Access Control Explained

496 Nesvin KN December 9, 2025 General 9280

Role Based Access Control (RBAC) Explained

Overview: This article explains how to implement **Role-Based Access Control (RBAC**) in SSH, detailing how to manage user access to servers, server groups, web portals, and specific actions based on their roles.

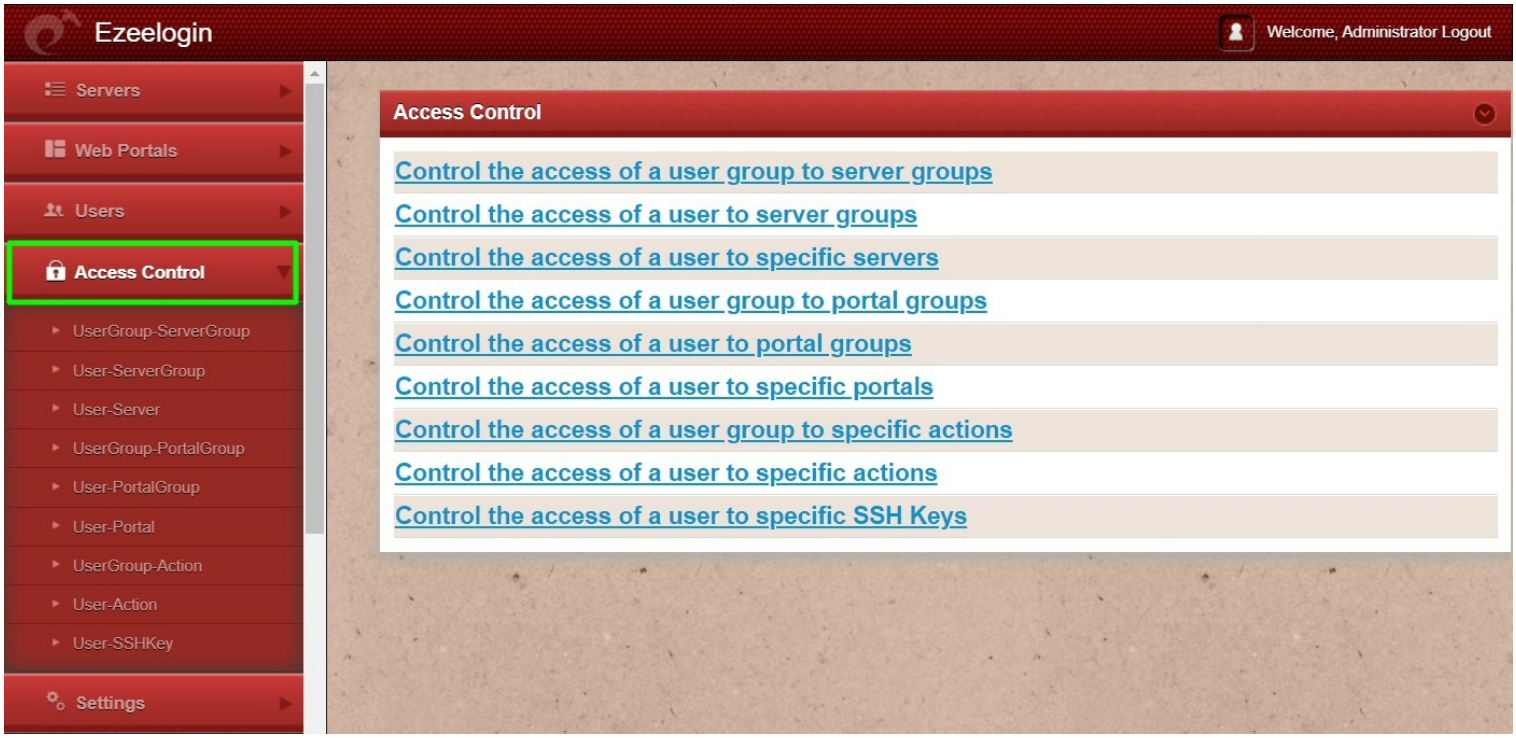
RBAC or **Role Based Access Control in SSH** is a method to *restrict the access of SSH users* or server administrators to the remote servers based on their role. Most of the enterprises are having thousands of servers. Granting SSH access to employees is a big headache or security concern for the companies. Using *Role based access control (RBAC),* we can ensure that ssh users or system administrators are using only the relevant information they needs to perform their task. We can restrict their access to only a particular group of servers and also can control their actions on those servers too.

How to grant role based access control in SSH?

Restrict user actions in server
Map ssh user to a particular server
Map ssh user to group of servers
Map ssh user group to single server
Map ssh user group to group of servers etc

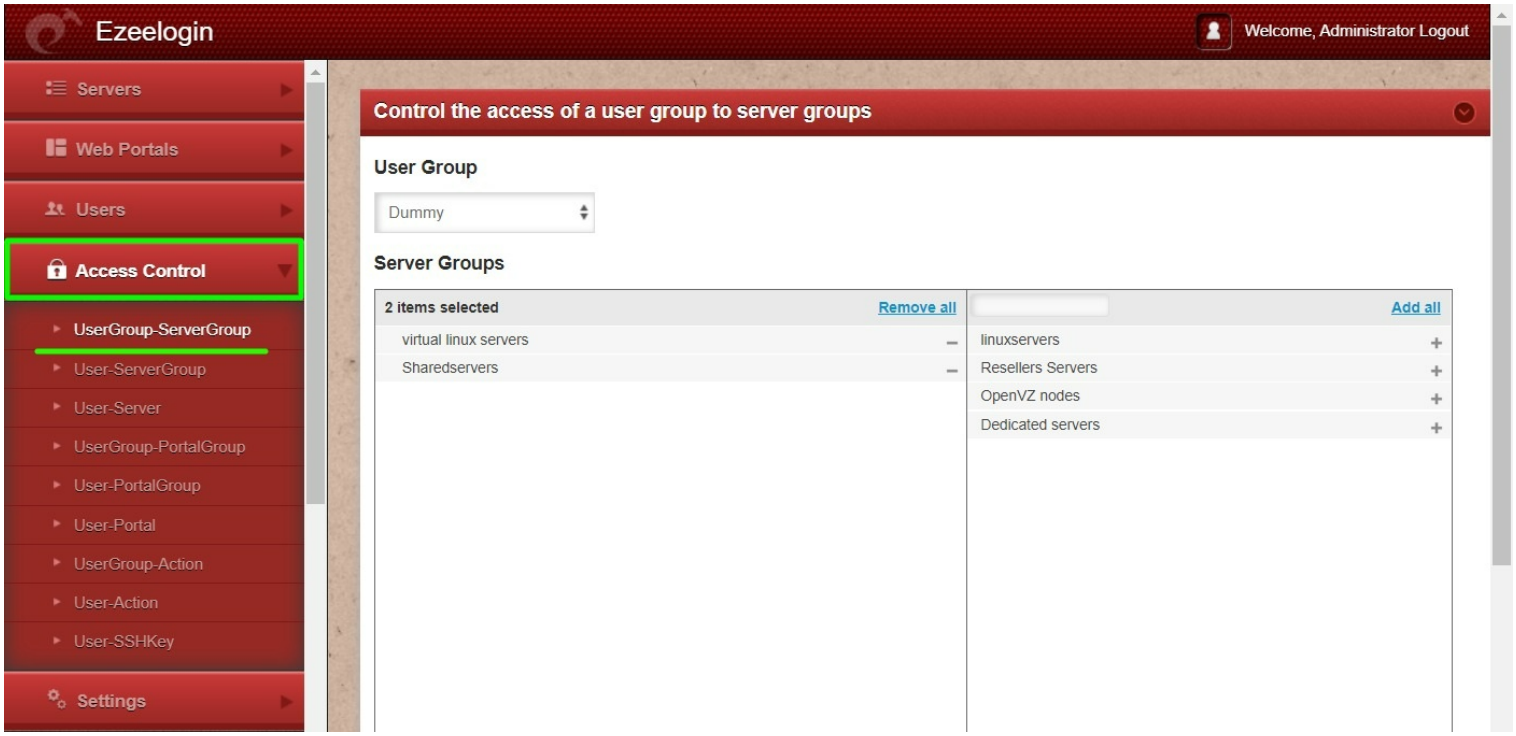
How to configure role based access control (rbac) in SSH ?

Group your staff and your servers into different categories and decide which user or group of users get access to which server or group of servers.



UserGroup to ServerGroup

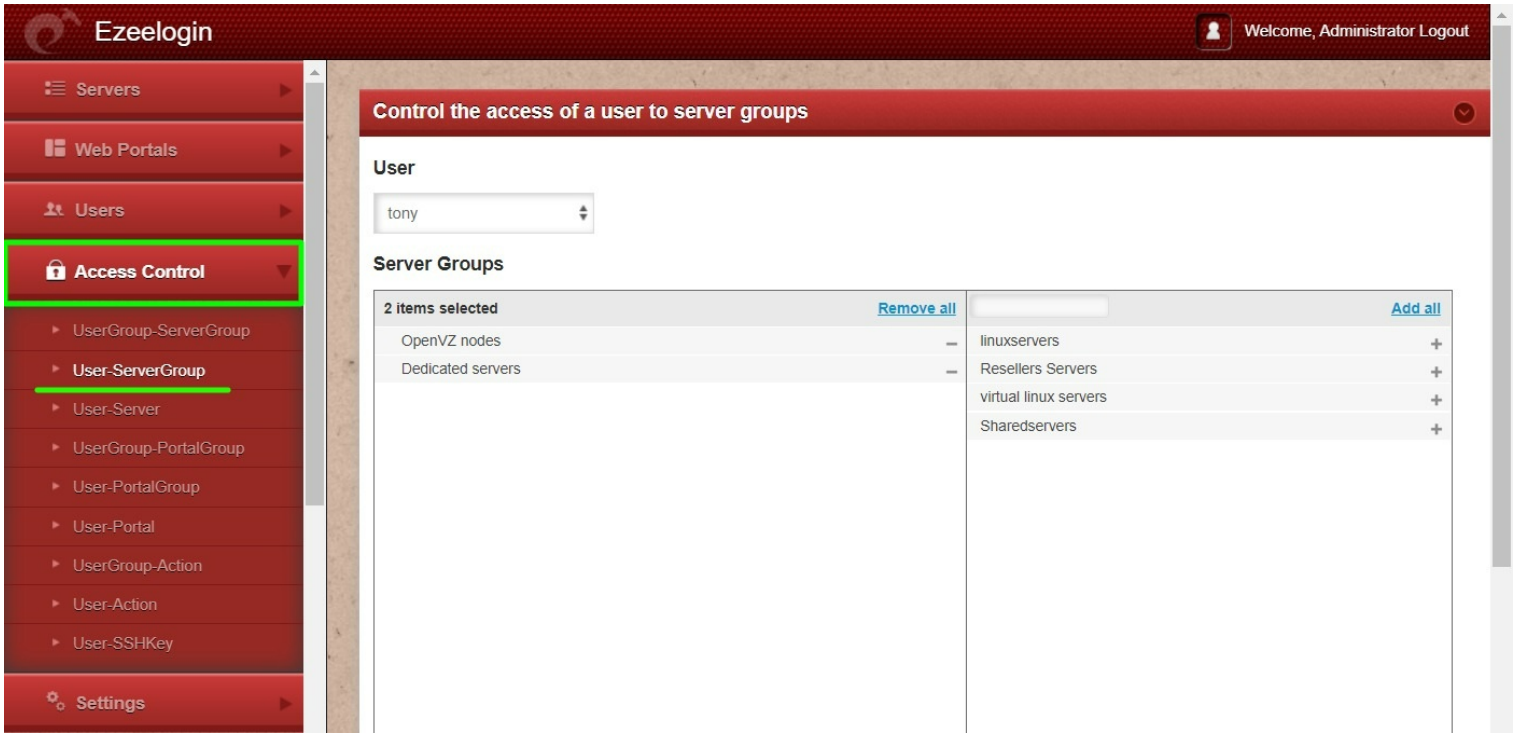
Enable or disable access to a group of servers (ServerGroups) for a group of users or in other words regulate access of user groups to server groups.



Select User group Use the drop down menu to choose the UserGroup whose accessibility needs to be altered.
Non-Accessible Server Groups The list of ServerGroups that is not accessible to the above selected UserGroup is in the right box. Use **Add All** to add all or use + to add them one by one.
Accessible Server Groups The list of ServerGroups that is accessible to the above selected UserGroup is in the left box. Use **Remove All** remove all server groups or use − to remove them one by one.
Click the **Save** button to save the changes.

User to ServerGroup

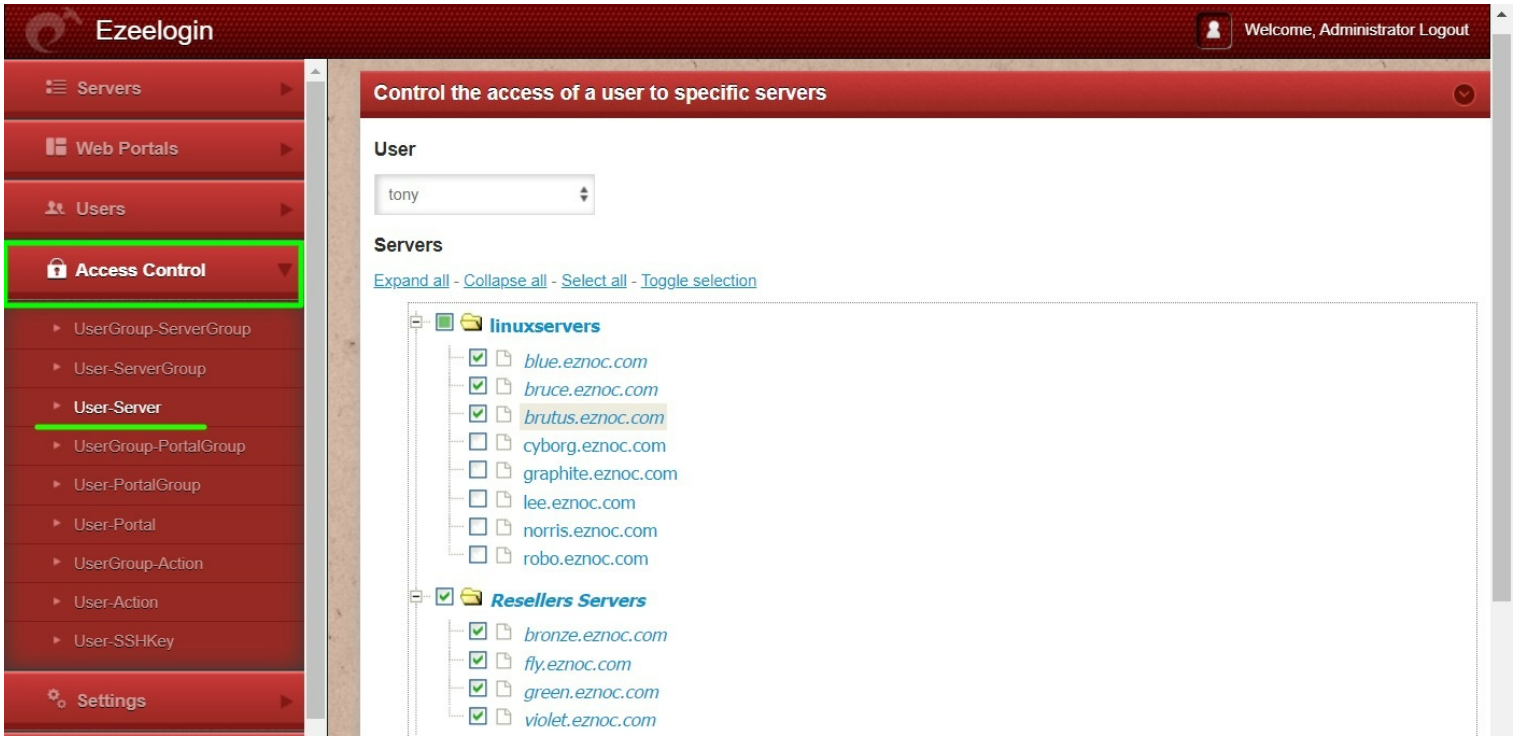
Enable or disable access to a group of servers (ServerGroups) for individual users or in other words regulate access of users to ServerGroups.



Select the User for which you need to change the access.
Select server group(s) from the non-accessible or accessible list as you want and move it to the other list using the + − operators.
Click the **Save** button to save the changes.

User to Server

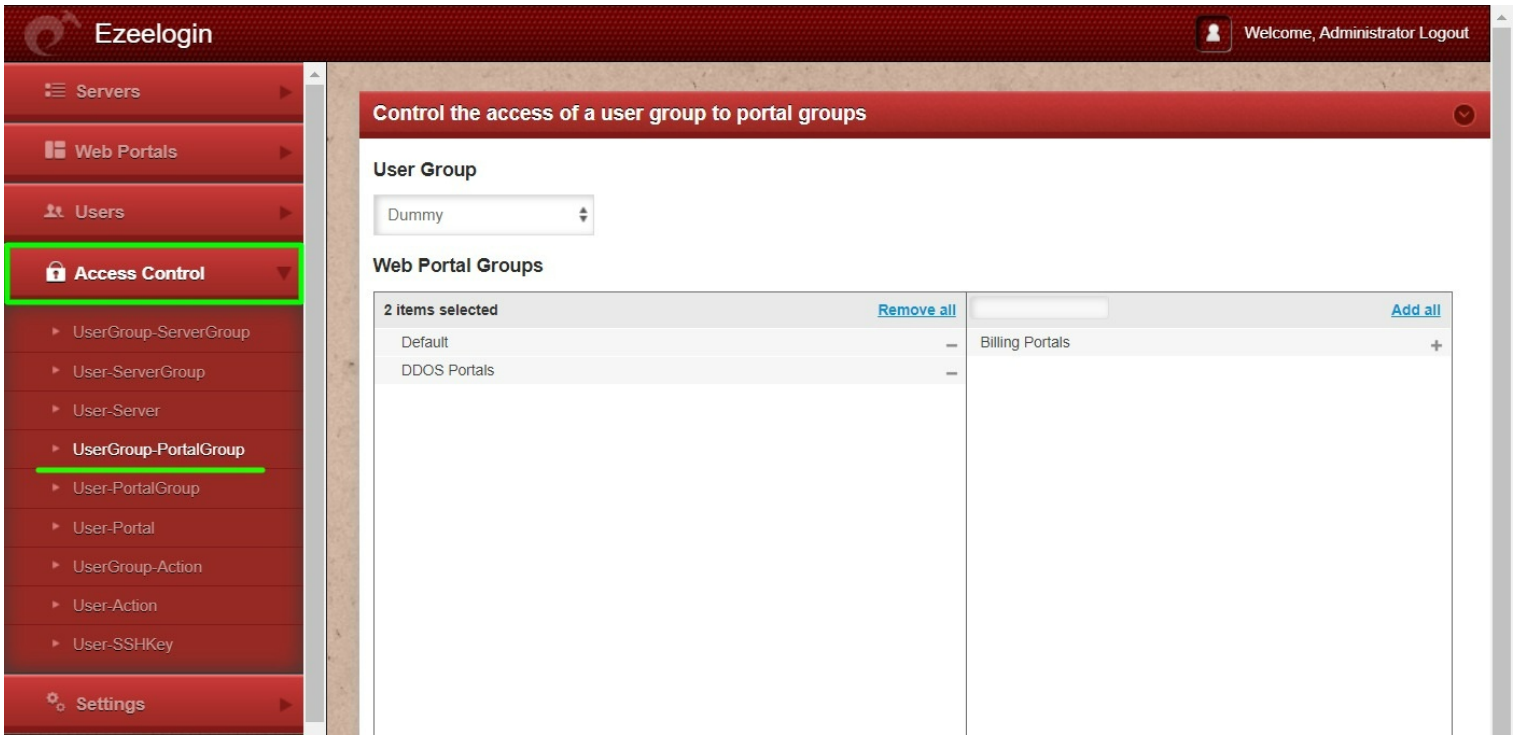
Enable or disable access to individual server for individual users or in other words regulate access of user to server.



Select the user for which you need to change the access using **SelectUser.**
Tick the checkboxes of ServerGroup or Servers that the user needs to be granted access to.
Click **Save** to save the changes.

UserGroup to WebPortalGroup

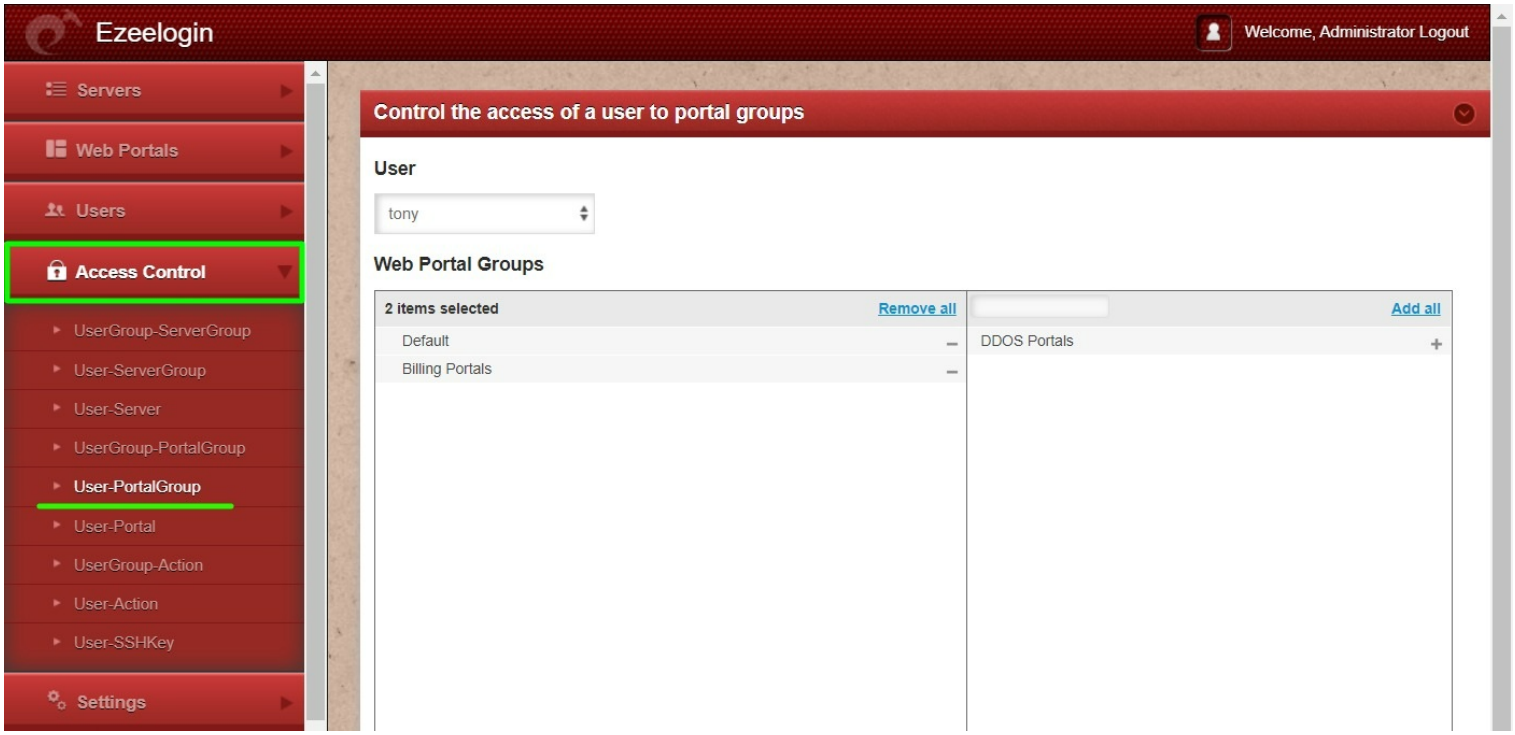
Enable or disable access to a groups of webportals (PortalGroups) for a group of users or in other words regulate access of usergroup to portalgroups.



Select User group Use the drop down menu to choose the UserGroup whose accessibility needs to be altered.
Non-Accessible Portal Groups The list of PortalGroups that is not accessible to the above selected UserGroup is in the right box. Use **Add All** to add all or use + to add them one by one.
Accessible Portal Groups The list of PortalGroups that is accessible to the above selected UserGroup is in the left box. Use **Remove All** remove all portal groups or use − to remove them one by one.
Click the **Save** button to save the changes.

User to WebPortalGroup

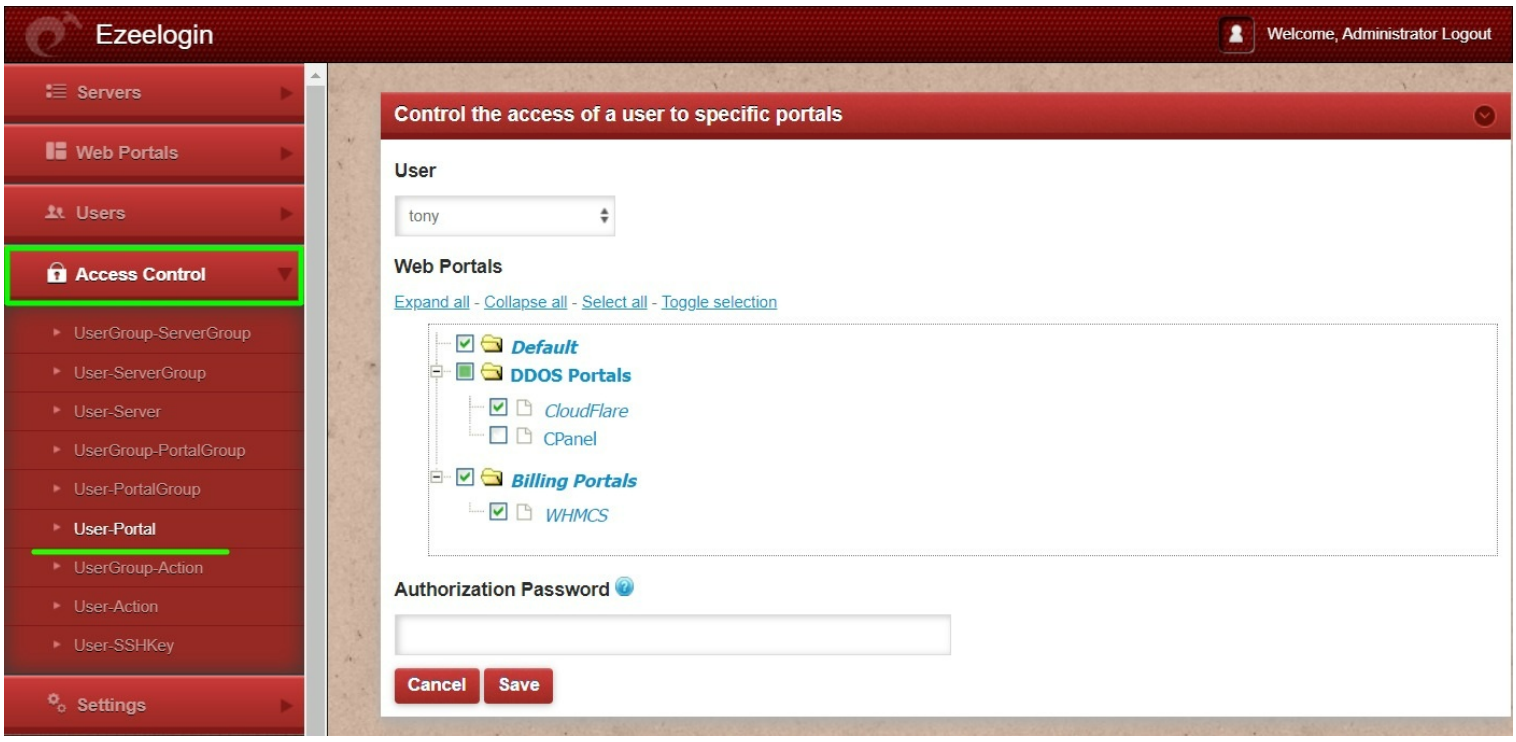
Enable or disable access to a groups of portals (PortalGroups) for individual users or in other words regulate access of users to PortalGroups.



Select the User for which you need to change the access.
Select WebPortalgroup(s) from the non-accessible or accessible list as you want and move it to the other list using the + − operators.
Click the **Save** button to save the changes.

User to WebPortal

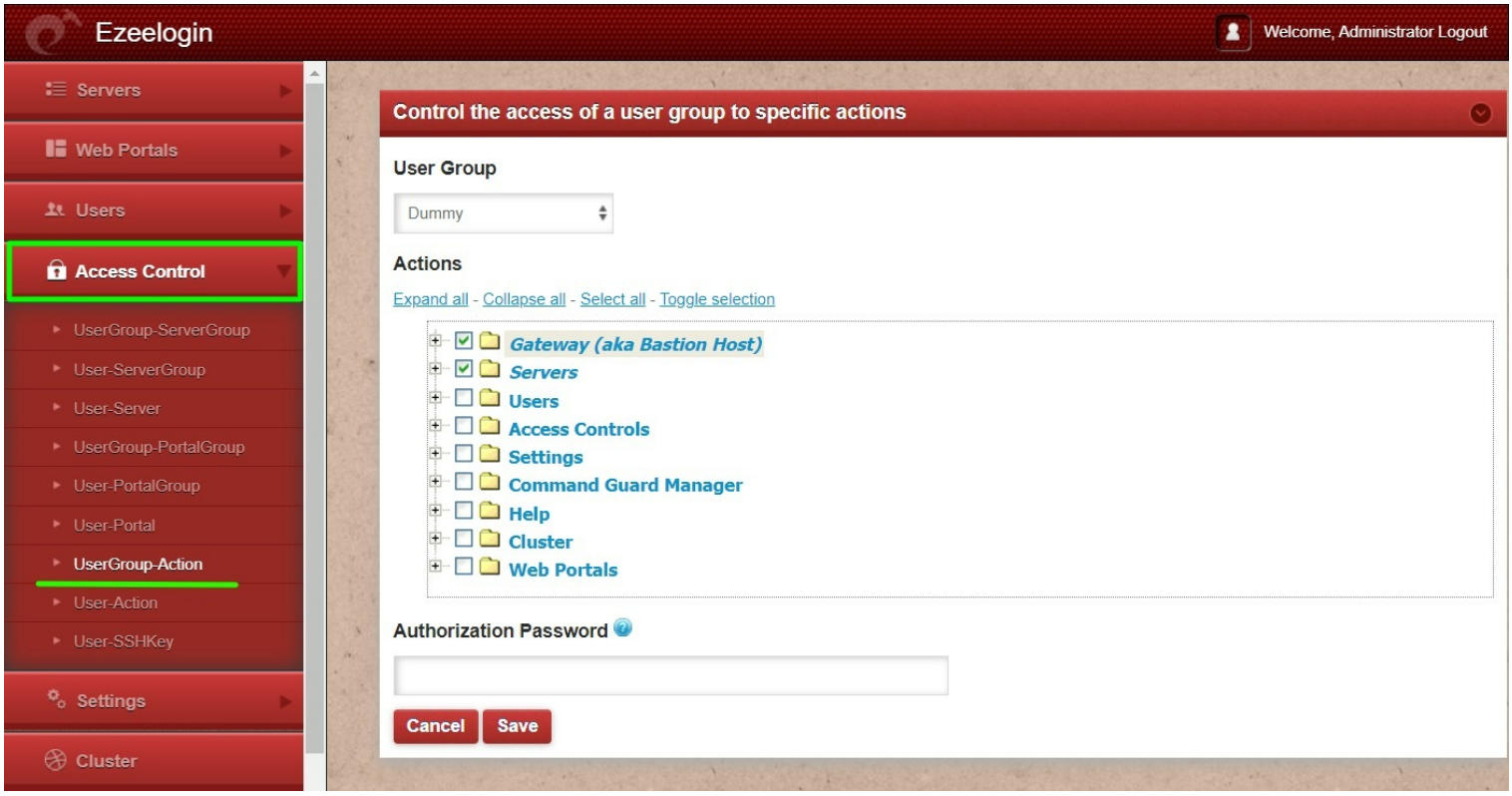
Enable or disable access to individual webportal for individual users or in other words regulate access of user to webportal.



Select the user for which you need to change the access from the User dropdown menu.
Tick the checkboxes of Webportal Group or Webportal that the user needs to be granted access to.
Click **Save** to save the changes.

Usergroup - Actions

Enable or disable access to webpanel features for Usergroups or in other words Control access of a UserGroup to webpanel features/backend servers access in ssh/ezsh features.



Gateway (aka Bastion Host)

Ezsh Shell	Allow/Disallow access to Ezsh shell for the gateway user
Allow SCP	Allow/Disallow SCP access for the gateway user
Allow SFTP	Allow/Disallow SFTP for the gateway user
Allow Mosh	Allow/Disallow MOSH for the gateway user

Servers

Server list	Ability to view server lists
Add server	Ability for the user to add a server
Edit server	Ability for the user to edit a server
Delete server	Ability for the user to delete server
View Server Details	Ability for the user to view the server details
View Super Groups	Ability for the user to view the super group
View password	Ability for the user to view the server password
View SSH Privatekey and Passphras	Ability to view ssh private key and passphrase in back-end
View encrypted server fields	Ability to view encrypted server field
Allow parallel shell	Ability to use parallel shell in ezsh shell
ControlPanel login	Ability to use passwordless controlpanel login
Datacenter login	Ability to use passwordless datacenter login
RDP login	Ability to use RDP login
IPMI login	Ability to use IPMI login
Remote console login	Ability to use remote console login
Reset server password	Ability to reset the server root passwords
Setup authentication key	Ability to resetup the ssh authentication key
Reset server fingerprint	Ability to reset the ssh fingerprint

Add server group	Ability to add the server group
Edit server group	Ability to edit the server group
Delete server group	Ability to delete server group
View mExec lists	Ability to view mExec lists
Add mExec list	Ability to add add new mExec lists
Edit mExec list	Ability to edit mExec list
Delete mExec list	Ability to delete mExec list
Change servers in mExec list	Ability to change servers in mExec list
Add Sub SSH User	Ability to add the sub ssh user
Delete Sub SSH User	Ability to delete sub ssh user
View Sub SSH User	Ability to view sub ssh user lists
Add Sub SSH User Maps	Ability to add the sub ssh user maps
Edit Sub SSH User Maps	Ability to edit sub ssh user maps
Delete Sub SSH User Maps	Ability to delete sub ssh user maps
View Sub SSH User Maps	Ability to view sub ssh user maps lists
Add Private Key	Ability to add private key
Edit Private Key	Ability to edit private key
Delete Private Key	Ability to delete private key
SSH Tunnel	Ability to establish SSH Tunnel from gateway to this server
Web SSH Console	Ability to SSH via web browsers such as Chrome/Firefox

Users

User list	Ability to view the Userlist
Add user	Ability to add a user
Edit user	Ability to edit a user
Delete user	Abiltiy to delete a user
Group list	Ability to view the group list
Add user group	Ability to add a usergroup
Edit user group	Ability to edit a usergroup
Delete user group	Ability to delete a usergroup
View SSH log	Ability to view ssh logs
View SCP log	Ability view scp logs
Web activity	Ability to view web activity logs
Shell Activity	Ability to view shell activity
Server Activity	Ability to view server activity
User Status	Ability to view user status
Work summary	Ability to view work summary
User status	Users status
Four eyes authorization privilege	User will able to view logs only when he is authorized by another user

Access Controls

UserGroup-ServerGroup	Grant privilege to choose UserGroup-ServerGroup action
User-ServerGroup	Grant privilege to user on User-ServerGroup action
User-Server	Grant privilege to user on the User-server action
User-Portalgroup	Grant privilege to user on User-Portalgroup action
User-Portal	Grant privilege to user on User-Portal action
UserGroup-Action	Grant privilege to user on UserGroup-Aciton
User-Action	Grant privilege to user on executing the User-Action action
User-SSHKey	Grant privilege to user on the User-SSHKey action
Reset All User Specifc Overrides	Grant privilege to user so that a user's acl is set back to default
Privilege to grant actions access	Grant privilege to user so that he can modify the access control of other users

Settings

All	Grant user all actions under settings tab

Command Guard Manager

All	Grant user All actions under the command guard manager tab

Help

All	Grant user All actions under Help tab

Cluster

All	Grant user All actions under Cluster tab

Web Portals

Webportal list	Ability to view the webportal list only
View Portal	Ability to view the details of a webportal with detailed view. This option has to be disabled along with the edit portal option below to prevent the display of webportal info
Add portal	Ability to add a new webportal
Edit portal	Ability to edit an exisiting webportal. This option has to be disabled along with the view portal option to prevent the display of webportal info
Webportal login	Ability to login into the portal with one click

User SSH Key

Enable or disable access to individual SSH Key for individual users or in other words regulate access of user to ssh key.

Select the user for which you need to change the access from the User drop down menu.
Tick the check boxes of SSH Key that the user needs to be granted access to.
Click **Save** to save the changes.

Related articles

Reset access control for Ezeelogin Gateway users

Role Based Access Control in SSH

Reset access control override

How to grant a user access to control panel

Online URL: https://www.ezeelogin.com/kb/article/access-control-explained-496.html