Security

Security Options

Securing your repository is achieved through many activities and not the result of a single feature. Attending to the physical security of the servers and good systems administration practices are a necessary first step. It is recommended that you prepare a security policy to determine the requirements, processes, and practices appropriate for your repository. Using your security policy, you choose which of Fedora's many options are right for your needs.

Quick Start Guide to Securing Your Repository

Here is a quick start guide that describes what you will need to do to configure your Fedora repository. It is recommended that you start with the new installer and one of the base security configurations it creates, and become familiar with the new installation and default security features. Then you can go back and experiment with customizing various aspects of your repository configuration and policies.

1. Select a base security configuration by running Fedora installer jar
    - Note: FeSL is now the default authentication implementation (via `AuthFilterJAAS` servlet filter). Classic servlet filter authentication (`FilterEnforceAuthn`) is deprecated and should be avoided if possible.
2. Optionally customize `fedora.fcfg` for your repository
3. Optionally customize XACML policies (repository-wide and object-specific policies)
4. Optionally customize fedora-users.xml for your repository and users
5. Optionally customize `server/config/spring/web/web.properties` or `server/config/spring/web/security.xml` to specify security parameters such as servlet filters and ssl characteristics.
6. Start the fedora server

Authorization via XACML

Fedora 2.0 hardcoded minimal authorization constraints, beyond those provided by specifications in Tomcat's web.xml file. Fedora now exposes these to customization by encoding them in the XACML standard. A complete description can be found in the documentation for the Fedora Authorization with XACML Policy Enforcement.

Default Repository Policies

Fedora ships with a set of default repository-wide XACML policies that approximate the minimal security level provided by Fedora. This set of repository-wide policies includes the following policies:

Custom Policies

Note that the default repository policies enforce a minimal level security (e.g., API-A is totally unrestricted). If you need a more customized level of access control what is provided by the default, you will need to add additional repository-wide policies or individual object-specific policies to customize your access environment. Refer to the Fedora XACML Policy Writing Guide document for more information about how to construct policies for your repository.

Unable to render {include} The included page could not be found.