Salient features

772 Jisna Joseph November 10, 2025 Features & Functionalities 1525

Ezeelogin Features Overview

Overview: This article outlines the key features provided by Ezeelogin. The platform is designed to enhance security, simplify management, and improve productivity in SSH gateway environments. Ezeelogin provides a robust suite of authentication, access control, auditing, automation, and productivity tools for managing SSH environments securely and efficiently.

1. Authentication & Access Control

1.a. Multi-Factor Authentication (MFA)

Secure your bastion host using two-factor authentication methods such as **Google Authenticator**, **DUO Security**, **YubiKey**, **FIDO2**, **Access Keyword**, or **RADIUS 2FA**.

> Enable/Disable 2FA [Two Factor Authentication] on Ezeelogin

1.b. Role-Based Access Control (RBAC)

Restrict access to remote servers based on user roles within your organization.

> Role Based Access Control (RBAC) Explained

1.c. Privileged Access Management (PAM)

Allow non-privileged users to temporarily gain root privileges with administrator approval.

> User privilege escalation for particular time

1.d. SAML Authentication

Login using **Single Sign-On (SSO)** for better access management and enhanced security.

> Integrating SSO/SAML with Ezeelogin PAM

1.e. AD/LDAP Authentication

Integrate **Active Directory (AD)** or **OpenLDAP** for centralized user authentication and improved user management.

> Integrate OpenLDAP / Windows Active Directory authentication

1.f. OpenID Connect (OIDC) Authentication

Authenticate users using **OpenID Connect (OIDC)** for seamless and secure login experiences.

> Authentication with OpenID connect

1.g. SSH Key rotation to remote servers

Automatically rotate SSH keys on remote servers at regular intervals to enhance security and prevent unauthorized access.

> SSH Key rotation to remote servers

1.h. Key Management

Centralize, encrypt, and manage SSH keys within Ezeelogin to simplify access control and ensure secure key handling.

> Key Management

---

2. Security & Compliance

2.a. SSH Key Management

Encrypt and manage SSH keys securely, allowing access to the SSH gateway with a single key.

> Different key based authentication to remote server

2.b. SSH User Expiry

Set expiry dates for SSH users to automatically revoke access after a specified period.

> How to set the expiry for Ezeelogin SSH gateway users?

2.c. Automated Password Resets

Regularly reset root passwords on Linux nodes to maintain compliance and enhance security.

> Cron for changing root passwords on servers periodically

2.d. Password Strength Configuration

Set minimum password lengths, enforce expiration, rotation, and limit reuse for better security.

> Enforce password policy or complexity to the Ezeelogin user's password

2.e. Password History Limit

Prevent users from reusing old passwords by setting a password history limit.

> Password History Limits for Gateway Users

2.f. Password Expiry & Rotation

Define password expiration policies to ensure regular password updates.

> Set SSH gateway user password lifetime

2.g. Force Password Change

Require users to change their passwords after audits or suspected breaches.

> Force a password change

2.h. Account Lockout Threshold

Prevent brute-force attacks by automatically locking user accounts after repeated failed login attempts.

> Account lockout Threshold

2.i. Maximum Days Without Login

Automatically lock accounts if users haven’t logged in for a specified duration.

> Set maximum days without login for SSH gateway users

2.j. Manage Concurrent SSH Connections

Control the maximum number of SSH sessions a user can establish concurrently to prevent performance issues.

> Limiting max SSH sessions to remote Linux devices

2.k. Rate Limiting in SSH Connections

Throttle or delay SSH connection attempts to manage user activity and prevent overloads.

> Rate Limiting in SSH Connections

2.l. IP Restrictions

Restrict or limit which IP addresses users can connect from to the SSH gateway.

> Configuring IP restrictions

2.m. Credential History Tracking

Maintain a record of credential changes for auditing and compliance.

> View the updated password history for remote servers

2.n. Prompt Reason for SSH Access

Require users to provide a justification before accessing SSH sessions for audit tracking.

> Prompt ssh gateway user to enter reason for ssh access

7.o. High Availability (HA)

Configure master-slave clusters to prevent single points of failure and ensure redundancy.

> Install slave / secondary node for high availability

---

3. Audit & Monitoring

3.a. SSH Session and Recording

Record and monitor SSH sessions for audit purposes to track user actions and commands.

> Record ssh sessions

3.b. RDP Session and Recording

Access **Windows servers** directly through your browser using RDP.

> Windows Server for RDP via browser

3.c. Audit Logging

Track and log all user activities within Ezeelogin for transparency and auditing.

> Audit logs and configurations

3.d. User Activity Reports

Generate and export user activity reports in CSV format for compliance and analysis.

> Generate user reports as CSV files

3.f. SIEM Integration

Forward logs to **Security Information and Event Management (SIEM)** tools for centralized monitoring.

> Integrating Ezeelogin PAM solution with SIEM

---

4. Productivity & Automation

4.a. Web Portals & Control Panels

Access popular web control panels directly with a single click.

> List of WebPortals and ControlPanels

4.b. Web SSH Client

SSH securely into servers directly from your browser without a dedicated SSH client.

> Set up the WebSSH console

4.c. RDP Support

Access **Windows servers** directly through your browser using RDP.

> Windows Server for RDP via browser

4.d. Command Guard

Restrict or filter commands executed on remote servers to prevent unauthorized actions.

> Restrict commands for gateway users on remote servers?

4.e. Parallel Shell

Execute commands simultaneously on multiple servers from the gateway interface.

> Parallel Shell - How to use it?

4.f. Automated Password Resets

Regularly reset root passwords on Linux nodes to maintain compliance and enhance security.

> Cron for changing root passwords on servers periodically

4.g. Secure File Transfer

Easily and securely transfer files between your desktop and remote servers.

> Transfer file from desktop machine to remote server

4.h. API Support

Automate user and server management tasks by integrating with Ezeelogin’s API.

> Manage Servers via API
> Manage users via API

4.i. High Availability (HA)

Configure master-slave clusters to prevent single points of failure and ensure redundancy.

> Install slave / secondary node for high availability

Online URL: https://www.ezeelogin.com/kb/article/salient-features-772.html