

Administering security realms

[Administering certificates](#)

[Administering Security](#)

[Administering users and groups](#)

To administer security realms via the Geronimo Administration Console the **Security Realms** portlet is available on the **Console Navigation** menu on the left hand side. This portlet allows you to add a new security realm or edit an existing one. To remove realms you would normally use the command line option with the Deployer tool.

Security Realms

This page lists all the available security realms. Server-wide security realms can be edited, while security realms deployed as part of a single application cannot (change the deployment plan in the application instead).

For each realm listed, you can click the **usage** link to see examples of how to use the realm from your application.

Name	Deployed As	Actions
geronimo-admin	Server-wide	Edit usage

[Add new security realm](#)

When you create a new realm you will have to choose from the following realm types available:

- [Certificate Properties File realm](#)
- [Database \(SQL\) realm](#)
- [LDAP realm](#)
- [Properties File realm](#)
- [Kerberos realm](#)

Other than the four available options which you can choose from Administration Console, you can also create your custom realm type when none of the above fits your business needs. This requires creating your own implementation of class `org.apache.geronimo.security.realm.providers`, which implements the `javax.security.auth.spi.LoginModule` interface.

If you defined your own security realm and plan to use it within your application, you must define a dependency to the security realm in the deployment plan file.