# ScreenMeet Architecture and Security

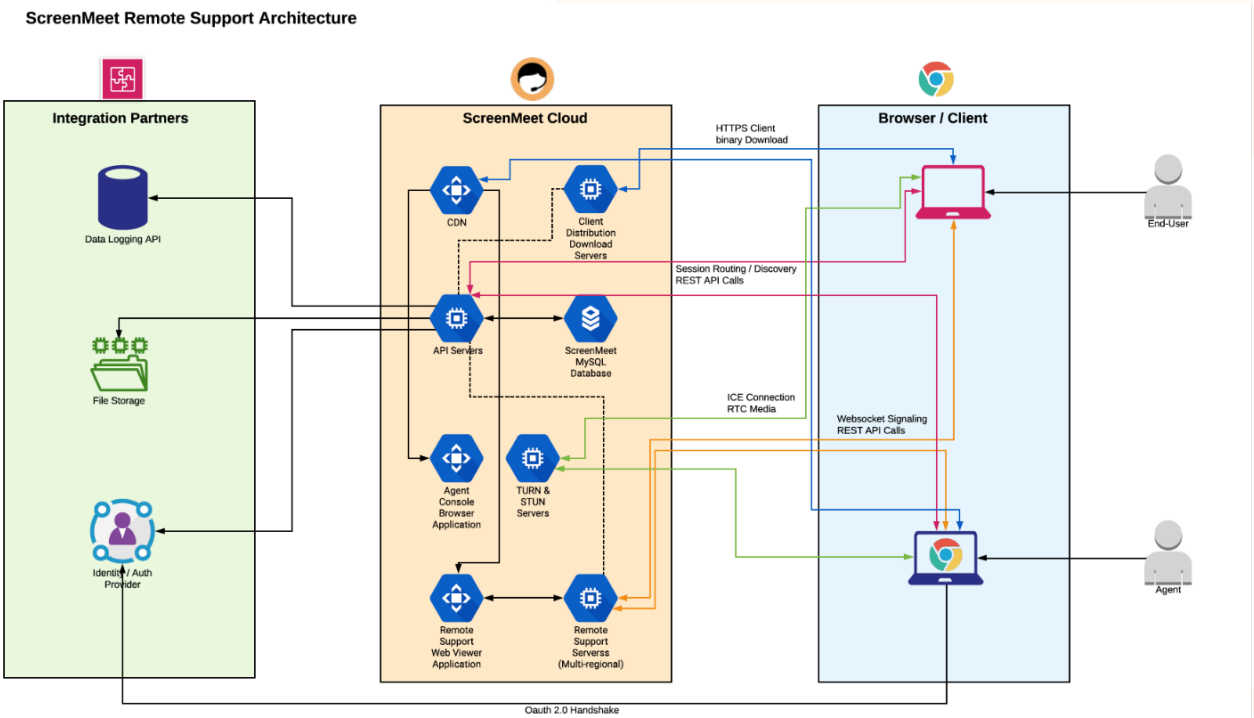
## Overview

ScreenMeet develops and operates real-time audio, video, co-browsing and remote support software that is cloud- native and web-based. Hosted globally at Amazon Web Services (“AWS”) data centers, ScreenMeet directly integrates into leading web-based 3rd party CRM and help desk solutions. With ScreenMeet, support agents from a web browser can see and remote control any web site, device, and any application in real-time over the Internet with the end-user’s consent. The simple and powerful nature of the product means that it saves time and reduces frustration when answering questions and resolving technical issues.

## Architecture

The ScreenMeet platform is fully redundant and globally distributed to ensure optimal performance regardless of geography. The cloud-native architecture ensures 24x7x365 availability as well as high throughput and low latency. The ScreenMeet technical operations team monitors the ScreenMeet platform around the clock to ensure uptime and is proactively alerted of any underlying issues.

As the diagram illustrates, the multi-tiered nature of ScreenMeet ensures high availability in a robust and secure manner.






Last updated December 2024

ScreenMeet

## Security

ScreenMeet makes security the top priority in the design, deployment, and maintenance of our network, platform, and applications. All ScreenMeet internal systems are on private networks requiring IP-based access for trusted Administrators only.

All data transmitted during a ScreenMeet session is encrypted using TLS and DTLS 1.2+. Any sensitive data at rest is AES-256-bit encrypted. All traffic is sent via port 443 for maximum firewall compatibility. This covers all data transmitted from the remote device to our application and from our application the Agent. During a ScreenMeet session, data is temporarily written to memory, then sent to the remote Agent's browser and then deleted. No data is permanently stored or retained on the end user or Agent's Device.

Further, each session is assigned a unique, 1 time key used to bridge the gap between the Agent and the end user. Finally, on PCs, the application auto-deletes after each session so there is no possibility for further access without the end users' consent and intent.

## Authentication

ScreenMeet adheres to your internal password policies. Authentication to ScreenMeet is via OAuth with your existing CRM platform credentials. As part of the integration, ScreenMeet roles are created, and you assign to the users or groups within your CRM to provide access.

## Data Storage

ScreenMeet session data captures no Personally Identifiable Information (PII). However, if session recording, file transfer or screenshot functionality is enabled some PII may be captured depending on what's visible on the screen or the content of the file.

To ensure regulatory compliance, ScreenMeet customers have the option to store associated files in their CRM platform, Amazon S3 Bucket or Azure Blob storage. Based on this approach and the ability to run session in specific geo's, ScreenMeet is able to meet GDPR compliance requirements.

## Firewall/Proxy Compatibility

ScreenMeet works over TCP/UDP Port 443 and "just works" on most networks. In the event you will need to configure your firewalls/proxies, whitelisting *.screenmeet.com and *.scrn.mt for port 443 via TCP and UDP should be sufficient. For more advanced requirements, we offer static IP addresses for whitelisting.

## SOC2 Type 2 and ISO 27001 Certification

ScreenMeet maintains annual SOC2 Type 2 and ISO 27001 certification. We make reports available under NDA to any customer who would like to review them.

## Learn More

For additional information, please visit screenmeet.com, email support@screenmeet.com or visit our documentation page.