EZEELOGIN

AN ISO 27001 & 9001 CERTIFIED COMPANY

Datasheet

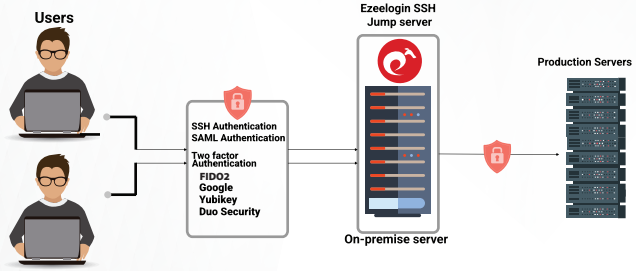
SSH Jump Server Software

What is Ezeelogin?

It is an SSH jump server solution designed to deploy an on-premise intermediate SSH gateway. This setup requires all staff, employees, and system administrators to first connect via SSH to this intermediary server before accessing remote servers, routers, and network switches. By implementing this SSH gateway, the primary objectives are to enhance security within your IT infrastructure and to meet various security compliance standards, including PCI DSS, ISO 27001, ISO 9001, GDPR and more. Additionally, it enhances operational efficiency and ensures better accountability.

*SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives system administrators a secure way to access a computer over an unsecured network.

How does it work?



Functional Highlights

- Centralized SSH access to servers to improve security and employee productivity
- Multi Factor Authentication (MFA) in SSH:
- Record and track user's SSH sessions
- Detailed logs and reporting to meet various security compliances
- Integrate with Active Directory/LDAP for easier user management
- No agent installation / custom modification on the remote machines
- Works with all Linux distributions

Features & Specifications

Remote Devices supported:	Linux servers, Cloud instances, switches, and routers or any devices with sshd protocol enabled
License types:	Standalone Internet based licenses
Access types:	SSH , HTTPS , RDP
Supported SSH Protocol:	Version 1, 2
Authentication method supported:	AD/LDAP SSO/SAML Internal
Client Authentication in Web:	http, https based authentication RADIUS,AD/LDAP,SAML
Client Authentication in SSH:	Password based Public Key based (RSA/DSA) RADIUS Pluggable Auth Modules (PAM)
Audit (Recording):	SSH
Compliances that can be met:	PCI DSS, ISO 27001, GDPR, HIPPA, NIST and many more
Multi Factor Authentication (MFA) in SSH:	Google Authenticator, Yubikey, Duo Security, RADIUS, FIDO2
Supported LDAP integrations:	Windows AD 2008, 2012, 2016, 2018, and Openldap 2.x for centralized authentication and management of users.
Supported Ciphers:	3des-cbc,blowfish-cbc cast128-cbc, arcfour arcfour128, arcfour256 aes128-cbc,aes192-cbc aes256-cbc rijndael-cbc@lysator.liu.se aes128-ctr,aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com chacha20-poly1305@openssh.com
Supported Key Exchange Algorithms:	diffie-hellman-group1-sha1 diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group-exchange-sha256 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 curve25519-sha256 curve25519-sha256
Client Tool:	Most SSH Clients (Terminal, Putty, Konsole, etc) Standard Browser

Single Sign-On	**Microsoft Azure SSO, GSuite SSO, Okta, OneLogin, AWS SSO, SSO using SAML 2.0 protocol**
Record SSH Sessions	**Maintain SSH log records with date and timestamps to track employees access to devices.**
Detailed Logs & Reporting	**Generate detailed user SSH access reports, including login/logout times to facilitate forensic analysis, cybersecurity audits, and to meet various compliance standards like PCI DSS, HIPAA, NIST, ISO 27001 and more**
SSH Key Management	**Configure user SSH Key expiry. Rotate SSH Keys periodically**
Master-Slave cluster for high availability	**Avoid lock out and single point failure.**
Role Based Access Control (RBAC) for ssh user access	**Group users and devices into different categories and grant access based on their role.**
Privileged Access Management (PAM)	**Grant the login privileges with which an SSH user would login into a remote device.**
Password management for users	**Enforce user password expiry User account disabled based on inactivity SSH user password rotation Enforce password strength**
Parallel Shell	**Execute commands on multiple servers simultaneously**
Intuitive and secure CLI interface	**Secure and efficient access to Linux servers, switches, and routers.**

Encryption Technologies used

- Hashing Algorithms used to hash web user credentials in the order of availability are SHA 512, SHA256, Blowfish, and DES
- Hashing Algorithm used to hash the system user credentials in UNIX backend is CRYPT
- Encryption Algorithm used for encrypting the ssh users log recorded in the file system is RC4
- Encryption algorithm used for encrypting sensitive information is 4096 bit RSA

System Requirements

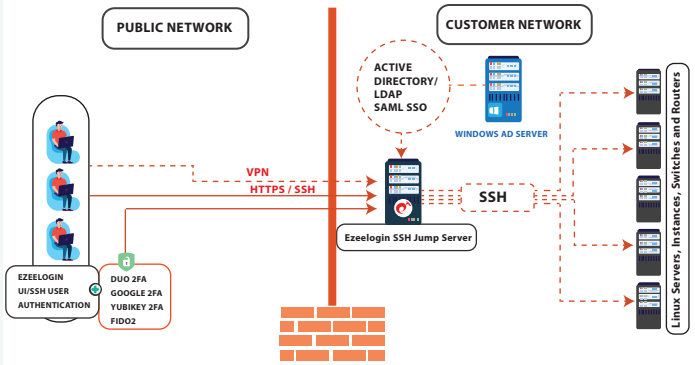
Hardware Requirements

Minimum 2GB Ram
Minimum 3 Ghz processing power
80GB Storage
Virtual Server or Dedicated server

Software Requirements

- OS Architecture (64 bit Linux[Centos/RHEL/Ubuntu /Debian]
- Web server (apache, lighttpd, nginx etc.)
- MySQL server
- PHP (from version 5.6.x to 7.4)
- Ioncube loader version 10 and above for PHP
- MySQLi extension for PHP
- JSON extension for PHP
- Mcrypt extension for PHP
- LDAP extension for PHP (for LDAP web panel authentication)
- DOM extension for PHP (for SAML authentication)
- OpenSSL
- NPM,GIT,LibX11, Linux Kernel >=4.4 (This is required only if Use Proxy function in webportal is used.)
- NodeJS (from version 12.x and above) (This is required only if WebSSH or WebRDP is used.)
- Outbound host and Port to be opened in firewall (not required for standalone license): license2.ezeelogin.com TCP 443

Deployment Diagram



Our Happy Customers

India Office

ADMOD Technologies Pvt. Ltd
AN ISO 27001 CERTIFIED COMPANY

Building No 27/309(A,B) Maveli Nagar,
Pipeline Road, Cochin
University PO , Kochi-682022, Kerala, India
Phone: +91 9567867452
Email: support@ezeelogin.com

USA Office

ADMOD, Inc, 2093 Philadelphia Pike, Claymont, New Castle, 19703 Delaware
Phone: +1 (302) 357-9527, +1 (302) 357-9007
Email: support@ezeelogin.com