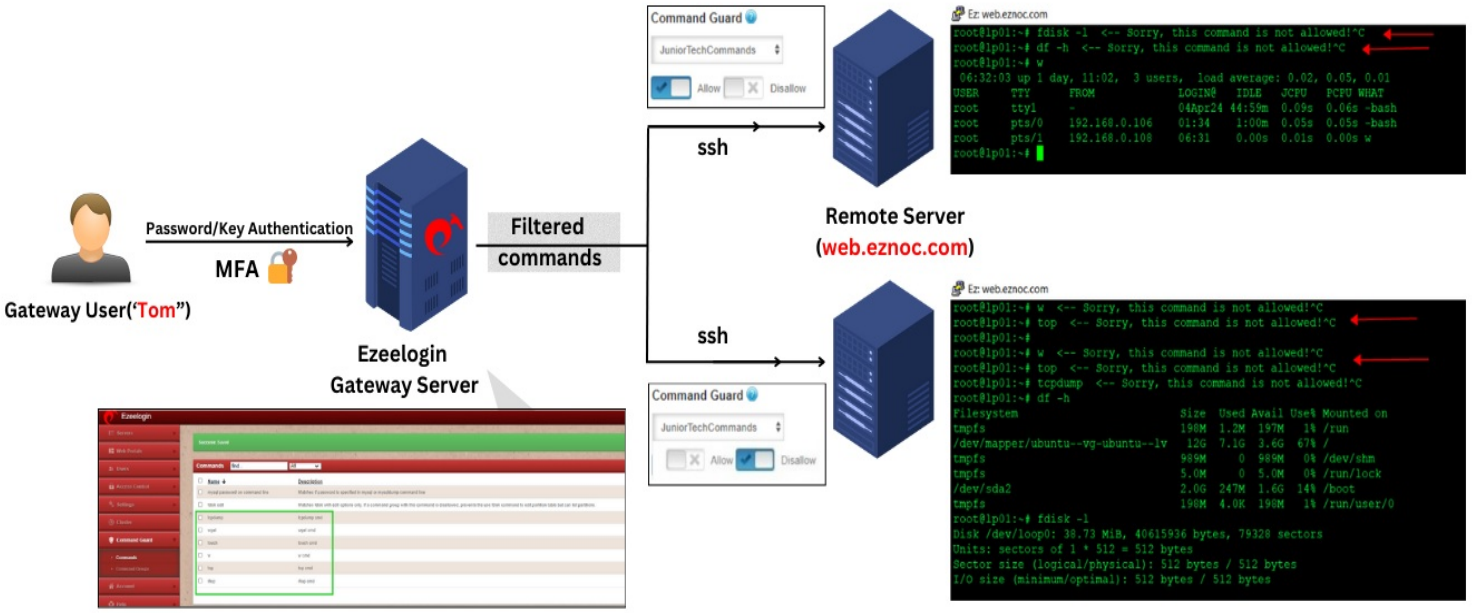
Filter commands executed on remote servers using command guard

10 Manu Chacko November 10, 2026 Features & Functionalities 13324

How to restrict commands for gateway users on remote servers?

Overview: In this article, we will configure a command guard in Ezeelogin such that an SSH gateway user "Tom" who is a JuniorTech would only run the following commands (wget, touch, w, top, tcpdump, iftop) on remote servers (kvm, vps, host nodes).

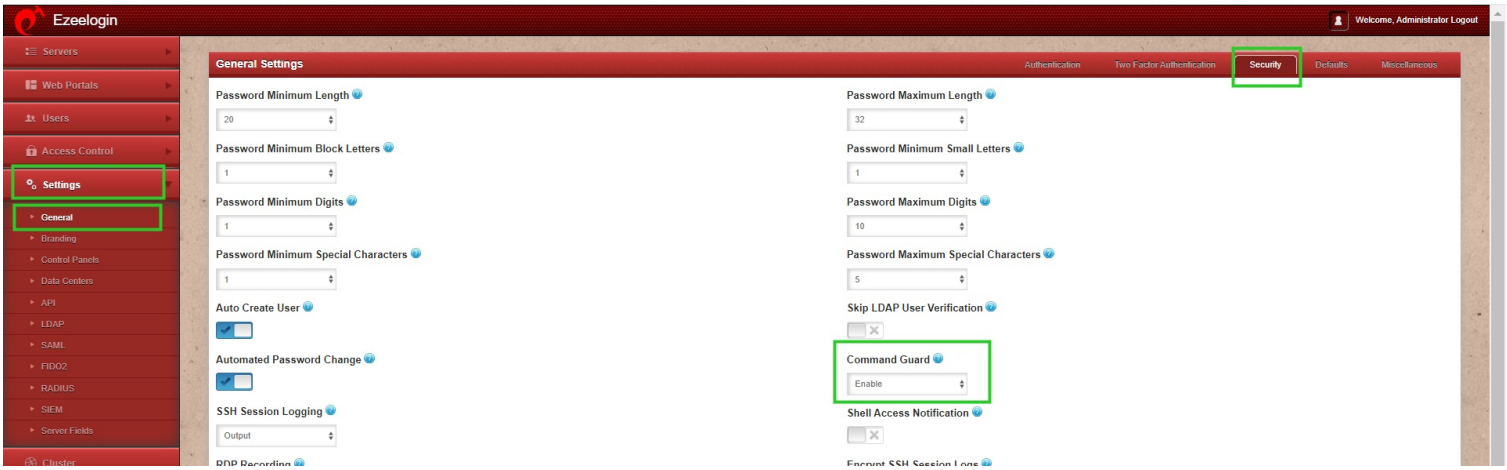


What is a command Guard?

Command guard is a feature that allows you to set up regular expression based filtering for commands entered on servers via the Ezeelogin shell.

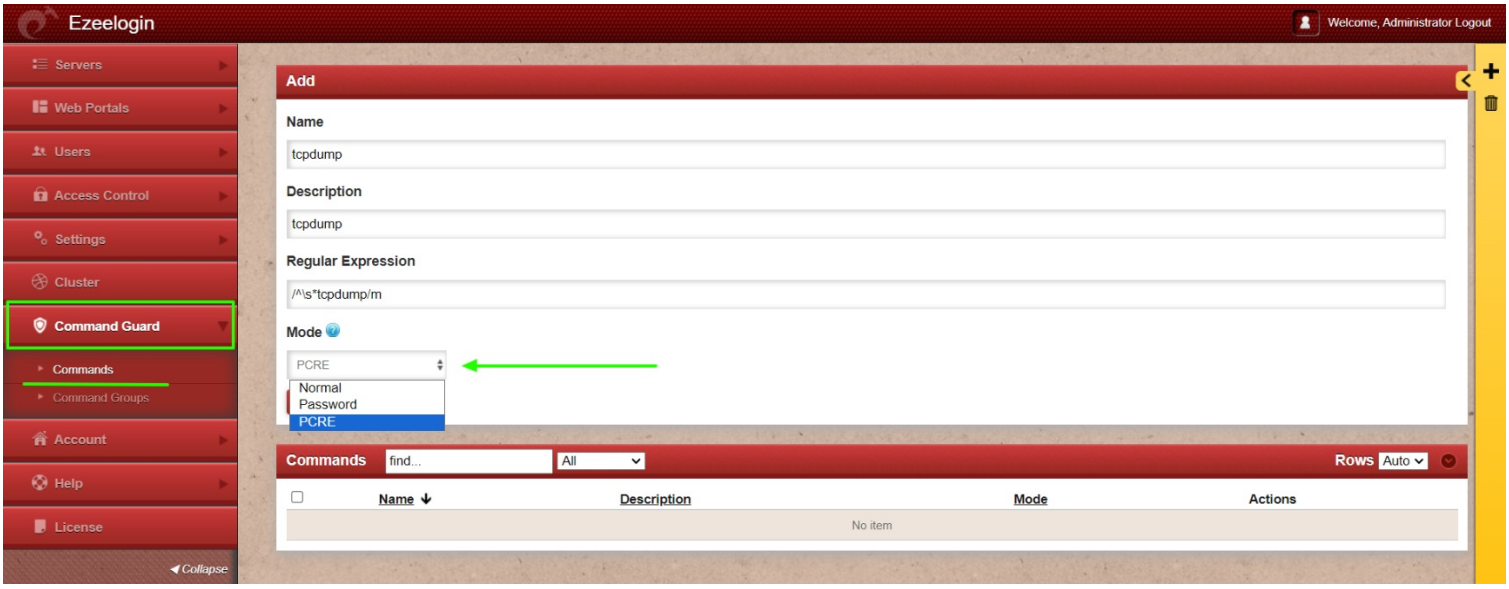
> Refer user manual for more details: https://www.ezeelogin.com/user_manual/CGM.html

Step 1: Enable command guard globally from **Ezeelogin GUI** -> **Settings** -> **General** -> **Security** -> **Command Guard** -> **Enable**

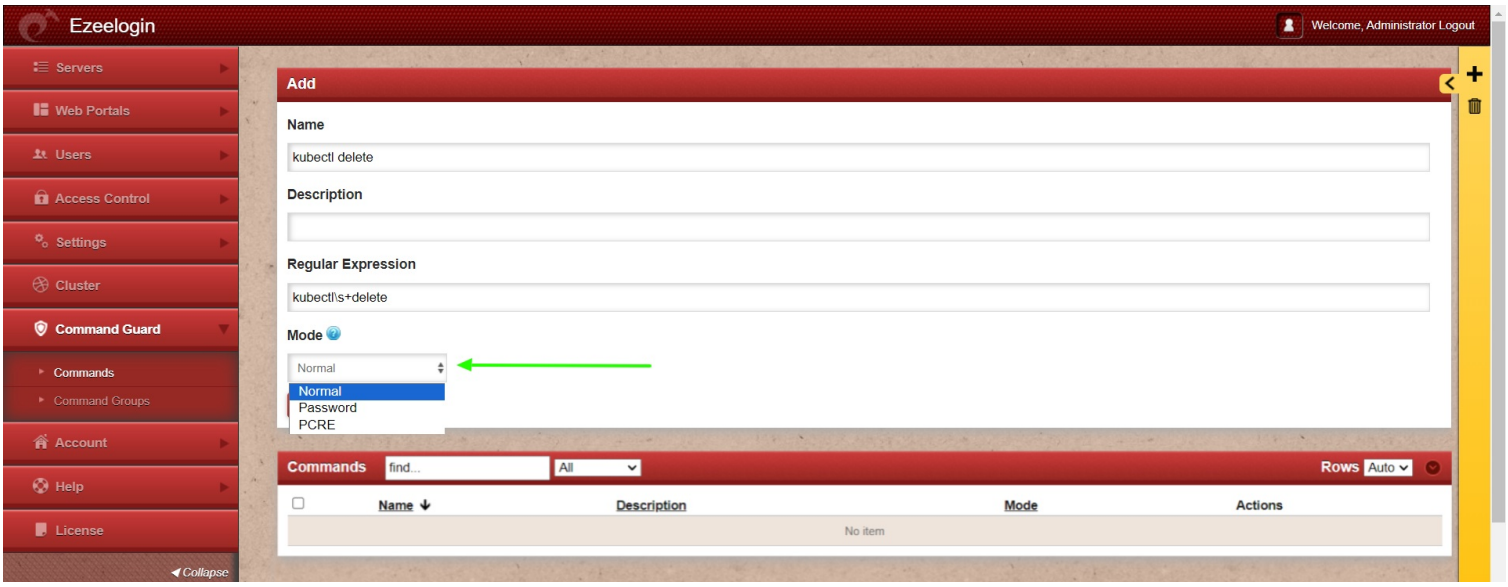


Step 2: Add the commands ("tcpdump, wget, touch, top" etc) in the command guard -> commands tab. **Select the mode (Normal, PCRE, or Password)** from the drop-down option to select the required option.

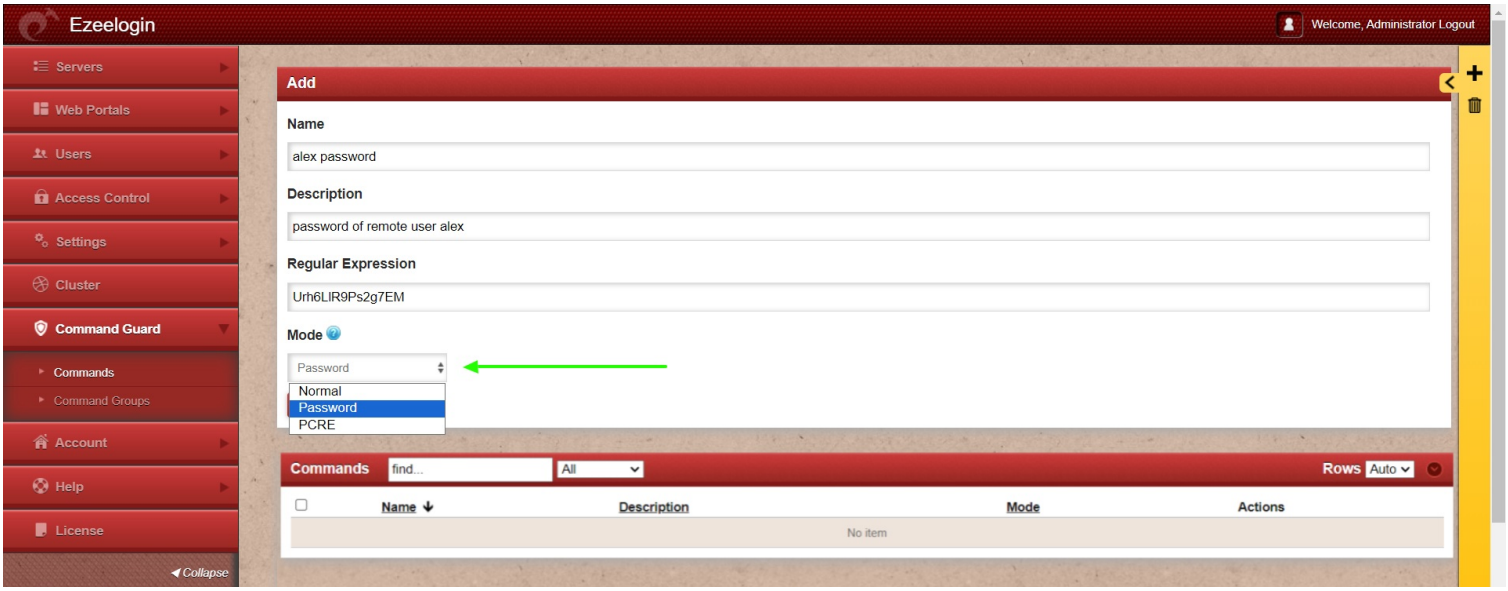
Step 2(A): Refer to the example below to add a **PCRE regular expression** (PCRE is more compatible and configurable).



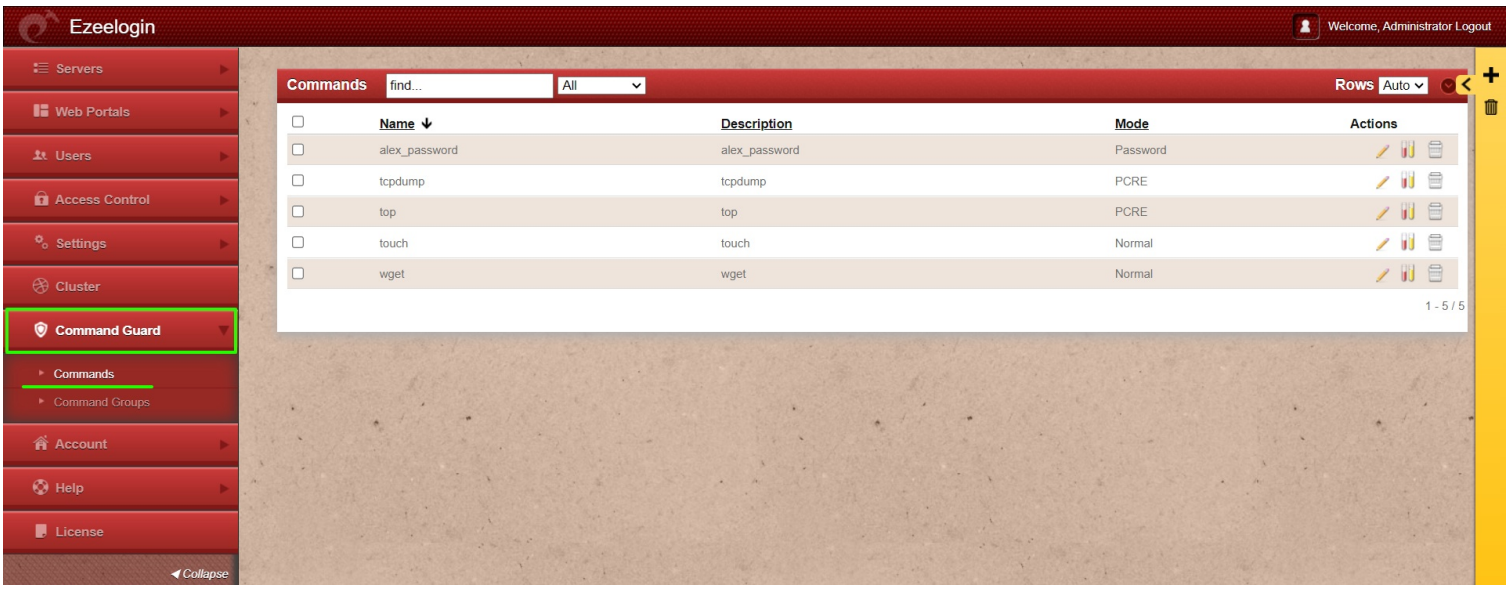
Step 2(B): Refer to the example below to add a **normal regular expression** that supports **POSIX regular expression**.



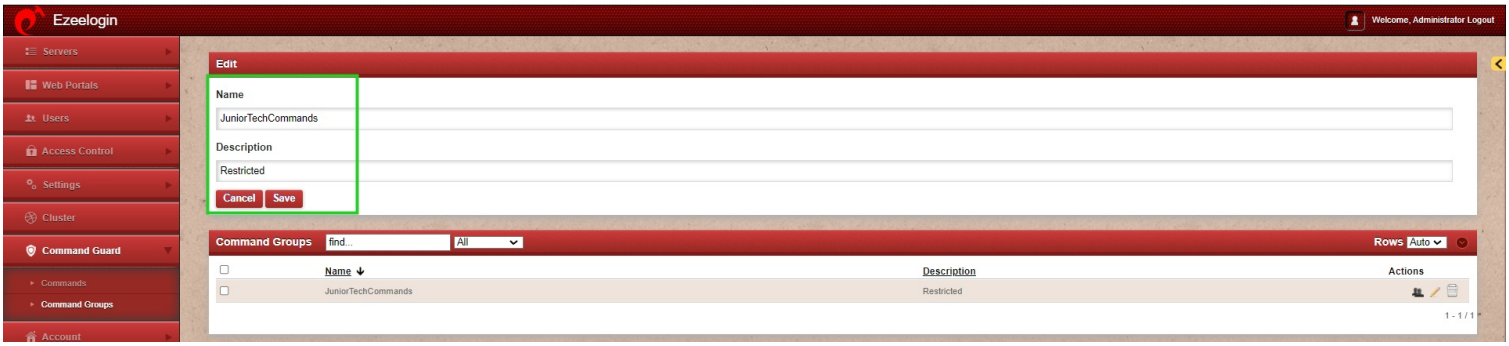
Step 2(C): Refer to the example below to add a **password for the remote user**, which can be used when the command guard is enabled and a remote user needs to switch users (the password will be saved in an encrypted format and cannot be viewed after saving).

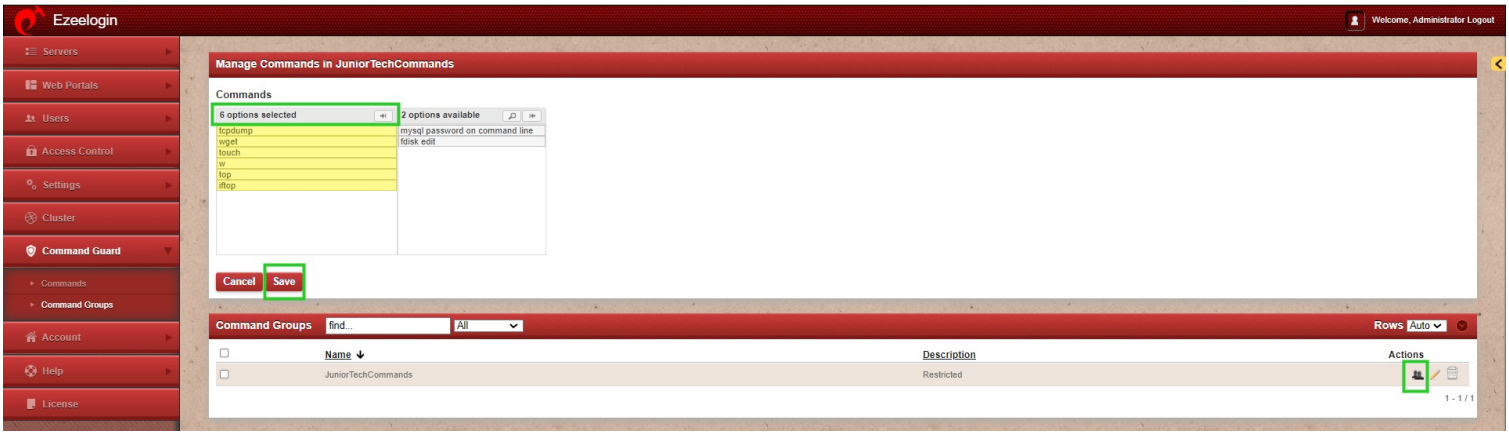


The command guard tab will list all the commands that have been added.



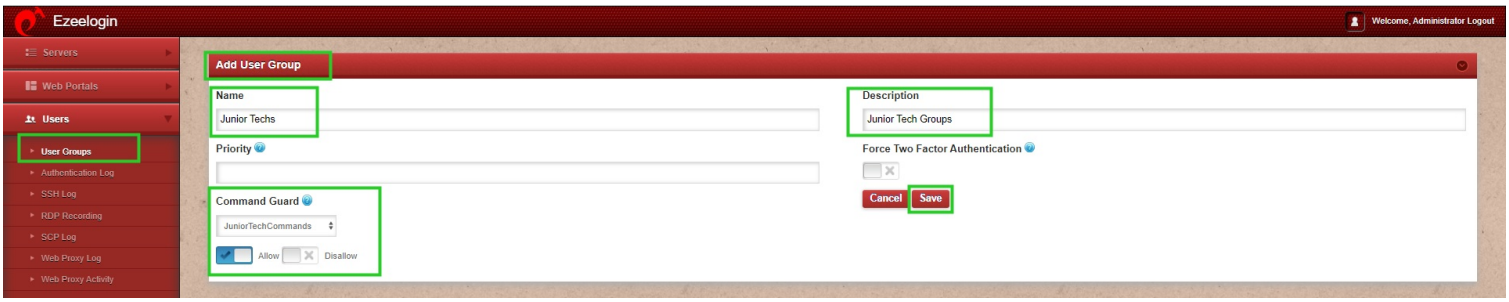
Step 3: **Create a command group** called "*JuniorTechCmds*" and assign the commands *"top,iftop,w,tcpdump,wget"* to the group.



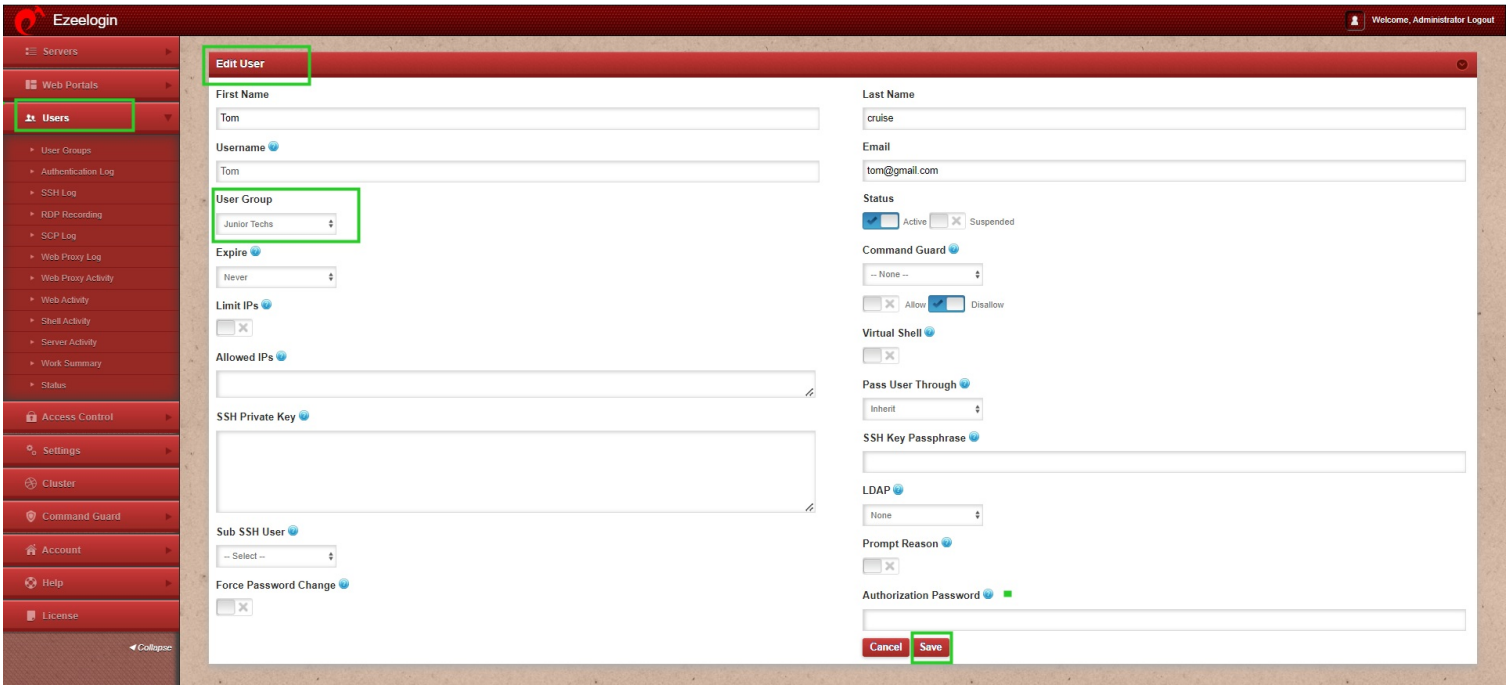


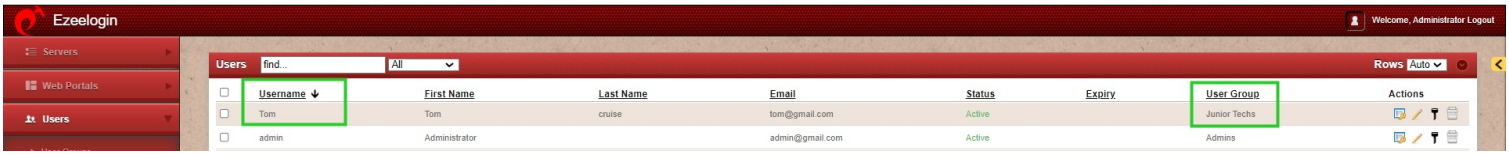
Step 4: Create a UserGroup called "*Junior Techs*" and assign the command group as shown below.

If the UserGroup already exists, then edit and select the "*JuniorTechCommands*" in Command Guard and click "Allow" and then "Save".



Step 5: **Edit the user** "*Tom*" and **assign the gateway user with the user group** "*Junior Techs*".

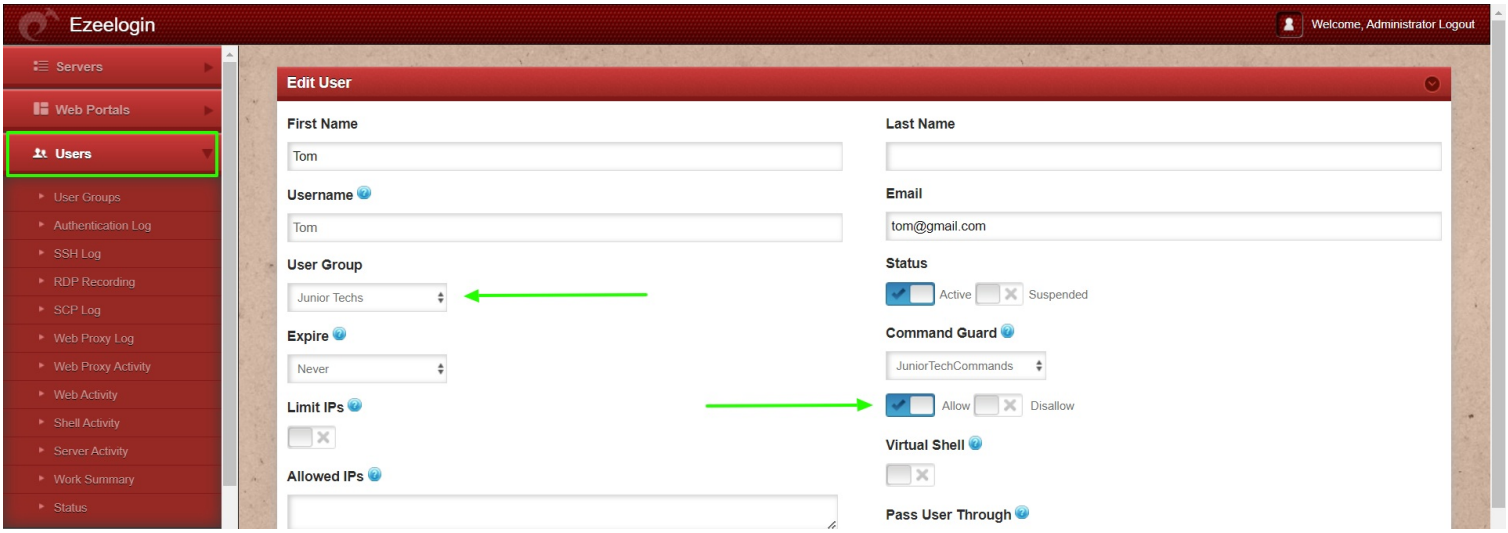




Step 6: Login into remote server "web.eznoc.com" via ezsh shell as user tom (UserGroup "*Junior Techs*")

The **user "*Tom*" would only be able to run the commands that are added in the command group "*JuniorTechCommands*".**

Step 6(A): The below example shows the user "*Tom*" is **allowed** to run only the command added in the "*JuniorTechcommands*"

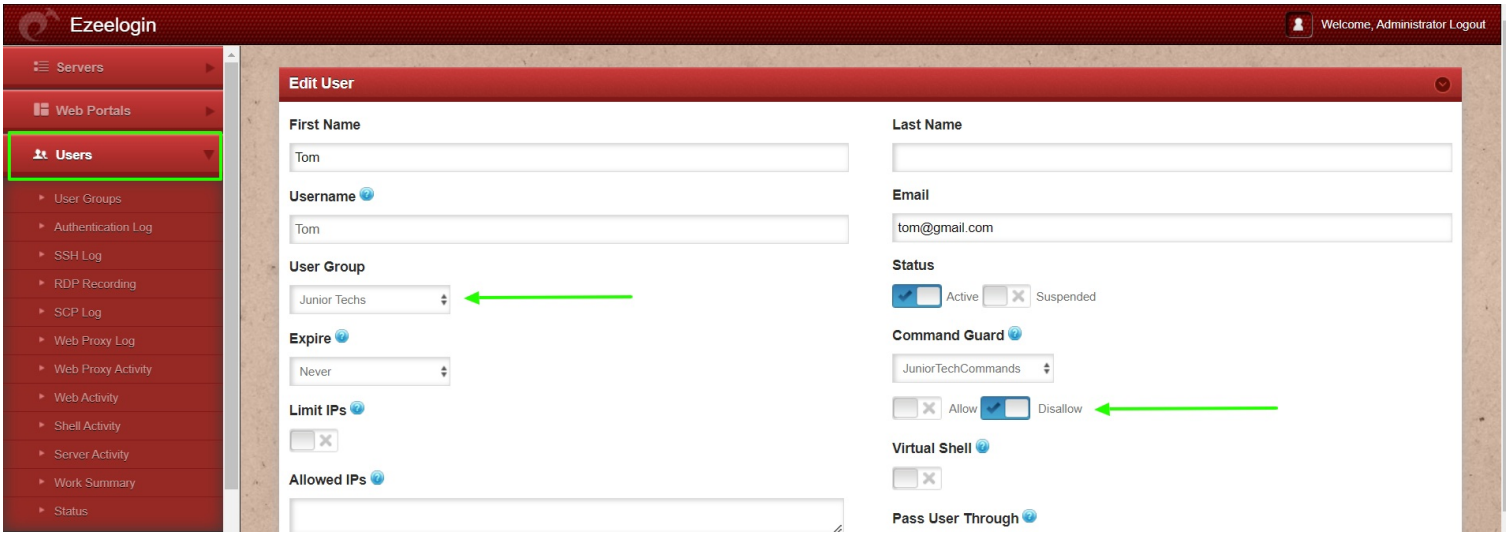




Allow will let the gateway users in the UserGroup execute only those commands matching the regular expression of commands in the command group.

Disallow will prevent the gateway users in the UserGroup from executing any of the commands matching the regular expression of commands in the command group and will let the user execute all other commands.

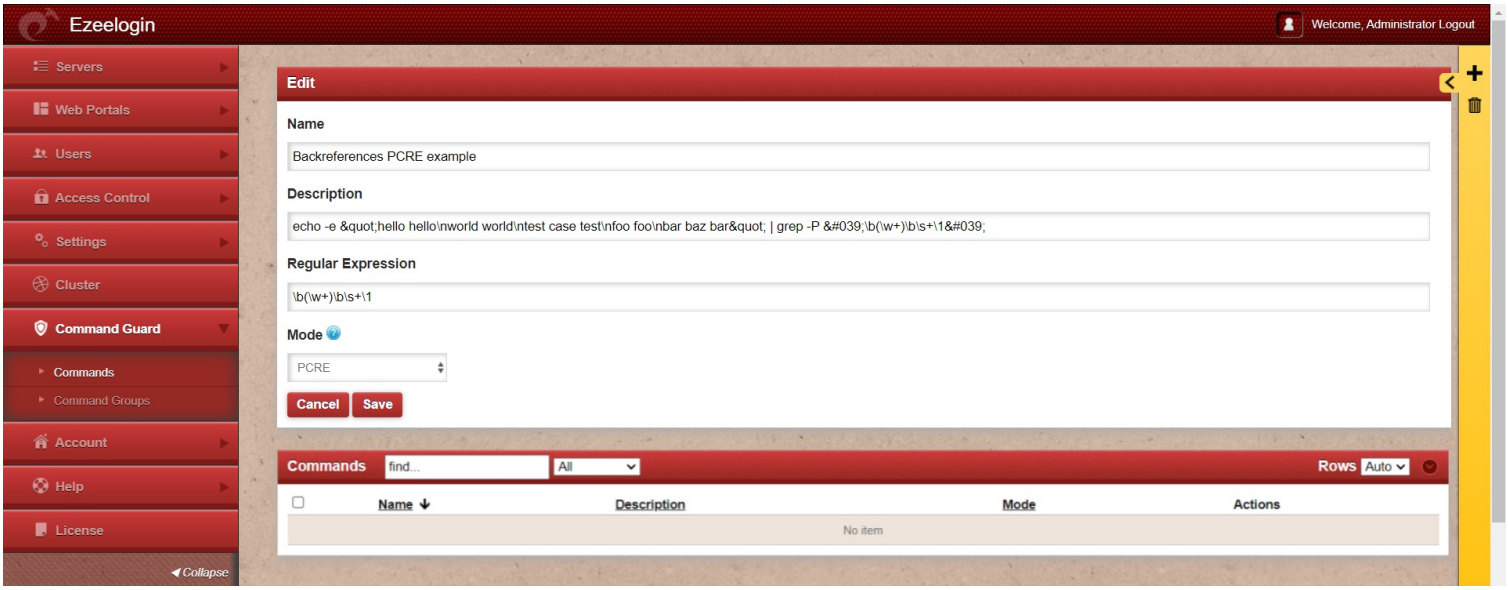
Step 6(B): The below example shows the user "*Tom*" is **not allowed** to run the command that is added to the "*JuniorTechcommands*" group.



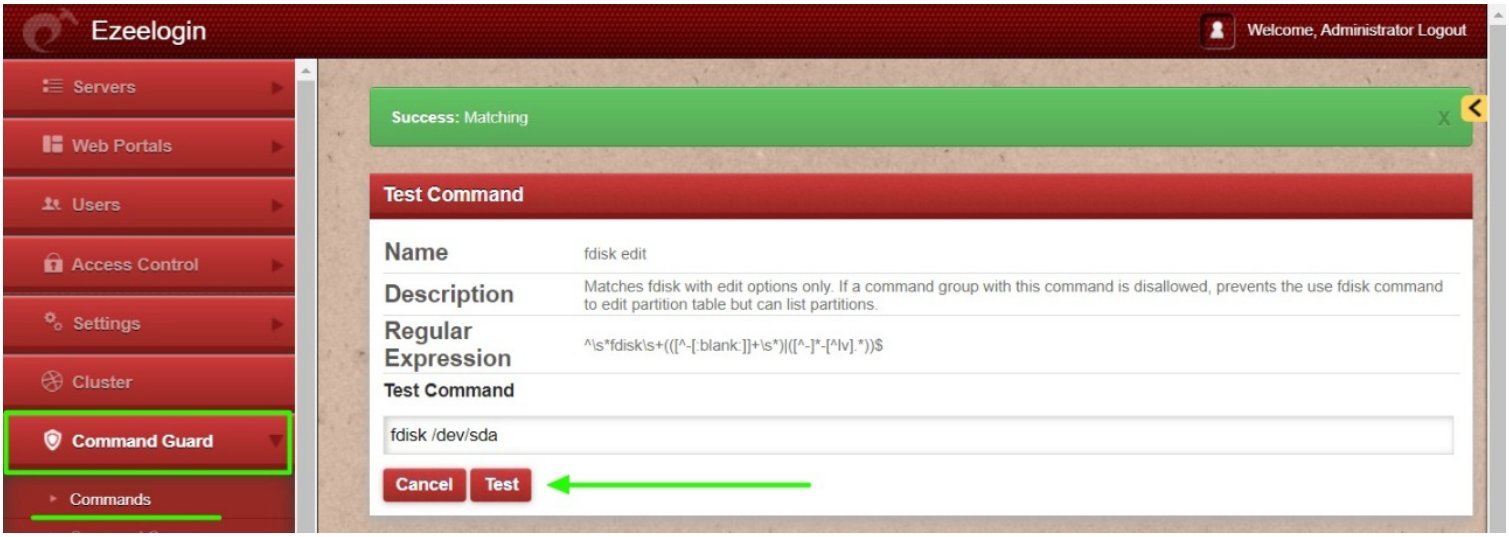


Refer to some examples of regular expressions:

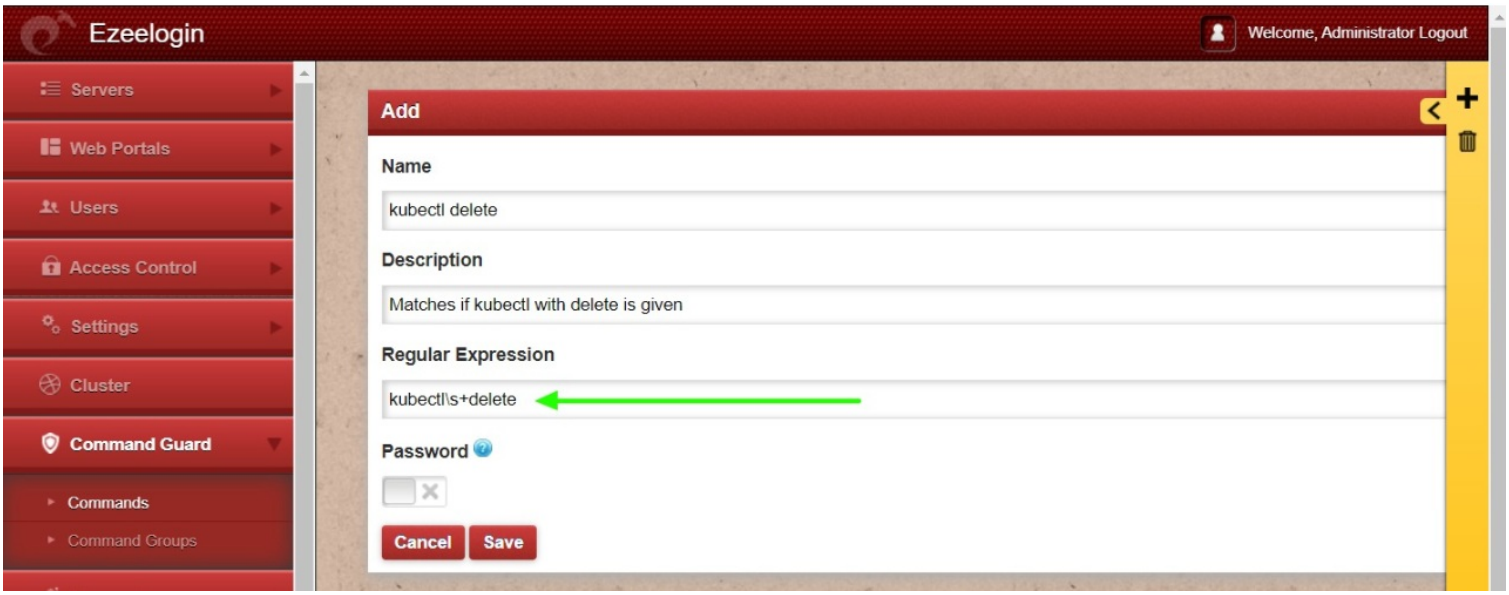
1. The following image shows an example of a regular expression to match PCRE formats.



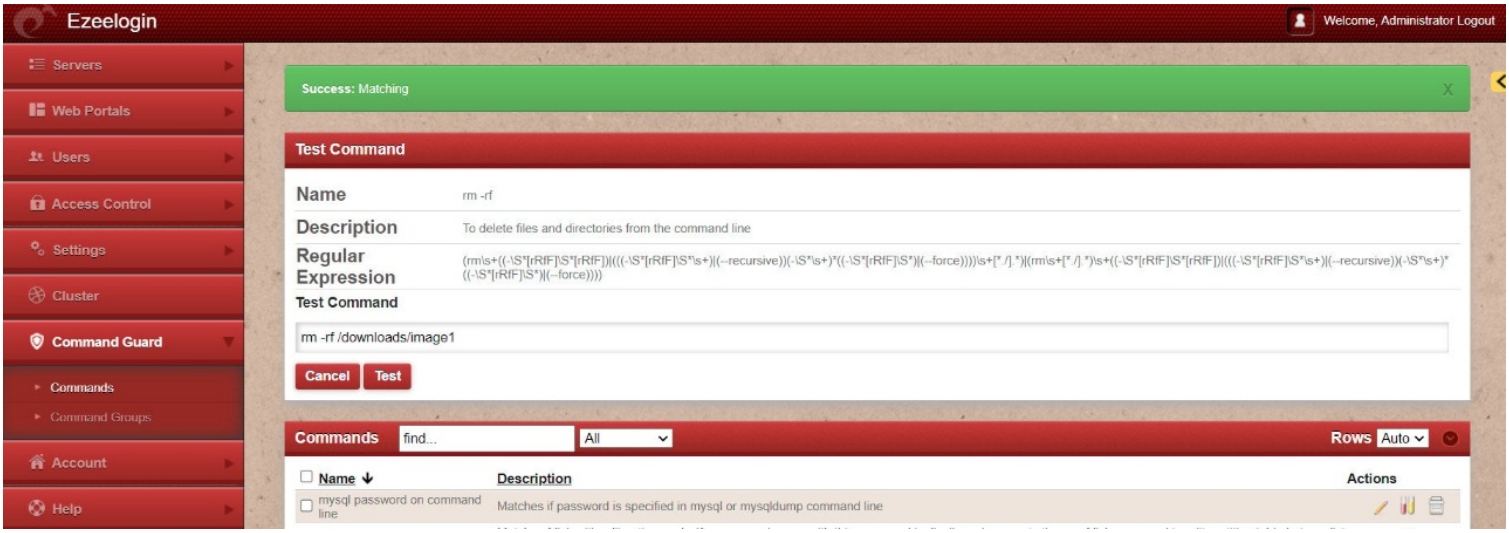
2. The following image shows another example of a regular expression to match fdisk with edit options only. If a command group with this command is disallowed, prevents the user *fdisk* command from editing the partition table but can list partitions.



3. The following image shows regular expressions to block a user from executing the " *kubectl* " command with the " delete " option.



4. The following image shows another example of a regular expression to delete files and directories from the command line with '' *rm -rf* ''.



IEEE Std 1003.2 (“POSIX.2”) regular expressions by **default**.

PCRE regular expression is supported by **Ezeelogin version 7.38.0**. **Upgrade to the latest version** to use this feature.

Note: Command guard is an experimental feature (user can bypass command guard by using scripts, up arrow key, tab key, etc).

Understanding command guard limitations

Command Guard functions as an input filter that checks commands explicitly typed by users. Its primary purpose is to help prevent the accidental execution of potentially dangerous commands. However, Command Guard is not designed to restrict the execution of binaries or enforce system-level command restrictions. Therefore, it does not filter commands executed through shell scripts or other indirect methods.

Recommended approach

To restrict unauthorized users from executing specific binaries or commands, we recommend the following:
Assign users non-root accounts instead of granting direct root access. Refer article for more details: How to add sub ssh users on remote servers and restrict commands via sudoers file
Use the sudo mechanism to control access to privileged binaries and commands. Refer article for more details: Privileged access management in Linux
Configure appropriate sudo permissions to ensure that users can execute only the commands authorized for their roles. Refer article for more details: How to add a subssh user with non privileged remote ssh login user

This approach provides system-level access control and is more suitable for restricting the execution of specific binaries or commands.

Related Articles:

User switching when command guard is enabled
Allow user to switch when command guard is disabled
Slowness in SSH Session
How to add sub ssh users on remote servers and restrict commands via sudoers file
Privileged access management in Linux
How to add a subssh user with non privileged remote ssh login user