Web Activity Log

451 Nesvin KN May 27, 2026 Features & Functionalities, General 5885

How to find detailed Web Activity Log in Ezeelogin

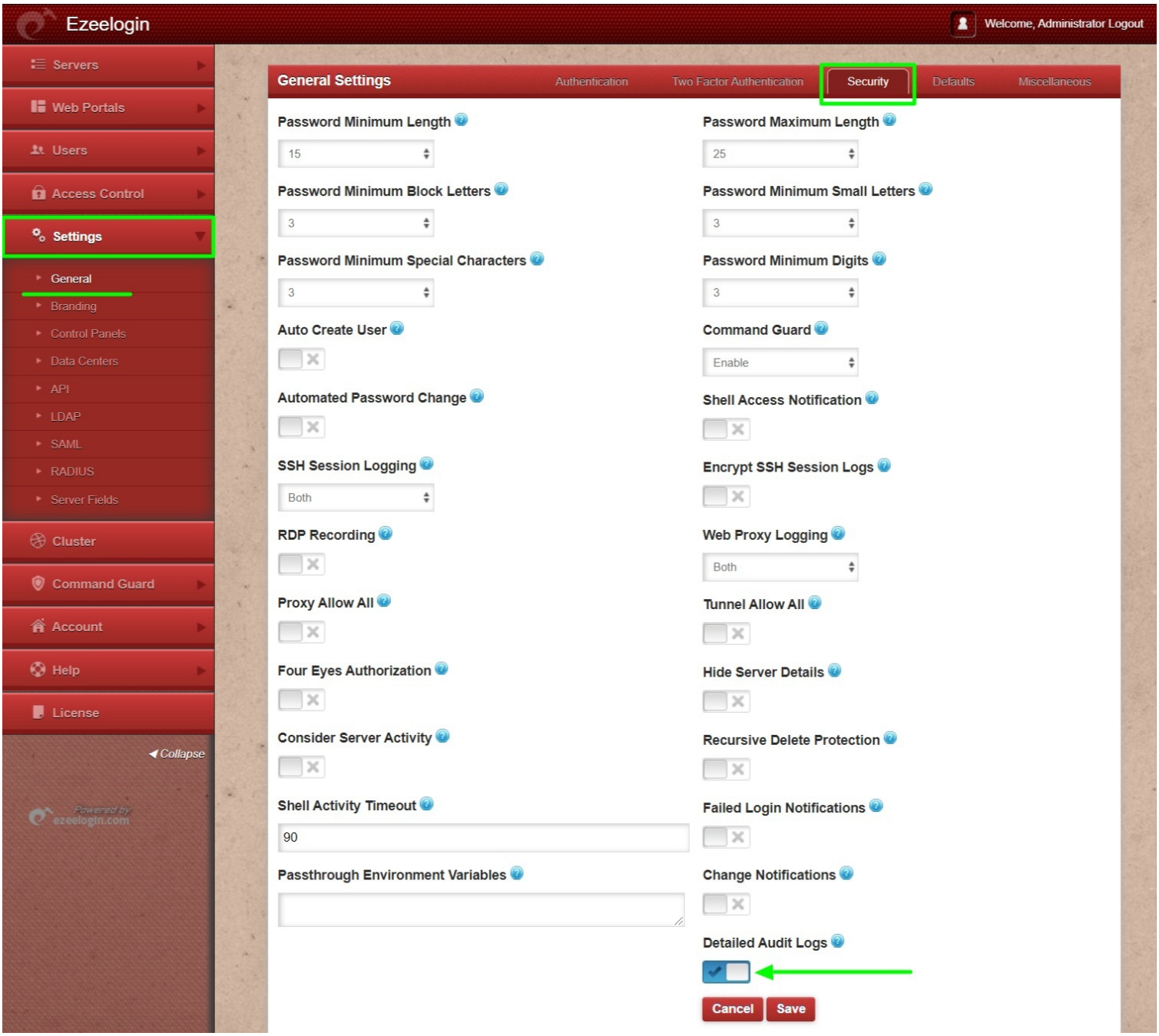
Overview: This article explains how to enable and retrieve web activity logs for monitoring user operations in various sections of the web GUI, ensuring compliance with security standards such as PCI DSS, ISO 27001, HIPAA, and others.

What is web activity log and how to find it?

The " Web Activity" log records the functions/operations performed by a user under various sections or tabs in the web gui. The recordings can later be retrieved based on the date & time for forensic or compliance(PCI DSS, ISO IS0 27001, HIPPA, NIST, FFIEC, SOC, SOX etc) purposes.

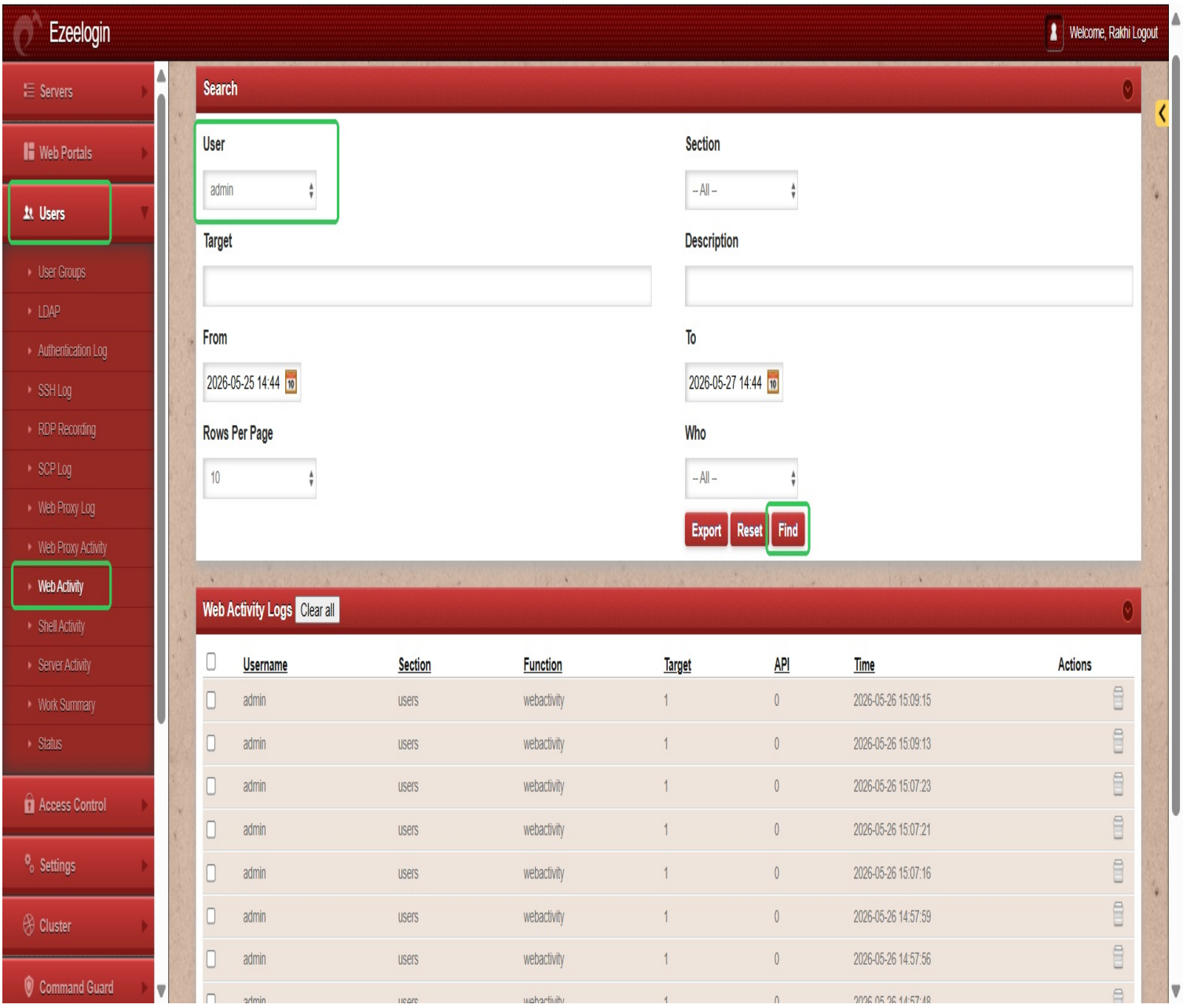
Privileged users can get the detailed log for these sections: Servers, Web Portals, Users, Access Control, Settings, Command Guard.

Step 1. Enable **Detailed Audit Log** under **Settings -> General -> Security** to get the detailed log in Web Activity.



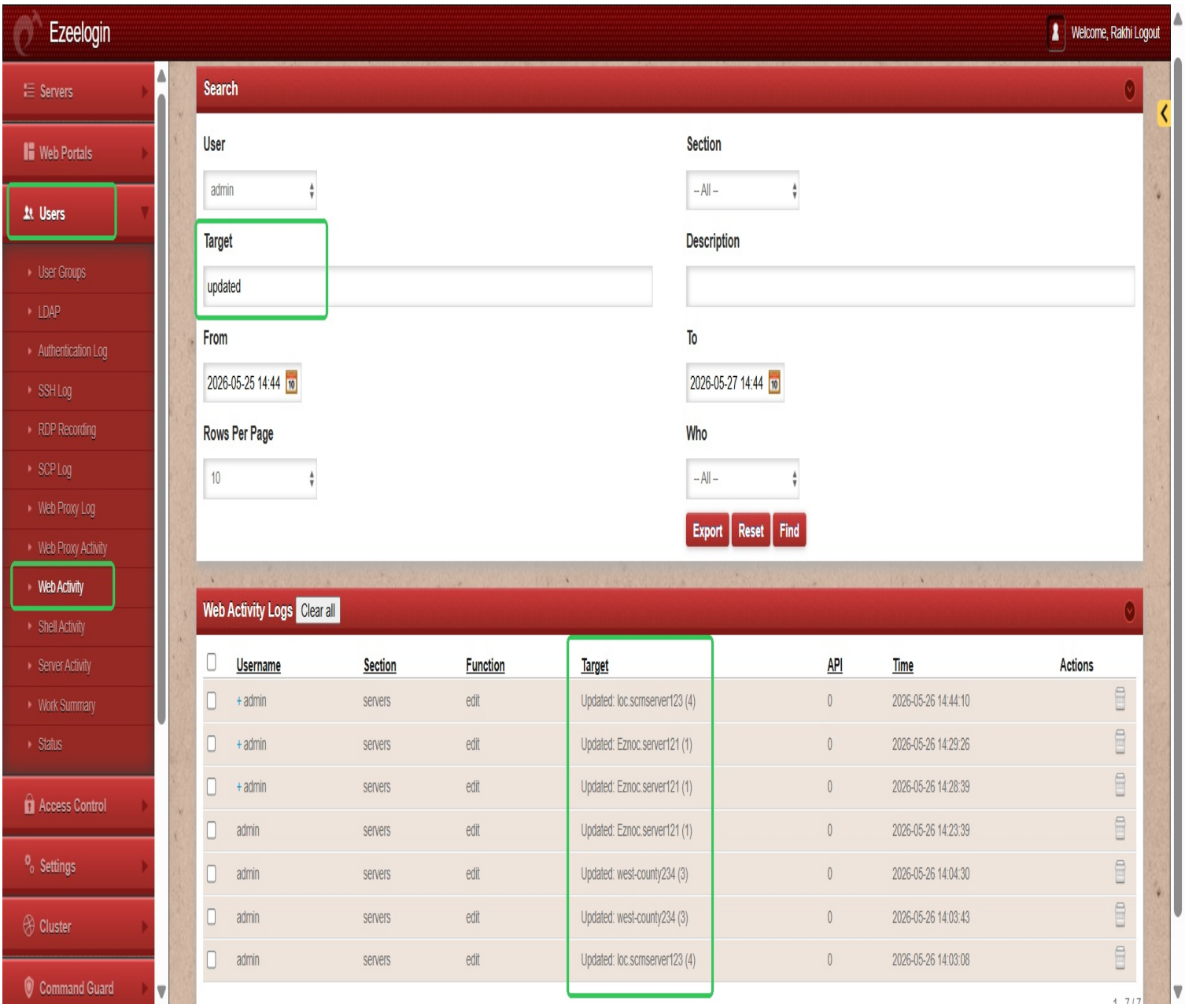
Step 2. Click on the **Users** -> **Web Activity** tab to access the web activity logs. The following image shows how to search web activity logs of admin user. To retrieve the web activity logs, select the **user**, select the **Section,** select the date ranges for which the logs has to be retrieved.

Note: Only the Super Admin User or the Privileged User can retrieve and access the web activity logs



How to get detailed logs of web activity from target and description?

Target - Denotes the changes made in remote server where the functions has been performed. (eg: updated, deleted, etc)



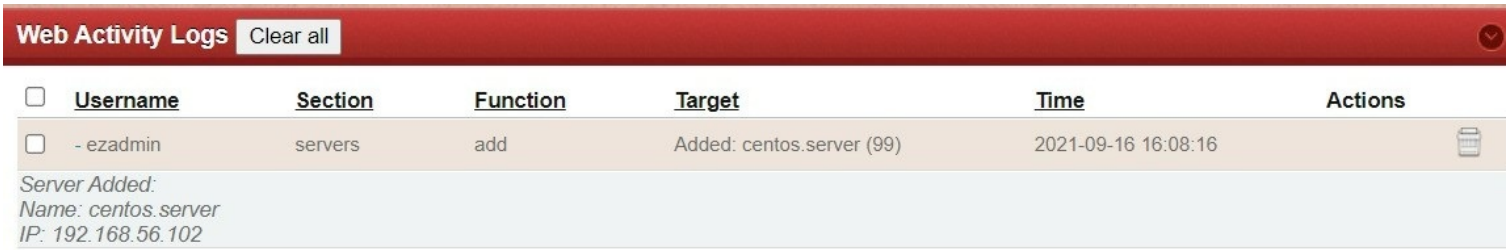
Description - Users can search for any available keyword only when logs are generated with the **Detailed Audit Log** option enabled. Refer below screenshot.

This enhancement to list the logs from Target and Description is available from **Ezeelogin version 7.46.0**

Refer to the screenshots below for detailed logs under the sections: Servers, Web Portals, Users, Access Control, Settings, and Command Guard.

1. SERVERS Tab (Section and Operations recorded)

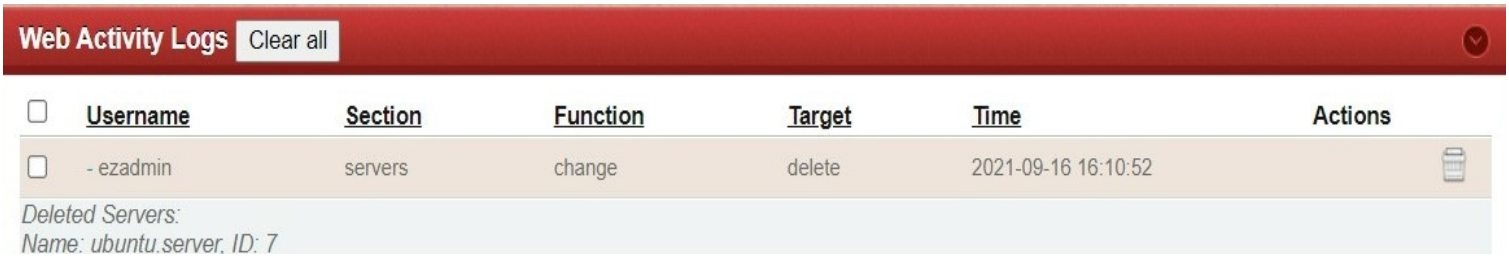
Add Server



Edit server

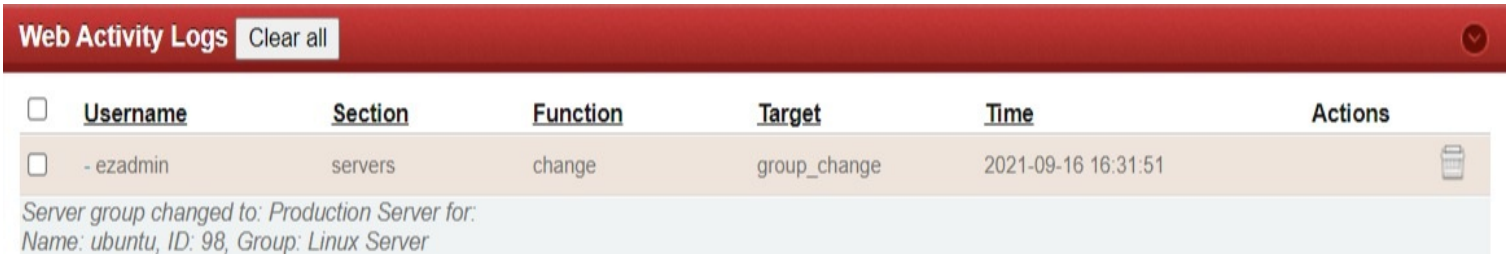
View server

Delete server

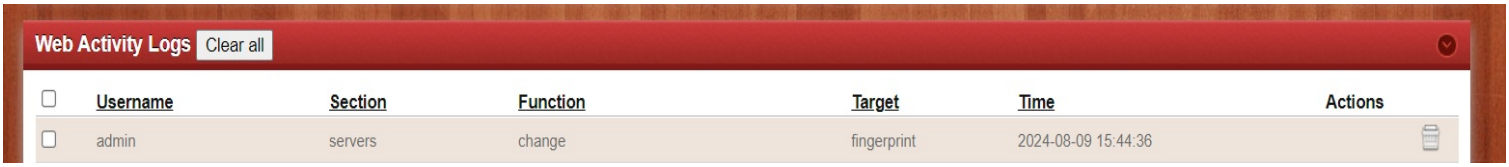


Enable / Disable SSH port

Change server group



Reset SSH fingerprint



Reset password on server

Setup SSH key on server

Setup SubSSH user on server

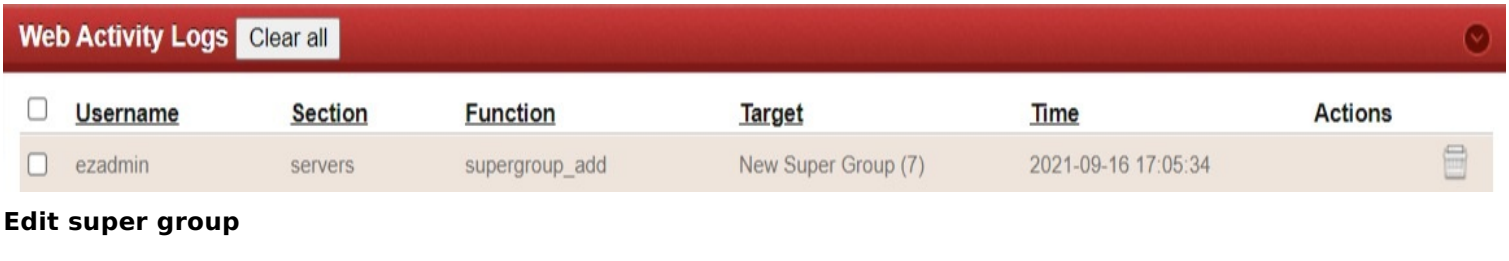
Add server group

Edit server group

View server group

Delete server group

Add super group

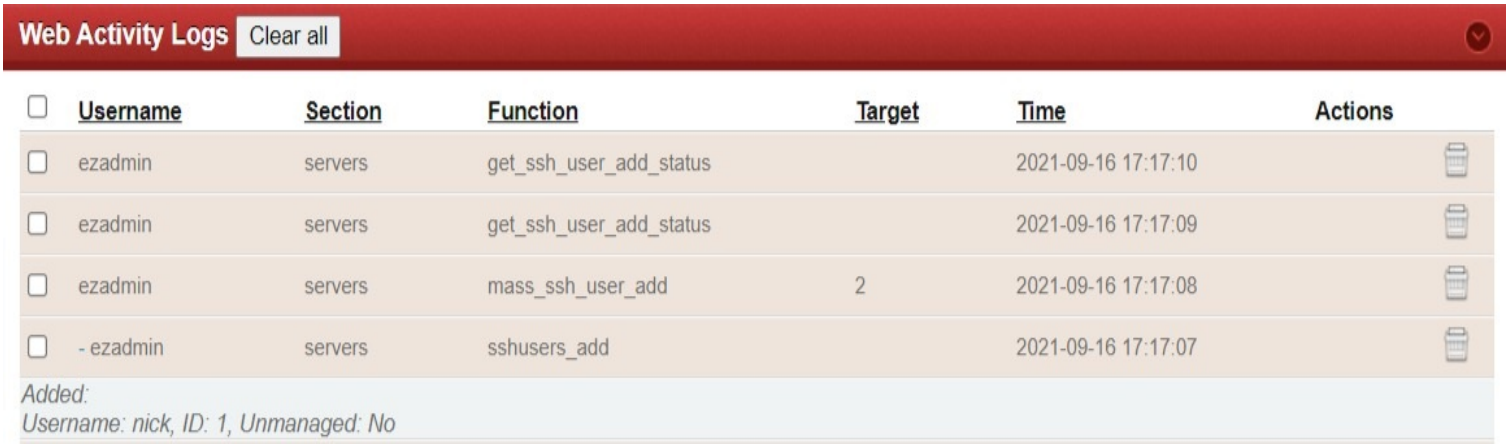


Edit super group

Add members to super group

Remove members from super group

Add SubSSH user



Edit SubSSH user

Delete SubSSH user

Add SubSSH user map

Edit SubSSH user map

Delete SubSSH user map

Web Activity Logs Clear all

Username	Section	Function	Target	Time	Actions
- ezadmin	servers	sshuser_assign_delete		2021-09-16 17:24:04	

Deleted:
User Group: Dummy (2)
Server Group: (12)
SSH User: (13)
ID: 3

Add mexec list

Web Activity Logs Clear all

Username	Section	Function	Target	Time	Actions
ezadmin	servers	mexeclist_add	new mexec list (2)	2021-09-16 19:05:40	

Edit mexec list

Web Activity Logs Clear all

Username	Section	Function	Target	Time	Actions
- ezadmin	servers	mexeclist_update	new mexec list (2)	2021-09-16 19:08:46	

mExec list updated (2):
Public: N -> Y

Add members to mexec list

Web Activity Logs Clear all

Username	Section	Function	Target	Time	Actions
- ezadmin	servers	mexeclist_members	2	2021-09-16 19:09:23	

Added:
Name:centos.server, ID: 99
Name:ubuntu.server, ID: 100

Remove members from mexec list

Web Activity Logs Clear all

Username	Section	Function	Target	Time	Actions
- ezadmin	servers	mexeclist_members	2	2021-09-16 19:09:57	

Removed:
Name:centos.server, ID: 99
Name:ubuntu.server, ID: 100

Delete mexec list

Web Activity Logs Clear all

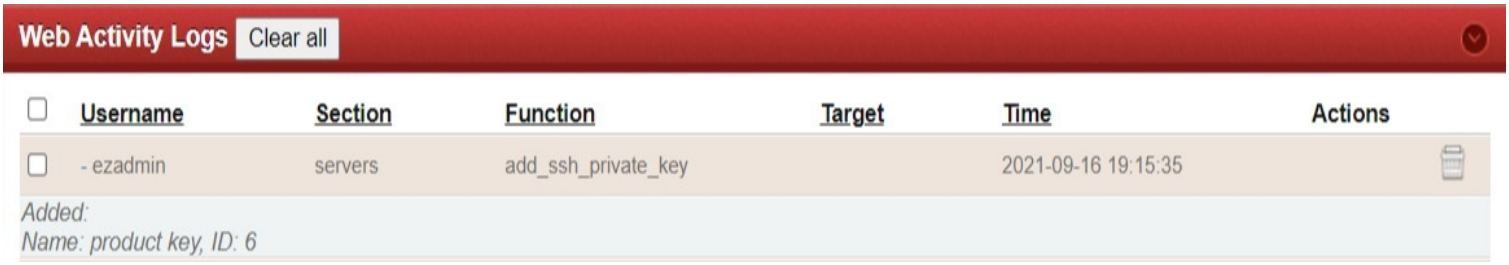
Username	Section	Function	Target	Time	Actions
- ezadmin	servers	mexeclist_delete		2021-09-16 19:10:32	

Deleted mExec Lists:
Name: new mexec list, ID: 2

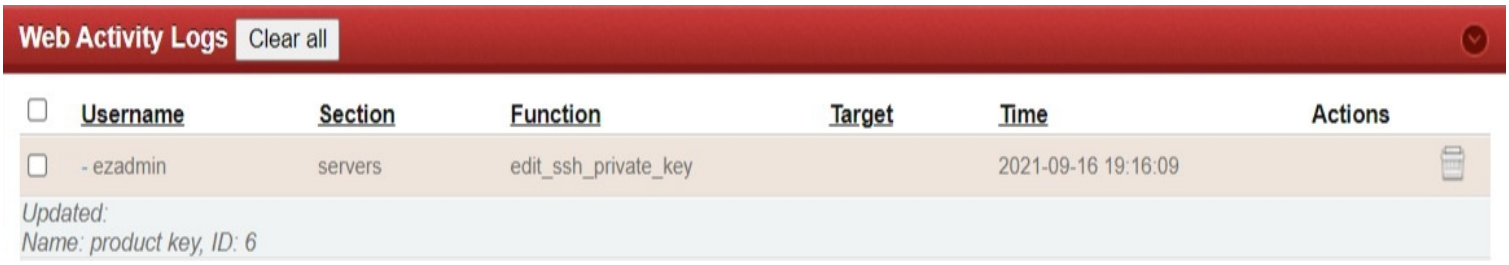
Import server

View global key

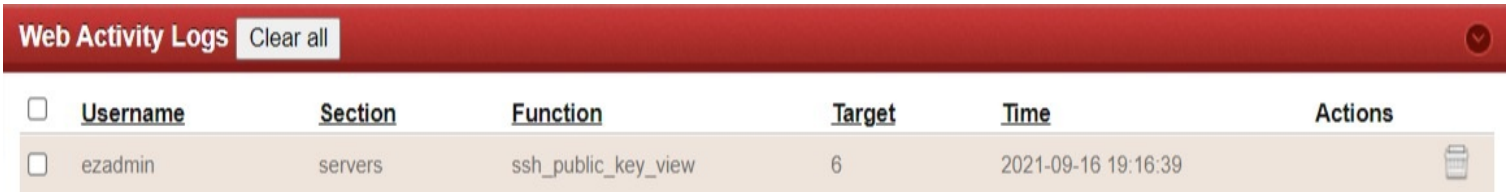
Add key management



Edit key management



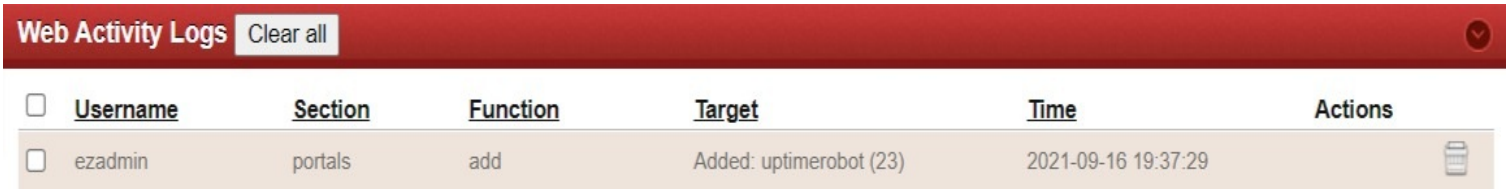
View key management



Delete key management

2. Web Portal Tab(Section and Operations recorded)

Add web portal



Edit web portal (changed portal group from portal group one to portal group two

View web portal

Login web portal

Delete web portal

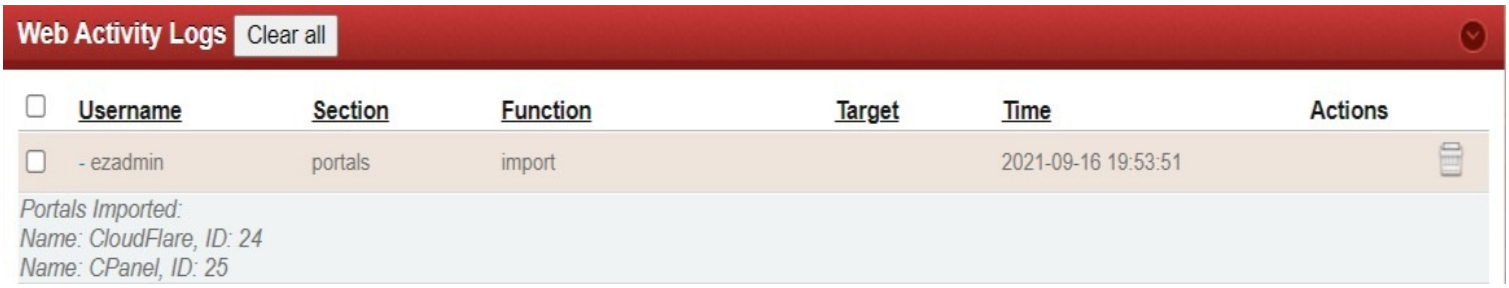
Add web portal group

Edit web portal group

View web portal group

Delete web portal group

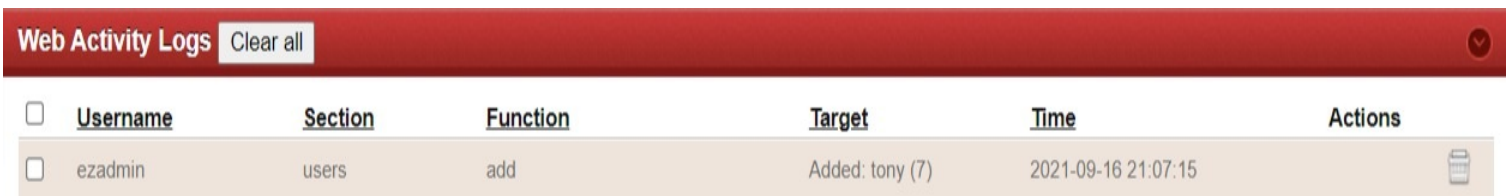
Import web portal



Export web portal

3. USER Tab (Section and Operations/ Functions recorded)

Add user



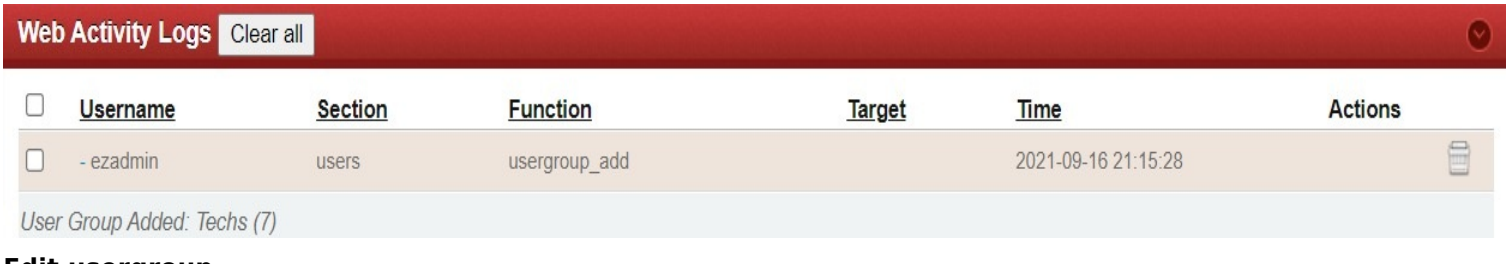
Edit user

Reset access control override

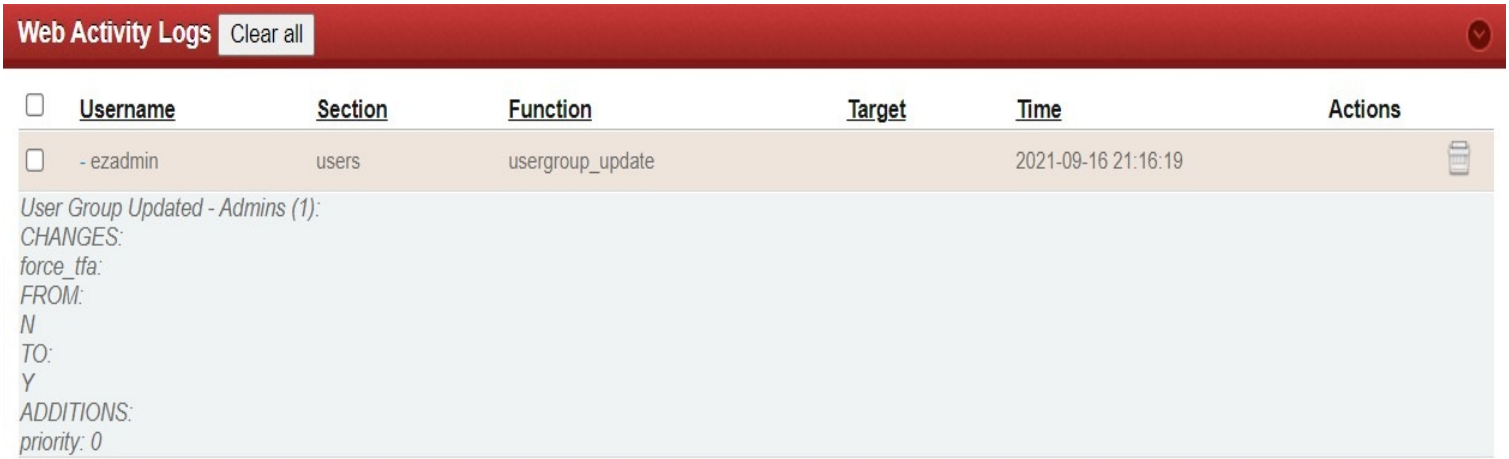
Reset password and security code

Delete user

Add usergroup

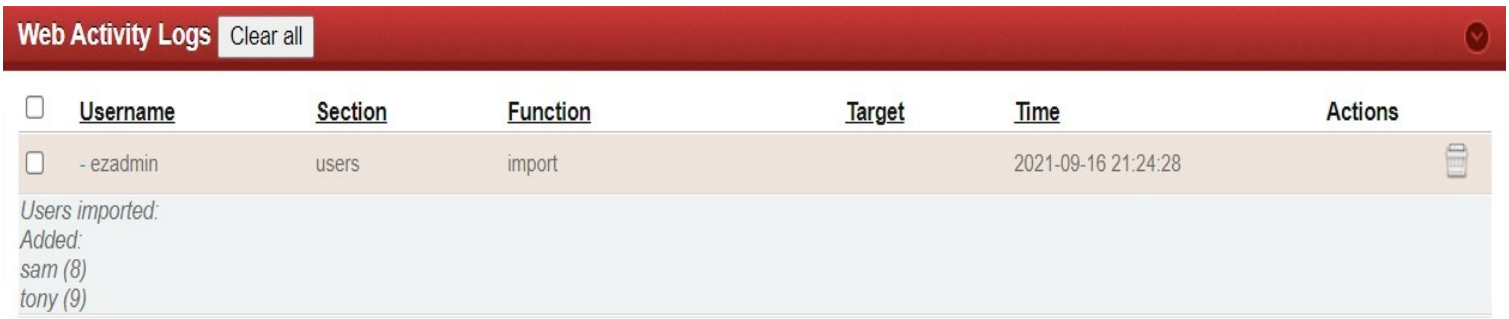


Edit usergroup



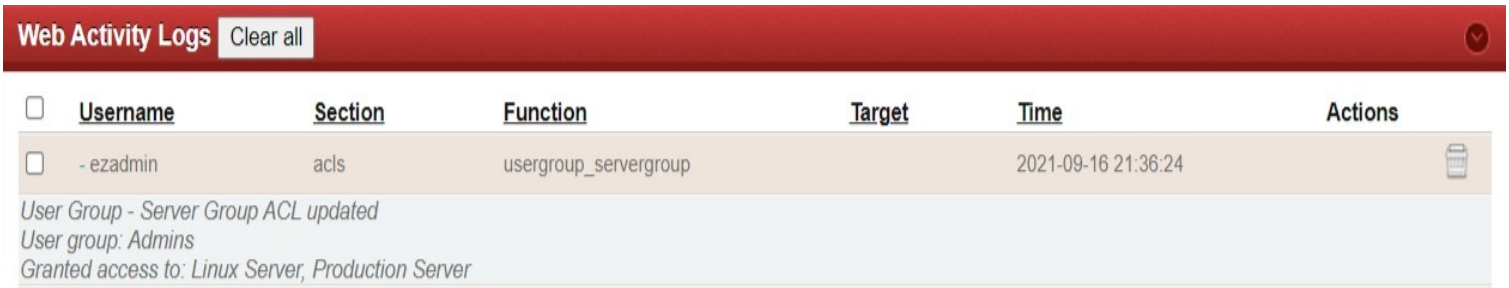
Delete usergroup

Import LDAP user



4. ACCESS CONTROL Tab (Section and Operations/ Functions recorded)

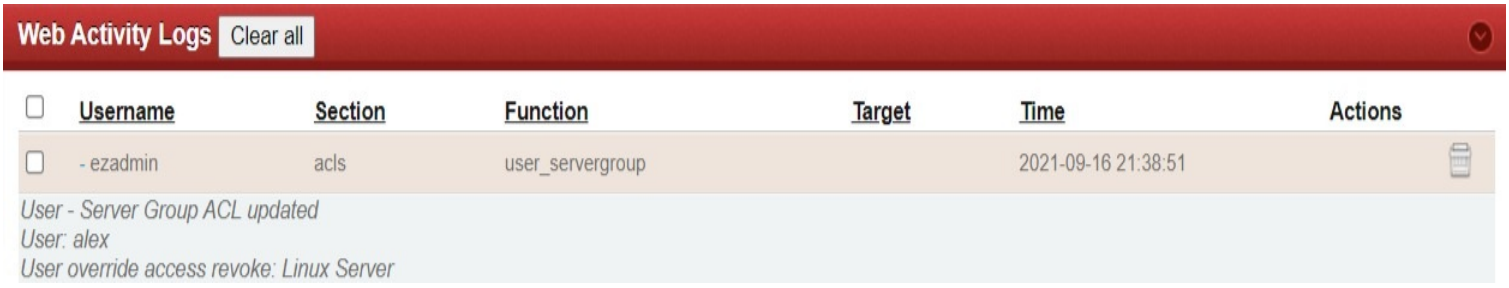
Add usergroup -servergroup



Remove usergroup - servergroup

Add user - servergroup

Remove user - servergroup



Add user - server

Remove user - server

Add usergroup -portalgroup

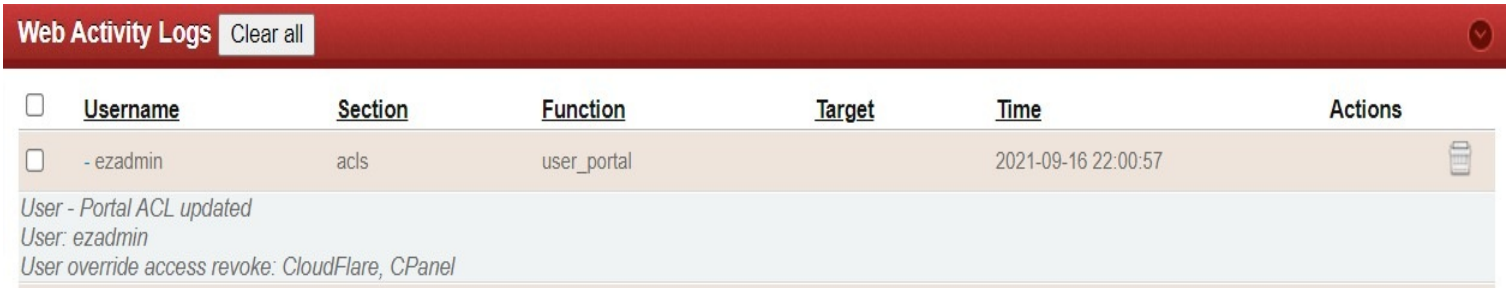
Remove usergroup - portalgroup

Add user - portalgroup

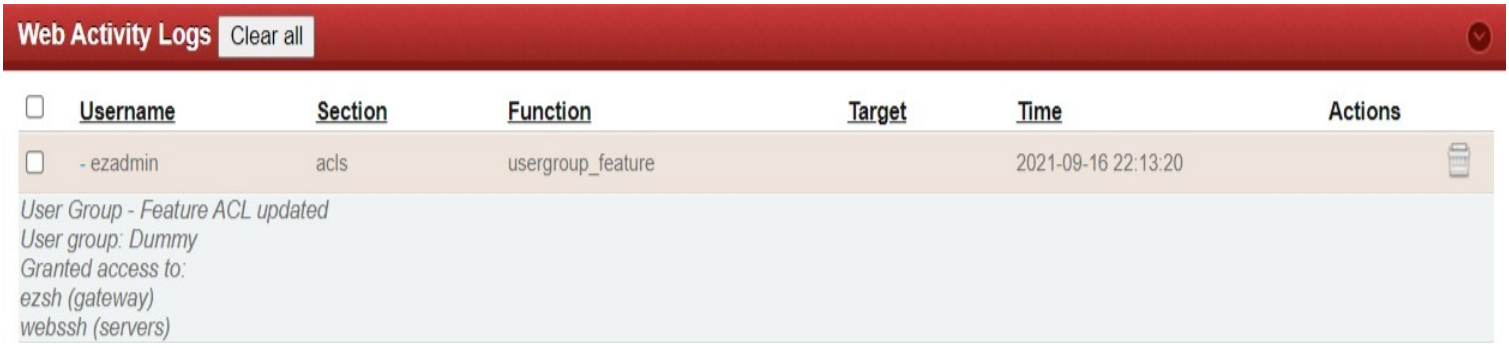
Remove user - portalgroup

Add user - portal

Remove user - portal



Add usergroup - action

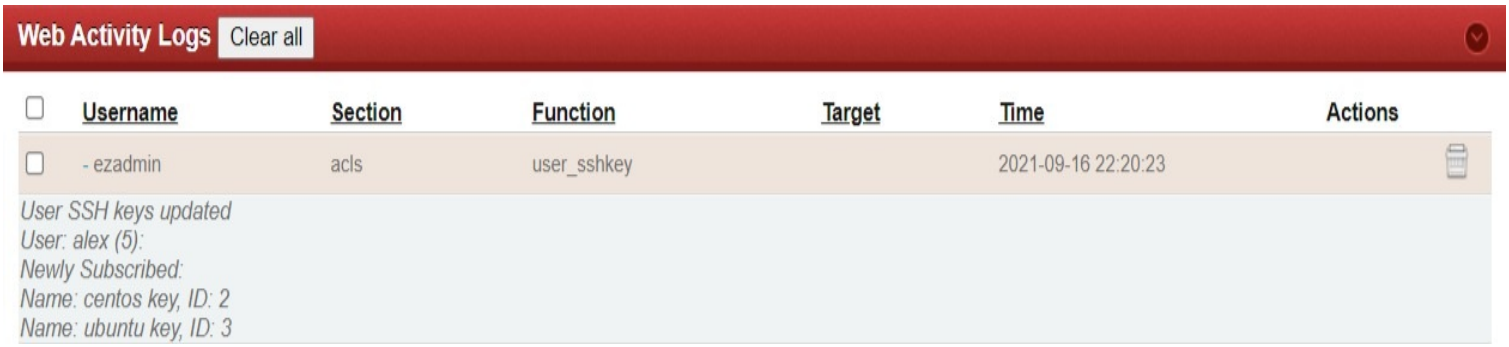


Remove usergroup - action

Add user - action

Remove user - action

Add user - SSHkey



Remove user - SSHkey

4. SETTINGS Tab (Section and Operations/ Functions recorded)

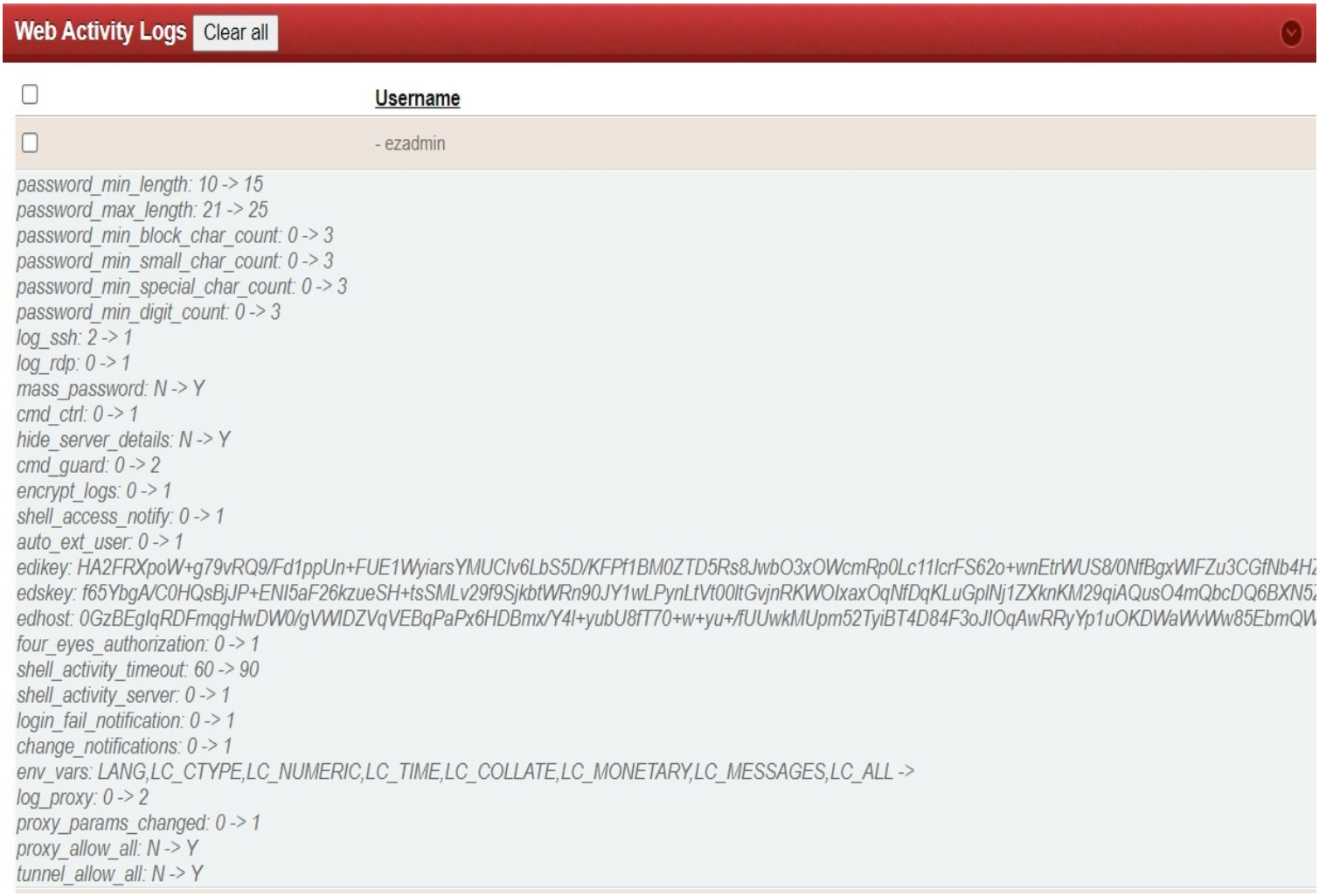
General > Authentication

sec_code_retry: 0 -> 3	Password / Security Code Retries
login_captcha: N -> V	Login captcha (N-disabled,V-reCAPTCHA v2,I- invisible reCAPTCHA)
web_auth: internal -> ldap	Web Panel Authentication
ldap_pam_ssh_authentication: N -> Y	External SSH Auth
browser_save_login: 0 -> 1	Allow Browsers To Save Login
nologin_days: 0 -> 5	Maximum Days Without Login
pwexp_days:	User Password Lifetime
recaptcha_sitekey:	reCAPTCHA Sitekey
recaptcha_secret:	reCAPTCHA Secret
security_code_ldap: N -> Y	Security Code LDAP

General > Two Factor Authentication

enable_duo: N -> Y	Enable Duo
enable_yubikey: N -> Y	Enable Yubikey
enable_google_authenticator: N -> Y	Enable Google Authenticator
enable_access_keyword: N -> Y	Enable Access Keyword
enable_radius_2fa: N -> Y	Enable Radius
two_factor_auth: 0 -> 1	Force Two Factor Authentication
googlekey_reuse: 0 -> 1	Allow Reuse Of Google Authenticator Code
eyc:	Yubico Client ID
eys:	Yubico Secret Key
yubi_sl: 0 -> 2	YubiKey Sync Level
edikey:	DUO Integration key
edskey:	DUO Secret key
edhost:	DUO API hostname
duo_email_user: N -> Y	Use Email ID for Duo login
skip_2fa_saml: N -> Y	Skip Two Factor Authentication For SAML

General > Security



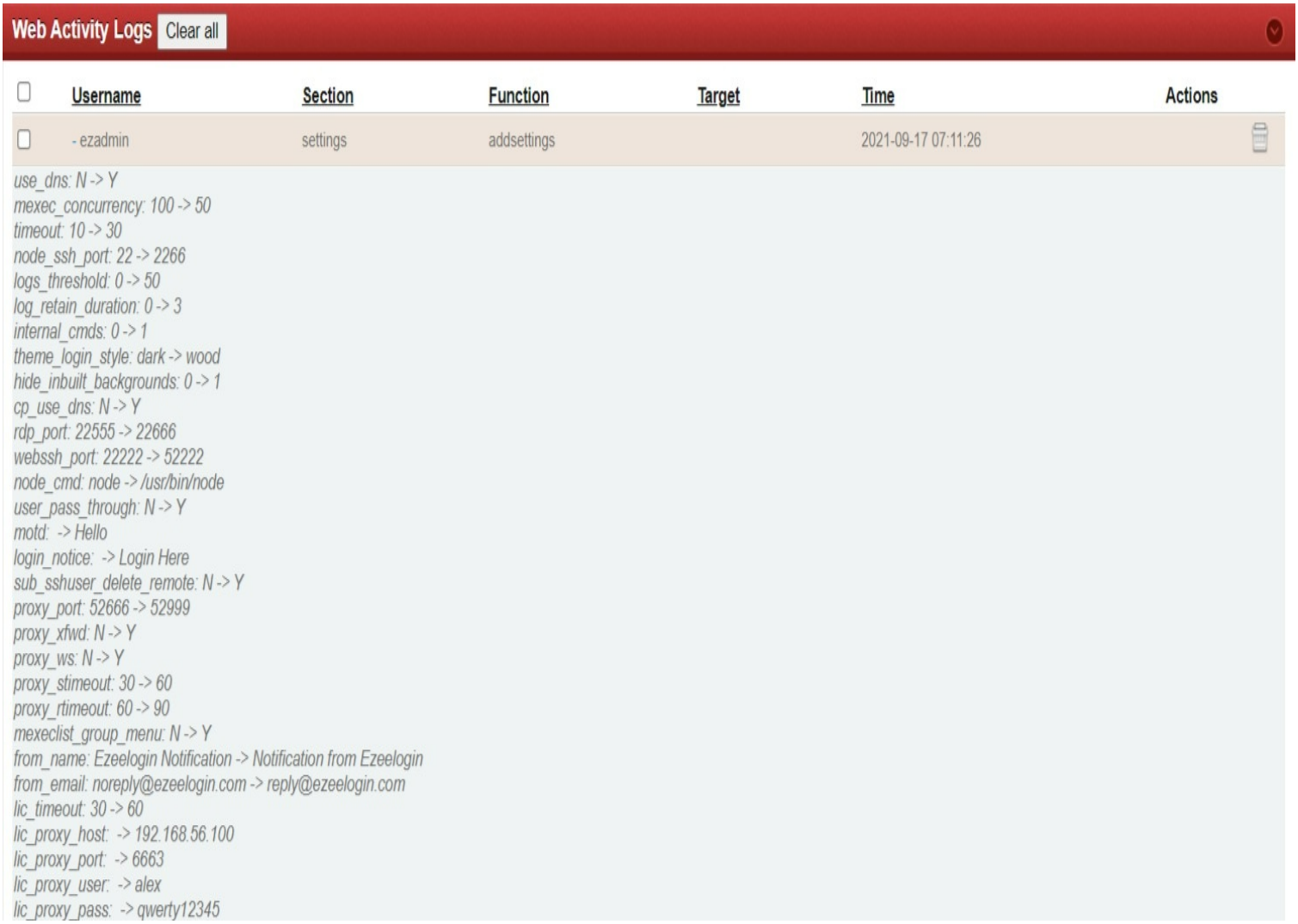
password_min_length: 10 -> 15	Password Minimum Length
password_max_length: 21 -> 25	Password Maximum Length
password_min_block_char_count: 0 -> 3	Password Minimum Block Letters
password_min_small_char_count: 0 -> 3	Password Minimum Small Letters
password_min_special_char_count: 0 -> 3	Password Minimum Special Characters
password_min_digit_count: 0 -> 3	Password Minimum Digits
log_ssh: 2 -> 1	SSH Session Logging (0-none,1-input,2-both,3-output)
log_rdp: 0 -> 1	RDP Recording
mass_password: N -> Y	Automated Password Change
cmd_ctrl: 0 -> 1	Recursive Delete Protection
hide_server_details: N -> Y	Hide Server Details
cmd_guard: 0 -> 2	Command Guard (0-disable, 2-enable)
encrypt_logs: 0 -> 1	Encrypt SSH Session Logs
shell_access_notify: 0 -> 1	Shell Access Notification
auto_ext_user: 0 -> 1	Auto Create User
edikey:	DUO Integration key
edskey:	DUO Secret key
edhost:	DUO API hostname
four_eyes_authorization: 0 -> 1	Four Eyes Authorization
shell_activity_timeout: 60 -> 90	Shell Activity Timeout
login_fail_notification: 0 -> 1	Failed Login Notifications
change_notifications: 0 -> 1	Change Notifications
env_vars: LANG,LC_CTYPE,LC_NUMERIC,,LC_COLLATE,LC_MONETARY,,LC_ALL	Passthrough Environment Variabless

->	
log_proxy: 0 -> 2	Web Proxy Logging (0-none,1-request,3-response,2-both)
proxy_allow_all: N -> Y	Proxy Allow All
tunnel_allow_all: N -> Y	Tunnel Allow All

General > Default

default_ssh_port: 22 -> 2266	Default SSH Port
default_rdp_port: 3366 -> 3399	Default RDP Port
default_ssh_user: root -> admin	Default SSH User
default_prompt1: -> :~#	Default First Prompt
default_prompt2: -> Password:	Default Password Prompt
default_prompt3: -> :~@	Default RootPrompt
default_cpid: 0 -> 1	Default Control Panel
default_cpid: 0 -> 1	Default Data Center
default_user_group: 2 -> 1	Default User Group

General > Miscellaneous



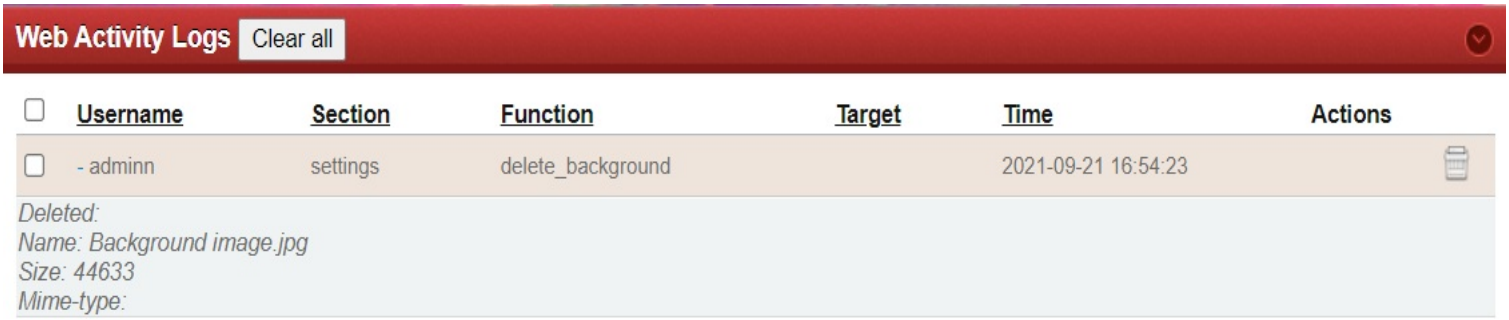
use_dns: N -> Y	Use DNS
mexec_concurrency: 100 -> 50	mExec Concurrency
timeout: 10 -> 30	SSH Timeout
node_ssh_port: 22 -> 2266	Gateway SSH Port
logs_threshold: 0 -> 50	Log Space Threshold (MB)
log_retain_duration: 0 -> 3	Log Retain Duration (months)
internal_cmds: 1 -> 0	Internal commands
theme_login_style: dark -> wood	Login theme
hide_inbuilt_backgrounds: 0 -> 1	Hide Inbuilt Backgounds
cp_use_dns: N -> Y	CP Use DNS
rdp_port: 22555 -> 22666	RDP Proxy Port
rdp_port_changed: 0 -> 1	RDP Port Changed
webssh_port: 22222 -> 52222	Web SSH Port
node_cmd: -> /usr/bin/node	NodeJS Command
user_pass_through: N -> Y	Pass User Through
motd: -> Hello	Message Of The Day
login_notice: -> Login Here	Login Page Notice
sub_sshuser_delete_remote: N -> Y	Delete Sub SSH Remote User

proxy_port: 52666 -> 52999	Web Proxy Porxy
proxy_xfwd: N -> Y	Web Proxy Forwarded Header
proxy_ws: N-> Y	Web Proxy Web Sockets
proxy_stimeout: 30 -> 60	Web Proxy Session Timeout
proxy_rtimeout: 60 -> 90	Web Proxy Request Timeout
mexeclist_group_menu: N -> Y	Mexec Lists in Group Menu
from_name: Ezeelogin Notification -> Notification from Ezeelogin	Notification From Name
from_email: noreply@ezeelogin.com -> reply@ezeelogin.com	Notification From Email
lic_timeout: 30 -> 60	License Timeout
lic_proxy_host: -> 192.168.56.100	Proxy Host
lic_proxy_port: -> 6663	Proxy Port
lic_proxy_user: -> alex	Proxy Username
lic_proxy_pass: -> qwerty12345	Proxy Password

Settings > Branding

Branding > Logo

Branding > Backgrounds



Settings > Control Panels :Add ControlPanel

Edit ControlPanel

Web Activity Logs Clear all

Username	Section	Function	Target	Time	Actions
- adminn	settings	editcp		2021-09-21 17:12:25	

CHANGES:
name:
FROM:
directadmin
TO:
DIRECTADMIN
description:
FROM:
Controlpanel
TO:
Controlpanels
protocol:
FROM:
https
TO:
http
port:
FROM:
2222
TO:
2223
request_uri:
FROM:
/CMD_LOGIN
TO:
/cmd_login
request_method:
FROM:
POST
TO:
GET
user_field:
FROM:
username
TO:
user
username:
FROM:
admin
TO:
root
passwd_field:
FROM:
password
TO:
pass
basic_auth:
FROM:
Y
TO:
N
extra_vars:
FROM:
PTUyZjA0NGZiYWNkNWI0NzMxZDRlMjkyOWU1NjY2MDc2
TO:
PTFiZTY2MzM0OGQ5Mjg4NWZjZDg4YTkwZDVhNWE0YTVl

Delete ControlPanel

Web Activity Logs Clear all

Username	Section	Function	Target	Time	Actions
- adminn	settings	deletecp		2021-09-21 17:21:50	

DIRECTADMIN

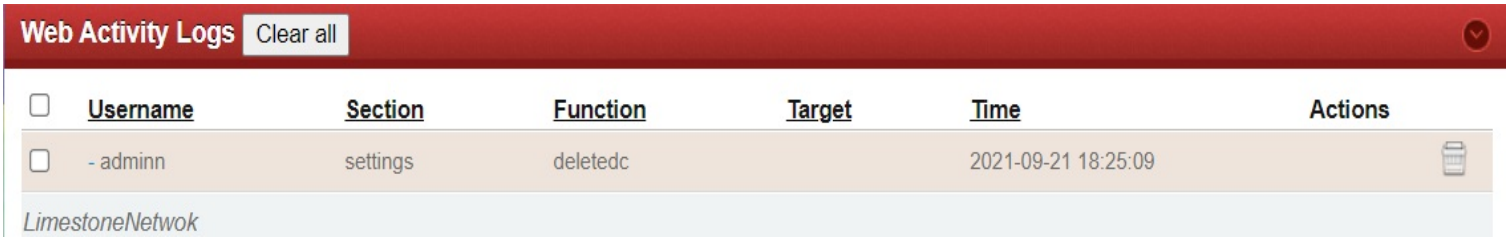
Settings>Data Centers : Add DataCenters

Web Activity Logs Clear all

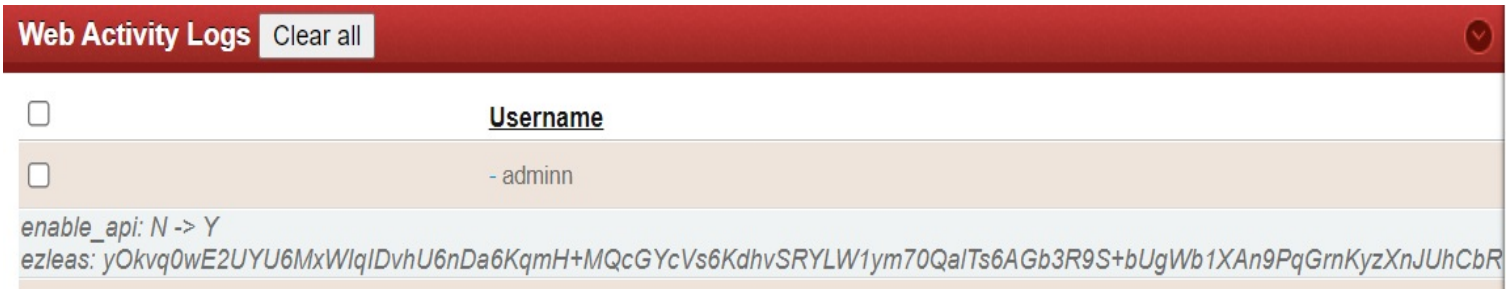
Username	Section	Function	Target	Time	Actions
- adminn	settings	addcp		2021-09-21 17:10:26	

Name: directadmin

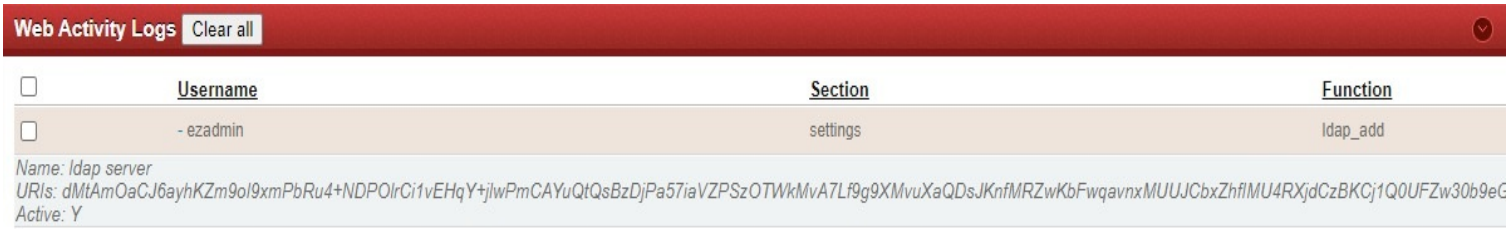
Delete Datacenters



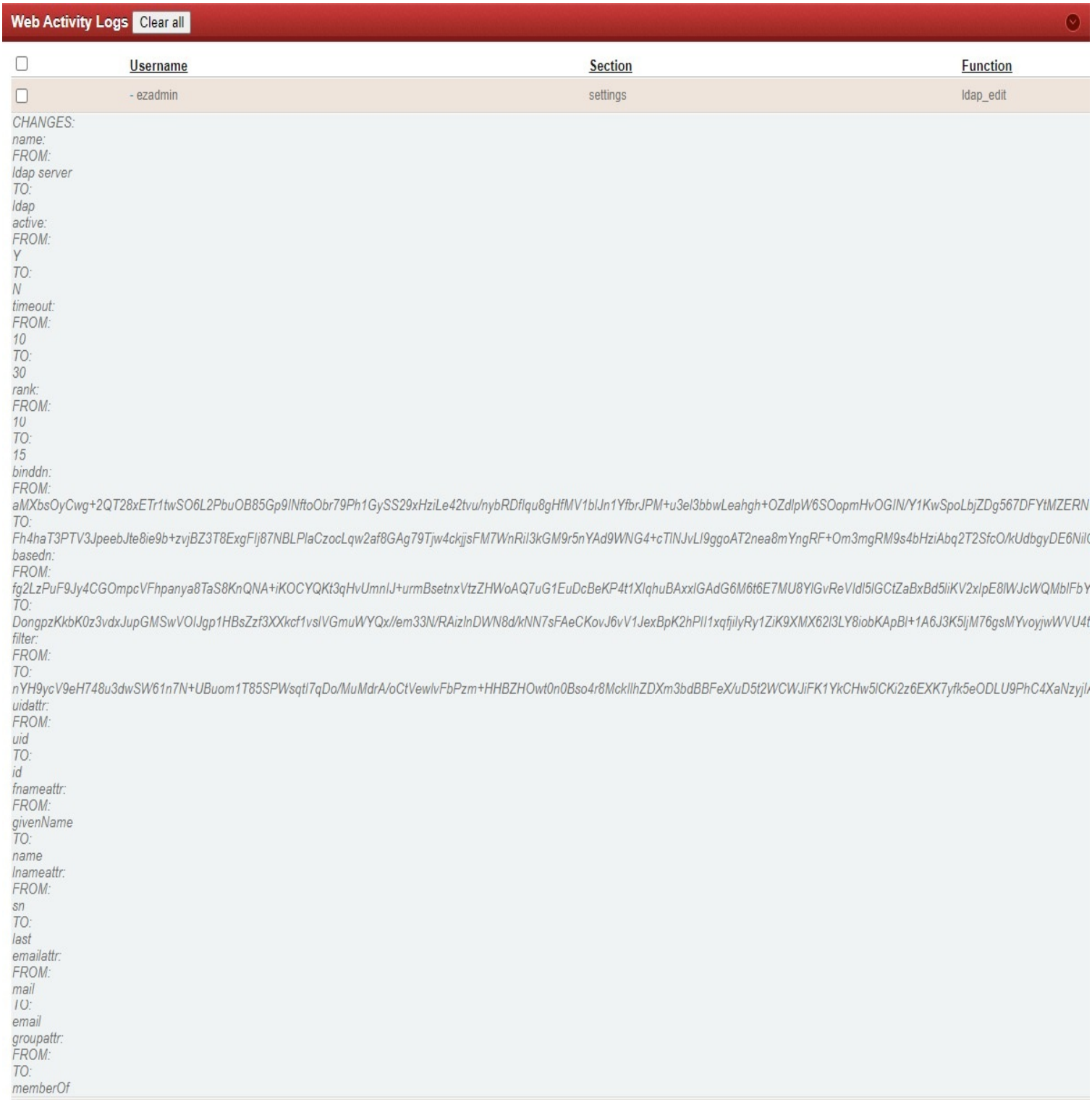
Settings>API



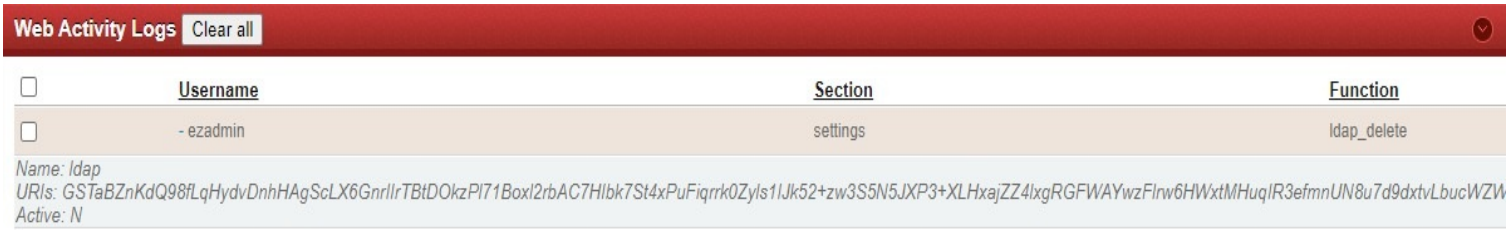
Settings > LDAP : Add LDAP



Edit LDAP



Delete LDAP

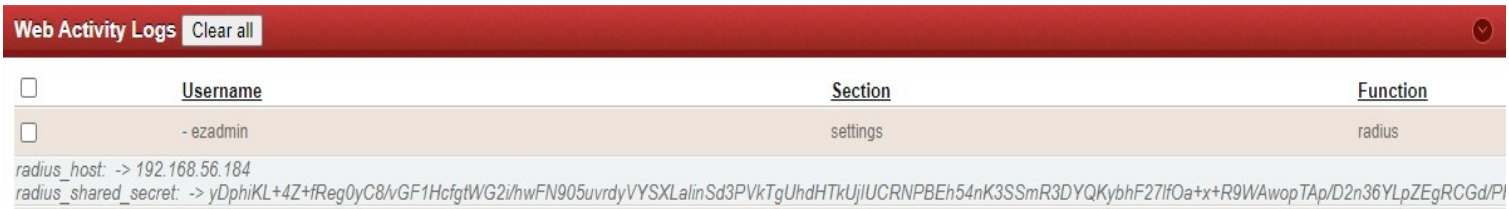


Settings > SAML

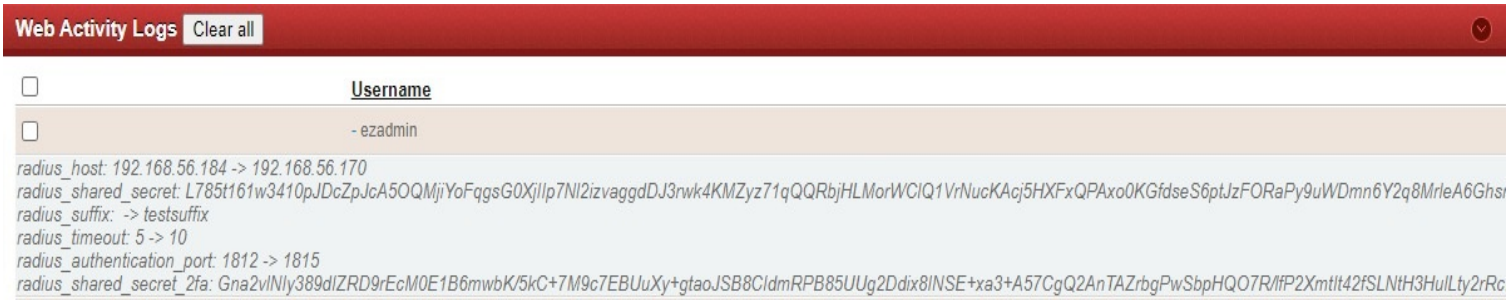
Fetch SAML

Save SAML

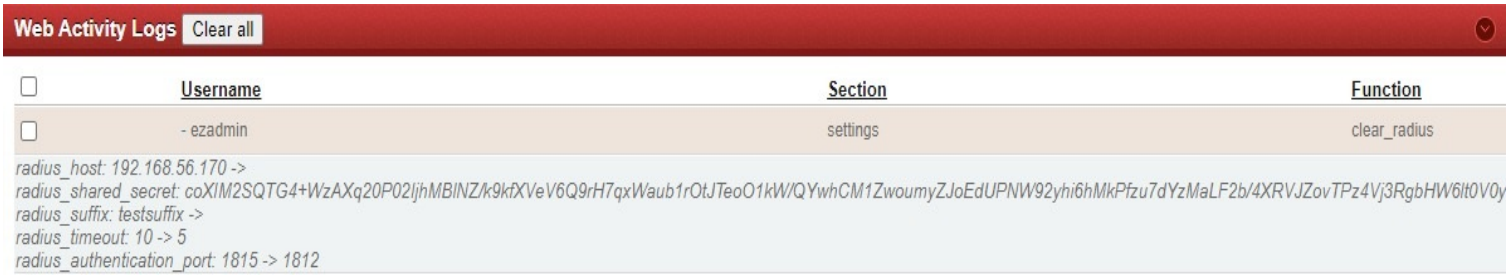
Settings > Radius : Add Radius



Edit Radius

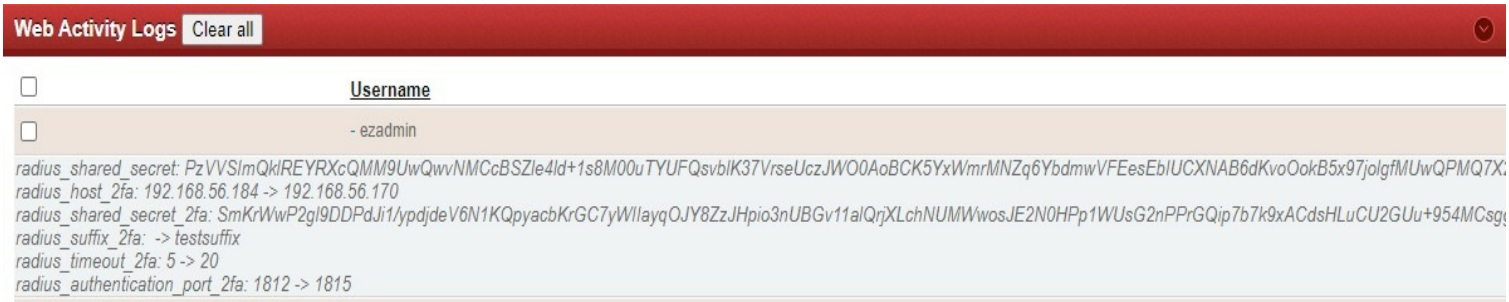


Clear Radius

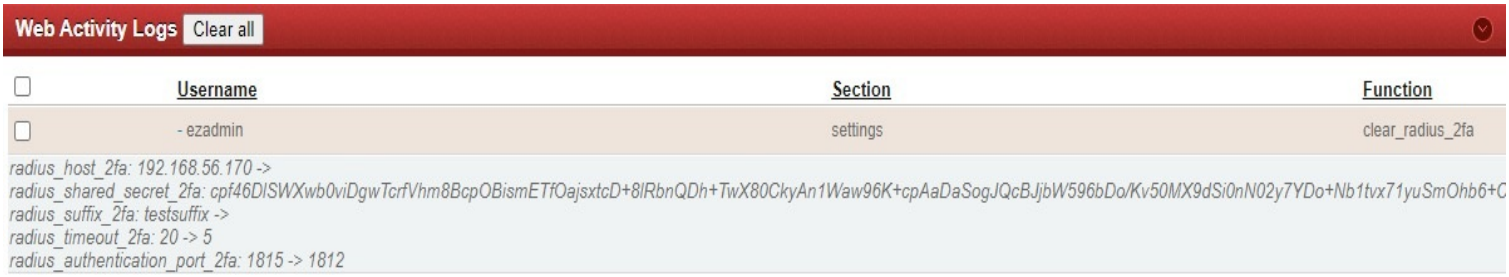


Add two factor Radius

Edit two factor Radius

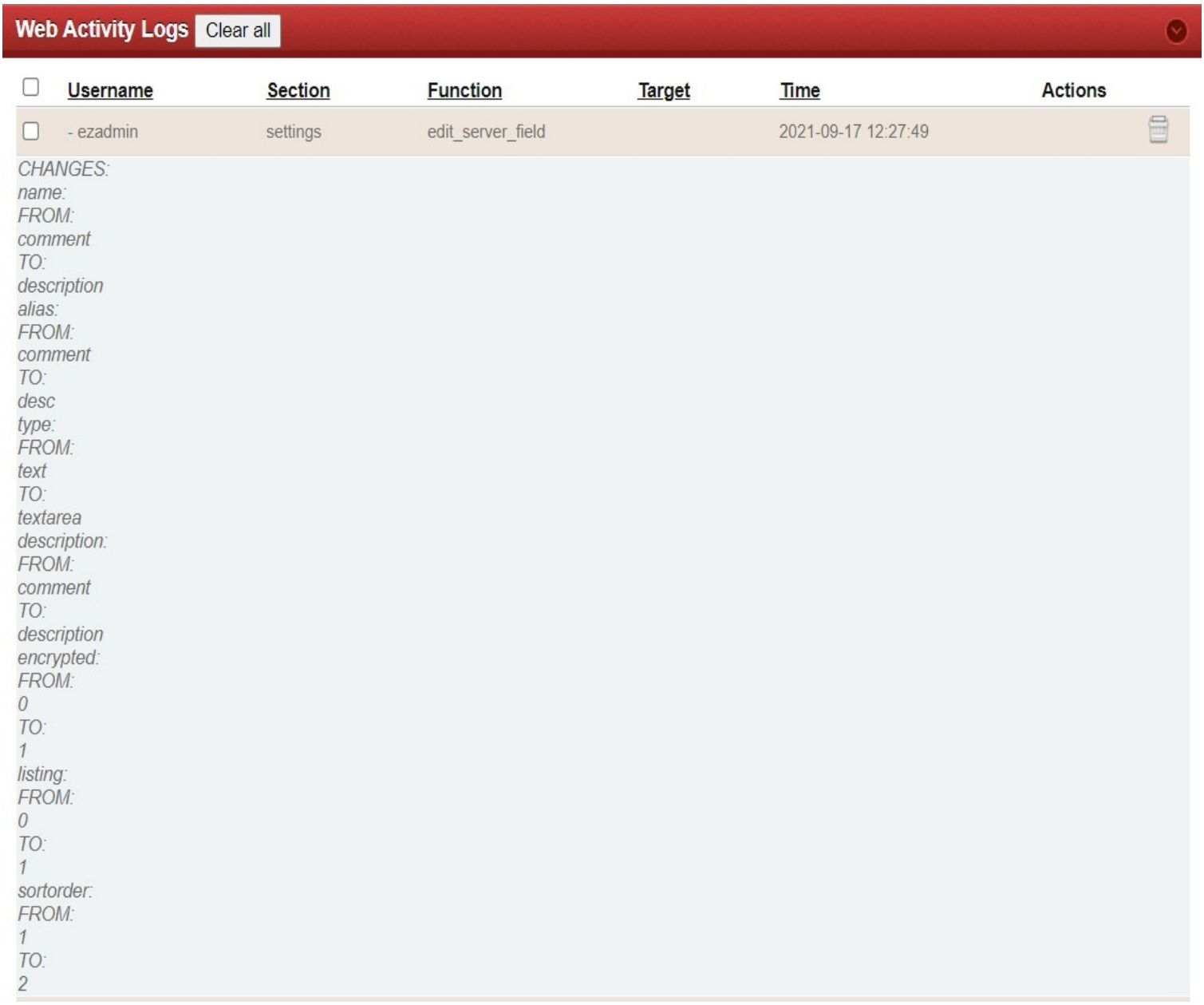


Clear two factor Radius



Setting > Server Fields : Add server field

Edit server filed



Delete server field

5. COMMAND GUARD Tab (Section and Operations/ Functions recorded)

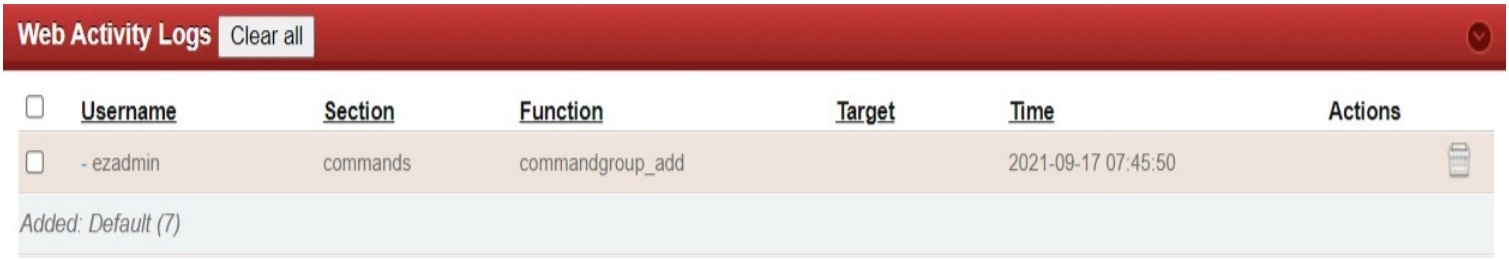
Add command

Edit command

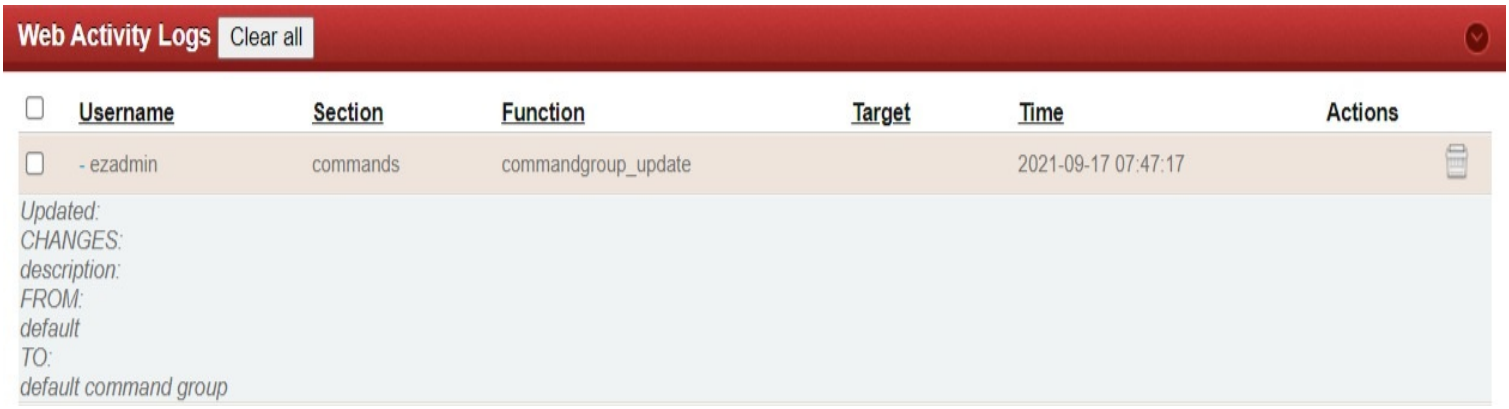
Test command

Delete command

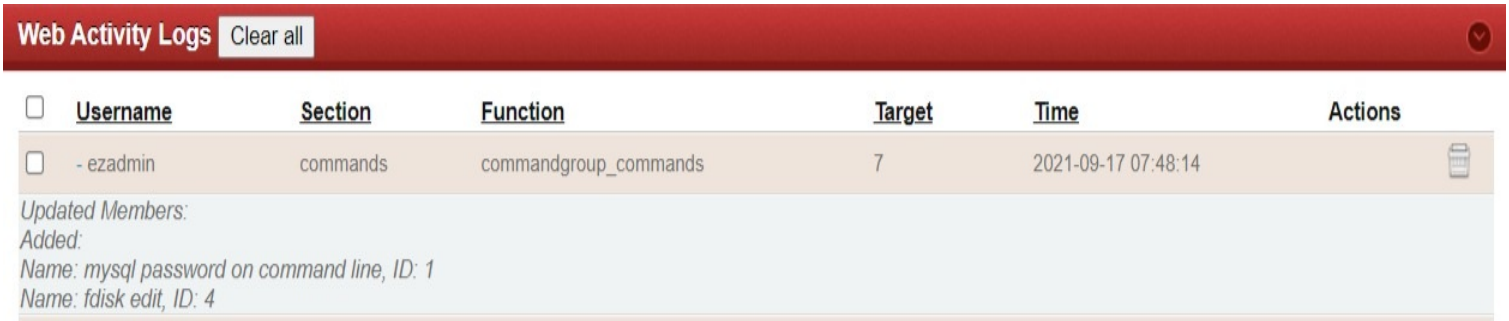
Add command group



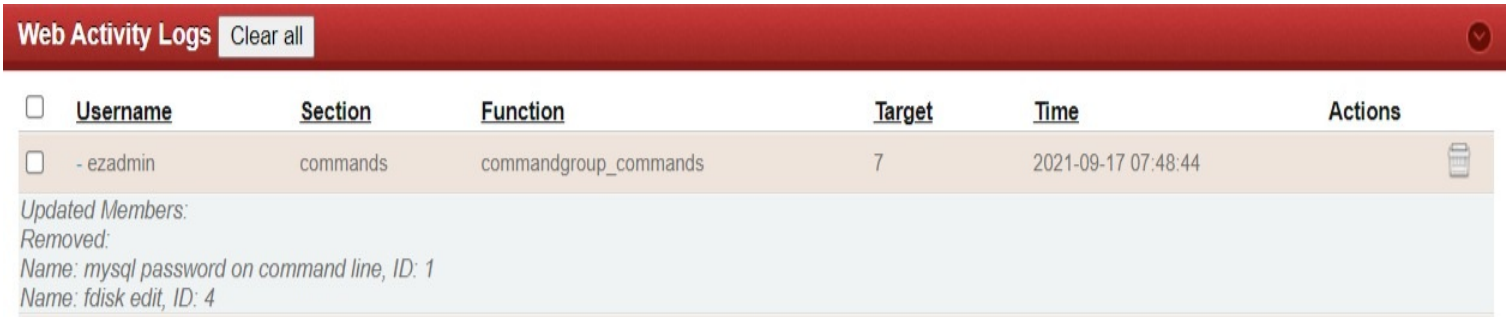
Edit command group



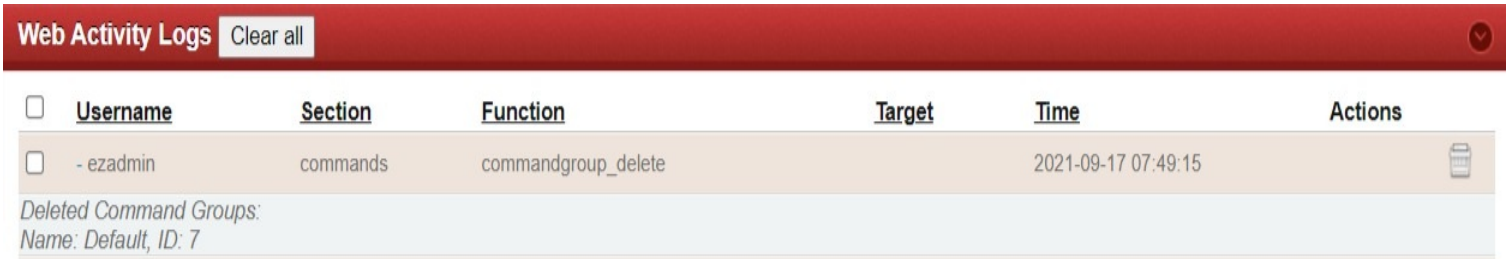
Add members to command group



Remove members from command group



Delete command group



Related Articles

How does " Web Activity" in Ezeelogin works?

Different logs of user

Online URL: https://www.ezeelogin.com/kb/article/web-activity-log-451.html