

Principal Providers

- [Configuration](#)
 - [Container Roles Principal Provider](#)
 - [HTTP Header Principal Provider](#)
 - [Delegate Header Principal Provider](#)

Fedora Principal Providers allow a Fedora repository to pull in user security and role designations from other sources (e.g. LDAP).

Principal Providers are implemented as servlet filters that are added to the Shiro filter chain between the initial authentication filter (ServletContainerAuthFilter) and the final authorization filter (WebACFilter).

Different derivatives of the PrincipalProvider class can be initialized differently, either through credential files, information sent via HTTP header, or by connecting to external information sources such as LDAP.

The container roles provider and header provider should **not** be used at the same time, and doing so will lead to undefined results.

Configuration

Container Roles Principal Provider

ContainerRolesPrincipalProvider is a PrincipalProvider that obtains its set of principals from web.xml.

1. Enable this provider by setting the [configuration property](#) `fcrepo.auth.principal.roles.enabled` to `true`.
2. Set `fcrepo.auth.principal.roles.list` to a comma separated list of roles
3. Update your web.xml `auth-constraint` element to contain your custom roles

For example, your `fcrepo.properties` file might look like this:

fcrepo.properties

```
fcrepo.auth.principal.roles.enabled=true
fcrepo.auth.principal.roles.list=fedoraUser,fedoraAdmin,tomcat-role-1,tomcat-role-2
```

And your web.xml would be updated to look like this:

web.xml

```
<web-app>
...
<security-constraint>
...
<auth-constraint>
  <role-name>fedoraUser</role-name>
  <role-name>fedoraAdmin</role-name>
  <role-name>tomcat-role-1</role-name>
  <role-name>tomcat-role-2</role-name>
</auth-constraint>
</security-constraint>
</web-app>
```

HTTP Header Principal Provider

HTTPHeaderPrincipalProvider is a Principal Provider that obtains its initial set of principals from HTTP header requests.

1. Enable this provider by setting the [configuration property](#) `fcrepo.auth.principal.header.enabled` to `true`.
2. Set `fcrepo.auth.principal.header.name` to the name of the header that contains the principals
3. Set `fcrepo.auth.principal.header.separator` to the character that is used to separate multiple principals in the header

For example, your `fcrepo.properties` file might look like this:

fcrepo.properties

```
fcrepo.auth.principal.header.enabled=true fcrepo.auth.principal.header.name=x-principal-header  
fcrepo.auth.principal.header.separator=,
```

Delegate Header Principal Provider

DelegateHeaderPrincipalProvider is a Principal Provider that uses the On-Behalf-Of HTTP header to switch the user principal to the principal given in the header. This switch is only performed if the authenticated user has the fedoraAdmin container role.

This provider is enabled by default. To disable it, set `fcrepo.auth.principal.delegate.enabled` to `false`.