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 October 8, 2024 Security Features 4739

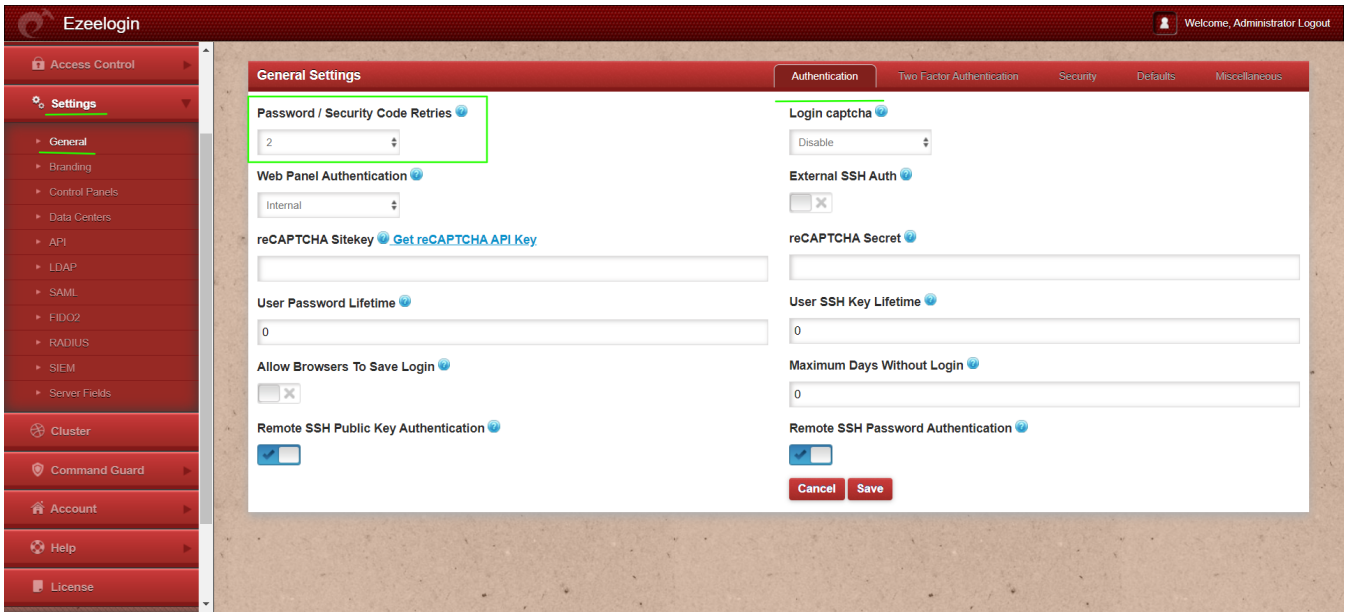
Ensuring Password Security Compliance in SSH Jump Hosts

Overview: This article describes configuring SSH jump hosts to enforce password security compliance by disallowing the reuse of previously used passwords, aligning with PCI DSS 3.2, SOX, HIPPA, NIST, MAS, FFIEC, SOC2, NERC CIP, and ISO 27001 standards.

In order to meet stringent security standards like PCI DSS 3.2, SOX, HIPPA, NIST, MAS, FFIEC, SOC2, NERC CIP, and ISO 27001, it is crucial to implement robust password management practices on SSH jump hosts. One of the essential requirements is to prevent users from reusing previously used passwords. This article outlines how to configure SSH jump hosts to enforce this policy effectively.

- To ensure that users are using a different password from the previous ones when they reset their password, set the variable **Settings -> General -> Authentication-> 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.


Ezeelogin
Welcome, Administrator Logout
Access Control
Settings
General
Branding
Control Panels
Data Centers
API
LDAP
SAML
FIDO2
RADIUS
SIEM
Server Fields
Cluster
Command Guard
Account
Help
License
General Settings
Authentication
Two Factor Authentication
Security
Defaults
Miscellaneous
Password / Security Code Retries
2
Login captcha
Disable
Web Panel Authentication
Internal
External SSH Auth
reCAPTCHA Sitekey
Get reCAPTCHA API Key
reCAPTCHA Secret
User Password Lifetime
0
User SSH Key Lifetime
0
Allow Browsers To Save Login
Maximum Days Without Login
0
Remote SSH Public Key Authentication
Remote SSH Password Authentication
Cancel
Save

Implementing these measures aligns with industry best practices and demonstrates a commitment to safeguarding sensitive information and maintaining compliance with stringent security standards.

Related Articles:

Prevent passwords from being recorded