EDR/XDR Firewall Configuration Guide

To ensure proper communication for EDR/XDR systems, please whitelist the following URLs, ports, and protocols in your firewall:

Ports and Protocols

- **HTTP:** 80, 8080
- **HTTPS/WebSocket (wss):** 443
- **DNS Resolution (UDP port 53):** Allowed

URLs to Whitelist

ACS URLs:

- Health Check: https://hh-agent-comm.seqrite.com/v1/agentcommunication/health
- Agent Info: https://hh-agent-comm.seqrite.com/v1/agentcommunication/info
- Telemetry Push: https://hh-agent-comm.seqrite.com/v1/telemetry/push
- Send Data: https://hh-agent-comm.seqrite.com/v1/agentcommunication/senddata-acs
- Fetch Data: https://hh-agent-comm.seqrite.com/v1/agentcommunication/fetchdata
- Upload File: https://hh-agent-comm.seqrite.com/v1/agentcommunication/uploadfile

Firewall Connector URL:

- Event Collector: https://7cqj27igr4.execute-api.ap-south-1.amazonaws.com/ga/edr/v10/event_collector/ingest

HA and XDR URLs:

- Secured CBS: https://cbssecured.seqrite.com
- Device CBS: https://cbsdevice.seqrite.com
- WebSocket URL: https://35bhfv3atb.execute-api.ap-south-1.amazonaws.com
- Quick Heal Update: https://dlupdate.quickheal.com
- Quick Heal Download: https://download.quickheal.com

Additional URLs:

- Notification: https://hh-agent-comm.seqrite.com/agentcommunication/senddata
- Legal Notices: https://account.seqrite.com/cas/qh/footer/en/Legal_notices.html
- OS Licenses: https://hawkkeye.seqrite.com/csm/static/onboarding/qh/footer/en/CAI_openSourceLicense.html
- Privacy Policy: https://www.seqrite.com/privacy-policy
- Terms: https://account.seqrite.com/cas/qh/footer/en/DISCLAIMER_AND_TERMS_CONDITIONS.html)
- Registration API: https://ds1ga-reg.seqrite.com/api/v1/sensor/register
- Registration API v2: https://ds1ga-reg.seqrite.com/api/v2/sensor/register
- Data Submission: https://ds1ga-sub.seqrite.com/api/v1/submitdata

- Renew Token: https://ds1ga-reg.seqrite.com/api/v1/sensor/token
- Host Update: https://ds1ga-reg.seqrite.com/api/v1/sensor/update
- Host Update v2: https://ds1ga-reg.seqrite.com/api/v2/sensor/update
- Offboard: https://ds1ga-reg.seqrite.com/api/v1/sensor/offboard
- Remediation Pull: https://ds1ga-rem.seqrite.com/api/v1/sensor/pull
- Live Query Enroll Node: https://prd-liveq.seqrite.com/livequery/api/v1/enrollnode

Important Notes

To address the issue of devices showing as disconnected on our backend due to web socket traffic being blocked by the customer's firewall, please follow the steps below:

1. **Disable SSL Inspection for the Specified Domain**:

Please configure your firewall to disable SSL inspection for the following URL/domain: `35bhfv3atb.execute-api.ap-south-1.amazonaws.com`. Alternatively, you may install a valid Fortinet CA certificate on the endpoints.

For guidance on how to disable SSL inspection or install the Fortinet CA certificate, refer to the following documentation: Fortinet SSL/TLS Deep Inspection Best Practices.

Without these configurations, you may encounter the error: "x509: certificate signed by unknown authority."

2. **Allow WebSocket Protocol (HTTP Upgrade)**:

Ensure that your firewall allows the WebSocket protocol (HTTP upgrade) for the domain: `35bhfv3atb.execute-api.ap-south-1.amazonaws.com`.

For more information on configuring WebSocket protocol permissions, please refer to: WebSocket Protocol Documentation.

Failure to enable this setting may result in receiving a "403 Forbidden" error.