Server administration plugin (standard)

July 8, 2008

1 Purpose

This plugin is not so much for dealing with everyday server tasks, as it is for providing a facility to implement them in. This plugin provides the following essential services:

- Command management - ironmod has its own commands system for plugins. This plugin is a central repository for all server commands, whether they be for regular users or for server administrators. It makes it easy to enforce access levels needed to use certain commands and provide a standard interface for people to write their own commands.
- Ban storage and management - This plugin provides ban services for other plugins and provides commands for managing bans.
- User storage - ironmod has its own user system, where each user gets a short little "handle" (name) and at the very least, an access level that determines how much power they have.
- User management - This plugin provides its own commands to manage users.

If you're familiar with Internet Relay Chat network services and the concept of users and access levels needed to use commands, then you'll be right at home.

2 Users

A user is represented by their "user handle", a lowercase name with only letters and the underscore (_) character. A user usually has at the very least an access level. Each user gets "user settings" which contain everything that we need to know about the user beside their handle. These settings are described later.

2.1 Access levels

Access levels are given to users to determine what commands they can access (commands may require a certain level of access before they can be used). This is very much the same as Digital Paint's own "commands.txt" configuration file and "login" entries for people. Access levels may also provide protection to users. For example, most plugins that have commands that can do "bad" things like kicking people will not allow you to kick a player in the server with a higher access level than you. Access levels range from 0 to 500. Here is the guide you should follow for assigning access levels to users:

- *Access level 0: Regular user.* This is the default access level for anyone in the server, you do not even need to have an entry in the server's user list.
- *Access level 1 to 99: VIP user.* This is for non-administrators that may get special priviledges on the server.
- *Access level 100 to 199: Junior administrator.* This is a low-level administrator, perhaps on trial.
- *Access level 200 to 299: Regular administrator.* This is the most common of administrator access levels. Mostly any plugin that exposes commands for administrators to use should and will use this access level (200).
- *Access level 300 to 399: Senior administrator.* This user is considered highly trustworthy and can add/remove other users, but can not look at another user's settings (the "usersettings" command) or set their own user settings manually (using "set" on themselves).
- *Access level 400 to 499: Server operator.* This user can do practically anything, including looking at the settings for other users and setting their own user settings (so they can give themselves more access if they want). This user is assumed to be in complete control of the server itself, anyway.
- *Access level 500: Server owner.* This is reserved for the server owner(s).

2.2 User settings

Each user has settings associated with their user handle. This plugin manages these settings and allows them to be modified directly by a server administrator (using the "set" command), although some of them may be controlled using other commands to. The purpose of this section is to list all of the settings that are used by this plugin. Be aware that although discouraged, other plugins can modify a user's settings (and even add new ones). Settings are simply key-value pairs. Here are the ones used by this plugin:

- "access" - This is the user's access level. It is highly discouraged that you use "set" to modify this. Removing this setting from a user may result in random errors from this plugin.
- "gblid" - This is a Digital Paint Global Login ID to recognize this user by. If a player is found to have this ID, they will automatically be recognized as this user.
- "cloak" - This is primarily to hide this player from informational command output, such as the "users" command. It does not guarantee complete invisibility though, since people can still guess your user handle and use something such as the "access" command to discover you.

3 Bans