

Certification Authority

{scrollbar}

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.

Certification Authority	[view]
<p>This portlet allows you to setup a Certification Authority (CA) and issue certificates in reply to Certificate Signing Requests (CSRs). <i>Setup Certification Authority</i> 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 <i>Issue New Certificate</i> function. Previously issued certificates can be viewed using <i>View Issued Certificate</i> function.</p> <p>CA is not running or the CA may not have been initialized. Please initialize the CA using the link provided below.</p> <p>Setup Certification Authority</p>	

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

[view]

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):	<input type="text" value="Geronimo's CA"/>
Division/Business Unit (OU):	<input type="text" value="Geronimo"/>
Company/Organization (O):	<input type="text" value="Apache"/>
City/Locality (L):	<input type="text" value="City"/>
State/Province (ST):	<input type="text" value="State"/>
Country Code (2 char) (C):	<input type="text" value="LK"/>

Key Details

Alias:	<input type="text" value="G_CA_key"/>
Key Algorithm:	<input type="text" value="RSA"/>
Key Size:	<input type="text" value="1024"/>
Password:	<input type="password" value="*****"/>
Confirm Password:	<input type="password" value="*****"/>

Certificate Details

Certificate Serial Number:	<input type="text" value="1"/>
Valid From Date(mm/dd/yyyy):	<input type="text" value="05/03/2007"/>
Valid To Date(mm/dd/yyyy):	<input type="text" value="05/03/2008"/>
Signature Algorithm:	<input type="text" value="MD5withRSA"/>

[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.

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