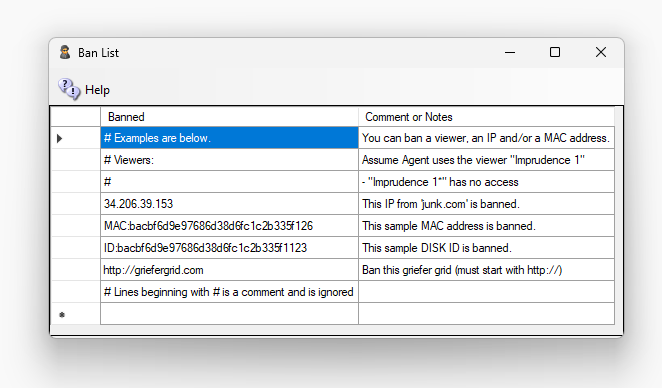
# Ban Lists

Bans can be set for Grids, IP addresses, Viewers, and MAC addresses. MAC addresses are a serial number found in Ethernet cards. These bans shut off incoming traffic by using Opensim Robust capabilities, and by adding entries to the Windows Firewall. They are not a total solution but can work in many cases. This may not be effective as the login name can be changed, the Viewer Name can be tweaked, they may have another PC with a different MAC, or they may have changed it, and the IP may change by the ISP or come from a VPN.

Syntax is shown below:



* Comments - # is a Comment
* IP - IP may be specified with four digits and dots or with /24 to cover 255.255.255.0 range. /16 will block all IPs in the range of 255.255.0.0.
* MAC: and the hex digits will ban by the hashed MAC address.
* Anything else is assumed to be a Viewer string.
* <http://(URL):Port> will ban this Grid.

Settings go into effect when you save the screen after making changes. For OsGrid, Metro and region servers, only IP bans will work since no robust is running on your Region server.

## Getting Ban Data

You can get the Login Name and Grid http://name:port, IP address, and MAC address of people from the Robust log as it happens. You can also look in the menu system at Help ->View Logs->Robust to view the log with Baretail.exe.

**Its is best to run the Robust log with log level set to INFO.**

A typical Robust Log entry would be as follows: (highlights are mine)

INFO (104) - OpenSim.Services.HypergridService.GatekeeperService [GATEKEEPER SERVICE]: Login request for Jo.Blow@ **www.xyz.com**:8002 @ http://www.xyz.com:8002/ (3be47575-06dd-46b0-8637-87a8967c432c) at ab8d7770-3782-21e4-8c41-1813211c9b88 using viewer **Firestorm-Releasex64 5.2.8.58205**, channel Firestorm-Releasex64, IP **52.8.203.221**, Mac **d5af8bee7e6a265c41e729416d570f57**, Id0 dac5b5d03d9bbe2225d2c91c3238d59f, Teleport Flags: ViaLogin. From region Her Place (2c53df18-143f-4340-ae73-f2885d9694d8) @ <http://grid.nope.com:8002/>

## Grid Ban

To ban the grid that the avatar who originally logged on, add [**http://www.xyz.com**:8002](http://www.xyz.com:8002). The “http://” and “:port” number is needed.

To ban the grid that the avatar teleported from (not necessarily her home grid) , add [**http://grid.nope.com**:8002](http://grid.nope.com:8002). The “http://” and “:port” number is needed.

## IP Ban

To ban an IP, add the IP as 4 numbers like this: 52.8.203.221. You can also add a /24 to the end to ban all IP addresses in the same range of 256 IP addresses. Use IP “52.8.203.0/24” to ban all users from IP 52.8.203.0 to IP 52.8.203.255.

## MAC Address Ban

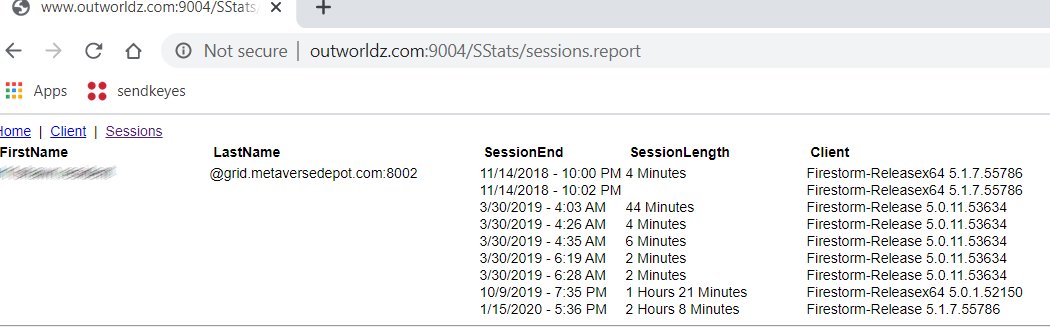
To ban a PC by the Ethernet card MAC address, add the word **MAC:** and then the MAC address from the robust log: “**MAC:d5af8bee7e6a265c41e729416d570f57**”.

## Viewer Ban

To ban a specific viewer, add the name and Revision. “Firestorm-Releasex64 5.2.8.58205”. To ban all version 5 Firestorms, add “Firestorm-Releasex64 5”.

## Copybot Viewers

To ban old copybot viewers such as DarkStorm, add “Firestorm-Releasex64 5.0.11”. These old viewers are rarely in use, except by copybotters.



There are several ways get data to ban by viewer. One way is to look in the Stats for your Welcome region. Another is to copy and paste it from the robust screen, or robust.log. Click your Welcome region in the Regions menu, then select the Statistics Button. This screen shows the “Sessions” tab, so you can see if someone is still using an old viewer recently. If so, they are a candidate to be a copybotter.

There is a Analyze Log button in the Log settings that will show you all MAC and Disk ID0’s that were seen.