zenzap

The Professional Work Chat App

The enterprise-grade communication platform built for IT and security teams.

Overview

Zenzap is a cutting-edge SaaS chat platform engineered specifically for the demanding needs of Enterprise IT and Security teams. We provide a secure, compliant, and highly functional environment for internal communication, collaboration, and incident response.

Our platform combines ease of use with enterprise-grade management capabilities, allowing IT departments to maintain full control over their data while ensuring adoption across all levels of technical proficiency.

Zenzap is available on the web, on mobile devices through the **Apple App Store** and **Google Play Store**, and as native desktop applications for **Windows and Mac.**

Download on the App Store

GET IT ON Google Play

macOS

Technical Architecture

Our platform is designed for resilience, scalability, and security from the ground up. Zenzap employs a microservices architecture, leveraging cloud-native technologies to ensure high availability and rapid feature deployment.

Core Infrastructure

You Control The Data.
All data is owned by the company, and while residing on employees device, can be easily remotely wiped, and once an employee leaves the organization, all data is automatically discarded.

Fast Chat.
Fast, intuitive chat using mechanics like local first storage and APNS encrypted push payloads, to provide a great chat experience, even if you in bad network conditions.

Encrypted Data Transmission.
All data in transit is secured using TLS 1.2+ encryption.

Separation of Duties.
Strict control layers segregate customer data, configuration, and application logic.

Key Architecture Principles

Component	Description
Local Encrypted Database	Each device maintains a secure, encrypted local database that replicates from the master database for offline access and fast performance. Administrators can remotely wipe or invalidate the local database at any time, rendering it unreadable on lost or compromised devices
Real-time Sync via WebSocket	All changes flow in real-time through secure WebSocket connections (TLS 1.2+) to all connected devices
Server-side Security Validation	All security-sensitive operations (adding/removing members, topic permissions) are validated on the server before propagating to devices
Enterprise Integration API	Dedicated API for your enterprise bots to create topics, send messages, and automate workflows—scoped exclusively to your organization
Remote Wipe & Revocation	Organization administrators can instantly revoke access and remotely wipe local databases on any device, ensuring data security when devices are lost, stolen, or when employees leave the organization

API & Integration Capabilities

- **RESTful API:** Comprehensive API access enables integration with existing enterprise systems, custom workflows, automated routine tasks, and data synchronization with internal platforms
- **Webhook Support:** Real-time event notifications for seamless automation workflows
- **Rate Limiting:** Configurable rate limits to protect system integrity

Platforms

- **Web:** All modern browsers (Chrome, Firefox, Safari, Edge)
- **Desktop:** Native applications for macOS and Windows
- **Mobile:** Native applications for iOS and Android
- **Data Sync:** Real-time synchronization across all devices

Security & Compliance

Zenzap is committed to meeting the highest standards of security and regulatory compliance to protect your sensitive enterprise communications.

Security Features

Encryption at Rest: AES-256 encryption for all stored data

Encryption in Transit: TLS 1.2+ for all data transmission

Single Sign-On (SSO): SAML 2.0 support for enterprise identity providers

User Provisioning: SCIM protocol for automated user lifecycle management

Role-Based Access: SAML attribute-based role assignment

Audit Logging: SIEM-compatible audit logs for security monitoring

BYOK: Bring Your Own Key support for file encryption

Cloud Recovery: Employees who lose their devices can recover messages and data from secure cloud backend

Instant Access Revocation: Administrators can immediately revoke access for users via SCIM, removing them from all groups

Remote Device Wipe: Access to lost or stolen devices can be revoked immediately, preventing unauthorized access

File Security & Data Loss Prevention

Zenzap provides comprehensive file security controls to protect sensitive documents shared within your organization:

Malware Scanning: All uploaded files are automatically scanned for malware, viruses, and malicious content before being made available to recipients.

Secure Perimeter: Configurable policy to disable downloading, saving, and exporting files outside of Zenzap, ensuring sensitive documents remain within your secure environment.

File Access Controls: Granular permissions for file sharing, viewing, and downloading based on user roles.

File Retention Policies: Customizable retention rules with automatic deletion after specified periods.

🔒 **Enterprise Control:** Administrators can enforce file security policies organization-wide, preventing data exfiltration while maintaining seamless collaboration.

Certifications & Compliance

Zenzap has successfully achieved **SOC 2 Type II certification**, providing assurance that our systems are designed and operating effectively to meet the SOC 2 trust principles:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

Zenzap is fully compliant with the **General Data Protection Regulation (GDPR)**, assuring that our systems and processes are designed to uphold the rights of individuals and meet EU data protection requirements:

- Lawful Data Processing
- Minimal Data Collection
- Data Accuracy
- Confidentiality of Personal Data
- Accountability

📋 For detailed information regarding our compliance posture, controls, and audit reports, please visit the [Zenzap Trust Center](#).

Data Residency

All Zenzap data is hosted exclusively on **Google Cloud Platform (GCP)** infrastructure within the European Union, ensuring compliance with regional data protection regulations.

Infrastructure

Component	Details
Cloud Provider	Google Cloud Platform (GCP)
Primary Region	Belgium (europe-west1)
Secondary Region	Frankfurt, Germany (europe-west1)
Data Sovereignty	All data remains within EU boundaries

Data Protection

Requirement	Implementation
Data Isolation	All customer data, including messages, files, and metadata, remains strictly within GCP's European data centers
GDPR Compliance	Full compliance with EU data privacy laws and regulations
Data Processing	All processing occurs within EEA boundaries—no data leaves the EU
Backup & Recovery	Geo-redundant backups across Frankfurt and Belgium regions
Failover	Automatic failover between EU regions for high availability

Authentication & Single Sign-On (SSO)

Zenzap integrates seamlessly with your existing identity providers to simplify user access management and enforce enterprise-grade security policies.

Supported Protocols & Providers

Protocol	Version	Status
SAML	2.0	Supported
SCIM	2.0	Supported
OAuth 2.0	—	Supported
OpenID Connect	1.0	Supported

Supported Identity Providers

Provider	SAML	SCIM	Documentation
Microsoft Entra ID (Azure AD)	✅	✅	Setup Guide
OpenID Connect	✅	✅	Setup Guide

Key SSO Features

- **Just-in-Time (JIT) Provisioning:** Automatically create user accounts on first login
- **Multi-Factor Authentication (MFA):** Enforce MFA through your identity provider
- **Centralized Access Control:** Manage access through your existing IAM policies
- **Role Mapping:** Map IdP groups/roles to Zenzap permissions via SAML attributes

📚 For detailed configuration guides, visit docs.zenzap.co

Network Configuration

For optimal performance and uninterrupted service, IT teams may need to configure network access for Zenzap services.

Required Domains

The following domains must be accessible from end-user devices and integration endpoints:

Domain	Purpose
app.zenzap.co	Main application
api.zenzap.co	API endpoints
https://firebasestorage.googleapis.com	Static assets and file delivery
prod-ws-pod01.zenzap.co	WebSocket connections for real-time messaging

Firewall Requirements

Protocol	Port	Direction	Purpose
HTTPS	443	Outbound	API & Application traffic
WSS	443	Outbound	WebSocket connections

Support & Resources

Resource	URL
Documentation	docs.zenzap.co
Trust Center	trust.zenzap.co
Enterprise Support	support@zenzap.co