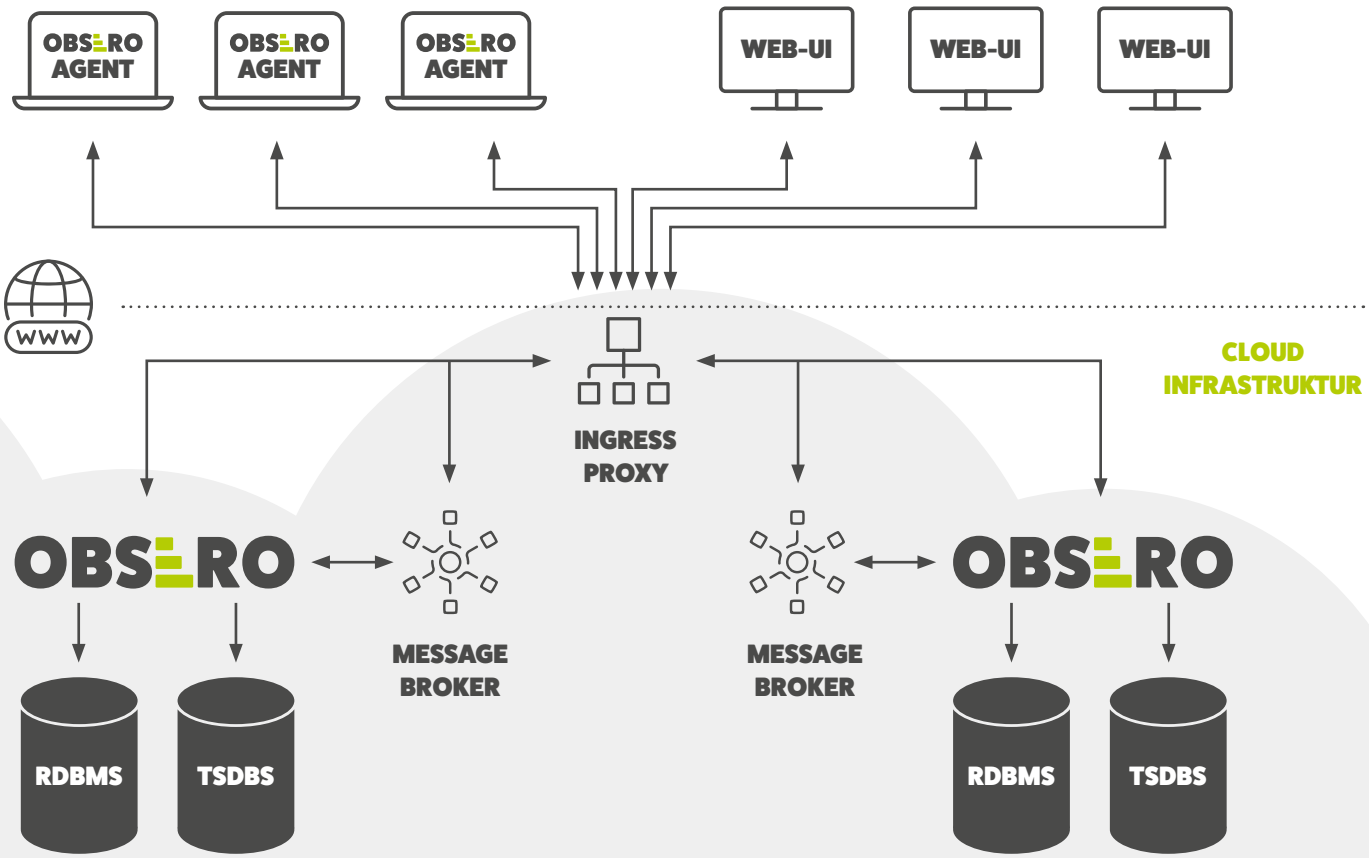
OBSERO SECURITY REFERENCE GUIDE

EINFÜHRUNG

Obsero ist eine hochsichere, Cloud-basierte Lösung für das zentrale Monitoring, die Steuerung und die statistische Auswertung aller angebundenen AV- und IT-Geräte. Die Plattform ermöglicht die Überwachung des Status von Geräten und Räumen in Echtzeit, Fernsteuerung von Geräten, Verwaltung von Konfigurationen, Auswertung detaillierter Nutzungsstatistiken sowie Alarmierungen bei auftretenden Fehlern. Durch intelligentes Energiemanagement lässt sich zudem der Energieverbrauch der Geräte und Räume optimieren.

Die Architektur basiert auf einer agentenbasierten Kommunikation zwischen lokalen Geräten und der zentralen Cloud-Infrastruktur, die höchste Sicherheitsstandards erfüllt.

SYSTEMARCHITEKTUR



SICHERES KOMMUNIKATIONSMODELL

Ein zentraler Sicherheitsaspekt der Obsero-Architektur ist das **Outbound-Only Prinzip**: Alle Verbindungen werden ausschließlich vom lokalen Agent zur Obsero Management Plattform initiiert.

Der Agent ist nicht direkt aus dem Internet erreichbar und es werden niemals eingehende Verbindungen zur lokalen Infrastruktur aufgebaut. Dies minimiert das Angriffsrisiko und ermöglicht den Betrieb auch in stark abgesicherten Netzwerkumgebungen.

KOMPONENTEN

- **Obsero Agent:** Lokale Software zur Gerätesteuerung und -überwachung
- **Obsero Management Plattform:** Cloud Applikation zur Verwaltung aller Obsero-Agents
- **Message-Broker:** Verschlüsselte Nachrichtenvermittlung
- **Web-UI:** Browser basierende Applikation für den Endanwender

KOMMUNIKATION & NETZWERKPROTOKOLLE

Obsero verwendet ausschließlich verschlüsselte Kommunikationsprotokolle, um die Sicherheit der Daten während der Übertragung zu gewährleisten.

MQTTS

Der Hauptkommunikationskanal für Echtzeitdaten zwischen Agent und der Obsero Management Plattform:

- TCP
  - IPv4 **xyz.obsero-av.com**
  - Port 11377*
- **TLS 1.3 Verschlüsselung**
- Client-ID basierte Authentifizierung über Credentials
- ACL basierte Trennung der einzelnen Obsero-Agents
- Dient der Übertragung der Gerätezustände und dem Empfang von Steuerdaten

HTTPS

Ergänzende Kommunikation für Verwaltungsaufgaben:

- TCP
  - IPv4 **xyz.obsero-av.com**
  - Port 443
- **Verschlüsselung: TLS 1.3, TLS 1.2, SSL Overall-Rating A**
  Die verwendeten Cipher sind mandantenspezifisch anpassbar.
- Übertragung von Binärdaten (Firmware, Raumbilder)
- Initiale Agent-Adoption (Zuordnung des Agents zu Mandanten)
- Kommunikation mit der Web-UI (Browser-Applikation)

BENUTZERROLLEN & ZUGRIFFSMANAGEMENT

Die Obsero Management Plattform bietet ein differenziertes Rollenkonzept, das präzise Steuerung von Zugriffsrechten ermöglicht und die Sicherheit der Installation maximiert.

- **ADMINISTRATOR**

  Gewährt vollständigen Zugriff auf alle Funktionen des Systems, einschließlich der Benutzerverwaltung. Es muss immer mindestens ein Administrator im System vorhanden sein, um die Administrierbarkeit sicherzustellen.

- **USER**

  Bietet eingeschränkten Zugriff auf Basis der vom Administrator zugewiesenen Rechten. Dieser Nutzer kann keine weiteren Benutzer hinzufügen oder Administratoren ernennen, hat jedoch vollen Zugriff auf die ihm zugewiesenen Bereiche.

- **BETRACHTER**

  Ermöglicht reinen Lesezugriff auf zugewiesene Räume und Geräte. Ideal für Stakeholder, die Einblick in den Status haben möchten, ohne Änderungen vornehmen zu können.

* Kann auf Kundenwunsch geändert werden

INFRASTRUKTUR & SICHERHEIT

LOKALE DATENSPEICHERUNG

Es werden keine Nutzdaten dauerhaft auf dem Obsero Agent gespeichert. Die gesamte Datenverarbeitung und -speicherung findet ausschließlich in der gesicherten Obsero Management Plattform statt.

RECHENZENTRUM

Sämtliche Infrastruktur zum Betrieb der Obsero Management Plattform befindet sich ausschließlich in deutschen Rechenzentren. Dies gewährleistet die Einhaltung deutscher und europäischer Datenschutzstandards (DSGVO) und bietet höchste Rechtssicherheit. Unsere Rechenzentren sind nach ISO / IEC 27001:2022 und SOC2 zertifiziert. Weiterhin liegt eine EMAS / ISO 14001 Zertifizierung vor.

VERSCHLÜSSELUNG – UMFASSENDER SCHUTZ AUF ALLEN EBENEN

Obsero implementiert ein mehrschichtiges Verschlüsselungskonzept, das Daten sowohl während der Übertragung als auch im Ruhezustand schützt.

VERSCHLÜSSELUNG IN TRANSIT (DATA IN TRANSIT)

Alle Datenübertragungen zwischen den Komponenten erfolgen ausschließlich über verschlüsselte Kanäle:

- TLS 1.3 für MQTTS-Kommunikation (Obsero Agent ↔ Obsero Management Plattform)
- HTTPS/TLS für REST API und Web-UI Zugriffe
- Keine unverschlüsselten Datenübertragungen über das Internet

VERSCHLÜSSELUNG AT REST (DATA AT REST)

Alle gespeicherten Daten sind umfassend geschützt:

- Full-Disk-Encryption auf allen Servern
- AES-256 Verschlüsselung für alle Datenbank-Backups mit Keyfile-Absicherung
- Verschlüsselte Speicherung sensibler Credentials mittels Argon2id und Bcrypt Algorithmen

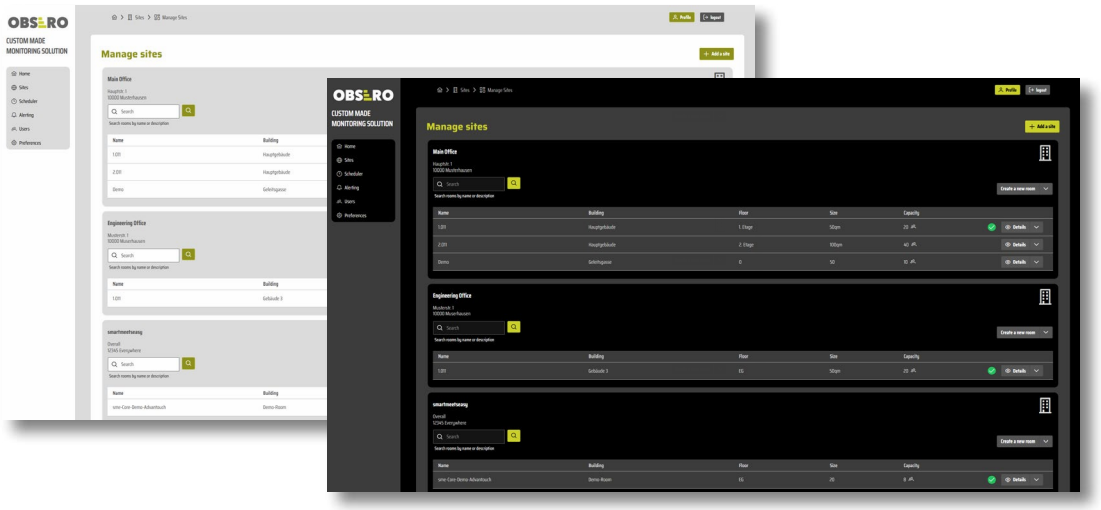
BACKUP-STRATEGIE

Obsero verwendet mindestens eine 3-2-1 Backup-Strategie:

- 3 Kopien der Daten
- 2 verschiedene Speichermedien
- 1 externe Kopie
- Alle Backups sind verschlüsselt

EXTERNE SERVICES

Die Obsero Management Plattform verwendet keinerlei externe Services oder Drittanbieter-Tools.
Es kann garantiert werden, dass kein Datentransfer außerhalb der Europäischen Union stattfindet.
Sämtliche Datenverarbeitung erfolgt innerhalb der eigenen, kontrollierten Infrastruktur.



DATENVERARBEITUNG & DATENSCHUTZ

GESPEICHERTE DATEN

Folgende Daten werden langfristig in der Obsero Management Plattform gespeichert, um den vollen Funktionsumfang der Plattform bereitzustellen:

- **Geräte- und Raumkonfigurationen:** Einstellungen, Zuordnungen und Parameter
- **Benutzer und Berechtigungen:** Authentifizierungsdaten und Zugriffsrechte
- **Zeitreihendaten:** Geräte- und Raumstatistiken für historische Auswertungen und Trendanalysen
- **Ereignisprotokolle:** System- und Geräteereignisse für Nachvollziehbarkeit

DATENSCHUTZ-COMPLIANCE

Die Anwendung folgt bei der Erhebung von personenbezogenen Daten den Prinzipien von Datenvermeidung und Datensparsamkeit. Es werden nur zum Betrieb notwendige personenbezogene Daten erhoben, verarbeitet oder gespeichert. Es werden keine personenbezogenen Nutzungsdaten von Geräten oder Räumen erhoben, verarbeitet oder gespeichert.

MANDANTENTRENNUNG – MULTI-TENANT ARCHITECTURE

Obsero gewährleistet eine vollständige Isolation zwischen verschiedenen Mandanten durch eine echte Multi-Tenant-Architektur auf Infrastrukturebene:

- **Eigene Datenbank** pro Mandant – keine gemeinsame Datenbasis
- **Eigener MQTT-Broker** pro Mandant – isolierte Kommunikationskanäle
- **Separate Deployment-Units –** Trennung der Instanzen
- **Getrennte virtuelle Netzwerke –** isolierte Datenkommunikation der Instanz-Dienste

Diese Architektur stellt sicher, dass Daten verschiedener Mandanten niemals in Berührung kommen und höchste Sicherheits- und Datenschutzanforderungen erfüllt werden.