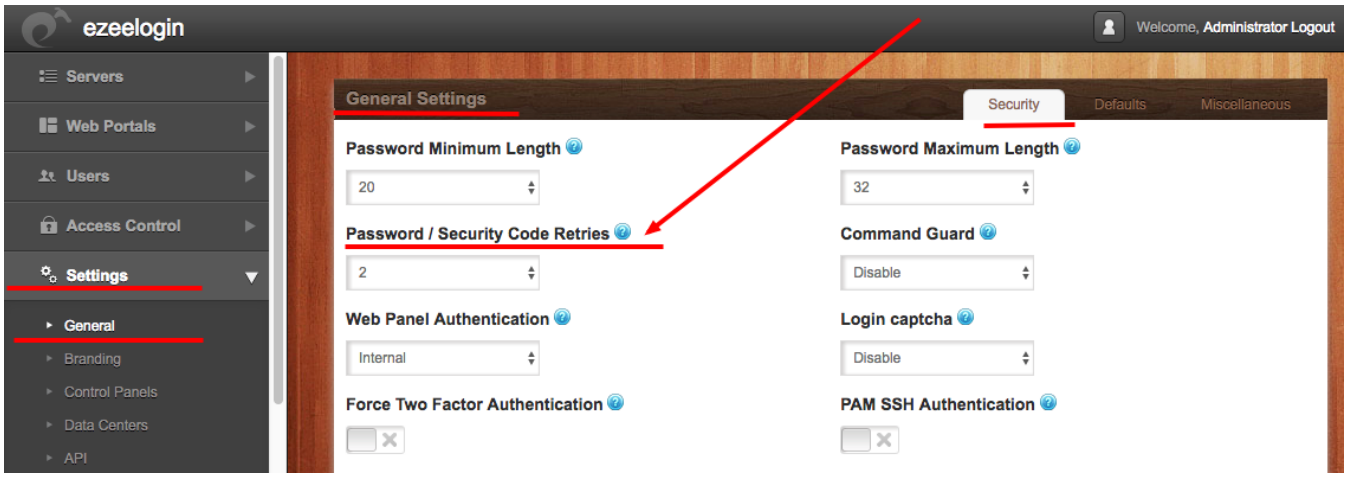
How to ensure that ssh jump host users are not using previous password set to meet security compliances such as PCI DSS , SOX, HIPAA , NIST , MAS, SOC2, FFIEC, NERC CIP , ISO 27001

193 admin March 1, 2018 Security Features 4296

To meet various security compliance like PCI DSS 3.2, SOX , HIPPA , NIST , MAS , FFIEC , SOC2, NERC CIP, ISO 27001 users should not be allowed to set a password that has been previously used. To ensure that users are using a different password from the previous ones when they reset their password, set the variable ***Settings->General->Security->Password/ Security Code Retries,*** so that when a user changes his password, the ssh jump host does not allow the last n passwords, n = number of password retries in settings plus one.

So you may set the number of password retries in settings to 2 to disallow the usage of the last 3 passwords.



Online URL: https://www.ezeelogin.com/kb/article/how-to-ensure-that-ssh-jump-host-users-are-not-using-previous-password-set-to-meet-security-compliances-such-as-pci-dss-sox-hipaa-nist-mas-soc2-ffiec-nerc-cip-iso-27001-193.html