIUS/L	DAP
okmar	Polynamic Access Policies	Name		Туре	Tunneling Protocol	Connection Profiles/Users Assigned To	
ĝ	Group Policies	AnyConnect		Internal	ssl-client	AnyConnect	
	Psec(IKEv1) Connection Profiles	DfltGrpPolicy (Syster	n Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup	p;Def
	IPsec(IKEv2) Connection Profiles	AnyConnect_MGMT	Tunnel	Internal	ikev2:ssl-client	AnyConnect_MGMT_Tunnel	
	Secure Mobility Solution						
	<ul> <li>Secure Mobility Solution</li> <li>Advanced</li> <li>Advanced</li> <li>Advanced</li> <li>Advanced Casentials</li> <li>AnyConnect Custom Attributes</li> <li>AnyConnect Custom Attributes</li> <li>AnyConnect Custom Attribute Names</li> <li>Imprecent Casentials</li> <li>AnyConnect Custom Attributes</li> <li>Advanced</li> <li>Clentless SSL VPN Access</li> <li>Advaload Users</li> <li>GLDP Attribute Map</li> <li>GLDP Context Control Users</li> <li>Secure Desktop Manager</li> <li>Certificate Management</li> <li>Language Localization</li> <li>Land Balancing</li> <li>DHCP Server</li> <li>DNS</li> <li>Advanced</li> </ul>						
	Device Setup						
	🟭 Firewall						
	Memote Access VPN						
	Site-to-Site VPN	Find:	00	Match Case			
	Device Management				Reset Apply		

Step 7. As shown in this image, navigate to Advanced > Split Tunneling. Configure the Policy as Tunnel All Networks.

• •	Edit Internal Gro	oup Policy: AnyConnect_MGMT_Tunnel	
General Servers	The VPN client makes split tunneling decisions on the basi fields.	s of a network list that can be specified below by providing the proper parameters to 'Policy' and 'I	Network Li
Split Tunneling	DNS Names: 🔽 Inherit		
Browser Proxy AnyConnect Client	Send All DNS Lookups Through Tunnel: 🗌 Inherit 💦	Yes 🕐 No	
IPsec(IKEv1) Client	Policy: Inherit	unnel All Networks	
	IPv6 Policy: 🗹 Inherit	•	
	Network List:	0	Manage
	Pressing this button to set up split exlusion for Web Securi Set up Split Exclusion for Web Security Intercept DHCP Configuration Message from Microsoft Cli	ty proxies. ents	
Find:	Next Previous		
	Help	Cancel	

Step 8. Navigate to Advanced > Anyconnect Client > Custom Attributes. Click Add, as shown in the image.

• • •	Edit Internal Group Policy: AnyConnect_MGMT_Tunnel
General Servers V Advanced Split Tunneling Browser Proxy V AnyConnect Client Login Setting Client Firewall Key Regeneration Dead Peer Detection Customization Custom Attributes IPsec(IKEv1) Client	Configuration of custom policy attributes.   Image: Configuration of custom policy attributes.     Type     Name of Value
Find:	Next Previous
	Help Cancel OK

Step 9. Choose the Attribute type as ManagementTunnelAllAllowed and choose the Value as true. Click OK, as shown in the image.

🕈 Add 🗹 Edit	t 📋 Delete	
Гуре		Name of Value
		Create Custom Attribute
	Attribute type	ManagementTunnelAllAllowed
	Attribute type.	
	Omit the value	
	Select Value:	true Manage
	Select value.	
		Help Cancel OK

Step 10. Click Apply to push the configuration to the ASA, as shown in the image.

🚮 Home 🍕 Configuration 📴 Monitoring 🚛	🕽 Save 🔇 Refresh 🔇 Back 🔘 Forw	rard 💡 Help Type topic Go			cisco
000 Remote Access VPN	○ ○ ○ Configuration > Remote Acc	cess VPN > Network (Client) Acces	s > Group Policies		
Pintroduction     Network (Client) Access     AnyConnect Connection Profiles     AnyConnect Customization/Localizati     AnyConnect Client Profile	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes i Add Tal Edit Delete As	roup is a collection of user-oriented VPN connection profiles and user ac- from an LDAP server you must use a sign	authorization attribute/value pairs that may be stored i counts. n <u>LDAP attribute map</u> .	nternally on the device or externally on a RADIUS/LDAP server. The	group
AryConnect Client Software     Dynamic Access Policies     Group Polices     Precent Policy Polices     Psec(IKEV1) Connection Profiles     Psec(IKEV2) Connection Profiles     Secure Mobility Solution	Name AnyConnect DfltGrpPolicy (System Default) AnyConnect_MGMT_Tunnel	Type Internal Internal Internal	Tunneling Protocol ssl-client ikev2;ikev2;i2tp-ipsec ikev2;ssl-client	Connection Profiles/Users Assigned To AryConnect DefaultRAGroup;Default/2LGroup;DefaultADMINGroup AnyConnect_MGMT_Tunnel	);DefaultWE
P ≧g Address Assignment     F S Address Assignment     F Address SSL VPN Access     AAA/Local Users     AAA/Local Users     AAA/Local Users     DaP Attribute Map     Go Local Users     Asserver Groups     Secure Depond Manager     B Secure Depond M					
G Language Localization					
Bevice Setup					
Stemote Access VPN           Site-to-Site VPN	Find:	Match Case			
Device Management			Reset		

CLI Configuration after the ManagementTunnelAllAllowed Custom Attribute is added:

<#root>

webvpn

enable outside

anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed

```
hsts
 enable
 max-age 31536000
 include-sub-domains
 no preload
 no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
ļ
anyconnect-custom-data ManagementTunnelAllAllowed true true
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelall
client-bypass-protocol enable
 address-pools value VPN_Pool
 anyconnect-custom ManagementTunnelAllAllowed value true
webvpn
```

anyconnect profiles value AnyConnect\_MGMT\_Profile type vpn-mgmt

## Verify

Verify the Management VPN tunnel connection on ASA CLI with the show vpn-sessiondb detail anyconnect command.

<#root>
ASA#
show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username :
vpnuser
Index : 10
Assigned IP :

192.168.10.1 Public IP : 10.65.84.175 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel : AnyConnect Premium License Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Hashing : 17238 Bytes Rx : 1988 Bytes Tx Pkts Tx : 12 Pkts Rx : 13 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : AnyConnect\_MGMT\_Tunnel Tunnel Group : AnyConnect\_MGMT\_Tunnel Login Time : 01:23:55 UTC Tue Apr 14 2020 : Oh:11m:36s Duration Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : c0a801010000a0005e9510ab Security Grp : none AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 --- Output Omitted ---DTLS-Tunnel: Tunnel ID : 10.3 Assigned IP : 192.168.10.1 Public IP : 10.65.84.175 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 57053 UDP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 18 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03036 Bytes Tx : 17238 Bytes Rx : 1988 Pkts Tx : 12 : 13 Pkts Rx Pkts Tx Drop : 0 Pkts Rx Drop : 0

Verify the Management VPN tunnel connection on ASDM.

Navigate to **Monitoring > VPN > VPN Statistics > Sessions**. Filter By **AnyConnect Client** to see the client session.

Home of Configuration M	onitoring 3 Save (	Refresh Sa	ck 🔘 Forward	Help Type topic Go					cisco
	Type AnyConnect Client SSL/TLS/DTLS	Active	1	Cumulative	Peak Concurrent 19 19		Inactive 1 1	2	0
VPN VPN Statistics VPN Statistics VPN Cluster Loads Crypto Statistics Compression Statistics Encryption Statistics Clobal IKE/IPsec Statistics VLAN Mapping Sessions Clientless SSL VPN Shared SSL VPN Shared SSL VPN WAN Connection Graphs WSA Sessions	Filter By AnyCo Username Vpnuser	Group Policy Genection Prefile AnyConnect_MGMT. AnyConnect_MGMT.	All Se Public IP Address Public IP Address .192.168.10.1 .10.65.84.175	Protocol Encryption AnyConnect-Parent AnyConnect-Parent: (1	Filte Login Time Duration 10:52:25 UTC 0h:01m:31s	r Bytes Tx Bytes Ru 34688 33954	Inactivity Oh:00m:00s	Audit : c0a80	Details Logout Ping
Interfaces  VPN  Routing  Properties	To sort VPN sessio Logout By: A	ns, right–click on th All Sessio ᅌ	ne above table and se	lect Table Sort Order fr Logout Sessions	om popup menu.				

### Verification of the Management VPN tunnel connection on the Client Machine:

Sisco AnyConnect Secure Mobil	ity Client	- 🗆 X	
cisco AnyCon	nect Secure Mobility C	lient	
Virtual Private Network (VPI	۷)	Diagnostics	
Preferences Statistics Route Detail	Is Firewall Message History		
Connection Information State: Tunnel Mode (IPv4):	Disconnected Not Available	Cisco AnyConnect Secure Mobility Client	- 🗆 X
Dynamic Tunnel Exclusion: Dynamic Tunnel Inclusion: Duration: Session Disconnect:	Not Available Not Available 00:00:00 None	VPN: Ready to connect.	✓ Connect
Management Connection State:	Connected (asa.example.com)		
Client (IPv4): Client (IPv6): Server:	Not Available Not Available Not Available	♦ ①	uluiu cisco
Bytes		A v	
	Re	set Export Stats	

### Troubleshoot

The new UI Statistics line (Management Connection State) can be used to troubleshoot management tunnel connectivity issues. These are the commonly seen error states:

Disconnected (disabled):

- The feature is disabled.
- Ensure that the management VPN profile was deployed to the client, via user tunnel connection (requires you to add the management VPN profile to the user tunnel-group policy) or out of band through the manual upload of the profile.
- Ensure that the management VPN profile is configured with a single host entry that includes a tunnel group.

Disconnected (trusted network):

• TND detected a trusted network so the management tunnel is not established.

Disconnected (user tunnel active):

• A user VPN tunnel is currently active.

Disconnected (process launch failed):

• A process launch failure was encountered when the management tunnel connection is attempted.

Disconnected (connect failed):

- A connection failure was encountered when the management tunnel is established.
- Ensure that the certificate authentication is configured in the tunnel group, no banner is present in the group policy, and the server certificate must be trusted.

Disconnected (invalid VPN configuration):

- An invalid split tunneling or client-bypass-protocol configuration was received from the VPN server.
- Check your configuration in the management tunnel-group policy against the documentation.

Disconnected (software update pending):

• An AnyConnect software update is currently pending.

Disconnected:

• The management tunnel is about to be established or can not be established for some other reason.

<u>Collect DART</u> for further troubleshooting.

### **Related Information**

- <u>Configuration of Management VPN Tunnel</u>
- <u>Troubleshooting Management VPN Tunnel</u>
- <u>Technical Support & Documentation Cisco Systems</u>