OneScreen™
Hype

SECURITY OVERVIEW

OneScreen™
by Clary Icon

United States Pakistan Colombia Mexico UAE
www.onescreensolutions.com +1 800-992-5279

OneScreen Hype Security Overview

Meeting Security

- OneScreen Hype uses SSL V1.2 for communication between servers and clients.
- Meeting moderators can remove users from ongoing meetings.
- Meetings will end automatically after a 24 hour timeout.
- All OneScreen Hype meeting executables are digitally signed.
- Meeting attendees can control the audio, video and data they transmit.

Account Security

- Users are protected by unique, and verified email addresses.
- Passwords are stored using secure hash functions, which are irreversible.

Server Security

- Standard Linux security features.

Network Security

- Can be protected by a Linux iptables firewall (default), an external firewall or third party firewall software. Note that third party software may require additional configuration to ensure proper OneScreen Hype server operation.

- OneScreen Hype client initiates an outbound connection to the OneScreen Hype server to establish communication. Clients typically do not need to make any firewall changes, as outbound traffic is generally allowed through firewalls. Desktop and mobile clients have the most robust firewall penetration technology and can communicate over a single TCP port (443 or 80), if that is all that is available. OneScreen Hype automatically selects the optimal firewall traversal method based on available ports. Ports will be used in combination, if they are available, for improved loss and latency performance.

All clients are assumed to have access to the OneScreen Hype (https://hype.claryicon.com) server via:

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- TCP 8081
- TCP 8086

Preferred media port for desktop & mobile clients:

UDP ports are media ports used to send and receive both audios and videos. These ports are selected automatically or they can be specified in a range.

Recommended port openings if hosting OneScreen Hype server behind a firewall.

Inbound Ports:

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- TCP 3001
- TCP 3004
- TCP 5060
- TCP 8081
- TCP 8082
- TCP 8086
- UDP Ports 10000 – 65535

UDP ports are automatically selected or a range can be specified in configuration.

Additional Configuration for SIP Endpoints

The OneScreen Hype server can inter-operate with SIP endpoints.

Calls originate from and terminate at the OneScreen Hype server.

For security, OneScreen Hype recommends that inbound SIP calls should be limited to authorized IP addresses.

Inbound SIP Ports Required:

- UDP Ports 10000 - 65535
- TCP/UDP Port 5060