Generating a certificate

To request a certificate from a Certificate Authority (CA), you will need to give them a Certificate Signing Request (CSR).

For instructions on how to generate a certificate please see https://docs.google.com/document/d/1FPXAE7U2yOGPUuQwE56ZwGEYkMEDTyf_8fqzdvrNwMw

Located at LAVA Drive > Information, Guides, and How To > Certificate Generation

Install

SAGE2 doesn't use the built in Windows hosting services, it uses Nodejs. Nodejs handles certificates itself using the **sage_install_folder/keys** folder. Someone might normally double click on a **.crt** or **.key** file to install into the default Windows service, this does not work for SAGE2.

Within the keys folder, each hostname/IP address will come in sets of three. Two .crt and one .key. By default, Windows binaries come with localhost and 127.0.0.1 files:

127.0.0.1-ca.crt 127.0.0.1-server.crt 127.0.0.1-server.key localhost-ca.crt localhost-server.crt localhost-server.key

The naming scheme must match and all three files are needed. However, CA wil only provide the server **.crt** file. The **.key** is generated when the CSR file is made. It is easier to let SAGE2 create the third file.

It is first recommended to let SAGE2 generate the three necessary files, if you have already been using certificates for the hostname and are updating them, the following steps may be skipped.

- Open the control panel, http://<hostname>:1000/
- Click on Admin
- Click on Wall configuration assisted
- Set the Hostname
- Save And Make Certificates, at the bottom of the page



The above steps will generate the three file set, where they will be located in the keys folder.

Contraction of the second prism			
Organize 🔻 🛛 Include in I	ibrary 🔻 Share with 💌 New fold	ler 8	= • 🔟
Favorites	Name	Date modified	Туре
📕 Downloads	퉬 bin	8/8/2018 6:35 AM	File folder
🧮 Desktop	鷆 config	9/29/2018 11:06 AM	File folder
SAGE2_Media	鷆 doc	8/8/2018 6:33 AM	File folder
	GU-sc ats	8/8/2018 6:33 AM	File folder
😹 Libraries 📃	📔 keys	8/8/2018 6:33 AM	File folder
Documents		8/8/2018 6:35 AM	File folder
Git Git	🍌 logs	9/29/2018 11:06 AM	File folder
J Music	🍌 node_modules	8/8/2018 6:34 AM	File folder
E Pictures	퉬 public	9/29/2018 11:06 AM	File folder
Videos	鷆 sabi.js	8/8/2018 6:35 AM	File folder
	鷆 src	8/8/2018 6:33 AM	File folder
👶 Homegroup	퉬 tmp	9/29/2018 11:47 AM	File folder
	AUTHORS	8/8/2018 6:33 AM	File
📮 Computer	📓 electron.js	8/8/2018 6:33 AM	JScript Script
🚢 Local Disk (C:) 🚽			

Organize 🔻 🛛 🖬 Op	ben	Print New folder		
Downloads Desktop SAGE2_Media		Name OG-GOLKEI GO-linux	Date modified 0/0/2010 0.55 AW 8/8/2018 6:33 AM	Type File
🗟 Libraries		GO-mac GO-windows.bat init webserver.bat	8/8/2018 6:33 AM 8/8/2018 6:33 AM 8/8/2018 6:33 AM	File Windows Batch Windows Batch
Git Music Pictures	ш	 init_webserver.cmd isit_webserver.cmd kalapawai.manoa.hawaii.edu-ca.crt 	8/8/2018 6:33 AM 8/8/2018 6:33 AM 10/8/2018 10:38 PM	Windows Com Shell Script Security Certific
🛃 Videos 🤣 Homegroup		kalapawai.manoa.hawaii.edu-server.crt	10/8/2018 10:38 PM 10/8/2018 10:38 PM 10/8/2018 10:38 PM 10/8/2018 10:38 PM	KEY File Security Certific
Computer Local Disk (C:)		Iocaniost-server.crt Iocalhost-server.key README.txt Iocal and	10/8/2018 10:38 PM 10/8/2018 10:38 PM 8/8/2018 6:33 AM	KEY File Text Document
👝 WDP 2TB (D:)	-	↓ vs.ext	8/8/2018 0:33 AM	EAT File

Now the certificate and key will need to be moved to the keys folder

- After submitting a CSR to a CA, they usually respond back with a download link to a variety of options for the certificate.
- Use the link and download the X509 Certificate only, Base64 encoded
 - If that that option is not available, get the **X509**, **Base64** file. It will need to be trimmed to work correctly through trial and error. More on this later.

←						
	Enrollment Successful					
•	Certificate Services Manager <support@cert-manager.com> to me ▼ Hello,</support@cert-manager.com>					
	You have successfully enrolled for an InCommon SSL certificate.					
	You now need to complete the following steps:					
	* Click the following link to download your SSL certificate (generally try to use a version that includes intermediates & root or your certificate may be rejected by some older clients					
	Format(s) most suitable for your server software: as X509, Base64 encoded: <u>https://cert-manager.com/customer/InCommon/ssl?action=download&sslld=1009543&format=x509</u>					
	Other available formats: as PKCS#7 Base64 encoded: https://cert-manager.com/customer/inCommon/ssl?action=download&sslid=1009543&format=base64 as PKCS#7 Bin encoded: https://cert-manager.com/customer/inCommon/ssl?action=download&sslid=1009543&format=bin as X509 Certificate only, Base64 encoded: https://cert-manager.com/customer/inCommon/ssl?action=download&sslid=1009543&format=x509CO					
	as X509 Intermediates/root only Reverse, Base64 encoded: https://cert-manager.com/customer/InCommon/ssl?action=download&sslid=1009543&format=x509IOR					

0

- Edit the downloaded file's name to match the **<hostname>-server.crt** file
- Then get the .key file that was generated when the CSR was generated and make its file name match the <hostname>-server.key file.
- Make duplicates of the .key and .crt file you just renamed.
 - Sometimes the CA will put a time limit to how long the **.crt** file download is available.
 - If the **.key** file is lost, it cannot be recovered and the **.crt** file becomes unusable.
 - Should the .key file be lost, usually CA will allow regeneration. Some will charge a fee for regeneration.
- Replace the old files with the ones you just name edited. The names should match the formatting of those generated using the control panel

Organize 🔻 🛛 🖻 Ope	n Print	New folder		•
\rm Downloads	 Name 	*	Date modified	Туре
Desktop		-linux	8/8/2018 6-33 AM	File
SAGE2_Media		-mac	8/8/2018 6:33 AM	File
	G GO	-windows.bat	8/8/2018 6:33 AM	Windows Batch
Libraries	init	webserver.bat	8/8/2018 6:33 AM	Windows Batch
 Documents Git Music 	🚳 init	_ _webserver.cmd	8/8/2018 6:33 AM	Windows Com
	E (81)	wakaan an ak	8/8/2018 6:33 AM	Shell Script
	🗔 kala	apawai.manoa.hawaii.edu-ca.crt	10/8/2018 10:38 PM	Security Certifie
Pictures Videos	🗔 kala	apawai.manoa.hawaii.edu-server.crt	10/8/2018 10:38 PM	Security Certifie
VILLED'S	📄 kala	apawai.manoa.hawaii.edu-server.key	10/8/2018 10:38 PM	KEY File
A Homegroup		UNION CONTE	10/8/2018 10:38 PM	Security Certific
Desktop SAGE2_Media SAGE2_Media Cournents Git Git Fictures Videos Homegroup Computer Local Disk (C:)	🗕 🗔 loc	alhost-server.crt	10/8/2018 10:38 PM	Security Certific
Computer	loc	alhost-server.key	10/8/2018 10:38 PM	KEY File
Local Disk (C:)	RE4	ADME.txt	8/8/2018 6:33 AM	Text Document
WDP 2TB (D;)	🗋 v3.	ext	8/8/2018 6:33 AM	EXT File
		III		•

- Restart SAGE2
- Test to see if it was installed
 - Connect to the SAGE2 interface using the certificate hostname
 - After the page loads, look at the address bar
 - \circ $\,$ To the left of the URL should be a lock icon
 - Click on the lock icon
 - If the information popup says "Secure Connection" then it has been installed correctly.
 - If there is no lock icon, it was not installed correctly

If the **X509 Certificate only, Base64 encoded** file is unavailable

You may have to manually reduce the X509, Base64 file.

This can be a guess and check process

For example this image shows that the contents of the X509, Base64

It contains four separate certificates for different usage cases.

However only one will work correctly

≣ kala	pawai_manoa_hawaii_edu.cer ×	ଜ୍ୟ 🎞 😶	••
1	BEGIN CERTIFICATE	STATE	
	MIIENjCCAx6gAwIBAgIBATANBgkqhkiG9w0BAQUFADBvMQswCQYDVQQGEwJTRTEU		
	MBIGA1UEChMLQWRkVHJ1c3QgQUIxJjAkBgNVBAsTHUFkZFRydXN0IEV4dGVybmFs		
	IFRUUCB0ZXR3b3JrMSIwIAYDVQQDEx1BZGRUcnVzdCBFeHR1cm5hbCBDQSBSb290		
	MB4XDTAwMDUzMDEwNDgz0FoXDTIwMDUzMDEwNDgz0FowbzELMAkGA1UEBhMCU0Ux		
	FDASBgNVBAoTC0FkZFRydXN0IEFCMSYwJAYDVQQLEx1BZGRUcnVzdCBFeHRlcm5h		
	bCBUVFAgTmV0d29yazEiMCAGA1UEAxMZQWRkVHJ1c3QgRXh0ZXJuYWwgQ0EgUm9v	ning yan antara da barana	
	dDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALf3GjPm8gAELTngTlvt		
	H7xsD821+i02zt6bET0XpClMfZ0fvUq8k+0DGu0Pz+VtUFrWlymUWoCwSXrbLpX9		
	uMq/NzgtHj6RQa1wVsfwTz/oMp50ysiQVOnGXw94nZpAPA6sYapeFI+eh6FqUNzX		
	mk6vBb0mcZSccbNQYArHE504B4YCq0moaSYYkKtMsE8jqzpPhNjfzp/haW+710LX		
	a0Tkx63ubUFfclpxCDezeWWkWaCUN/cALw3CknLa0Dhy2xSoRcRdKn23tNbE7qzN		
	E0S3ySvdQwAl+mG5aWpYIxG3pz0PVnVZ9c0p10a3CitlttNCbxWyuHv77+ldU9U0		
	WicCAwEAAa0B3DCB2TAdBgNVHQ4EFgQUrb2YejS0Jvf6xCZU7w094CTLVBowCwYD		
	VR0PBAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wgZkGA1UdIwSBkTCBjoAUrb2YejS0		
	Jvf6xCZU7w094CTLVBqhc6RxMG8xCzAJBgNVBAYTAlNFMRQwEgYDVQQKEwtBZGRU		
	cnVzdCBBQjEmMCQGA1UECxMdQWRkVHJ1c3QgRXh0ZXJuYWwgVFRQIE5ldHdvcmsx		
	IjAgBgNVBAMTGUFkZFRydXN0IEV4dGVybmFsIENBIFJvb3SCAQEwDQYJKoZIhvcN		
	AQEFBQADggEBALCb4IUlwtYj4g+WBpKdQZic2YR5gdkeWxQHIzZlj7DYd7usQWxH		
	YINRsPkyPef89iYTx4AWpb9a/IfPeHmJIZriTAcKhjW88t5RxNKWt9x+Tu5w/Rw5		
	6wwCURQtjr0W4MHfRnXnJK3s9EK0hZNwEGe6nQY1ShjTK3rMUUKhemPR5ruhxSvC		
22	Nr4TDea9Y355e6cJDUCrat2PisP29owaQgVR1EX1n6diIWgVIEM8med8vSTYqZEX		
	c4g/Vhsx0Bi0cQ+azcgOno4uG+GMmIPLHzHxREzGBHNJdmAPx/i9F4BrLunMTA5a		
	mnkPIAou1Z5jJh5VkpTYghdae9C8x490hgQ=		
	END CERTIFICATE		
	BEGIN CERTIFICATE		
	MIIFdzCCBF+gAwIBAgIQE+oocFv0700MNmMJgGFDNjANBgkqhkiG9w0BAQwFADBv		
	MQswCQYDVQQGEwJTRTEUMBIGA1UEChMLQWRkVHJ1c3QgQUIxJjAkBgNVBAsTHUFk		
	ZFRydXN0IEV4dGVybmFsIFRUUCB0ZXR3b3JrMSIwIAYDVQQDExlBZGRUcnVzdCBF		
	eHRlcm5hbCBDQSBSb290MB4XDTAwMDUzMDEwNDgz0FoXDTIwMDUzMDEwNDgz0Fow		
	gYgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwp0ZXcgSmVyc2V5MRQwEgYDVQQHEwtK		
32	ZXJzZXkgQ2l0eTEeMBwGA1UEChMVVGhlIFVTRVJUUlVTVCB0ZXR3b3JrMS4wLAYD		

Make a copy of the file and try test each of the certificate section one at a time.

---BEGIN CERTIFICATE---

<hash>

---END CERTIFICATE----

It will not work correctly if all of them are in the file at the same time.

The contents should only contain one cert section, just like the localhost file

	≣ loca	lhost-server.crt ×	ල්	•••
		BEGIN CERTIFICATE		
		MIIDCzCCAf0gAwIBAgIJAPcRar8RZN0dMA0GCSqGSIb3DQEBCwUAMBQxEjAQBgNV		
		BAMTCWxvY2FsaG9zdDAeFw0x0DA4MDgwNjMzMDFaFw0x0TA4MDgwNjMzMDFaMBQx		
		EjAQBgNVBAMTCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC		
		ggEBAMd+C49VU3DGHlmKReD6tNhkdl3EqsTs6QmfZRYMEGiFUNT6C60ZEWq02tsN		
		yRee2tmgZXmnTnmri3w+xmQ9Zo/YGlBl6v5XJL8tCV7WQcKS0yDSZ+yTgxAbjfib		_
		wjExYyDUqUrlSMx0v9ox5H3JlL0HPbhghykV7KXDf1MA3YlWQRWmGUbH/SfRRBVU		
		QZxJUmDZ1hxojmoCPYIGL0GBJ/zXbXNKwkgsw/gueoOh5aEQP2ZKZS0XH8aleCP7		
	9	HJl05ZhA+vzIVIJ54þoKfx9f5FGIdCNWcx/eoHi0YeqyJVenpsJB7W4tBvU8Q6Q6		
F	10	my6aNJC66HmjKSQm26q7VjeZmAUCAwEAAaNgMF4wLgYDVR0jBCcwJaEYpBYwFDES		
		MBAGA1UEAxMJbG9jYWxob3N0ggkA9xFqvxFk050wCQYDVR0TBAIwADALBgNVHQ8E		
	12	BAMCBPAwFAYDVR0RBA0wC4IJbG9jYWxob3N0MA0GCSqGSIb3DQEBCwUAA4IBAQDC		
		T3GrrZ/fVdvDl10CiJdoIeCib2t2nJqwffvnOw+GlConrYfvO87CWUSd+FaqGRL+		
	14	j2YCy3Afp3iQHMh5hezrZZ3J9TCvKJe/B1fnDulvfJUzC1rJBYzW3cfQbUwoi8zy		
	15	vuyeVTuS6KifVqT/N6UnIkY4dwaRvPdlKE1emE9tTeXdcfUNMZqCzjTAW+oocQrk		
	16	pxHQdgu1SYq1BNbJq8A1U+z2HZGgl4Ngvygkj8ppkQDj//REDFzdyctcP8gSN1NU		
		FbetWpARwjybfFUon0UudjFWxY2u/EqDts/JR0l81AB74270IEXnmo5XJHJRA9vn		
	18	wPaWoEnQnblH00/9UMYu		
	19	END CERTIFICATE		
	20			