OneScreen™
Home Screen

SECURITY GUIDE

OneScreen™
by Clary Icon

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

OneScreen Home Screen Security Guide

Account Security

- OneScreen Home Screen servers encrypt all data in transit with AES256 encryption
- Users are protected by unique, verified email addresses.
- Passwords are stored in encrypted form.

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 Home Screen server operation.

- The OneScreen Home Screen client initiates an outbound connection to the OneScreen Home Screen 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 46000), if that is all that is available. OneScreen Home Screen

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. Standard RTSP traffic can be used and inspected by firewalls.

All clients are assumed to have access to the OneScreen Home Screen server via:

- TCP 80 (HTTP)
- TCP 8081
- TCP 8082
- TCP 443 (HTTPS)

Preferred media port for desktop & mobile clients:

- UDP Port 46000

Alternate media ports for desktop & mobile clients:

- TCP Port 46000
- RTSP TCP Port 554
- TCP and UDP Ports 10000 - 65535

Recommended Port Openings If Hosting OneScreen Home Screen server Behind a Firewall

Inbound Ports:

- TCP 80 (HTTP)
- TCP 8081
- TCP 8082
- TCP 443 (HTTPS)
- RTSP TCP Port 554
- UDP Ports 10000 – 65535
- TCP 10000-16000
- TCP Ports 8000 - 65535
- Allow all outbound TCP & UDP traffic

Additional Configuration for H.323 & SIP Endpoints

The OneScreen Home Screen server can inter-operate with H.323 (Feature to be added soon) and SIP endpoints. Calls originate from and terminate at the OneScreen Home Screen server, not the desktop or mobile clients. No additional port openings are required for outbound H.323 & SIP calls. As firewall traversal for H.323 and SIP protocols is not robust, additional firewall configuration at the endpoint location may be required. Contact the device vendor for assistance.

For security, OneScreen Home Screen recommends that inbound H.323 and SIP calls should be limited to authorized IP addresses.

Inbound H.323 Ports Required:

- TCP Port 1720
- UDP Ports 10000 - 65535 Inbound SIP Ports Required:
- TCP/UDP Port 5060
- TCP/UDP Port 5026
- UDP Ports 10000 - 65535