Sysadmin Guide

Generated on 2026-05-26

Contents

Sysadmin

Welcome to the installation guide for ConneX. This document is intended for system administrators who will be setting up and maintaining the environment required to run ConneX.

ConneX requires a Linux operating system. An Ubuntu LTS version is the recommended Linux distribution. The installation guide assumes *Ubuntu Linux* as the operating system and the availability of the *systemd* process and service manager.

Tech stack

The AP software is built using a client-server architecture, where the client (front-end) communicates with the server (backend) over a REST HTTP API.

- **Database:** The transactional database for metadata storage is PostgreSQL.
- **Backend:** Backend services are written in Java using OpenJDK 17. Major frameworks are Spring Boot, Spring Security, JPA/Hibernate and Apache Commons. *Testcontainers* and *JUnit* are used for unit and integration testing.
- **Front-end:** The front-end web apps are written in Javascript with the React framework and Ant Design UI library.

Hosting requirements

ConneX can be deployed on-premise or in the AWS and Azure public clouds. It can be deployed entirely on a single virtual machine (VM), or by deploying the various services on separate VMs. For an on-premise deployment on a single VM, the following requirements apply.

Hardware

- Virtual machine or physical server
- Linux operating system, Ubuntu 24.04 LTS recommended
- 32 GB RAM
- 8 CPU, ideally 16 or 32 CPU
- 500 GB SSD storage

Network

- 300 Kbps network bandwidth per user
- 1 Gbps network transfer between servers (if more than one)

Components

- Internet connection with public IP address
- SSH external access
- Terminal root access
- Domain name
- SSL certificate
- SMTP email server
- Backup strategy for local and off-site backups
- Monitoring of uptime and alerting for downtime
- Vulnerability scan and security hardening

Security

This page covers the security principles and security posture for ConneX.

Software security

This section describes various security aspects of the ConneX software.

- **Encryption in of secrets:** Secrets including API keys and passwords are encrypted using the Tink cryptographic library for Java from Google, a high-assurance framework which provides industry-standard security primitives. ConneX employs *Authenticated Encryption with Associated Data* (AEAD) key types to ensure confidentiality of secrets and the cryptographic integrity required to prevent unauthorized tampering.

- **Encryption at rest:** Full disk encryption (FDE) using LUKS (Linux Unified Key Setup) is the recommended approach for encrypting data at rest. As modern CPUs support AES-NI hardware acceleration, the performance hit for ClickHouse high-throughput reads is negligible.
- **Encryption in transit:** Data pipelines (connectors) communicate securely with source systems through the HTTPS protocol, reinforced by industry-standard strong cipher suites. This approach ensures that data is fully encrypted in transit, providing high-assurance security as data moves across the network.
- **Security framework:** User and client authentication in ConneX is managed through the industry-standard Spring Security framework, ensuring that all access controls and authentication and authorization workflows meet modern enterprise standards.
- **Hashing of user passwords:** ConneX user account passwords are secured with one-way cryptographic hashing using the industry-standard BCrypt algorithm. This approach ensures that credentials are never stored in a reversible or human-readable format, providing protection against brute-force and rainbow table attacks.
- **Single Sign-On (SSO):** ConneX supports the OIDC standard for authentication protol and with that the major identity providers including Keycloak, Google Identity Platform and Azure Entra ID. ConneX supports Single Sign-On authentication flows across applications through the OIDC standard.
- **Multi-Factor Authentication (MFA):** ConneX supports multi-factor authentication using *Time-Based One-Time Passwords* (TOTP) and authenticator apps including *Google Authenticator* and *Authy*, providing a strong, second layer of protection for user accounts.
- **Secure by default:** ConneX follows the *Secure by default* and *Least privilege* principles. The software is designed and configured with strict security settings and out of the box. Users are encouraged to grant only the permissions necessary to perform primary functions. This reduces the attack surface and the risk for misconfiguration.
- **Static Application Security Testing (SAST):** The ConneX software is developed using CI/CD where *Static Application Security Testing* (SAST) is integrated in the build pipeline. The SAST tool automatically scans for critical security flaws, including the OWASP Top 10 security risks.

Managed hosting security

This section describes various security aspects of the ConneX managed hosting offering from BAO Systems.

- **Web Application Firewall (WAF):** The WAF stops attacks at the doorstep by inspecting incoming traffic against the latest OWASP Core Rule Set, blocking malicious behavior and abnormal patterns before they reach your application. The WAF continuously evolves with the threat landscape, helping ensure that only legitimate traffic is allowed through.
- **Encryption at rest:** Data is encrypted at rest using *Amazon EBS Encryption* for full disk encryption. The entire EBS volume (virtual disk), where the database files, logs, and buffer data files reside, are encrypted, protecting against unauthorized access to the data storage.
- **Proactive patching:** A strucured schedule for patching of packages and libraries ensures staying ahead of threats. BAO Systems is continuosly monitoring for zero-day vulnerabilities and proactively applies patches to ensure the system stays secure, while providing the flexibility to specify patching windows to balance uptime and security.

- **Performance monitoring:** BAO Systems ensures platform stability through continuous, real-time infrastructure monitoring. Grafana, Prometheus and Zabbix are leveraged to track performance trends and resource utilization to detect anomalies. This allows for proactive intervention before users are impacted, maintaining a controlled and reliable environment.
- **Infrastructure as code:** The hosting server fleet is fully managed via Infrastructure as Code, ensuring strict consistency across all environments. By automating configuration with Ansible and Rundeck, BAO Systems enforces consistency and security standards and enable rapid disaster recovery with rapid and complete rebuild of entire environments.
- **Dynamic Application Security Testing (DAST):** BAO Systems employs continuous automated scanning and Dynamic Application Security Testing (DAST) to identify weaknesses across infrastructure and applications. Issues are prioritized by severity, tracked and remediated according to industry best practice. This proactive cycle ensures that vulnerabilities are neutralized before they pose a risk.
- **Single Sign-On:** BAO Systems help streamline access and login across ConneX and the your application ecosystem through Single Sign-On. ConneX is integrated with your existing identity provider, including Google Identity Platform and Microsoft Entra ID, alternatively, host a dedicated Keycloak instance to provide secure authentication.
- **Application level security:** The managed hosting offering follows the Mozilla web security guidelines and standard web security recommendations, providing protection against cross-site request forgery, cross-site scripting, session hijacking and other common threats.