Doc type Migration guide IIIIII CISCO The bridge to possible

Migration Guide

DigiCert (Symantec) Certificate to Cisco PKI Certificate on Cisco SD-WAN Controllers

Table of Contents

1

Goal of this Document	3
Pre-requisites	3
Migration Steps to Install Signed Cisco PKI Certificate to Controllers	4
Option1: Automated certificate signing through Cisco Systems	4
Key Considerations:	5
Step1: Verify Cisco Plug and Play (PnP) portal connectivity	5
Step 2: Configure Smart Account credentials	6
Step 2: Configure vManage certificate settings	7
Step 3: Generate certificate signing requests	7
Step 4: Sign and install certificate signing requests	8
Option 2: Manual certificate signing through Cisco Systems	10
Step 1: Configure vManage certificate settings	10
Step 2: Generate Certificate Signing Requests	11
Step 3: Submit and sign the certificate signing requests	12
Step 4: Install the signed certificates	14
Verification:	15
Additional Resources:	16

1

Goal of this Document

The primary goal of the document is to provide technical guidance on the steps needed to successfully migrate DigiCert (Symantec) certificate to Cisco PKI certificate on the Cisco SD-WAN controllers solution. It includes automated and manual methods for obtaining signed controller certificates from Cisco Plug and Play portal.

This guide assumes that the vBond, vSmart and vManage controllers are already deployed with certificate provided by DigiCert (Symantec).

Pre-requisites

- Recommended software version to migrate to Cisco PKI certificate are SD-WAN controllers and vEdge routers to run 19.2.3+ and XE SD-WAN routers to run 16.12+
- You will need a Smart Account and Virtual Account at http://software.cisco.com to use the automated or manual method. The Smart Account credentials should be configured in the vManage GUI under Administration>Settings>Smart Account Credentials
- It is important that the Virtual Account in the Cisco PnP portal has a controller profile defined, and the organization name in the profile must match the organization name in the vManage GUI
- To check if DigiCert is installed, go to configured settings on vManage dashboard under Administration – Settings. If Symantec Automated/manual option is chosen, then it indicates that DigiCert certificates are installed.
- Ensure that Cisco root certificates are loaded on the WAN Edge devices before converting to Cisco PKI else the WAN Edge devices will not come up onto the network
- For XE SD-WAN routers, verify using the command: show sdwan certificate root-cacert | inc Cisco

C8Kv_Router# show sdwan certificate root-ca-cert | inc Cisco Issuer: OU=Arcturus, O=Cisco, CN=Internal Customer Root CA Subject: O=Cisco, OU=Albireo, CN=Viptela SubCA Issuer: OU=Arcturus, O=Cisco, CN=Internal Customer Root CA Subject: OU=Arcturus, O=Cisco, CN=Internal Customer Root CA For vEdge routers, verify using the command: show certificate root-ca-cert | inc Cisco

vEdge# show certificate root-ca-cert | inc Cisco
 Issuer: OU=Arcturus, O=Cisco, CN=Internal Customer Root CA Subject: O=Cisco,
 OU=Albireo, CN=Viptela SubCA Issuer: OU=Arcturus, O=Cisco, CN=Internal Customer
 Root CA Subject: OU=Arcturus, O=Cisco, CN=Internal Customer Root CA

Note:

- 1. For Cisco XE SD-WAN and Viptela Edge (vEdge) routers (running 19.2 or higher), Cisco PKI root certificate are bundled in the software by default or distributed by the PnP or ZTP server when the WAN edge is automatically provisioned
- 2. Reach out to TAC support if there are any issues with migration or if Cisco SD-WAN controllers run on version below 19.2.3 to get support on upgrade/migration process

Migration Steps to Install Signed Cisco PKI Certificate to Controllers

Option1: Automated certificate signing through Cisco Systems

With this option, certificate signing requests are automatically sent to the Cisco PnP cloud service where the certificate is signed. The vManage then automatically retrieves the certificate and installs on itself and vBond, vSmart controllers as well.



Key Considerations:

- Time taken to complete automated migration process (for vManage, vSmart & vBond controllers): ~ 15 minutes
- Control Connection expected to flap during certificate migration process
- vBond & vSmart controller downtime during migration: ~ 1 minute
- No service impact on WAN Edge routers

Step1: Verify Cisco Plug and Play (PnP) portal connectivity

- 1. A DNS server needs to be configured to resolve the hostname cloudsso.cisco.com and subsequently apx.cisco.com and swapi.cisco.com using ping command.
- 2. To validate if vManage can reach the Cisco PnP server, go to the vManage CLI, type in vshell, then type "curl https://cloudsso.cisco.com". You should see a message that the host is live.
- 3. Type in "curl https://apx.cisco.com" and you should get an html response from the server that the service unavailable. If the servers are not reachable, you should see "Failed to connect" messages. If they both succeed, then the automated process should work. Type in exit to end vshell mode.

vmanage:~\$ curl https://cloudsso.cisco.com
cloudsso is live
cloudsso2 is live
vmanage:~\$ curl https://apx.cisco.com
<html><body><h1>503 Service Unavailable</h1></body></html>
No server is available to handle this request.
vmanage:~\$

Note: Try curl -k "Cisco PnP Server URL" if you see SSL root certificate issue.

Step 2: Configure Smart Account credentials

Before you can enable automatic signing of Cisco certificates, Smart Account credentials must be configured. h

- 1. On the vManage GUI, Go to Administration>Settings.
- 2. At the bottom of the page, go to the right of Smart Account Credentials and click Edit.
- 3. Enter the Username and Password that gives you access to your Smart Account information at <u>https://software.cisco.com</u>.

≡	cisco vManage	💽 Select Resource Group 🗸 🌰 📋 🌲	Ø	admin 🔻
	ADMINISTRATION SETTINGS			
▫	Statistics Configuration	Collection Interval: 30 minutes	View	Edit
٠	Maintenance Window	Not Configured		Edit
٩	Identity Provider Settings	Disabled	View	Edit
ŵ	Statistics Database Configuration	c		
**	Google Map API Key	Maps API Key: AlzaSyA1PwZsBfTR4-PLCErEsI6qMfEiqnRV898	View	Edit
	Software Install Timeout	Download timeout: 60 mins.; Activate timeout: 30 mins.	View	Edit
	IPS Signature Update	Disabled	View	Edit
(Smart Account Credentials			
	Username			- 1
	username			- 1
	Password			_
				- 1
Ì	Save Cancel	2		

4. Click Save.

Step 2: Configure vManage certificate settings

- 1. On the vManage Administration > Settings page, go to the right of Controller Certificate Authorization and click Edit.
- 2. Select Cisco Automated (Recommended). If you change the setting, you will get a popup window asking to confirm the Certificate Authorization change. Click Proceed.
- 3. Select the Validity Period. Minimum is 1 year and maximum is 2 years.
- 4. Set the Certificate Retrieve Interval. This is the interval the vManage will check on whether the signed certificates are available after the CSR has been submitted. The default is 60 minutes, so you may want to decrease this value. Minimum is 1 minute, and maximum is 60 minutes.

Note: Recommended minimum interval is 3-4 minutes for successful certificate retrieval.

≡	cisco VManage		Select Resource Group 🗸	٠	B A) 🧿	adr	nin 🔻
۵	Configuration >	ADMINISTRATION SETTINGS						
*	Tools >	Organization Name	VAISH-SDWAN-LAB-AWS				View	Â
	Maintenance >	vBond	172.16.10.183 : 12346			View	Edit	
*	Administration >	Alarm Notifications	Disabled			View	Edit	
	Manage Users	Hardware WAN Edge Certificate Authorization	Onbox			View	Edit	
	Cluster Management	Controller Certificate Authorization	Manual	1				
	Integration Management	Certificate Signing by: Cisco (Recommended) Sym	antec O Manual O Enterprise Root Certificate					
	Root CA Management	Sync Root Certificate (Please sync root cert to all connected of	levices before saving Cisco PKI mechanism)					
	Disaster Recovery	1 Year 🗢						
	VPN Groups	Certificate Retrieve Interval						
	Colo Groups							
	VPN Segments							
	License Management	Save Cancel						

5. Click the Save button.

Step 3: Generate certificate signing requests

Next, generate and submit certificate signing requests.

- 1. Navigate to Configuration > Certificates and click the Controllers tab
- 2. On the right side of vManage, click three dots (...) and select Generate CSR from the drop-down box.
- 3. A pop-up window states that the generated CSR has been sent to Cisco for signing. Click Close.

≡	diala cisco	' Cisco vManage				📀 Select Resource Group 🗸	•	Û	¥0	Ø	admin 🔻
	\$ co	ONFIGURATION CERTIN	FICATES							1 Install	Certificate
	WAN	Edge List Controller	rs TLS Proxy								
	> Se	end to vBond									
۳ م	Q			Search Options 🗸						S T	otal Rows: 3
	->-	Controller Type	Hostname	System IP	Expiration Date	uuid		Op	peration Stat	tus	
**	>	vBond	vbond	30.30.30.30	25 May 2022 11:59:59	abd92540-a0b2-4cd4-bb2d-05fdbf565a	33	In	stalled		••• ^
	>	vSmart	vsmart	20.20.20.20	25 May 2022 11:59:59	f681eede-e738-4eb4-94c2-324d699161	af	VB	ond Update	d	
"	>	vManage	vManage	11.11.11.11	25 May 2022 11:59:59	5145d19f-e28a-4baa-856d-1d98866283	ob	VB	ond Update	d	
										View CSR View Certii Generate C Reset RSA Invalidate	ficate

4. Repeat the process for the vSmart and vBond controllers.

=	cisco	Cisco vManage			Select Resource Group 🗸	•	Þ	۰	0	
-	\$ co	NFIGURATION CERTIN	FICATES							
	WAN	Edge List Controller	rs TLS Proxy							
-	> Ser	nd to vBond								
*									-	
a,									C	99
<u>_</u>	Q			Search Options 😒					T	otal Rows: 3
	- 2			Containe ID. Punientian Data						
*	×	vBond	-	Cor	^		-	791FAD2C577	87A2CF1B	5 : ******
68	×	vSmart	7	IP Address: 172.31.10.204		or Sig	-	No certificate	installed	÷
	>	vManage	ymanage	The generated CSR has been sent to Cisco for	signing.		-	69D968CFFC	C16BEFF29	:
					Class					
				L	Close					

Step 4: Sign and install certificate signing requests

The signing and installation of the Cisco certificates are completely automated. To view the status:

- 1. Go to https://software.cisco.com and login if prompted.
- 2. Click on Manage Devices under the Network Plug and Play section.

Smart Licensi	ng	
Cisco Smart Licensing is a flexible licensing mo	del that streamlines how you activate and manage s	oftware.
For customers		
	Newsers	
Existing account	New account	Account administration
Start by getting access to your company's existing Smart Account.	Don't have an account? Create one now.	Update information and manage your users.
Submit request >	Create account >	Manage account >
	[]	
Smart Software Manager	Network Plug and Play	
Convert classic to Smart Licenses.	Automate device discovery and activation on-prem or from the cloud.	
Manage licenses >	Manage devices >	

- 3. Ensure the proper Virtual Account is chosen in the upper right-hand corner. This is the Virtual Account with the controller profile of the organization name used for the SD-WAN overlay.
- 4. Click Certificates

When a CSR is generated, you will see an enrollment request and the Status changes to In Process. When the request is signed, the Status changes to Completed.

Cisco Software C	entral	cis	ili. co		Q (%)	⊕ ^{US} EN
Cisco Software Central > Plug and	Play Connect			I PNP SDWAI	N POC 👻 vaganesa_AWS 👻	
Plug and Play Con	nect				Feedback Support Help	
+ Generate Certificate						
Certificate	Туре	Validity Period	Last Modified	Statos	Actions	
VSMART_8E088CEF-2217-4981-B Enrollment Request!	SD-WAN	One Year	2021-May-21, 19:10:46	Inprocess		
VMANAGE_AAD662CD-2210-424 Enrollment Request!	SD-WAN	One Year	2021-May-20, 23:27:33	Completed	■ <u></u>	

The vManage will automatically check at the configured interval for the signed certificates and install them.

Controller Type Hostname System IP Expiration Date Operation Status Site ID Certificate Senial 2 VBond - - 21 May 2022 7:11:40 ab92 Installed - 153AE217170A211B0BF9 2 VBond - - 21 May 2022 7:01:40 ab92 Installed - 153AE217170A211B0BF9	Controller Type Hostname System IP Expiration Date usid Operation Status Site ID Certificate Serial VBond - - 21 May 2022 7:11:40 abd92 Installed - 153AE217170A211B08F9 vSmart - 21 May 2022 7:047 1fo7/4 v8ond Updated 737CBCED00983922A9BE
Operation Status Site ID Certificate Sectal Q Search Options ~ Total Operation Status Site ID Certificate Sectal > vBond - - 21 May 2022 7:11:40 abd92 Installed - 153AE217170A211B0EP9 > vSmart - - 21 May 2022 7:0047 11074 Vend Updated - 7370E0E00098922A9EE	Med Weiter Stream Strea
Q Search Options ~ Total Controller Type Hostname System IP Exploration Date uuid Operation Status Site ID Certificate Sectial V 88nd - - 21 May 2022 71:14.0 abd92 Installed - 153AE217170A211B0BF9 V 98ndt - - 21 May 2022 70:047 107/14 Vend Updated - 73708E0E00069922A98E	Beach Options System IP Expiration Date wild Operation Status Sife ID Certificate Serial VBond - 2 1May 2022 7:1140 abd92 Installed - 153AE217170A21180BFp vSmart - 2 1May 2022 7:047 1forf.4 vBond Updated - 737CBCE0D0983922A9BE
Q Search Options v Total Controller Type Hostname System IP Expiration Date uud Operation Status Site ID Certificate Serial > vBond - - 21 May 2022 7:11:40 abd92 Installed - 153AE211710A211B0BF9 > vSmart - - 21 May 2022 7:047 107/14 Vendu Updated - 7370BCE00098922A9BE	Controller Type Hostmanne System IP Expiration Date unid Operation Status Stile ID Certificate Serial VBond - 21 May 2022 7:1140 abd92 Installed - 153AE217170A21180BF9 vSmart - 21 May 2022 7:047 10774 vBond Updated - 737CBCE000989392A9BE
Controller Type Hostname System IP Expiration Date uud Operation Status Trie ID Certificate Serial > vBond - - 21 May 2022 7:11:40 abd92 Installed - 153AE217170A21180EF9 > vSmart - - 21 May 2022 7:047 107/14 Vend Updated - 753AE217570A21180EF9	Controller Type Hostname System IP Expiration Date uuid Operation Status Site ID Certificate Serial vBond - - 21 May 2022 7:1140 abd92 Installed - 153AE217170A21180BF9 vSmart - 21 May 2022 7:047 10774 vBond Updated - 7372BCE0D0983922A9BE
Controller Type Hostname System IP Expiration Date uidi Operation Status Ste ID Certificate Semial > VBond - - 21 May 2022 7:11:404 July Installed - 153AE217170A211B0EF9 > vSmart - - 21 May 2022 7:01-404 July Installed - 153AE217070A211B0EF9	Controller Type Hostname System IP Expiration Date uuid Operation Status Ste ID Certificate Serial vBond - - 21 May 2022 7:11:40 abd92 Installed - 1S3AE217170A211B0BF9 vSmart - 21 May 2022 7:01:47 1074 vBond Updated - 7372BCE0D0983922A9BE
vector - - 21 May 2022 7:11:40 abd92 Installed - 153AE217170A211B0BF9 vector - - 21 May 2022 7:00 47 10774 vector 737CBCE000983922A9BE.	vBond - - 21 May 2022 7:11:40 abd92 Installed - IssAE217170A211B0BF9 vSmart - - 21 May 2022 7:00:47 1f074 vBond Updated - 7372BCE0D0983922A9BE
vsmart – – 21 May 2022 7:00:47 1f07f4 vBond Updated – 737CBCE0D0983922A9BE.	vSmart – – 21 May 2022 7:00:47 1f07f4 vBond Updated – 737CBCE0D0983922A9BE
vManage vmanage 5.5.5.5 20 May 2022 11:06:28 67810 vBond Updated L 69D968CFFC1C16BEFF29	vManage vmanage 5.5.5. 20 May 2022 11:06:28 67810 vBond Updated - 69D968CFFC1C16BEFF29

Option 2: Manual certificate signing through Cisco Systems

With this option, certificate signing requests are manually submitted by the administrator to the Cisco PnP portal, where the certificate is signed. The administrator can then download the resulting certificates from the PnP portal and manually install them in vManage.



Step 1: Configure vManage certificate settings

- 1. On the vManage GUI, go to Administration>Settings
- 2. To the right of Controller Certificate Authorization, Click Edit

3. Select Manual if it is not already selected. If this is a change from the current configuration, you may get a pop-up window asking to confirm that you want to change the certificate authority which is used for authentication. Click Proceed

=	ol) CIS	Cisco vManage	Select	t Resource Group 🗸	•	ê	<u></u> 29	0	admin 🔻
	*	ADMINISTRATION SETTINGS							
▫		Organization Name	VAISH-SDWAN-LAB-AWS						View
٠		vBond	172.16.10.183 : 12346					View	Edit
۹.		Alarm Notifications	Disabled					View	Edit
ŵ		Hardware WAN Edge Certificate Authorization	Onbox					View	Edit
**	ſ	Controller Certificate Authorization	Manual					Close	Edit
		Certificate Signing by: O Cisco (Recommended) O Syn	antec Manual Enterprise Root Certificate	0					
		WAN Edge Cloud Certificate Authorization	Automated					View	Edit
		Web Server Certificate	31 Mar 2024 4:40:53 PM				(SR Certi	ficate
		Enterprise Feature Certificate Authorization						View	Edit

4. Click the Save button

Step 2: Generate Certificate Signing Requests

- 1. Navigate to Configuration > Certificates and click the Controllers tab
- 2. On the right side of vManage, click three dots (...) and select Generate CSR from the drop-down box

iliiili cisco	' Cisco vManage				📀 Select Resource Group 🗸		Û	# 0	0	admin 🔻
¢ c	ONFIGURATION CERT	TIFICATES							🛓 Instal	l Certificate
WAN	N Edge List Controll	ers TLS Proxy								
> s	end to vBond									
0										
Q			Search Options 🗸							Total Rows: 3
>	Controller Type	Hostname	System IP	Expiration Date	uuid			peration Sta	itus	
>	vBond	vbond	30.30.30.30	25 May 2022 11:59:59	abd92540-a0b2-4cd4-bb2d-05fdbf565a	33	Ir	nstalled		••• ^
>	vSmart	vsmart	20.20.20.20	25 May 2022 11:59:59	f681eede-e738-4eb4-94c2-324d699161	af	v	Bond Update	ed	
>	vManage	vManage	11.11.11.11	25 May 2022 11:59:59	5145d19f-e28a-4baa-856d-1d98866283	0b	v	Bond Update	ed	
									View CSF View Cert Generate Reset RS Invalidate	tificate CSR A

3. A pop-up window appears with the certificate signing request. Copy the certificate signing request to submit for signing

cisco Vivianage	Select Resource Group V	• 8	÷.	6	admin .
CONFIGURATION CERTIFICATES				± Install Ce	rtificate
WAN Edge List Controllers TLS Proxy					
> Send to vBond					
	CSR X			0	~
	ID Addrage: 5555			CO	Be
Q	F Address. 0.0.0			Tota	I Rows:
Controller Type			Certificate		
> vBond	MIDUZCCAjsCAQAwgdIxCzAJBgNVBAYTAIVTMRMwEQYDVQQIEwpDYWxpZm9y		153AE217	170A211B0BF9	
> vSmart	bmlh MREwDwYDVQQHEwhTYW4gSm9zZTEcMBoGA1UECxMTVkFJU0gtU0RXQU4tTE		737CBCE0	D0983922A9BI	E
> vManage	FCLUFX UzEUMBIGA1UEChMLVmlwdGVsYSBMTEMxQzBBBgNVBAMTOnZtYW5hZ2UtNjc		69D968CF	FC1C16BEFF29	
	4MTAy ZGUtMGJmNi00NGRkLTg0MDUtYzFjNDc40Tg4OGU1LTEudmlwdGVsYS5jb20xIjA				
	g BakahkiG9w0BC0EWE3N1cHBvcnRAdmlwdGVsYS5ib20waaEiMA0GCSaGSib3D				
	QEB ADIIAA4IRDwawonEKAoIRAODul I/+WXMbol luzamb0Zv II IBI kfKalzBbi IZAoAvOlu				
	F/				
	Class				
	Close				

- 4. Click Close. You can always view or download the CSR again by clicking three dots (...) to the right of the controller and selecting View CSR from the drop-down menu
- 5. Repeat the process for the vSmart and vBond controllers

Step 3: Submit and sign the certificate signing requests

Next, the CSRs will be submitted to the Certificate Authority to be signed. This needs to be done for each controller.

- 1. Go to the Certificate portal at: https://software.cisco.com and login if prompted
- 2. Click Plug and Play Connect under the Network Plug and Play section
- Ensure the correct Virtual Account is chosen in the upper right-hand corner. This is the Virtual Account with the controller profile of the organization name used for the SD-WAN overlay
- 4. Click Certificates
- 5. Click the Generate Certificate button. The Generate Certificate window is displayed
- Next to Certificate Name, enter a name for the certificate (VMANAGE) 7. Next to Certificate Signing Request, paste the CSR copied from the vManage GUI. Be certain to include the "---BEGIN CERTIFICATE REQUEST---" and "---END CERTIFICATE REQUEST---" wording.

- 7. Next to Validity Period, choose a timeframe for how long you want the certificate to be valid. Minimum is 1 month, and maximum is 2 years.
- 8. Optionally, next to Description, type a description of the certificate (Certificate for vManage)

9. Click the Next button

Plug and Play Connect	t				Feedback	Support Help			
Devices Controller Profiles Network Certif		tificates Manage External Virtual Account Event Log Transactions							
Generate Certificate									
STEP 1 Identify Certificate	STEP 2 Review & Subr	nit	STEP 3 Results						
Identify Certificate Enter Certificate details and click Next to p	roceed to the nex	t step							
* Certificate Name	VMA	NAGE							
Certificate Signing Request	E MUD MRE VZEV ZGV Baka AQU 45MI Rv74 12QI	EGIN CER UZCCAISC/ WDwYDVQ JMBIGA1U IMGJMNI00 InkiG9w0B0 AA4IBDwA1 2CkDgyJX+ w1BH60IG0 M8ZxfWIKV	TIFICATE REQUEST QAPagdIxCzAJBaN/VBA/TAVI/ QHEwhTYW4gSym9zZTEcMBo/ COMML/mwdGVx/SBM/TEMxC NGRkLTa0MDU/YzFINDe40Tg ZGWE3A14BxcRR4dm/wdG/ xggEKA0BAQDyU/+WXMhoUy bU9vmKZGR[6A0H8xcR2dm]dD bU9vmKZGR[6A0H8xcR2dm]dD SAzIIsFITcLEITiKnGdQQQBdb	MRMwEQYDVQQIEwpDYWxaZm9ybmlh SA1UECxMTYKFJU9atU0RXQU4ITEFCLUEX zzBBgJNVBANTOnZIYW5hZ2UINic4MTAy 4QGU1JTEudrhwidGVxYS5b20xl6a (%75b220xa6EMA9CSQ25b3D2EB zamb0ZxJUBLkIKajrBhU7ApAyQluF/ af0/b61x3T0FTNvY309b7M+wWApt +gCIKDUYTBAv5kSBW1F2aCk+Lseh k2TLyxZbhEwEkSw2TM25H9Ep3					
* Validity Period	One	One Year							
Туре	SD-WA	AN							
Description	Max	characters	not to exceed 255						
Cancel						Next			

10.On the next screen, review and click Submit

- 11.A message will indicate that a certificate was successfully requested. Click Done
- 12.When the processing is complete, the status will show as Completed. Refresh the page if required
- 13.To the right under the Actions column, click the down arrow to download the certificate

Cisco	oftware Central	ultu cisc	1- :0		Q (@) ⊕US EN
Cisco Software	Central > Plug and Play Connect				Image: PNP SDWAN POC ▼ vaganesa_AWS ▼	
Plug an	l Play Connect				Feedback Support Help	
Devices Co	troller Profiles Network Certificates	Manage External Virtual Account Event L	og Transactions			
+ Genera	e Certificate					•
Certificate	Туре	Validity Period	Last Modified	Status	Actions	
VMANAGE	SD-WAN	One Year	2021-May-21, 21:15:11		Completed	

14.Repeat Step 3 for the vBond and vSmart controllers

Step 4: Install the signed certificates

Signed certificates are downloaded directly from the Plug and Play Connect portal in the previous procedure. The resulting certificates are uploaded and installed manually in vManage.

- 1. Go to Configuration > Certificates and click the Controllers tab
- 2. In the top right of the screen, click the Install Certificate button. No specific controller needs to be selected. vManage applies them to the proper controller
- 3. Paste the contents of the certificate into the window or click Select a file and choose the certificate to upload. Note that vManage looks for a .pem file, but the certificate may have been downloaded with a .cer extension instead. The difference in extension names does not cause any issues

	cisco vManage	Select Resource Group 🗸		•				
	CONFIGURATION CERTIFICATES					▲ Insta	all Certificate	
	WAN Edge List Controllers TLS Proxy				L			-1
Å	Send to vBond	Install Certificate X						
						(DOE	
	Q	Certificate Text Select a file Ly9vY3NwLmludGVybmFsaG9zdG5hbWVzLmNvbTBHBgNVHR8EQDA+MDygOqA					Total Rows: 3	5
÷	Controller Type	4hjZodHRw0i8vY3JsLmludGVybmFsaG9zdG5hbWVzLmNvbS9DSVNDT1ZJUFRF TEFTVUJDQS5jcmwwHQYDVR00BBYEFCyl/5yl4n6iw2kMdxEjHvH0yDs5MA4GA	us					
	> vBond	1UdDwEB/wQEAwIFoDANBgkqhkiG9w0BAQsFAAOCAgEApb6kY4AehWmAiPT94 MqZ3d2l8iy7ugj6WxNX5JSL1qZKqI+j/e1aewATbEJosOZ/eGL7P2wMMUrr//dNvf			153AE2	17170A211B	80BF9	ŀ
68	> vSmart	W0FYWTXJbwJwr5v3SQ7NRmhbSebblQbcSQctftqamt7xTtT4v1UhVcbw7zSLp6I ae8c0tHLnhwLeURuHZM7bg65dkw0DXwhEBN3PHzkBw0l0Qdar6+NHgkHek1z/	1		737CBC	E0D0983922	2A9BE	
9	→ vManage	ASxXpphOtAo9sAKzigLwNQO0/F96vpj+pEn5v66JpBeF/eXT79V6EyfqovUZhbX78 YcQVJ33WRAgCrRakC8JNTcbr/7wh/EO1Vb6QDk8EEXSBfqxDR1wopNNehW3xe M0otdEMFw60Vi87XreMChJ7WQL025j96F7np5E/Z+nC8bPecL5r8EHV38RTpS PSJXh576KuMpB51anu0h6VL9yN036yl0RyQo-458JcJq5q45voo9a6ABrUCB8Even p5H04RH-MuK00+gVPVFaAv2DL2MSeUQ(#8b21d92-9hbL3ms/w0gIFOG)DQq7s UngxdmupDMxBmexcvF2IA9DuPDg2z3uxITg5C6PrTDc+0q65KzbmLK/6vTVk ZMZVALXmbEvzo+no2FC/R6gLBU00/3f0r/3PEQm2IUnsfulSKb23fsmCjzg7G1X zVdAYSvEqedder0ktWn3z4M8kXzn+IhZNDDw-	1	-	28FC8E	3E4223EBA9	198CF	
		Install Cancel						

4. Click Install to get the certificate installed

cisco	' Cisco vManage				🔮 Se	lect Resou	urce Group 🗸	•	ê	<u>۽</u>	@	admin
¢ co	ONFIGURATION CERTIFIC	ATES									🛓 Install Ce	rtificat
WAN	Edge List Controllers	TLS Proxy										
► Se	end to vBond											
											0	0
Q			Search Options	~							Tota	l Rows
>	Controller Type		Hostname	System IP	Expiration Date	uuid	Operation Status	Site	ID	Certificate	Serial	
>	vBond			-	21 May 2022 7:11:40	abd92	Installed	-		153AE217	170A211B0BF9	
>	vSmart		-	-	21 May 2022 7:00:47	1f07f4	vBond Updated	-		737CBCE0	D0983922A9BI	
>	vManage		vmanage	5.5.5.5	21 May 2022 9:03:04	67810	vBond Updated	-		28FC8E8E	4223EBA99BCF	
	C											

5. Repeat the procedure for all the additional controllers

Verification:

- Go to the vManage dashboard. You should now see vSmart, vBond, and vManage icons with a green up arrow. This indicates that the control connections from the vManage to the other controllers are up. The Control Status box indicates the control connection of the vManage to the vSmart. Control connections cannot be completed without valid certificates. Any warnings or invalid certificates associated with control connections are also shown on the dashboard.
- 2. Go to Configuration > Certificates and click the Controllers tab. The Operation Status shows Installed for the vBond and vBond Updated for the remaining controller types
- 3. Other CLI commands to check certificate details on Cisco SD-WAN Controllers via SSH connection:
 - show control local-properties
 - show certificate validity
 - show certificate installed
 - show certificate root-ca-cert

<u>Note</u>: If you encounter any issues with certificate migration or if control plane/data plane restoration doesn't happen, please reach out to TAC support to create a service window.

Additional Resources:

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwancontroller-cert-deploy-guide.html

Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)