Frame Remoting Protocol

Frame Remoting Protocol (FRP) defines the communication between an end user's device with a browser or Frame App and the remote virtual machine running the Frame Guest Agent (FGA).

Frame Remoting Protocol (FRP) 8

Frame Remoting Protocol 8 (FRP8) is the latest remoting protocol for, based on WebRTC. FRP8, by default, uses UDP as its transport layer. FRP8 provides customers with an extensive list of new features that were previously unavailable with FRP7.

Once FRP8 is enabled for a Frame Account, the following features/enhancements become available:

- Improved audio/video synchronization which better adapts to poor network conditions (packet loss, network jitter) by utilizing UDP instead of TCP for transport
- Webcam support
- High-quality microphone redirection from the endpoint device to the session.
- Generic USB Redirection support in Frame App for Windows (requires Frame Virtual USB Driver to be installed on Frame Sandbox/workload VMs) allows local USB devices to be passed into the Frame session using an USB Filter Driver included with Frame App for Windows.
- App Mode 2.0 for Application Launchpads, which delivers a more intuitive user experience by providing a Windows desktop with default lockdowns to the Desktop, Start Menu, Taskbar, Notification Area/System Tray, etc.

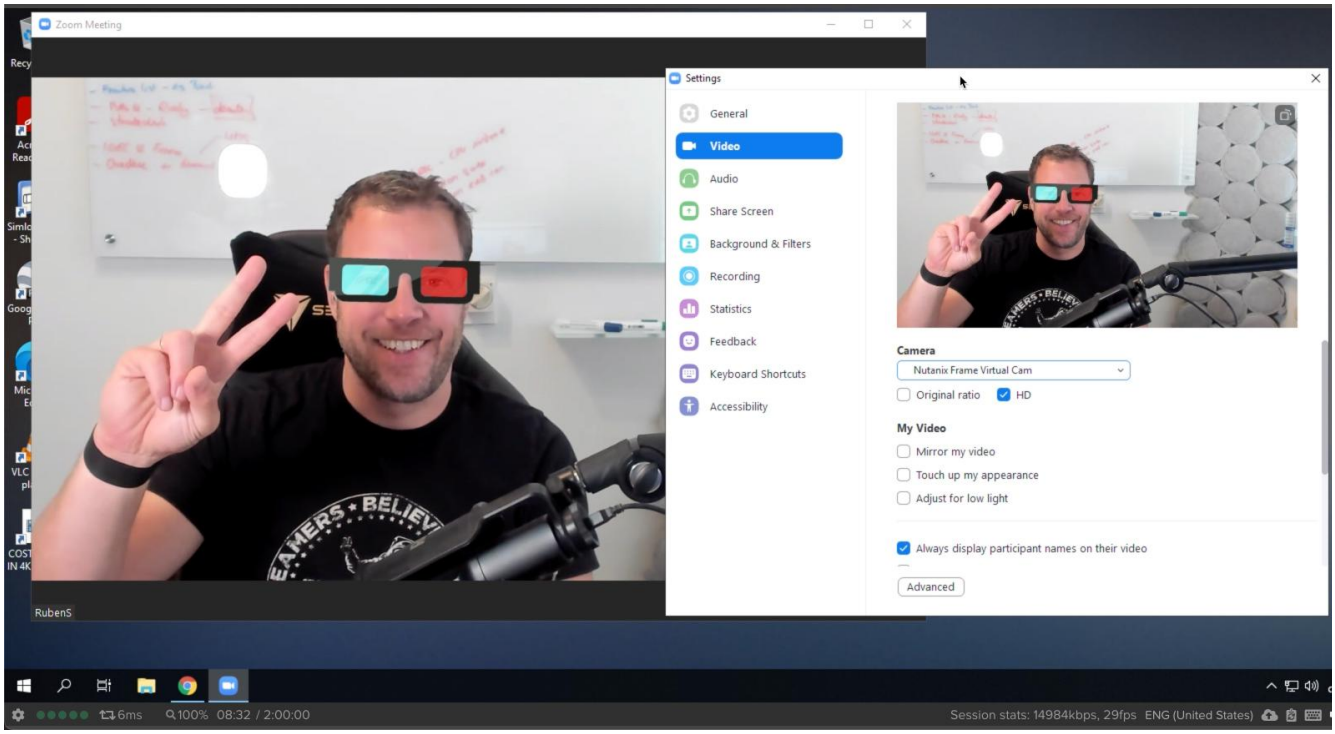
Features

Each new feature of FRP8 is documented below. Administrators may wish to provide their end users with the Session Features End User Guide to understand how they can use these features in a session.

Webcam Support and Microphone Enhancement

FRP8 sessions utilize WebRTC technology, which enables Frame to efficiently capture audio/video data from the endpoint device and stream it to the VM in real time. WebRTC provides a seamless webcam and microphone experience to those using applications such as Zoom, Microsoft Teams, Slack, Google Meet, Cisco Webex, or any other audio/video telephony

solutions running natively within a Frame session.



Frame Session with Zoom

Webcam and microphone support can be enabled by administrators from the Session Settings page in the account's Dashboard. Multiple webcams are supported in the session, end users need simply to select the desired device. End user instructions for these features can be found here.

> **Attention**
> User experience with audio and video-conferencing solutions within a Frame session depends significantly on the networking conditions (bandwidth, latency, packet loss, network jitter, packet shaping, QoS, etc.) between the user and the Frame VM and from the Frame VM to the Internet. POC testing at scale is strongly recommended to ensure satisfactory user experience.

Prerequisites

Use of FRP8 requires the following prerequisites:

- Networking configuration, as described in our Network Requirements documentation for FRP8 and your specific deployment model.
- Use of Frame Guest Agent 8.1 or greater, as discussed in our Frame Guest Agent 8 documentation in all Frame-managed workload VMs (Sandbox, Utility Server, test/production instances).

- OS firewall (e.g., Windows Firewall or third-party firewall) configuration changes to support the required TCP/UDP ports.
- Streaming Gateway Appliance (SGA) 4 or greater (version 3 is being deprecated soon), if required, as discussed in our Streaming Gateway Appliance documentation.

Configuration

Once the prerequisites have been met for FRP8, Administrators can enable FRP8 in Session Settings (Dashboard > Settings > Session).

> If the Frame Account was created in **public cloud using Frame-managed networking** and the FRP8-required ports are not enabled, you will need to first enable the ports and then enable use of FRP8. FRP8 cannot be enabled until the required ports have been opened, as shown in the image above.

Enabling FRP8 on a Frame account using Frame-managed networking results in the following:

- For Frame accounts using public cloud infrastructure:
  - Inbound protocols/ports udp/4503-4509 and tcp/4503-4509 on the workload VPC/VNET and udp/3478 on the SGA VPC/VNET (if SGA is auto-deployed during account creation) are enabled through security group updates.
- FRP 8.0 protocol is enabled for Frame sessions.

For Frame accounts using customer-managed networking (AHV or public cloud), the Frame administrator is responsible for ensuring the required FRP8 network requirements are satisfied before FRP8 is enabled in Session Settings.

Revision #25
Created 1 October 2025 04:53:55
Updated 26 March 2026 14:31:22 by Dominik Conrad