

Certification Authority

{scrollbar}

INLINE

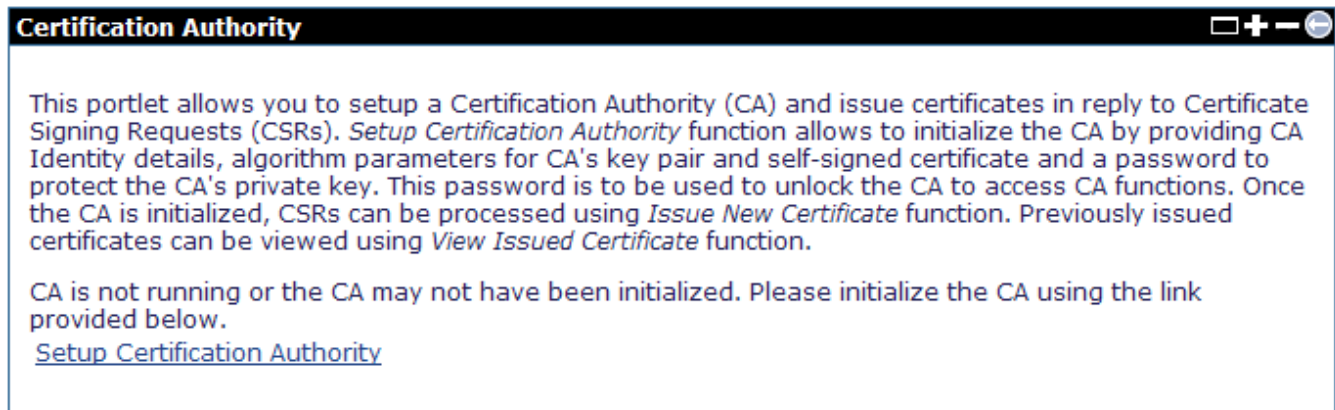
This release of Apache Geronimo allows you to define your own Certification Authority (CA) and issue certificates in reply to Certificate Signing Requests (CSR).

The Certification Authority portlet is available by clicking **Certificate Authority** on the left menu in the Geronimo Administration Console.

- [#Configuring a Certification Authority](#)
- [#Signing certificate requests](#)

Configuring a Certification Authority

The first time you call this portlet the CA is not yet configured so you will see a screen similar to this one.



Click on **Setup Certification Authority** to configure Geronimo as a CA.

This process is somewhat similar to defining keystores and certificates as covered in the [Administering certificates](#), this is in the sense that you should be prepared to provide similar type of information.

The first step is defining the Certification Authority details as illustrated in the following image. The information entered in this form will be used to create the Certification Authority and respective self-signed key pairs.

Certification Authority



Setup Certification Authority - Step 1: Enter CA details

On this screen you can enter the Certification Authority (CA) details, algorithm parameters for CA's keypair, algorithm for CA's self signed certificate and a password to protect the CA's private key. The next screen will let you review this information before generating the CA's keypair and self-signed certificate.

Certification Authority's Identity

Common Name (CN):
Division/Business Unit (OU):
Company/Organization (O):
City/Locality (L):
State/Province (ST):
Country Code (2 char) (C):

Key Details

Alias:
Key Algorithm:
Key Size:
Password:
Confirm Password:

Certificate Details

Certificate Serial Number:
Valid From Date(mm/dd/yyyy):
Valid To Date(mm/dd/yyyy):
Signature Algorithm:

[Cancel](#)

This is an "information gathering" step, at this point you are not creating any certificates yet. Click on **Review CA Details** and then on **Setup Certification Authority**.

Once created you will see a confirmation message **CA Setup is successful!** along with the details for the certificate you just created.

Certification Authority Details

This screen shows the details of CA's certificate and keypair. *Highest Serial Number* shows the highest of serial number of any certificate issued by this CA. *Certificate Text* shows the CA's certificate in base64 encoded form. This text can be used by the certificate requestors to designate this CA as a trusted CA in their software.

CA Setup is successful!

Certificate Details

Version: 3

Subject: C=US, ST=State, L=City, O=Apache, OU=Geronimo, CN=Geronimo's CA

Issuer: C=US, ST=State, L=City, O=Apache, OU=Geronimo, CN=Geronimo's CA

Serial Number: 1

Valid From: Thu Feb 01 00:00:00 CST 2007

Valid To: Fri Feb 01 00:00:00 CST 2008

Signature Alg: MD5withRSA

Public Key Alg: RSA

Key Size: 1024

Finger prints: SHA1 = 39:09:01:E2:B4:C1:49:E1:4C:6A:FD:AB:DE:74:7E:88:03:FC:16:A1
MD5 = CB:E9:C5:84:64:28:50:A9:70:65:9D:EE:DE:D3:4C:8F

Highest Serial Number: 1

Base64 encoded Certificate Text

```
-----BEGIN CERTIFICATE-----
MIICQDCCAaugAwIBAgIBATALBgqhkiG9w0BAQQwaDEWMBQGA1UEAxMNRR2Vyb25pbW8ncyBDQTER
MA8GA1UECxMIR2Vyb25pbW8xDzANBgNVBAoTBkFwYWN0ZTENMA8GA1UEBxMEQ210eTEOMAwGA1UE
CBMFU3RhdGUxCzAJBgNVBAYTA1VTMB4XDTA3MDIwMTA2MDAwMFoXDTA4MDIwMTA2MDAwMFowaDEW
MBQGA1UEAxMNRR2Vyb25pbW8ncyBDQTERMA8GA1UECxMIR2Vyb25pbW8xDzANBgNVBAoTBkFwYWN0
ZTENMA8GA1UEBxMEQ210eTEOMAwGA1UECBMFU3RhdGUxCzAJBgNVBAYTA1VTMIGfMA0GCSqGSIb3
DQEBAQUAA4GNADCBiQKBgQDBaDWSKZP2moQLpkBbnpVB79qV0FyyQcRt68NvQ9jzb5l2cZDOn6Rs
23gNWkE6/eGoLYjuPgDSvh2qFL79ufng5NdJmP2qoiKbOty+Kpm/8VRNE/d8nJs6gsA/nlHd9Jz
Y/c6CoEUTJwFNpGNwkaExg25vnBN+3HHC7FMbDfnxwIDAQABMA8GA1UEBxMEQ210eTEOMAwGA1UE
BxMEQ210eTEOMAwGA1UEBxMEQ210eTEOMAwGA1UEBxMEQ210eTEOMAwGA1UEBxMEQ210eTEOMAw
xU4IVElJERb7Y10o737mPqkCKho7901tndlpGWzkPyESk8ErijoP0dAgNihT2jUVWd0Lj4GsAr3D
IG3kNDhKSui5bUymSdr1ZM1DirufUVAiiFLekylptO15CWcxjdHb2kEPUImL2jj0H2alpLpf0h7w
cm36sysLyBxdAQ==
-----END CERTIFICATE-----
```

[Back to CA home](#)

Next time you access the **Certification Authority** portlet you should see the the CA you just created. From this portlet now you can manage CSRs, review and issue certificates.

Certification Authority



This portlet allows you to setup a Certification Authority (CA) and issue certificates in reply to Certificate Signing Requests (CSRs). *Setup Certification Authority* function allows to initialize the CA by providing CA Identity details, algorithm parameters for CA's key pair and self-signed certificate and a password to protect the CA's private key. This password is to be used to unlock the CA to access CA functions. Once the CA is initialized, CSRs can be processed using *Issue New Certificate* function. Previously issued certificates can be viewed using *View Issued Certificate* function.

CA has been initialized. CA functions can be accessed using the links provided below.

[Lock CA](#)

[View CA Details](#)

[Publish CA Certificate](#)

[Requests to be verified](#)

[Requests to be fulfilled](#)

[Issue New Certificate](#)

[View Issued Certificate](#)

Signing certificate requests

The [Certificate Properties File Realm](#) section cover in great detail how to create a new keystore and certificate and how to create a CSR and then import the CA's reply. In this section we will focus on how the CA manages and signs the client CSR.

We will start from the point where you generate the CSR, here is the example we used for the [Certificate Properties File Realm](#) section.