Best Practices for Ezeelogin: A Guide to Standard Security Configurations

747 Manu Chacko May 8, 2025 Security Compliances 2551

Best *practices* for ensuring Security with Ezeelogin

Overview: Implementing secure access with Ezeelogin is essential for safeguarding your organization's resources. By following these best practices, you can ensure robust identity management, enforce multi-factor authentication, significantly enhance your security posture

1. SSH User Expiry
Ezeelogin allows you to set an expiry time for SSH users, ensuring that access is automatically revoked after a specified period. This feature is essential for developers or system administrators who require temporary access to deploy code, safeguarding your systems from unnecessary exposure.
Reference: Configuring SSH User Expiry

2. Identity and Access Management (IAM)
With Ezeelogin, you can precisely control which developers or system administrators have access to specific Linux production nodes. You can designate whether a user logs in as a non-privileged user or as ‘root,’ allowing for more granular access management.
Reference: Setting Up IAM in Ezeelogin

3. Access Control (RBAC)
Assign roles and permissions to effectively manage user privileges. Define role requirements and specify which resources each role can access.
Reference:Implementing RBAC

4. Multi-Factor Authentication (2FA)
Easily integrate Fido2, Yubikey, DUO Security, or Google Two-Factor Authentication when your staff accesses Linux nodes. This added layer of security significantly reduces the risk of unauthorized access.
Reference: Integrating 2FA

5. SSH Session Recording
Monitor and record SSH sessions to understand user actions on your Linux nodes. This feature is invaluable for audits, enabling you to track who did what, when, and where.
Reference: Configuring SSH Session Recording

6. SSH Key Management
Ezeelogin simplifies SSH key management by encrypting all keys and allowing users to access the SSH jump gateway with just one key. This addresses the complexities of managing multiple keys for various users.
Reference: Managing SSH Keys

7. Automated Password Resets
Regularly reset root passwords on your Linux nodes to maintain security compliance. Direct root access should be disabled for an added layer of security.
Reference: Setting Up Automated Password Resets

8. Centralized User Authentication and SSO Integration
Authenticate your staff through LDAP or Active Directory, streamlining access management across your organization. Additionally, Ezeelogin seamlessly integrates with various SSO providers, including Google SSO, AWS SSO, Azure SSO, JumpCloud SSO, Okta SSO, and OneLogin SSO. This integration simplifies user management and enhances security.
Reference: Configuring LDAP/AD

Reference: Integrating SSO/SAML

9. Account Lockout Threshold
To prevent brute force attacks, Ezeelogin automatically locks accounts after a predetermined number of failed login attempts.
Reference: Setting Account Lockout Threshold

10. Password Strength Configuration
Set minimum password lengths, enforce password expiration and rotation, and limit password reuse to enhance security compliance.
Reference: Configuring Password Policies

11. Password History Limit
Prevent the reuse of previous passwords to maintain security compliance. By enforcing a history limit, you ensure that users cannot revert to old passwords, enhancing overall security.
Reference: Configuring Password History Limit

12. User Password Expiry and Rotation
You can set policies for password expiration and rotation to further enhance security, ensuring that passwords are regularly updated and reducing the risk of unauthorized access.
Reference: Setting Up Password Expiry and Rotation

13. Force Password Change
Enforce a password change for users when necessary, such as during security audits or after a potential breach. This ensures that compromised passwords are updated promptly.
Reference: Setting Up Force Password Change

14. Maximum Days Without Login
Automatically lock accounts if users have not logged in for a specified number of days. This feature helps reduce the risk of orphaned accounts that could be exploited.
Reference: Configuring Maximum Days Without Login

15. Audit Logging
Ezeelogin maintains detailed logs of all user account changes, crucial for tracking user actions and forensic analysis in case of incidents.
Reference: Configuring Audit Logging

16. SIEM Integration
Ezeelogin supports integration with SIEM solutions like Splunk, Syslog, and ELK, providing centralized logging capabilities for comprehensive audit log management.
Reference: Integrating with SIEM

17. Manage concurrent SSH connections

Maximum concurrent remote login(MCRL) feature helps the system administrators to control the concurrent SSH sessions that a user can establish on the remote Linux devices and prevent potential performance bottlenecks.

Reference: limiting max SSH sessions to remote Linux devices

18. Rate Limiting in SSH Connections

Throttle delay in SSH is a method to manage and restrict the active SSH sessions or login attempts to remote Linux devices. Remote Login Throttle Delay (RLTD) feature help the System Administrator to limit the users active ssh sessions to a remote server.

Reference: Rate Limiting in SSH Connections

Online URL: https://www.ezeelogin.com/kb/article/best-practices-for-ezeelogin-a-guide-to-standard-security-configurations-747.html