fatal: no matching mac found: unable to ssh due to strict cipher set for pci dss compliance on remote box

138 admin October 4, 2024 Common Errors & Troubleshooting 15154

SSH Connection Error: No Matching MAC Found Due to Strict Cipher Set for PCI DSS Compliance

Overview: This article helps to resolve SSH connection error arising from strict cipher requirements under PCI DSS compliance by upgrading Ezeelogin to version 7.2.6 or above to align with security standards and ensure connectivity

FAQ: Unable to SSH to remote servers that have strict ciphers enabled. On the target server's side we see the error: "**fatal: no matching mac found: client hmac-sha1,hmac-sha1-96,hmac-md5,hmac-md5-96,hmac-ripemd160,hmac-ripemd160@openssh.com server hmac-sha2-512,hmac-sha2-256**".

FAQ: The following ciphers are enabled on my remote box and unable to SSH from the Ezeelogin SSH jump box

KexAlgorithms diffie-hellman-group-exchange-sha256
MACs hmac-sha2-512,hmac-sha2-256
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
It's for PCI compliance

Ans: **Upgrade to Ezeelogin version 7.2.6 and above.**

Related Articles:

Ensure that users are not using last-used passwords

Online URL: https://www.ezeelogin.com/kb/article/fatal-no-matching-mac-found-unable-to-ssh-due-to-strict-cipher-set-for-pci-dss-compliance-on-remote-box-138.html