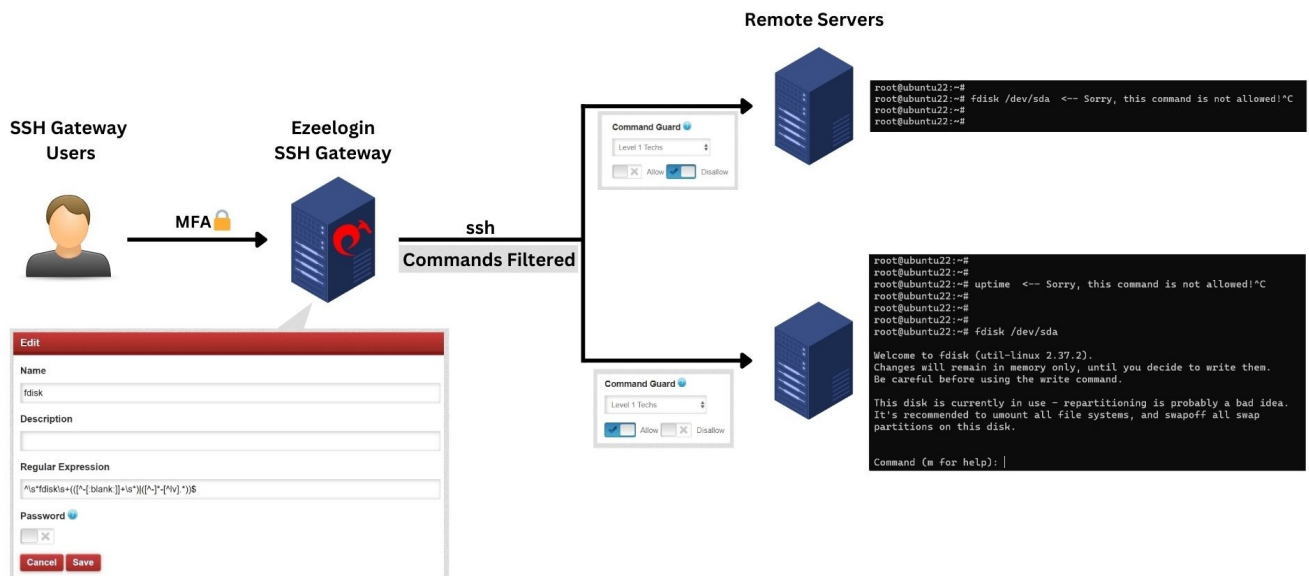


Filter command executed on remote servers using command guard

10 Manu Chacko November 16, 2023 [Security Features](#) 7129

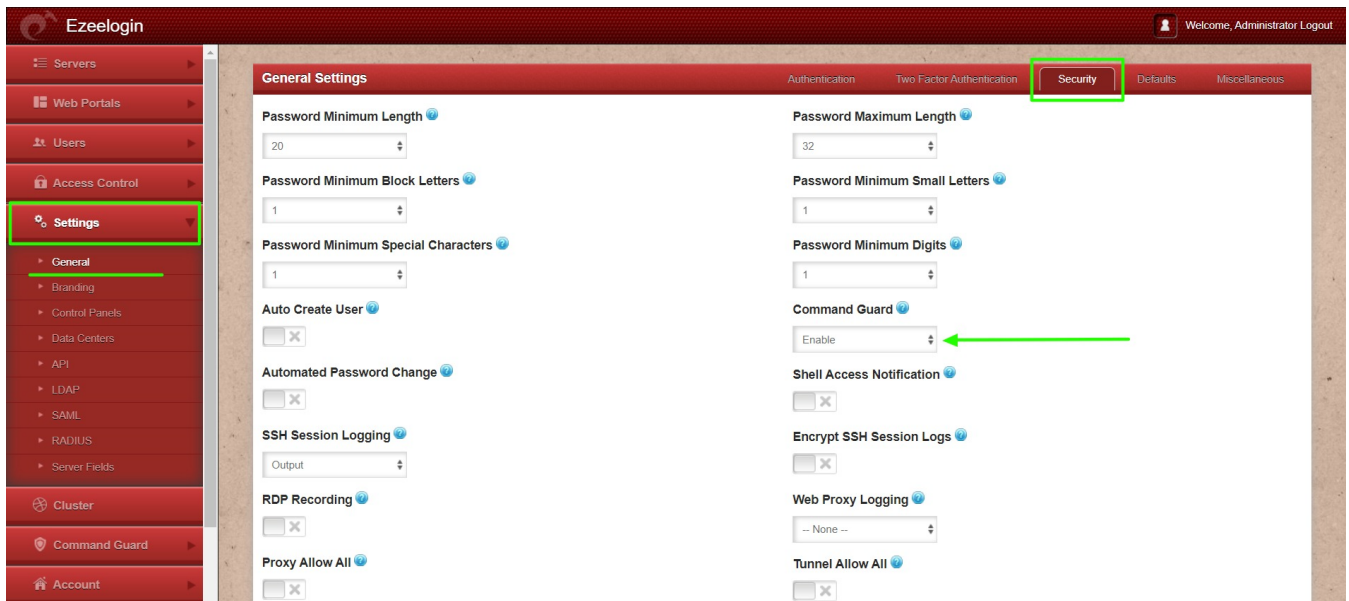
How to restrict commands that a gateway user can execute on remote servers in Ezeelogin?




Ezeelogin uses **IEEE Std 1003.2 (“POSIX.2”)** regular expressions in the command guard.

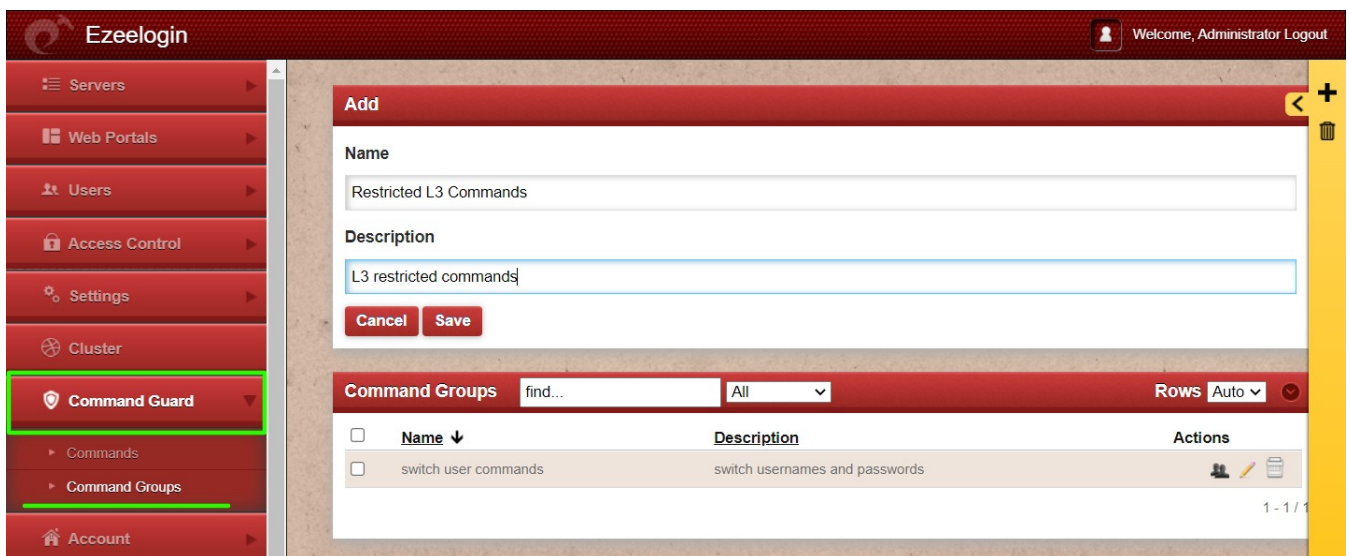
Note: Command guard is an experimental feature (user can bypass command guard by using scripts, up arrow key, tab key, etc).

1. **Enable command guard** from Ezeelogin GUI > Settings > General > Security > Command Guard > Enable


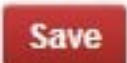


2. Add a **command group** from Ezeelogin GUI > Command Guard > Command Groups > Add Group

Click  on the right menu to open add command group form.



3. Add command from Ezeelogin GUI > Command Guard > Commands > Add command

Click  add command form. Enter the name and regular expression for the command you want to add and click .

Ezeelogin Welcome, Administrator Logout

Command Guard

Edit

Name
fdisk edit

Description
Matches fdisk with edit options only. If a command group with this command is disallowed, prevents the use fdisk command to edit parti

Regular Expression
^ls*fdisk[s+((^[.blank:]]+s*))((^[^]*-[^\\v].*))\$

Password

Cancel Save

Refer below example to test if a string matches the regular expression given for a command, click on the test



icon towards the right of the command in the command list.

Ezeelogin Welcome, Administrator Logout

Command Guard

Test Command

Name
fdisk edit

Description
Matches fdisk with edit options only. If a command group with this command is disallowed, prevents the use fdisk command to edit partition table but can list partitions.

Regular Expression
^ls*fdisk[s+((^[.blank:]]+s*))((^[^]*-[^\\v].*))\$

Test Command
fdisk /dev/sda

Cancel Test

Success: Matching

Commands find... All Rows Auto

Name	Description	Actions
<input type="checkbox"/> mysql password on command line	Matches if password is specified in mysql or mysqldump command line	
<input type="checkbox"/> fdisk edit	Matches fdisk with edit options only. If a command group with this command is disallowed, prevents the use fdisk command to edit partition table but can list partitions.	
<input type="checkbox"/> su		

For example, the following image shows regular expressions to block a user from executing the "kubectl " command with the " delete " option.

Ezeelogin

Welcome, Administrator Logout

Servers

Web Portals

Users

Access Control

Settings

Cluster

Command Guard

Commands

Command Groups

Account

Help

License

Add

Name

kubectl delete

Description

Matches if kubectl with delete is given

Regular Expression

kubectl's+delete

Password

Cancel

Save

Commands

find...

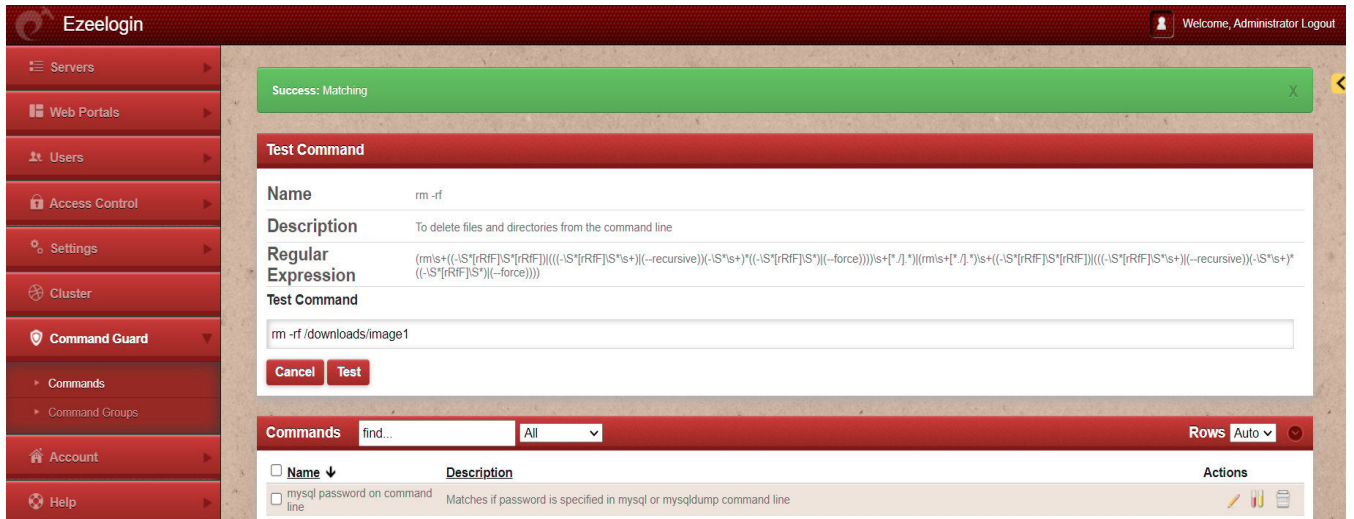
All

Rows

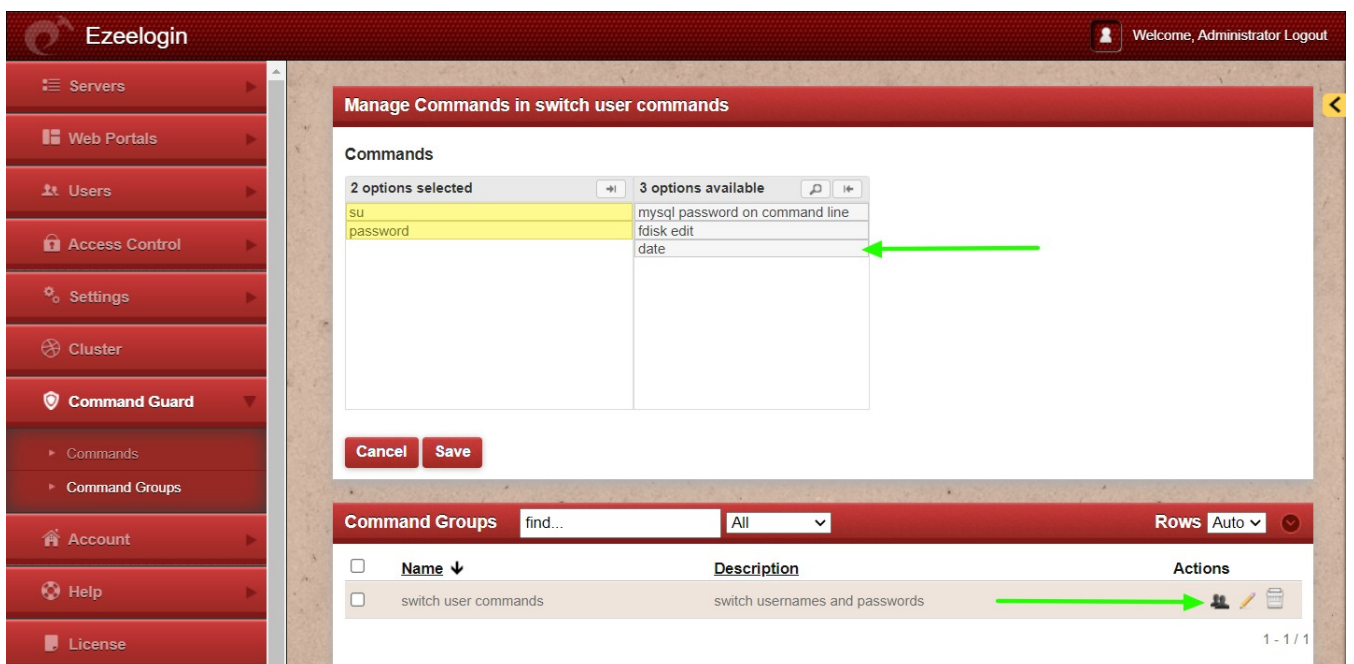
Auto

Name	Description	Actions
mysql password on command line	Matches if password is specified in mysql or mysqldump command line	
fdisk edit	Matches fdisk with edit options only. If a command group with this command is disallowed, prevents the use fdisk command to edit partition table but can list partitions.	

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



4. Add the command to Command Group from **Ezeelogin GUI > Command Guard > Command group > Actions** > Click on the Commands icon



Refer user manual: https://www.ezeelogin.com/user_manual/CGM.html

5. Edit the user, choose the command group, and Allow / Disallow commands for the user.

Select the command group from the drop down windows and select Allow / Disallow to allow or disallow

ezeelogin

Welcome, ezadmin Logout

Servers

Web Portals

Users

User Groups

LDAP

SSH Log

SCP Log

Web Proxy Log

Web Activity

Shell Activity

Server Activity

Work Summary

Status

Access Control

Settings

Cluster

Command Guard

Account

Help

Edit User

First Name

Administrator

Username

ezadmin

User Group

Admins

Expire

Never

Limit IPs

Allowed IPs

SSH Private Key

Sub SSH User

-- Select --

Last Name

Email

administrator@eznoc.com

Status

☒ Active ☐ Suspended

Command Guard

Level 1 Tects

Limit IPs

☒ Allow ☐ Disallow

Virtual Shell

Pass User Through

Yes

SSH Key Passphrase

LDAP

None

Authorization Password

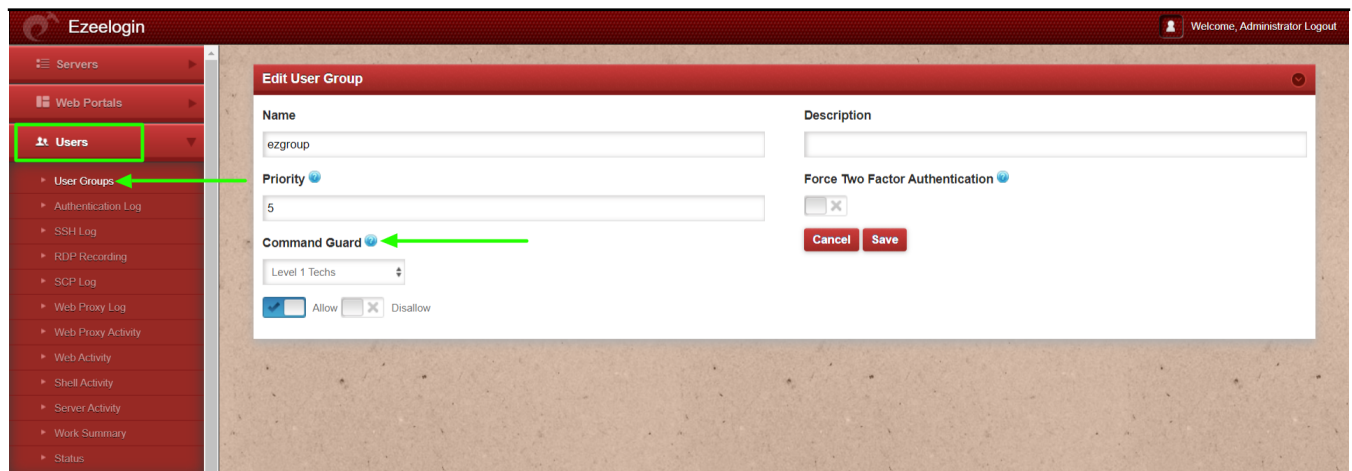
Cancel

Save



You can also edit the user group, choose the command group, and select **Allow** / **Disallow** to allow or disallow commands in the command group.

This feature is available from Ezeelogin version 7.36.0. Refer article to [upgrade Ezeelogin to the latest version](#).



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

Disallow will prevent the 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.

How to allow the user to switch when the command guard is enabled?

1. The following image shows how to **add the regular expression for the switch user**.

Edit

Name
switch user

Description

Regular Expression
su -

Password

Commands find... All Rows Auto

Name	Description	Actions
<input type="checkbox"/> mysql password on command line	Matches if password is specified in mysql or mysqldump command line	

2. Add the password of the user in the regular expression field and enable the password button to save it with hashing.

Edit

Name
john password

Description
password of user john

Regular Expression
2@#&E!ZTm8k^

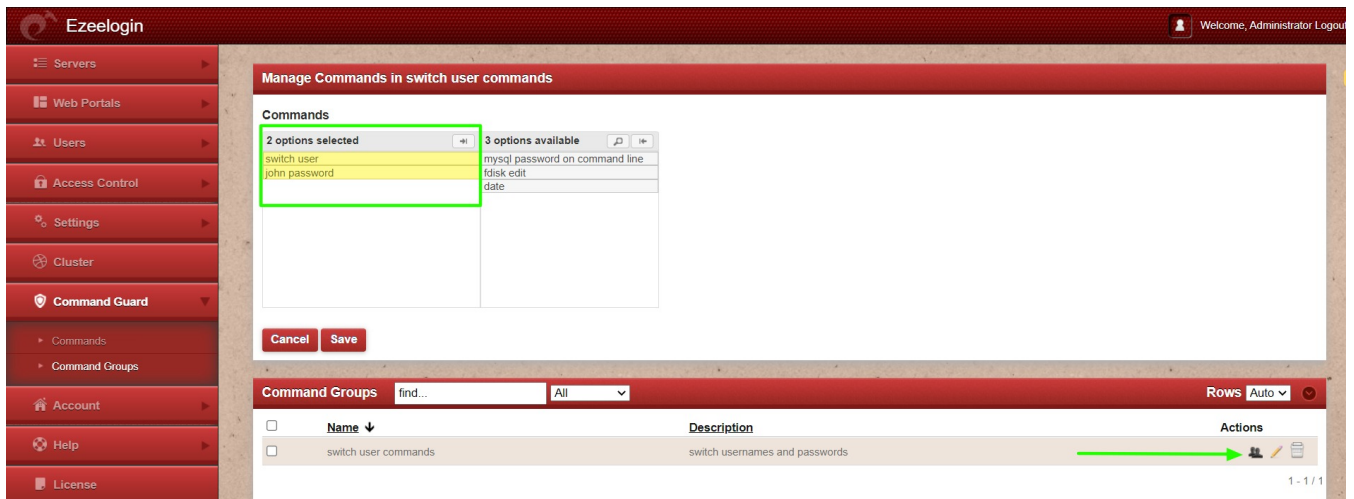
Password

Commands find... All Rows Auto

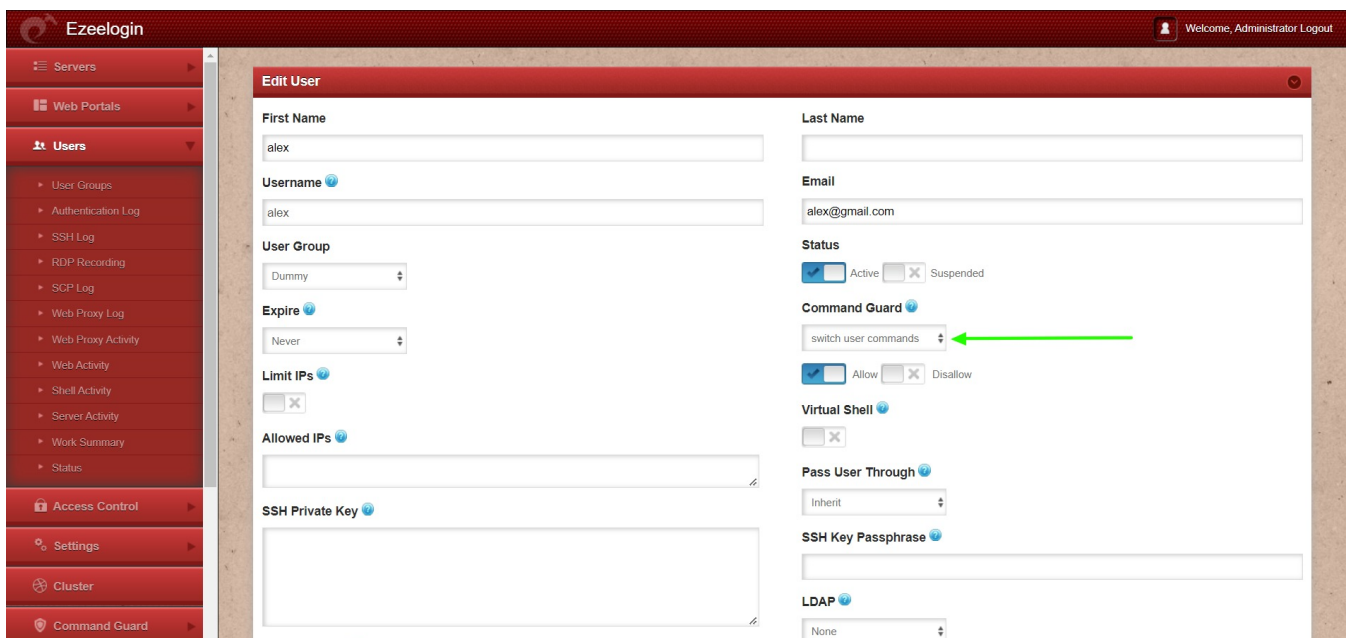
Name	Description	Actions
<input type="checkbox"/> mysql password on command line	Matches if password is specified in mysql or mysqldump command line	
<input type="checkbox"/> fdisk edit	Matches fdisk with edit options only. If a command group with this command is disallowed, prevents the use fdisk command to edit partition table but can list partitions.	
<input type="checkbox"/> su		
<input type="checkbox"/> password		
<input type="checkbox"/> date		

1 - 5 / 5


3. Navigate to command guard group -> click on the command's icon and select all commands that need to be added to the group.



4. Edit the user, select the command guard group from the dropdown, and enable allow to allow those commands for that user.



5. Login to the ezsh (Ezeelogin shell) as the same user, type in **su - username** to switch user, and provide the correct password when prompted. Refer to the below example.



```
Ez: ubuntu.server
tony@ubuntu22:~$
tony@ubuntu22:~$ date <-- Sorry, this command is not allowed!^C
tony@ubuntu22:~$
tony@ubuntu22:~$
tony@ubuntu22:~$ su - john
Password:
john@ubuntu22:~$
john@ubuntu22:~$
john@ubuntu22:~$ █
```

Related Articles

[Slowness in SSH Session](#)

Online URL:

<https://www.ezeelogin.com/kb/article/filter-command-executed-on-remote-servers-using-command-guard-10.html>