

SSL VPN Firewall CSR CISCO ASA SSL Installation:

1. Open the Cisco ASDM, then Under the Remote Access VPN windowpane, then in the Configuration tab, expand Certificate Management and click 'CA Certificates'.





2. Click the 'Add' button.

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Add
					Edit
					Show Det
					Request
					Delete



 Assign a 'Trustpoint Name' to the certificate (e.g. DigiCertCA2), And select the 'Install from a file' Radio Button and browse to DigiCertCA2.crt. Then click 'Install Certificate'. Then repeat this process of adding a new trustpoint and installing the certificate file for 'DigiCertCA.crt'.

Trustpoint Name: DigiCertCA2	Ð
C Paste certificate in PEM format:	
	_
C Use SCEP:	
SCEP URL: http://	
Retry Period: 1 minutes	
Retry Count: 0 (Use 0 to indica	ate unlimited retries)
	More Options
Install Certificate Cancel Help	

You should then see the Certificate listed with the Trustpoint Name you assigned to it.

4. Then under Remote Access VPN, expand 'Certificate Management' to 'Identity Certificates'.

Select the identity you created for the CSR with the 'Expiry Date' shown as pending and click **Install**, then select yourdomaincom.crt and click **Install ID Certificate File**. Once installed the Expiry Date will no longer show 'Pending'.



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Add
our_domain_com.crt]	Not Available	Pending	DigiCertCA2	Unknown	Show Details
					Delete
					Export
					Install
					Patrach

藬 Install Identity cert	ficate				×
Identity Certificate	C:\Certs\yourdo	main_com.crt]	
Paste the certificat	e data in base-64 f	ormat:			
]
Install Cert	icate	Cancel	Help		



 The certificate now needs to be enabled. On the lower left, click Advanced > SSL Settings. Then, select the interface you want SSL enabled for and click Edit.





anfiguration > Device Management > Advanced	> <u>SSL Settings</u>		
onfigure SSL parameters. These parameters affect both	ASDM and SSL VPN access.		
he SSL version for the security appliance to negotiate as he SSL version for the security appliance to negotiate as	a "server": Any 💌 a "client": Any 💌		
ncryption			
Available Algorithms	Add >>	Active Algorithms	Move Up
RC4-MD5		AE5128-SHA1	Line Course
DES-SHA1	<< Remove	AES256-SHA1	Move Down
NULL-SHA1		3DES-SHA1	
		RC4-SHA1	
Specify which certificates, if any, should be used for SS Interface DM2	L authentication on each interface. The fallback certificate Trustpoint	e will be used on interfaces not associated with a certificate Load Balancing Trustpoint	e of their own.
inside			
outside			

6. On the next screen, click the drop-down menu and for **Primary Enrolled Certificate** select your certificate then click **Ok**.

🚰 Select SSL Certificate	×
Specify enrolled trustpoints to be us interface. To enroll a trustpoint, go > Enrollment.	ed for SSL authentication and VPN load balancing on the DMZ to Configuration > Features > Device Administration > Certificate
Interface:	DMZ
Primary Enrolled Certificate:	None
Load Balancing Enrolled Certificate:	None DM2 cn:=www.yourdomain.com, ou=IT, o=YourCompany Inc.
ОК	Cancel Help

The ADSM will then show your certificate details under trust point.