

Replacing default Realm in Geronimo

 [OpenID](#)

 [Administering Security](#)

[Using SPNEGO in Geronimo](#) 

This article is about how to replace default .properties realm geronimo-admin with SQL or LDAP realms.

By default, Geronimo is using a .properties file realm for authentication named geronimo-admin, which is used by JMX server, Administration Console, Online-deploy and MEJB applications. However, you may not want to use it for production use. Alternatively, you can use database(SQL) or LDAP realms in a production environment. To demonstrate how to replace the default realm, we will use 2 samples as followed:

- [With a database\(SQL\) realm](#)
- [With a LDAP realm](#)

With a database(SQL) realm

In this example, we will use an embedded Derby database as the security provider.

1. Create a database named SecurityDatabase using **DB manager** on the administration console;
2. Create two tables Users and Groups to store user credential and group information;

```
create table users(username varchar(15),password varchar(15));
create table groups(username varchar(15),groupname varchar(15));
insert into users values('userone','p1');
insert into users values('usertwo','p2');
insert into users values('userthree','p3');
insert into groups values('userone','admin');
insert into groups values('usertwo','admin');
insert into groups values('userthree','user');
```

3. Create an Derby XA database pool named SecurityDatabasePool using **Database Pools** on the console;
4. Stop the server and update module org.apache.geronimo.framework/server-security-config/2.2-SNAPSHOT/car in the <Geronimo_Home>/var/config/config.xml file to enable the SQL realm.

```

<module name="org.apache.geronimo.framework/server-security-config/2.2-SNAPSHOT/car">
  <gbean name="org.apache.geronimo.framework/server-security-config/2.2-SNAPSHOT/car?
ServiceModule=org.apache.geronimo.framework/server-security-config/2.2-SNAPSHOT/car, j2eeType=LoginModule,
name=security-realm" gbeanInfo="org.apache.geronimo.security.jaas.LoginModuleGBean">
    <attribute name="loginModuleClass">org.apache.geronimo.security.realm.providers.
SQLLoginModule</attribute>
    <attribute name="options">dataSourceName=SecurityDatabasePool
                                databasesourceApplication=null
                                groupSelect=select username, groupname from groups where username=?
                                userSelect=select username, password from users where username=?<
/attribute>
    <attribute name="loginDomainName">geronimo-admin</attribute>
  </gbean>
  <gbean name="geronimo-admin">
    <reference name="LoginModuleConfiguration">
      <pattern>
        <name>realm-login-use</name>
      </pattern>
    </reference>
  </gbean>
  <gbean name="org.apache.geronimo.framework/server-security-config/2.2-SNAPSHOT/car?
ServiceModule=org.apache.geronimo.framework/server-security-config/2.2-SNAPSHOT/car,
j2eeType=LoginModuleUse, name=realm-login-use" gbeanInfo="org.apache.geronimo.security.jaas.
JaasLoginModuleUse">
    <attribute name="controlFlag">REQUIRED</attribute>
    <reference name="LoginModule">
      <pattern>
        <name>security-realm</name>
      </pattern>
    </reference>
  </gbean>
</module>

```

Where

- *geronimo_admin* is the same realm name as the original one. You might use another name instead, by doing so, you have to replace the security realm name in all other applications that were using the same security constraint as console.

5. Then, restart the server and try to login with user name *userone* and password *p1*. You will see the newly created SQL realm working.

With a LDAP realm

To replace the default .properties file realm using a LDAP realm, the configuration is nearly identical to the sample above. The only difference is to use `org.apache.geronimo.security.realm.providers.LDAPLoginModule` as `LoginModuleClass`. Here is the code snippet you can use in `config.xml`:

```

<module name="org.apache.geronimo.framework/server-security-config/2.2-SNAPSHOT/car">
  <gbean name="org.apache.geronimo.framework/server-security-config/2.2-SNAPSHOT/car?ServiceModule=org.
apache.geronimo.framework/server-security-config/2.2-SNAPSHOT/car,j2eeType=LoginModule,name=security-realm"
gbeanInfo="org.apache.geronimo.security.jaas.LoginModuleGBean">
    <attribute name="loginModuleClass">org.apache.geronimo.security.realm.providers.LDAPLoginModule<
/attribute>
    <attribute name="options">roleSearchMatching=uniqueMember={0}
                                userSearchMatching=uid={0}
                                userBase=ou=users,ou=system
                                connectionUsername=uid=admin,ou=system
                                roleName=cn
                                userSearchSubtree=true
                                authentication=simple
                                initialContextFactory=com.sun.jndi.ldap.LdapCtxFactory
                                roleBase=ou=groups,ou=system
                                connectionPassword=secret
                                connectionURL=ldap://9.186.10.16:10389
                                roleSearchSubtree=true</attribute>
    <attribute name="loginDomainName">geronimo-admin</attribute>
  </gbean>
  <gbean name="geronimo-admin">
    <reference name="LoginModuleConfiguration">
      <pattern>
        <name>realm-login-use</name>
      </pattern>
    </reference>
  </gbean>
  <gbean name="org.apache.geronimo.framework/server-security-config/2.2-SNAPSHOT/car?ServiceModule=org.
apache.geronimo.framework/server-security-config/2.2-SNAPSHOT/car,j2eeType=LoginModuleUse,name=realm-login-use"
gbeanInfo="org.apache.geronimo.security.jaas.JaasLoginModuleUse">
    <attribute name="controlFlag">REQUIRED</attribute>
    <reference name="LoginModule">
      <pattern>
        <name>security-realm</name>
      </pattern>
    </reference>
  </gbean>
</module>

```