KRAMER

USER MANUAL

Kramer KronoMeet Security Guide

P/N: 2900-301362 Rev 1

Contents

Introduction

Kramer KronoMeet Cloud-Based Room Scheduling and Meeting Management Platform helps organizations around the world transform their meeting spaces by deliver compelling digital experiences. This helps engage customers, get business done faster, and work more effectively. **Kramer KronoMeet** seamlessly integrates into existing enterprise systems and business applications. It empowers employees across your organization to increase their operational efficiency, reduce risks associated with human failure, and create an intuitive and modern end-to-end digital experience.

Kramer security practices are strongly bound into the internal security culture as well as the research and development processes of **Kramer KronoMeet**.

Kramer KronoMeet supports comprehensive network technology and maintains strategic partnerships with cloud providers that protect your data with industry-leading security standards. These standards help protect your organization and your employee data aligning with the most critical applications. This allows your organization to adapt to changing environments and meet market requirements.

An easy to handle license management system and the robust cloud infrastructure backbone of **Kramer KronoMeet** round out the stability of the system.

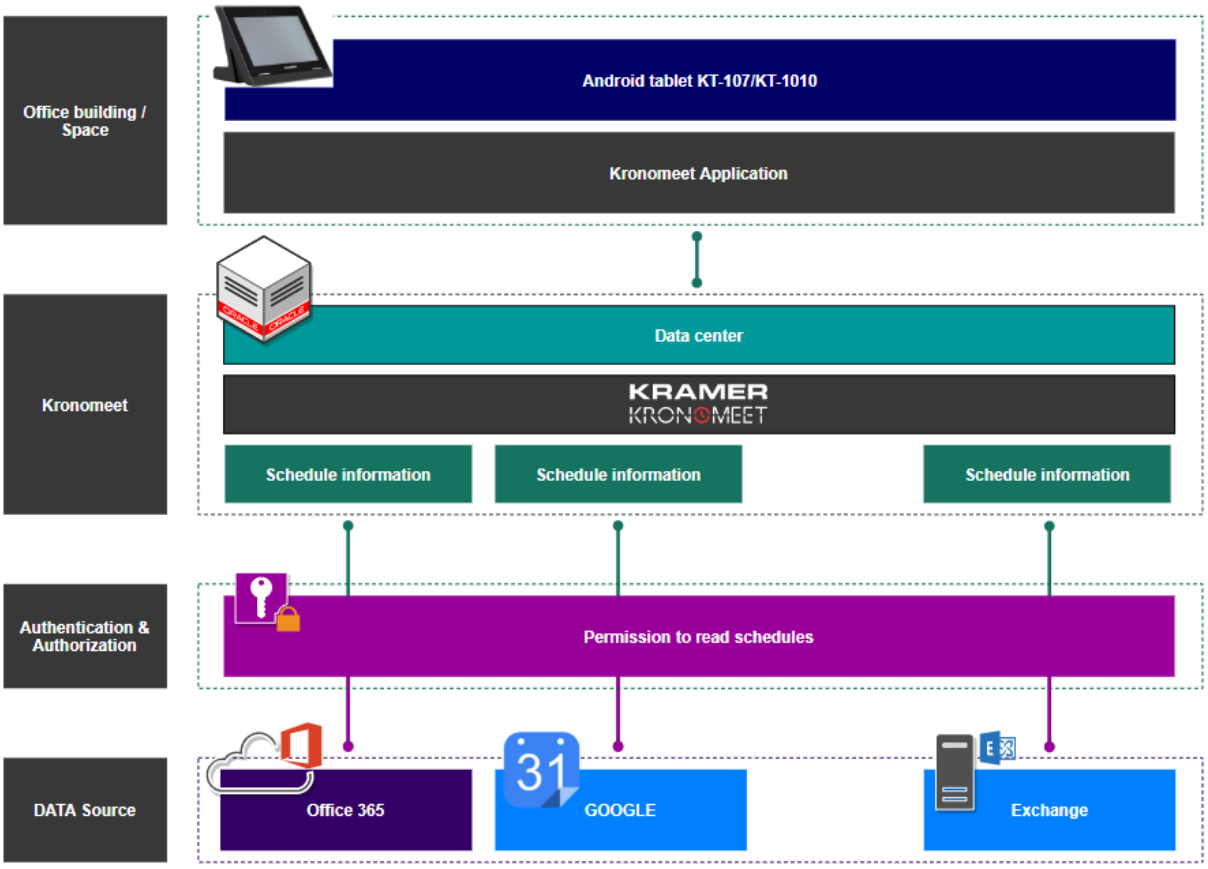

Figure 1: **Kramer KronoMeet** Data Flow Structure

Cloud Data Center

The **Kramer KronoMeet** cloud data center is part of the Oracle cloud space and is designed to tolerate system or hardware failures with minimal client impact to ensure a constant and smooth workflow. All **Kramer KronoMeet** servers are part of the Oracle Cloud Farms in the United States.

Backup Policy

Kramer maintains a high level of operational quality and works to ensure that customers are not impacted by unplanned outages. To do so, Kramer follows a schedule of regular backups that aligns with the Oracle Silver Plan policy to ensure full reliability and data loss protection. The backup schedule is as follows:

- Weekly incremental backups at midnight every Sunday, retained for 4 weeks.
- Monthly incremental backups at midnight on the first day of each month, retained for 12 months.
- Yearly full backups at midnight January 1st, retained for 5 years.

Update policy

Kramer KronoMeet allows administrators to work freely within an up-to-date environment that delivers a familiar browser-based experience for setups. **Kramer KronoMeet** uses an automatic and manual update model to ensure fast and secure updates across the whole data center. Updates are regularly rolled out on a monthly basis. Updates that are flagged as critical may initiate a process that leads to them being rolled out earlier.

Outages

In case of an unplanned outage, Kramer commits to work as fast as possible to restore full access to the data and bound services as well as to processes that may also be affected. Within a 24-hour period, upon the declaration of an outage or a critical data center situation, Kramer commits to return the data center to normal operation.

Security

Kramer is aware of constantly evolving security threats and takes this topic very seriously. We constantly monitor and improve our products, applications, and services. We have developed routines that enable us to meet the growing demands and challenges of security in today's quickly changing environments.

Server Encryption

Kramer KronoMeet services use an exhaustive approach to help ensure the availability, confidentiality, and integrity of your data while keeping it protected from others locally with the Oracle managed key protection system.

Communication Encryption

Kramer KronoMeet services are designed with privacy in mind. The **Kramer KronoMeet** cloud works with encrypted communication only. All data and communication benefit from strong encryption and the supported Hypertext Transfer Protocol Secure (HTTPS). TLS (Transport Layer Security) 1.2 encrypted communication ensures that data in transit is also heavily protected.

- All **Kramer KronoMeet** servers run behind a firewall with only required ports open. All open ports are over TLS 1.2 with certificate level encryption.
- Web communication uses TLS 1.2 encryption with an additional IP blocking mechanism to avoid multithread attacks and more.
- App communication uses TLS 1.2 with an additional security mechanism to ensure stable, reliable, and secure communication. App communication also goes through a middle sever at all times to avoid direct connection to any database or web component. The middle server constantly forwards requests and sends responses back to the initiator.
- **Kramer KronoMeet** does not provide any government with direct or systematic access to customer data.

Ports & Domains

- 5671 – Middle server TLS 1.2 – https://rabbit.kronomeet.com
- 443 – Web portal TLS 1.2 – https://kronomeet.com

Bandwidth

There is a clear need for bandwidth when operating **Kramer KronoMeet** room booking system. Every 2 minutes the system checks or pushes schedules being entered. Further, the system requests the device status such as power state. Each loop consumes a maximum amount of 10kbps. The actual bandwidth needs for an entire organization varies according to the number of devices and event bookings in the organization.

KRAMER

P/N: 2900-301362 Rev: 1

For the latest information on our products and a list of Kramer distributors, visit our website where updates to this user manual may be found.

We welcome your questions, comments, and feedback.

www.KramerAV.com
info@KramerAV.com