452 Lakeshore Parkway, Suite 210
Rock Hill, SC 29730

+1 803-802-2404

www.bepoz.com

Secure Facility Whitelisting & Network Requirements for ScreenConnect

Purpose of This Document

This document provides the network requirements needed to ensure ScreenConnect (ConnectWise Control) remote access operates reliably in secured, restricted, or highly filtered environments.

Quick Checklist

- ✓ Outbound TCP 443 allowed to ScreenConnect cloud services
- ✓ Outbound WebSocket traffic allowed over TCP 443
- ✓ Allow the following domains and subdomains:
  - *.screenconnect.com
  - *.connectwise.com
  - *.cloud.screenconnect.com
  - *.control.screenconnect.com
  - Relay URI: relay://instance-ceyy1u-relay.screenconnect.com:443/
  - Web Server URI: https://bepoz.screenconnect.com
  - Relay IP: 51.161.144.246
- ✓ SSL inspection bypass highly recommended
- ✓ Ensure DPI/URL filtering does not block WebSocket or long-lived HTTPS sessions

Required Outbound Ports & Protocols

- ✓ TCP 443 outbound (required)
- ✓ TCP 80 outbound (optional fallback)

Required Domains & URLs

452 Lakeshore Parkway, Suite 210
Rock Hill, SC 29730

+1 803-802-2404

www.bepoz.com

- *.screenconnect.com
- *.connectwise.com
- *.cloud.screenconnect.com
- *.control.screenconnect.com

SSL Inspection / DPI Requirements

ScreenConnect relies on WebSockets over TLS. SSL inspection must allow or bypass these connections.

Why Whitelisting Is Required

ScreenConnect uses encrypted outbound connections to cloud relay servers. Whitelisting ensures secure and stable connectivity without requiring inbound rules.

Troubleshooting Indicators

- Sessions disconnecting
- Screen not loading for the technician
- 'Unable to connect to relay server' errors

Contact & Support

Our team can provide region-specific hostnames, IP ranges if required, and assist with testing connectivity. Click here to contact support.