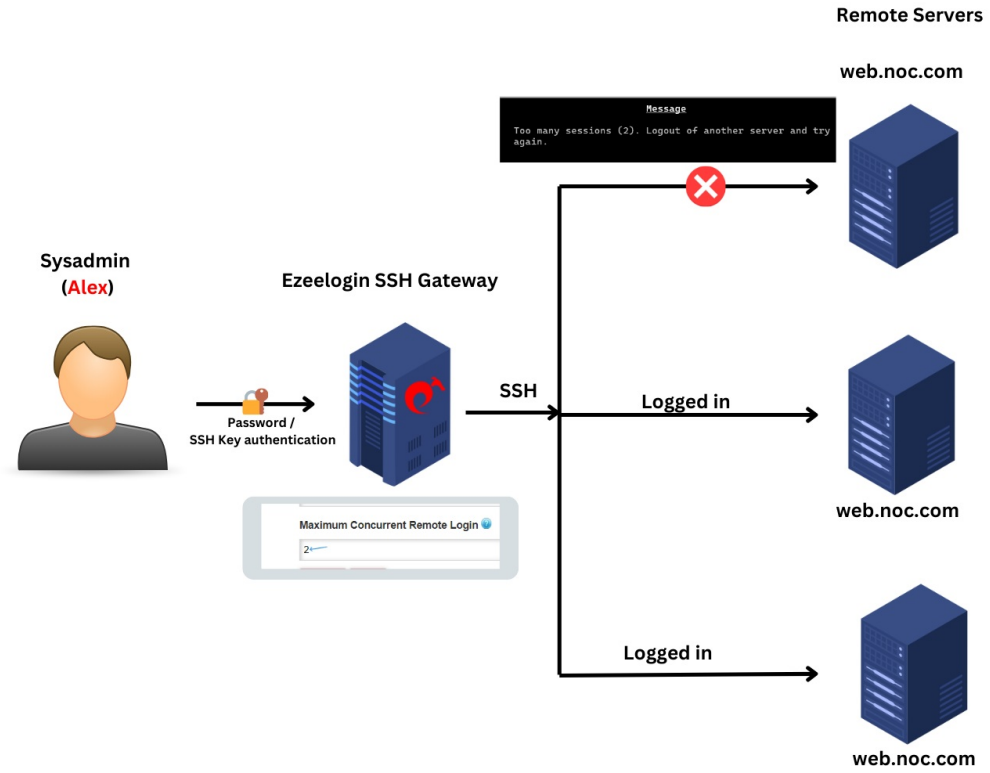
Manage concurrent SSH connections

729 Santhi April 29, 2025 Features & Functionalities 4552

How to limit max SSH sessions to remote Linux devices?

Overview: This article describes how to restrict concurrent SSH sessions on remote Linux devices using Ezeelogin's MCRL feature to enhance security and system performance.

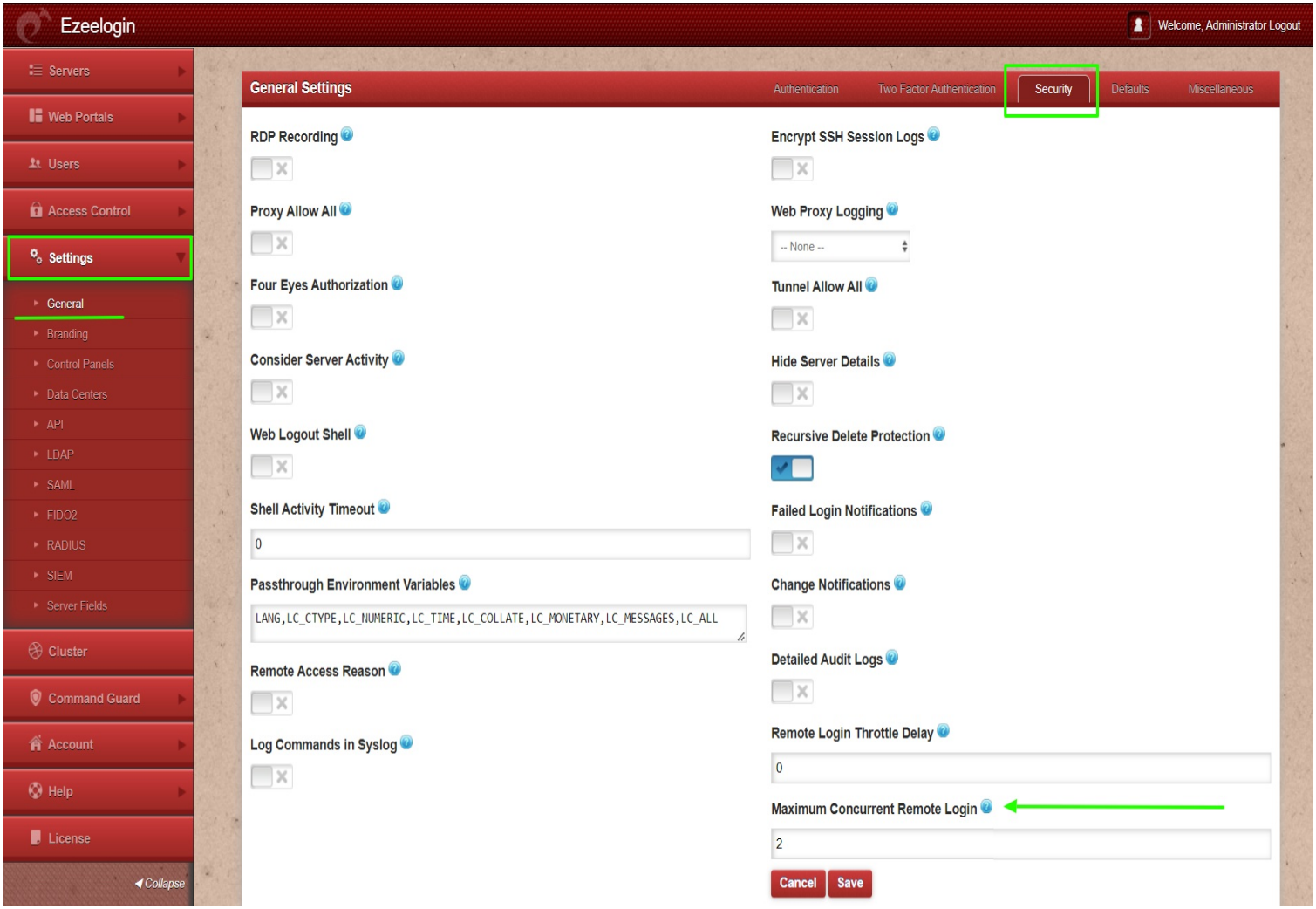
Limiting the maximum concurrent SSH sessions to remote Linux devices is essential for maintaining server security and preventing unauthorized access. **"Maximum concurrent remote login(MCRL)"** feature helps the system administrators to control the concurrent SSH sessions that a user can establish on the remote Linux devices and prevent potential performance bottlenecks.



For example, if the MCRL is set to 2, the user can have only 2 active ssh sessions to the remote servers.

Here is the steps to set maximum concurrent remote login (MCRL) in Ezeelogin.

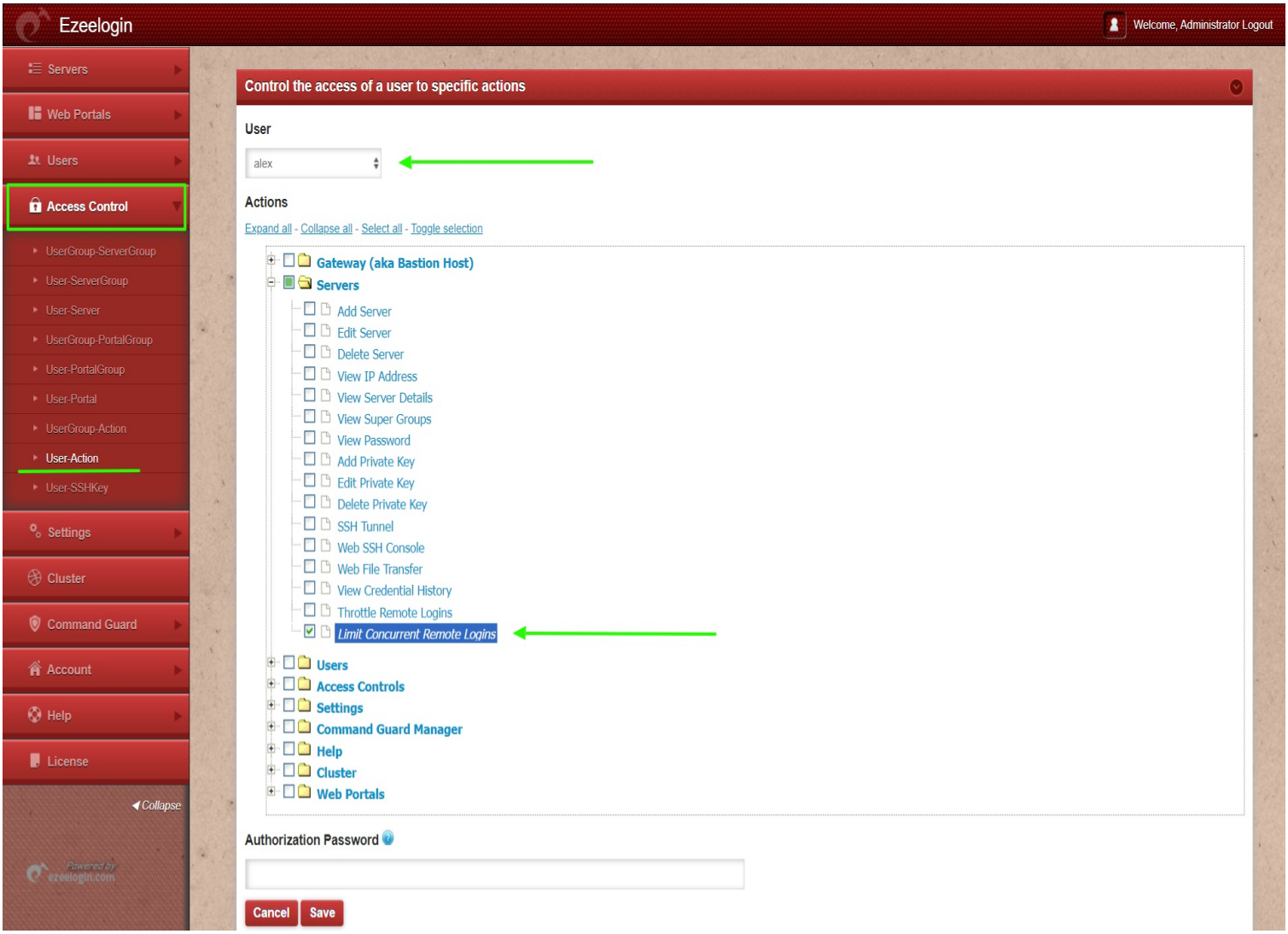
Step 1: Set the **'Maximum Concurrent Remote Login (MCRL)'** globally from the GUI located within the 'Security' tab under general settings".



Step 2: To configure **MCRL for the individual user** '**Alex**', proceed with **step 2.a**, or alternatively, proceed directly to **step 2.b** to configure **RLTD for the user group** '**Sysadmin**'."

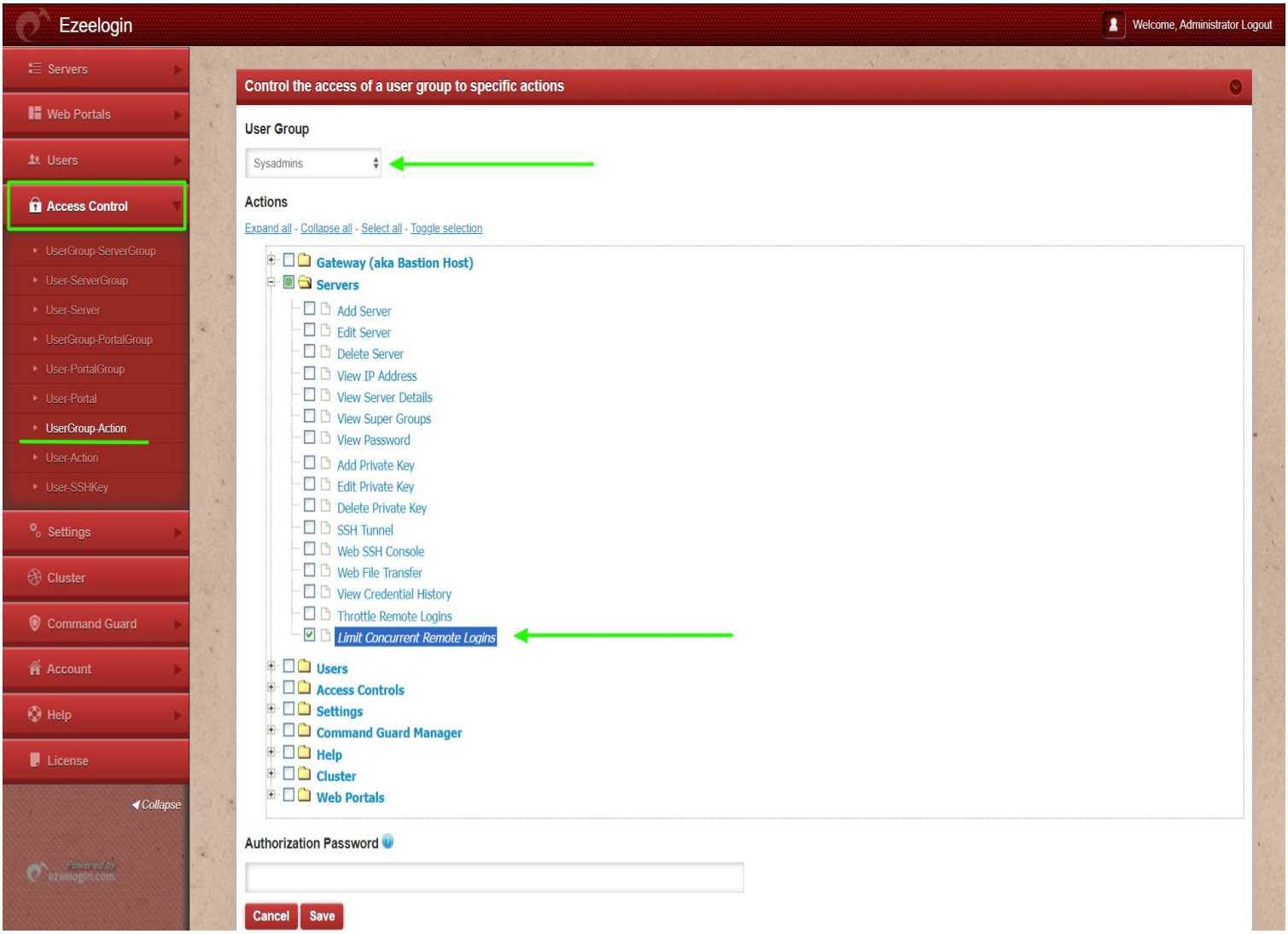
Step 2(A): How to **set Maximum Concurrent Remote Login for a specific user**?

Enable **'Limit Concurrent Remote Login'** for the user '**Alex**' using the 'user-action' option available under 'Access Control'.



Step 2(B): How to set **Maximum Concurrent Remote Login** for a the **user group 'Sysadmins'**?

Enable **'Limit Concurrent Remote Login'** for the user group **'Sysadmins**' using the 'usergroup-action' option available under 'Access Control'.



In this scenario, the maximum concurrent remote login is configured to 2. If the user '**Alex**' attempts to initiate more than 2 concurrent SSH sessions, they will encounter a prompt displaying ***"Too many sessions (2). Logout of another server and try again,"*** effectively restricting additional SSH connections. This method demonstrates how Ezeelogin gateway enforces limitations on maximum SSH connections.

In Conclusion, limiting the maximum concurrent SSH sessions offers several advantages. Firstly, it enhances security by reducing the attack surface and mitigating the risks of unauthorized access attempts. Secondly, it optimizes server performance by ensuring resources are efficiently allocated, preventing overload situations. Additionally, it facilitates easier monitoring and management of SSH sessions, enhancing overall system stability and operational efficiency.

Error: After enabling MCRL, if you come across an error with too many logged-in sessions even though you have no active sessions currently.



Refer to this article for resolution:

Showing Stale Connections.

This feature is available from **Ezeelogin version 7.38.0**. To update your existing Ezeelogin to the latest version, refer to the **article.**

Superadmin user (user created at the time of Ezeelogin installation) is not affected by RLTD and MCRL.

Related Article:

How to set throttle delay in SSH?

Online URL: https://www.ezeelogin.com/kb/article/manage-concurrent-ssh-connections-729.html