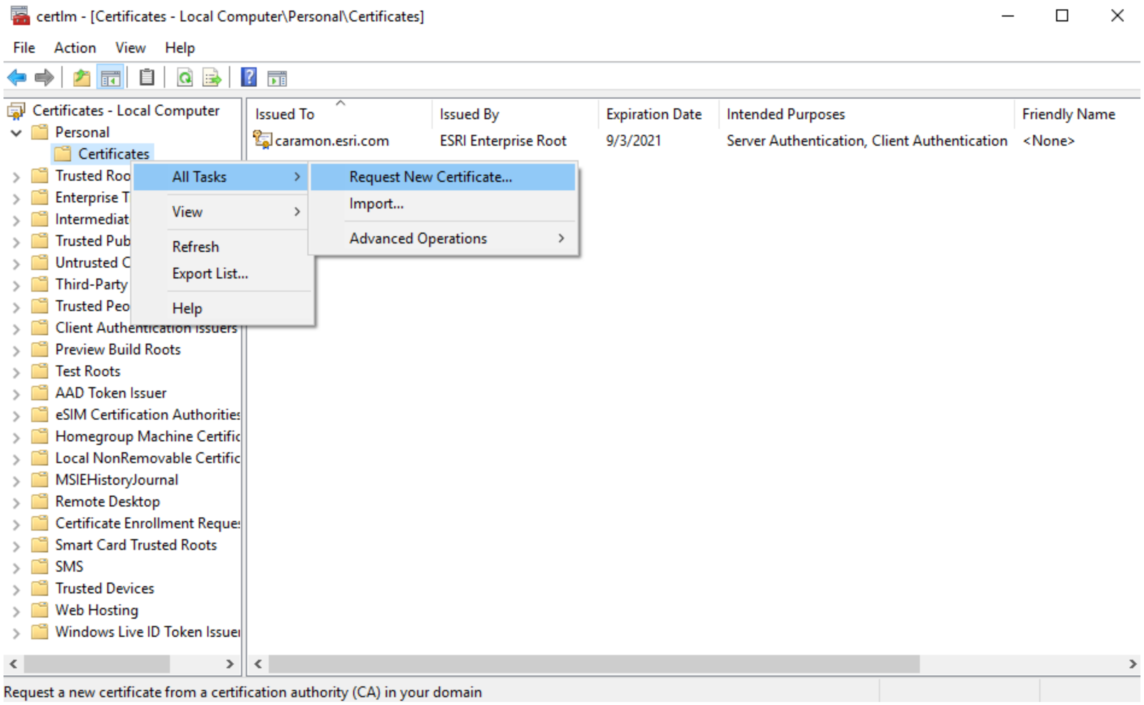
<u>Configuring SSL Certificates for a Machine Using Domain Enrollment</u>

- As an administrator, run the windows ***certlm.msc*** to manage your *<u>computer's</u>* certificates
- Expand **Personal > Certificates** and review any currently applied certificates
  - The goal is to create a certificate which satisfies both 'Client Authentication' and 'Server Authentication'
- Right-click to select **Certificates** and from its context menu choose ***All Tasks > Request New Certificate***
- Select an enrollment policy configured by your system administrator …

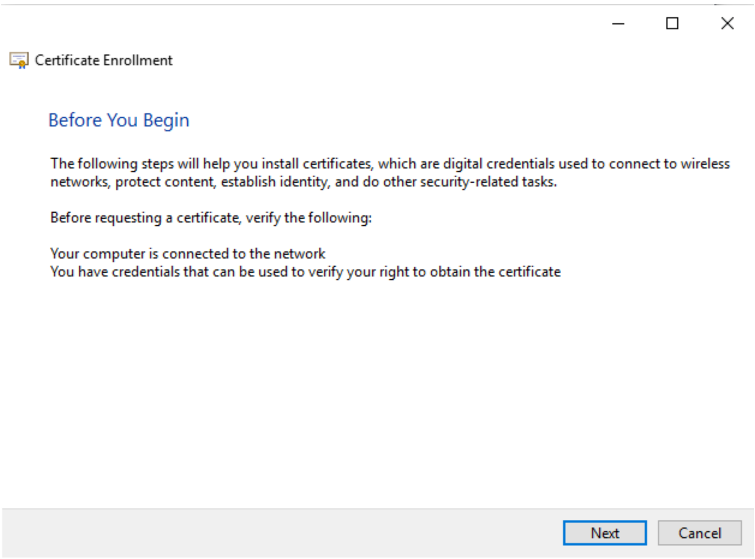
  It is a distinct possibility that certificates I generate against our 'Active Directory Enrollment Policy' are automatically trusted by servers, here within Esri (e.g. those on the .esri.com domain) because of group policies pushed out to all machines. This is where my knowledge of certificates begins to fail.

  What I'm showing below is what works for me, in our environment, on our servers.



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
caramon.esri.com	ESRI Enterprise Root	9/3/2021	Server Authentication, Client Authentication	<None>

Request a new certificate from a certification authority (CA) in your domain

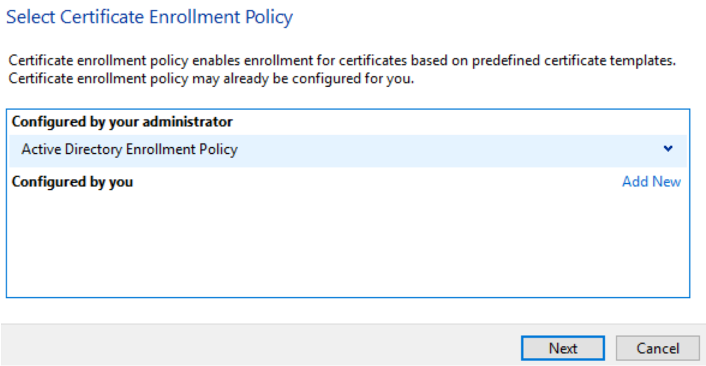


Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate



Select Certificate Enrollment Policy

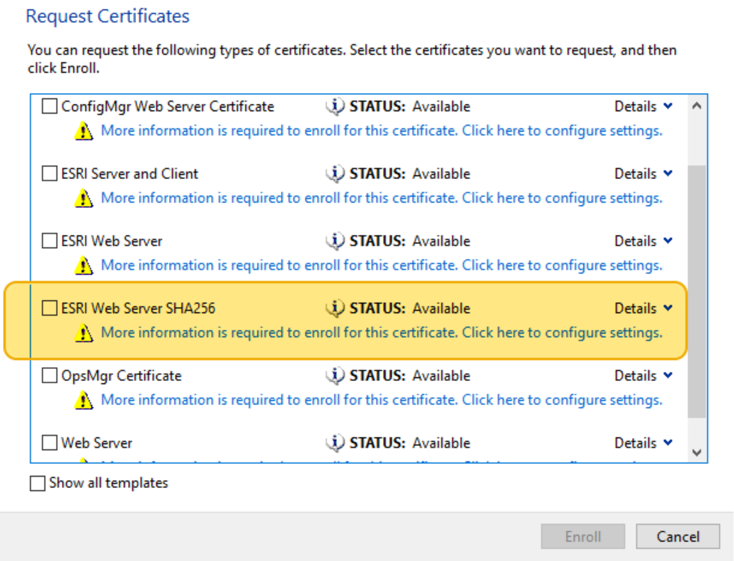
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy

Configured by you

- I always select the ***ESRI Web Server SHA256*** certificate type. There are a couple of specific properties I have to specify before this template can be used … so I have to click the *More information is required…* link and enter the server's common name and a DNS Subject Alternative Name as shown below.



Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

□ ConfigMgr Web Server Certificate — **STATUS:** Available — Details
More information is required to enroll for this certificate. Click here to configure settings.

□ ESRI Server and Client — **STATUS:** Available — Details
More information is required to enroll for this certificate. Click here to configure settings.

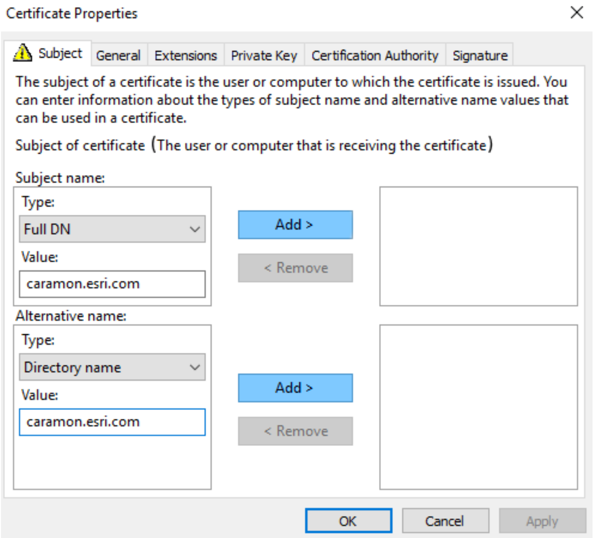
□ ESRI Web Server — **STATUS:** Available — Details
More information is required to enroll for this certificate. Click here to configure settings.

□ ESRI Web Server SHA256 — **STATUS:** Available — Details
More information is required to enroll for this certificate. Click here to configure settings.

□ OpsMgr Certificate — **STATUS:** Available — Details
More information is required to enroll for this certificate. Click here to configure settings.

□ Web Server — **STATUS:** Available — Details

□ Show all templates



Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate (The user or computer that is receiving the certificate)

Subject name:

Type: Full DN

Value: caramon.esri.com

Alternative name:

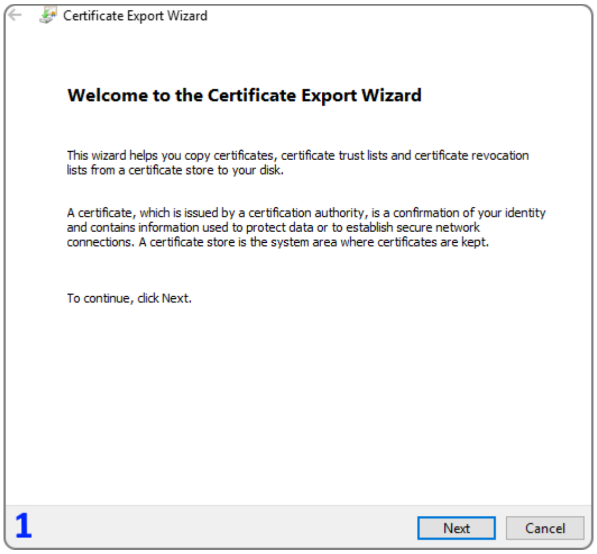
Type: Directory name

Value: caramon.esri.com

- Make sure you 'Add' both the *CN* (Common Name) and *DNS* (Subject Alternative Name) so they show in the open windows to the right; the windows are empty in the screenshot above. Click 'Apply' then click 'OK'.
- Note that I *always* specify the machine's FQDN when here … in the screenshot my machine's FQDN is ***caramon.esri.com***

- ✓ the configured certificate type (e.g. ESRI Web Server SAH256) and click ***Enroll***.
  You should see a message that the certificate has been successfully enrolled.

- Right-click the certificate which now displays in the ***certlm*** Microsoft Management Console.
  Select **All Tasks > Export** and follow the screenshots below to export a PFX certificate file with the machine's private key.

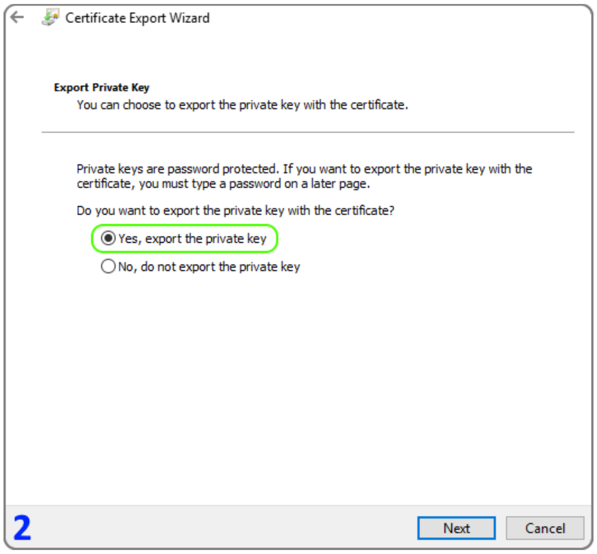

Certificate Export Wizard

Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.


Certificate Export Wizard

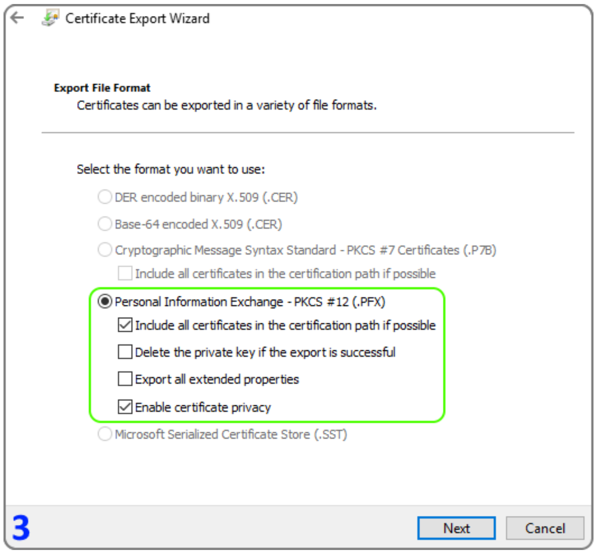
Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key


Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

  □ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

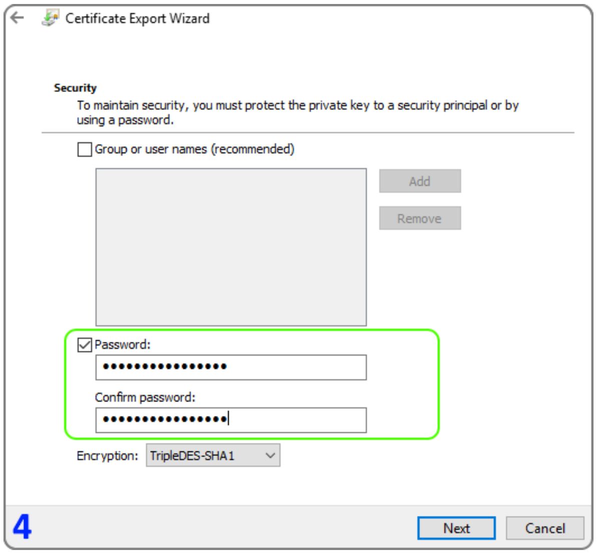
  ☑ Include all certificates in the certification path if possible

  □ Delete the private key if the export is successful

  □ Export all extended properties

  ☑ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)


Certificate Export Wizard

Security
To maintain security, you must protect the private key to a security principal or by using a password.

□ Group or user names (recommended)

☑ Password:
•••••••••••••••

Confirm password:
•••••••••••••••

Encryption: TripleDES-SHA1

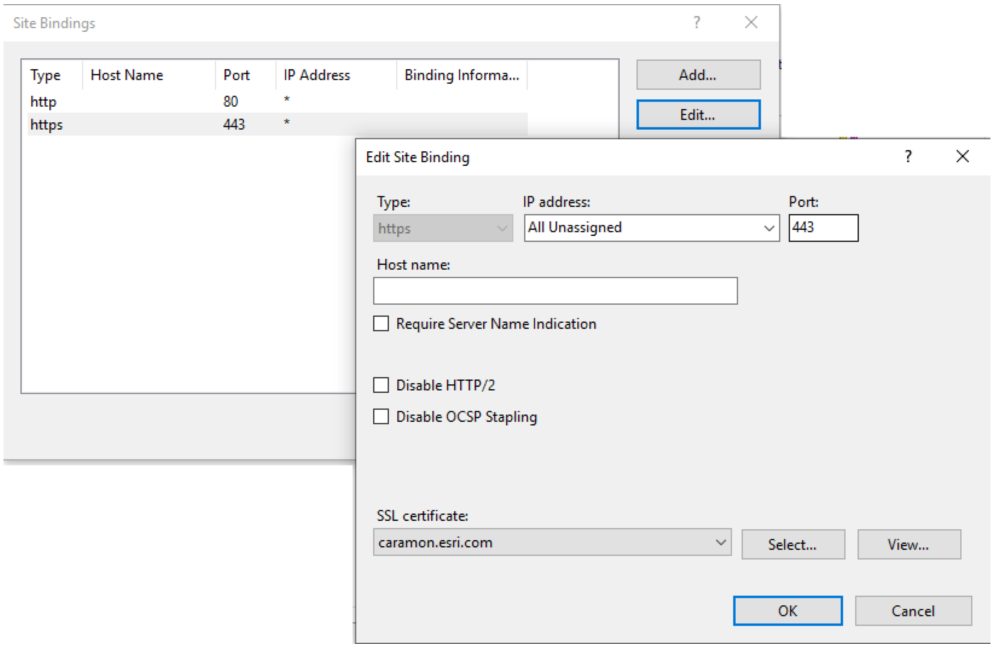
- You should now have a PFX file in some local folder like C:\certs\caramon.pfx

- Open Microsoft IIS management console

  - Confirm that your certificate shows when you select the server and double-click **Server Certificates**

  - Expand the server so you see its 'Application Pools' and 'Site'
    Right-click 'Default Web Site' and select ***Edit Bindings***

  - Make sure the IIS Manager has HTTPS listed as a site binding and the certificate you just created is bound to HTTPS



Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

Edit Site Binding

Type: https

IP address: All Unassigned

Port: 443

Host name:

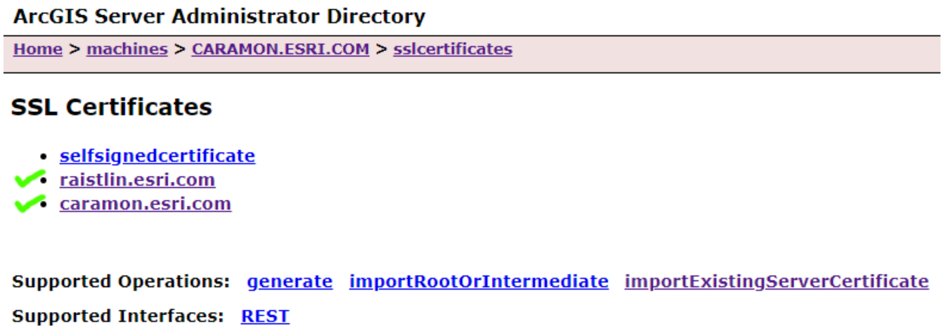
□ Require Server Name Indication

□ Disable HTTP/2

□ Disable OCSP Stapling

SSL certificate: caramon.esri.com

- Now you can log-in to ArcGIS Server’s Admin API and set this certificate as the site’s **Web server SSL Certificate**



ArcGIS Server Administrator Directory

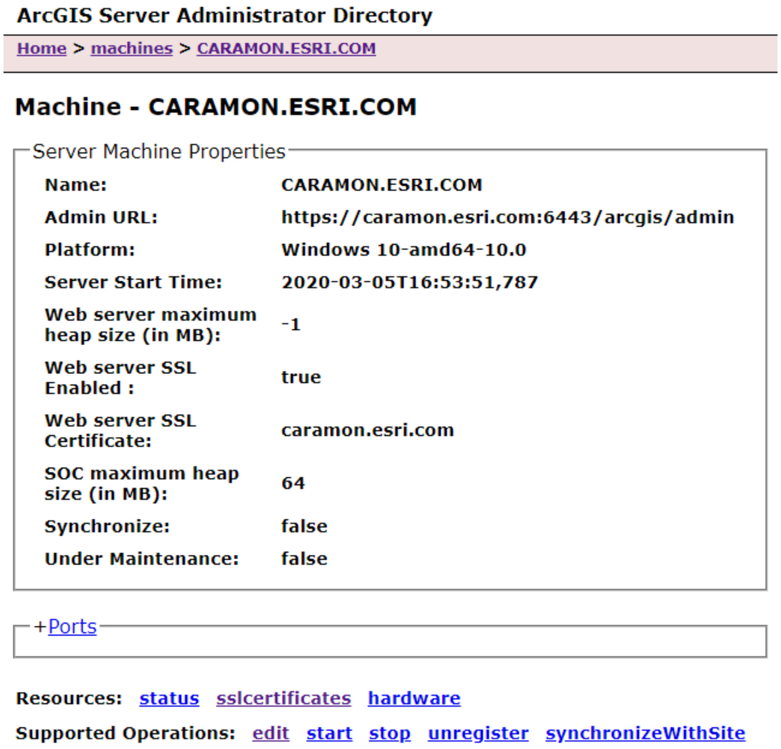
Home > machines > CARAMON.ESRI.COM > sslcertificates

SSL Certificates

- selfsignedcertificate
- ✓ raistlin.esri.com
- ✓ caramon.esri.com

Supported Operations: generate importRootOrIntermediate importExistingServerCertificate

Supported Interfaces: REST



ArcGIS Server Administrator Directory

Home > machines > CARAMON.ESRI.COM

Machine - CARAMON.ESRI.COM

Server Machine Properties

Name:	CARAMON.ESRI.COM
Admin URL:	https://caramon.esri.com:6443/arcgis/admin
Platform:	Windows 10-amd64-10.0
Server Start Time:	2020-03-05T16:53:51,787
Web server maximum heap size (in MB):	-1
Web server SSL Enabled :	true
Web server SSL Certificate:	caramon.esri.com
SOC maximum heap size (in MB):	64
Synchronize:	false
Under Maintenance:	false

+Ports

Resources: status sslcertificates hardware

Supported Operations: edit start stop unregister synchronizeWithSite

- Notice in the previous pair of screenshots that there are _two_ server certificates listed.
    - The first, **caramon.esri.com** is _this_ machine's certificate (my Laptop)
      I imported this using the ***ImportExistingServerCertificate*** option and loading the PFX file for CARAMON
    - I also set the **Web server SSL Certificate** on _this_ machine to _this_ machine's certificate. When I do this, ArcGIS Server will re-start. Be careful that you give this restart sufficient time to complete.
    - The second, **raistlin.esri.com**, is my _other_ machine's certificate (my Desktop machine)
      I also imported this using ***ImportExistingServerCertificate*** and loading the PFX file for RAISTLN
    - I suppose, technically, CARAMON does not need RAISTLN's private key. I probably could have generated a *.cer file for RAISTLIN rather than a *.pfx and used **ImportRootOrIntermediate** rather than importing the PFX using **ImportExistingServerCertificate** … but it is my habit that _all_ machines have each other's private keys and full certification.

This … the fact that every machine has every other machine's certificates … is what allows me to place machines into a single ArcGIS Server site and have GeoEvent Server instances running on each machine coordinate through the site for a multi-machine deployment.

It is also required for nominal server-to-server communications. For example, say RAISTLIN and CARAMON were both operating independently, running beneath their own ArcGIS Server installations, each with their own AGS site. If I wanted to register https://raistlin.esri.com:6443/arcigs with the server CARAMON as a server connection so that CARAMON could discover and use services discoverable in the ArcGIS REST Services Directory on RAISTLIN, I would have to configure SSL certificates as I've illustrated above so that CARAMON trusts RAISTLIN and vice versa.

I've also found that anything related to ***Stream Services*** requires that the subscribing machine trust the machine hosting the stream service – which should also be the machine running GeoEvent Server whose JVM is what actually hosts the stream service's web socket.

Do not forget – when you have a Portal for ArcGIS included in your deployment – you have to import all of the machine certificates (plural) into the Portal configuration using its Administrative API _separately_ from the certificate import you complete using the ArcGIS Server Admin API.