

Contents

- [Security](#)
- [Basics](#)
- [Doing things based on IP address](#)
- [Realms and whatnot](#)
- [Other options](#)

Security

Basics

- Use a sitewide error handler, so you do not disclose sensitive information about your system.
- Use SSL if you have users logging into your site, even if it's a self-signed cert.
- Run Railo under a dedicated user with limited access
- Remove the Railo admin files if not needed
- lots of other stuff. Search for "hardening coldfusion".

Doing things based on IP address

One method of doing things based on IP addresses is [URL Rewriting](#). Another is using a front end web server, or the servlet container itself to manage access. Yet another, which is really the same as the first, is to use the URLRewriteFilter.

The nice thing about the URLRewriteFilter, is that it is not servlet container specific. The same WAR will deploy with the same rules anywhere the WAR runs, be it JBoss/Tomcat, Jetty, Resin, or GlassFish.

Realms and whatnot

And then there's Realms and whatnot, the Java security stuff which is part of the servlet spec.

Other options

There's the WS-Security standard, with a project implementing this for CFML here <http://wss4cf.riaforge.org/> as well.

