Drovio

WHITEPAPER

Security & Privacy

Last revision: March 15, 2021

Drovio has been designed with security and privacy as a top priority. Based on WebRTC, we leverage a **P2P architecture** to handle customer communications, whether it is for screen sharing, audio chat, file transfer or messaging. The communication between our customer endpoints is end-to-end encrypted and **85% of any screen sharing sessions don't even cross our own servers** (see TURN below): we can't see or hear what you're doing. Also, we only store the minimum information needed to provide the service.

We're working with large businesses and now so well that guaranteeing all of this is sometime not enough, concerns do remain. That's why **we've built a complete on-premises offer** for our most demanding customers that requires no Internet connection and thus no communication whatsoever with our servers. Contact us to learn more and get a quote.

Whether you're interested in our Online (SaaS) or Enterprise (on-premises) offer, what follows may still applies, unless stated otherwise.

Host (Online offer)

The Drovio website, blog and Online services are hosted on Amazon AWS in Oregon (USA). Customer data is stored on AWS RDS (Oregon, USA). Multiple instances are running to form a cluster, ensuring redundancy, load balancing and preventing any outage from happening. Alarms are in place to detect any administrative access (on our Production and Development environments) and increase in traffic, allowing us to deploy more instances within a few clicks.

Encryption

Data in transit

Strong encryption protocols are used for any data transferred between the Drovio clients and the Drovio servers, including TLS 1.2 and SHA2 signatures when it comes to authentication and account management on Drovio Online.

Screen sharing, calls including audio and video, messaging, file transfers and any other data shared between users are done so through P2P connections, using protocols such as DTLS SRTP (UDP version of TLS on top of Secure Real-Time Protocol with AES-128 encryption) for audio/video and DTLS SCTP (Stream Control Transmission Protocol) for data (including mouse, keyboard inputs, text chat, shared files…).

Data at rest

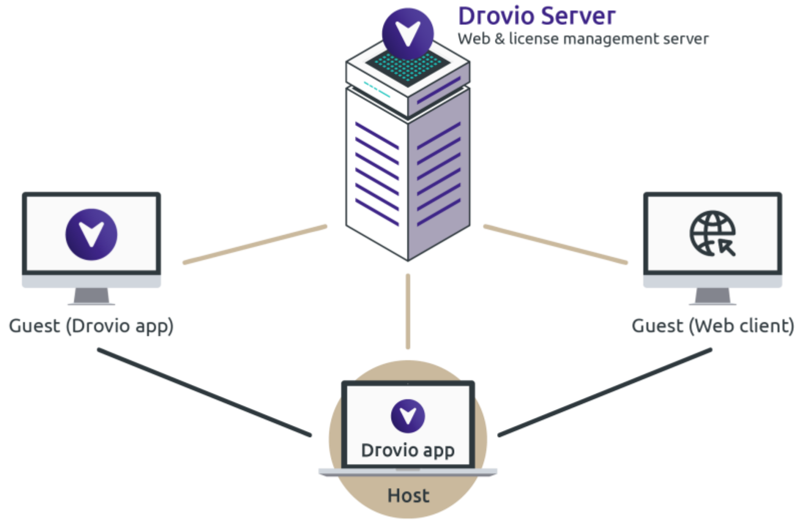
Data at rest is stored on PostgreSQL databases.

Drovio Online uses AWS RDS to securely store customer data using AES-256 encryption on database instances, backups and read replicas.

How Drovio works

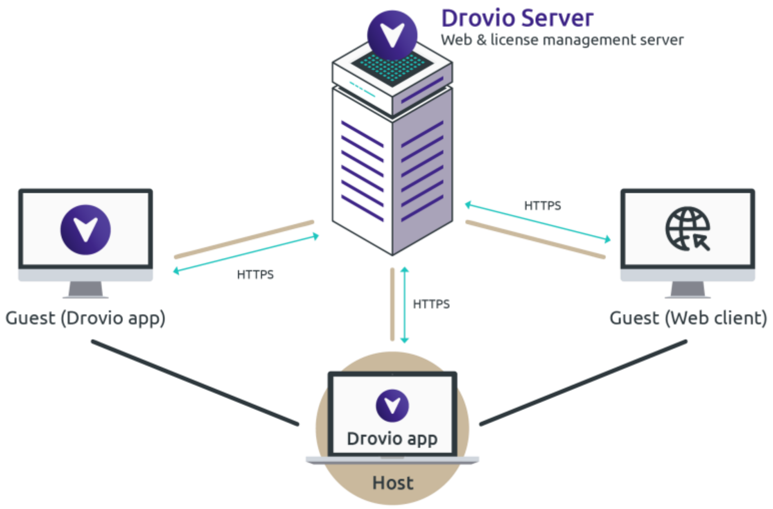
Drovio is based on WebRTC to deliver a stunning fast and low latency experience using the best audio and video encoding technologies such as VP8, VP9 and H.264, while maintaining a highly secure and privacy-aware P2P architecture.

Overview



Drovio comes with a server software Drovio Server (available on our Enterprise offer only) and a client software Drovio (the Drovio app). The solution provides a web client allowing users to join any screen sharing sessions or calls without having to download, install or subscribe to anything. Drovio is based on WebRTC and relies on a P2P architecture.

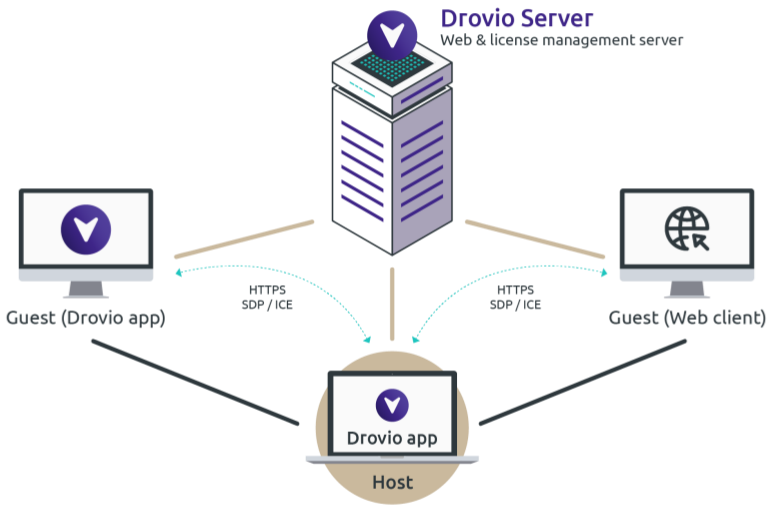
Authentication



Authentication on Drovio operates over HTTPS (TLS v1.2). WebSocket connections are initiated between Drovio Server and the clients to handle the overall signaling process.

Protocol(s)/Port(s): **HTTPS**

Signaling process

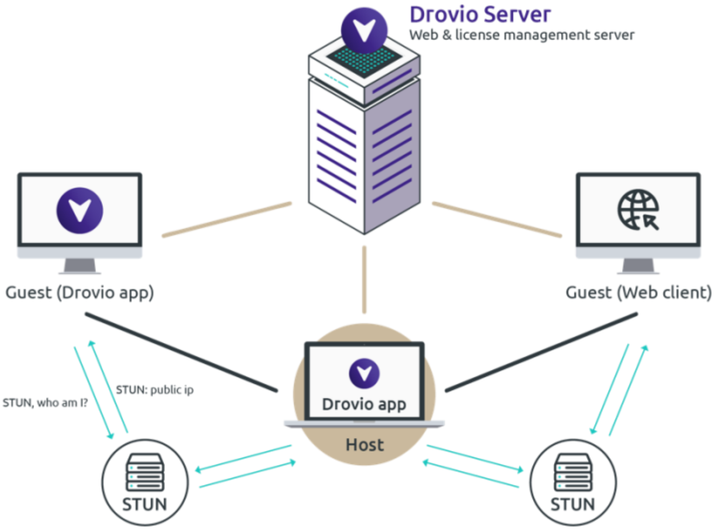


The signaling process, as per the WebRTC terminology, refers to the exchange of streaming media (audio/video codecs) and network capabilities between endpoints (the clients). This operates over WebSocket on Drovio.

To this end, SDP (Session Description Protocol) is employed to enumerate supported streaming media. Meanwhile, available ICE candidates are gathered on each endpoints, referring to a possible IP address, port and transport layer. They are then exchanged, constituting ICE candidate pairs. Multiple ICE candidate pairs will be elected but only one will be selected to ensure the P2P communication (unless an ICE reset occurs, requiring to renegotiate the connection and select another pair: Drovio handles this seamlessly).

Protocol(s)/Port(s): **HTTPS (with WebSocket)**

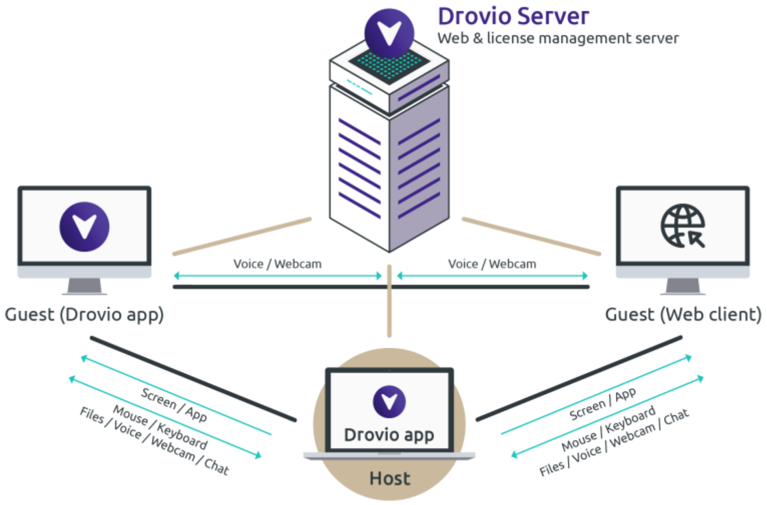
STUN



During the signaling process, clients may use a STUN server (Session Traversal Utilities for NAT) in order to, as the name suggests, cross any NAT. Their unique purpose is to answer the question “what is my public IP?”.

Protocol(s)/Port(s): **UDP 443**

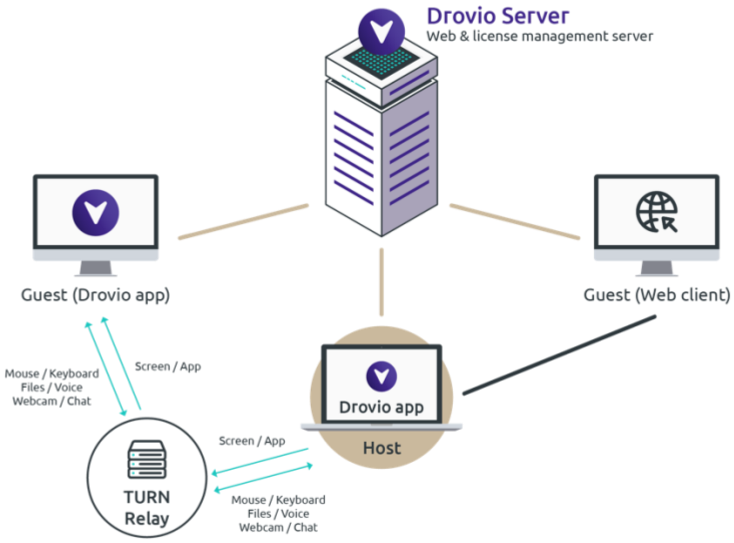
Screen sharing



P2P connections then operate between clients. A live video stream of the host screen or app is sent to the guests, along with any audio stream (microphone or system audio). Guests may share their microphones too and send mouse/keyboard inputs. Drovio Server is not involved during the screen sharing session, except to collect various statistics to improve user experience as described below.

Protocol(s)/Port(s): **DTLS SRTP, DTLS SCTP (UDP 1024-65535, inbound/outbound)**

TURN



When firewalls or NAT rules are too restrictive, direct P2P connections can't be established between clients. Relay servers (TURN for Traversal Using Relays around NAT) are thus used to forward packets from one client to the other. The communication remains end-to-end encrypted, we can't see or hear anything even if we wanted to. On our Online offer, STUN/TURN servers are hosted on AWS and deployed all over the world, used by 15% of all screen sharing sessions. The geographically closest server to a user is used when needed. Those servers are optional with our Enterprise offer, we can help you to deploy your own STUN/TURN servers when screen sharing over the Internet is required.

Protocol(s)/Port(s): **UDP/TCP 443, UDP 49152-65535**

What we store (Online offer)

Service

We only store the minimum customer data needed to deliver the service:

- Email address
- Salted and hashed password or an access token when sign in with Slack or GitHub is used; nothing is stored when using SSO
- Display name

Invoices

When it comes to payment through the Drovio Online service, we also store additional information for invoicing purposes:

- First Name
- Last Name
- Address
- Company Name (optional)
- VAT Number (optional)

We don't store any customer credit card information in our databases. We rely on a PCI-compliant service provider for payment processing, Stripe.

Statistics

In order to constantly improve the user experience and be able to assist you when encountering any issue, we collect some information about the usage being made of our service, including but not limited to:

- Connection events with app version, OS name and version
- Session started and ended events
- New contacts
- Invites to join a session (over email, direct link or from the contact list)
- User has joined/quit (with their already stored email identity when using the integrated client)
- Presenter role swapped
- Connection types (direct, NAT'd or relayed)

We're committed to respect your privacy, that's why we make it a point to only collect basic information that allows us to improve the service.

Network & Endpoint Security

Drovio Production and Development environments are hosted on separate networks that are geographically distant and in data centers that have no direct link between them (AWS for Production and a French datacenter for Development).

Production servers are only publicly accessible when needed and minimal, strictly necessary ranges of ports are opened. We log, monitor and internally audit our environments with alerts in place to indicate any potential intrusion.

We use encryption keys, VPN and/or have 2 factor authentication enabled to access the servers on our Production, whether it houses our customer data or not. Drovio adheres to the least privilege practices and role-based permissions when provisioning access.

The personnel is required to use unique, complex passwords and our approved password manager when possible. Access to the office is protected with a key and a digicode.

Data retention

Customer data is removed upon request. Backups are automatically destroyed within 15 days.

Penetration testing

We do our own internal penetration testing on a quarter basis. We also welcome our customers to do their own tests: our Enterprise offer comes with a free trial period that can be employed to this end.

Security certifications

We don't have any security certifications at the moment but as the company grows, we'll remedy that.

Conclusion

We're committed to protect our customer data. We've designed Drovio from the ground up with this objective in mind, making sure we only handle the bare minimum information needed about our customers to provide the service.

For our most demanding customers that still have high concerns regarding privacy and security, we've built an Enterprise offer (on-premises) letting them deploy the whole solution on their own servers with no Internet connection needed and thus no communication whatsoever with our servers. Contact us to learn more and get a quote.