ExaGrid Secure Remote Support Gateway

The ExaGrid Secure Remote Support Gateway (also referred to as Gateway) is a secure method for ExaGrid Support to access customer ExaGrid servers remotely. The system provides an always-on connection to ExaGrid using industry-standard Transport Layer Security (TLS) and Secure Shell (SSH) protocols. Only ExaGrid support personnel can connect to customer ExaGrid servers.

Connection to ExaGrid Support

Once enabled and configured, the client installed on ExaGrid devices maintains a continuous connection to ExaGrid via TLS 1.2. Upon request from an ExaGrid Support representative, one or more additional outbound connections will be made to facilitate data connection tunnels.

Pinned certificate verification ensures the client will only connect to the system at ExaGrid. Tunnel connections are secured with SSH public key authentication and dynamic firewall rules, ensuring only the requesting support user can gain access.

All connections to ExaGrid are made over TLS and TCP. Outbound connections to port 443 are the only firewall requirement for supporting the client. If port 443 is unavailable, then port 12975 will be used instead. All communications are encrypted using the high security AES-256 cipher.

Security and Authentication

All accesses to customer equipment are logged at ExaGrid. Security configuration at ExaGrid ensures that only valid Support users on the ExaGrid support network may connect to customer systems, and all requests to access customer equipment are logged.

Support user accounts are protected by cryptographically generated two-factor authentication (OATH TOTP), ensuring leaked credentials cannot be used to access customer systems.

Registration

The client connects to ExaGrid using a TCP connection secured with TLS. Server certificates are verified to ensure the client is connecting to only the ExaGrid Remote Support Gateway. Once connected, the client negotiates a Control connection. This is done by providing the following information:

- Registration code (first connection after install only)
- Host key (subsequent connections only)
- SSH public key
- System and site UUID, serial and model numbers, and friendly site name

The client provides a registration code on first connection, or a host key on subsequent connections. The registration code is a single use code that must be typed in upon client installation. The registration code is provided by ExaGrid Support, is time sensitive, and will expire after 20 minutes. Without a valid registration code, the client will not be able to register with the server. The registration code is generated using secure cryptographic algorithms and cannot be practically predicted.

Upon successful initial registration, a host key is provided to the client automatically, which the client will use for all subsequent connections. This key is also generated using cryptographic algorithms.

The client uses SSH public key authentication to ensure all data is protected in transit:

- Client generates a unique keypair on installation
- Upon connection to server, the client public keys, as well as the device's OS public key is sent and recorded by the server
- When requesting access, the Support representative's access tool pushes its public key to the customer device, which then gets registered for temporary SSH access

Combined, these actions ensure only the requesting support representative is given access. Due to the nature of the protocol, all data is encrypted end-to-end, with the Remote Support Gateway having zero knowledge of the contents of the data passed through it.

Keep-Alive Messages

Keep alive messages are sent every 30 seconds from both the server and the client. If no keep alive message is received for two minutes, then the client will close all connections, wait 60 seconds, and open a new connection to the server.

Access Tunnels

Access Tunnels are reverse tunnels set up on-demand between the server at ExaGrid and the customer ExaGrid

ExaGrid Secure Remote Support Gateway

server. These tunnels allow a support user at ExaGrid to open web or shell connections to a customer device. Tunnels are only established when an ExaGrid support user specifically requests access to a customer device.

A support user will first request access to a customer device. If no tunnels are already established to the device, then the server will send a message to the client with the required tunnel connection parameters.

After receiving the message, the client opens a new connection to the server, but negotiates an additional "SSH over TLS" connection. During negotiation, both the TLS certificate and the SSH fingerprint of the server are verified by the client. The server also verifies the client's SSH public key to verify the customer device's authorization to open tunnel connections. The client uses the supplied parameters to negotiate one or more reverse TCP tunnels. Upon successful connection, the server at ExaGrid updates its security profile to allow access to the requesting support user.

The requesting user at ExaGrid support can then access the customer equipment for a limited time. Upon expiration, any tunnels established to customer equipment are automatically shut down, and access controls are updated.

Registration Flow

Client		Server
Connect	---------->	**Accept**
Verify Server Certificate		
Challenge	<---------->	**Response**
Register	<---------->	**Verify**
Send Host Key		Validate host key
Send SSH public key		Record SSH key
	<----------	**Acknowledge or Disconnect**
	<----------	**Send keep-alive messages**

Access Tunnel Flow

Client		Server
	<----------	**Open Tunnel**
New connection	---------->	**Accept**
Verify Server Certificate		Receive Tunnel Challenge
Send Tunnel Challenge		
SSH Negotiation	<---------->	**SSH Negotiation**
Verify server SSH fingerprint		Validate client SSH fingerprint
Set up reverse tunnel		Establish reverse tunnel
Acknowledge or Error	---------->	**Update security rules**

Frequently Asked Questions

Is this secure?

ExaGrid Systems takes security very seriously. The system has been implemented to best-known security practices.

- All communications are encrypted using the industry standard TLS protocol and the AES-256 cipher.
- The client verifies digital signatures, which ensures that it will only connect to the server system at ExaGrid.
- Only clients installed with the assistance of ExaGrid Support can connect to the server system at ExaGrid.
- Access controls at ExaGrid ensure only approved users can access customer devices, and all accesses are tracked.
- The server system is based on a hardened, minimalist configuration
- Server components run in separate, limited accounts, further locked down with per-process mandatory access controls. This ensures even successful remote code execution attacks will be ineffective
- Layered firewall rules ensure only explicitly authorized traffic is allowed, dropping all other traffic

What ports must I open on my firewall?

To make a successful connection, the client requires the ability to open outgoing connections to the server at ExaGrid on TCP port 443. If port 443 is not available, port 12975 can be used. No incoming ports need to be opened on your firewall.

To which system does the client connect?

The client connects to sgw.exagrid.com on either TCP port 443 or 12975, depending upon your network requirements. The port to use will be determined automatically by the client.

Who can access my system?

ExaGrid Support personnel logged in the ExaGrid corporate network can request access to customer devices. Connections can only be made from within the ExaGrid support network, only by users in the correct permissions group, and only after passing two-factor authentication.

ExaGrid Secure Remote Support Gateway

Can I manage this myself?

Yes. Integration with the ExaGrid user interface is included in ExaGrid Software 6.0 and higher. You will need to coordinate with your ExaGrid Support representative, as initialization through the UI requires a time sensitive Registration Code.

Can I use a HTTP proxy?

Yes. The client can connect to the server through HTTP proxy. This can be configured via the ExaGrid user interface.

If your HTTP proxy has an Access Control List configured, please configure it to allow connections to sgw.exagrid.com (port 443 or 12975) from any installed ExaGrid server.

Can I disable access?

Yes. Once the client has been installed and registered, you can enable or disable the client via the ExaGrid user interface.

Can I manually approve or deny access to my ExaGrid server?

Yes. The client can be configured to require your approval before ExaGrid Support can connect to your system. Your ExaGrid support representative can show you how to approve access to your device for the number of hours you specify. Once that period has elapsed, your approval will be required again before a support representative will be able to resume accessing your system.

This feature can be managed through the ExaGrid user interface.

I have a device that intercepts HTTPS connections (i.e., WebSense). Does this require any special configuration settings?

Yes. TLS and SSH certificate pinning ensure the client will only connect to the server at ExaGrid. Devices that intercept TLS traffic replace server certificates in-flight, which will cause connections to the Remote Support Gateway to fail.

If you have a device that intercepts and decrypts TLS traffic, you must configure your device to pass client traffic without modification. ExaGrid recommends placing an exception for traffic going to sgw.exagrid.com, or alternatively any TLS traffic (via ports 443 or 12975) originating from ExaGrid server IP addresses at your site.

Which hashing algorithms and block cipher modes are used?

At the time of this writing, TLS connections are secured with the ECDHE-RSA-AES256-GCM-SHA384 cipher suite. This uses ECDHE for key agreement, AES-256 for encryption, GCM for the block cipher mode, and SHA-384 for hashing and HMAC verification.

Wrapped SSH connections are secured with the AES256-CTR cipher suite. This uses ECDH-SHA2-NISTP256 for key agreement, AES-256 for encryption, CTR for the block cipher mode, and SHA-256 for hashing and HMAC verification.

Due the extensible nature of TLS and SSH, the software can be transparently upgraded to more advanced protocol versions and cryptographic algorithms in the future.

What about TLS 1.3?

TLS 1.3 offers exciting performance, security, and privacy improvements while simplifying the protocol for more error-free deployments. The Remote Support Gateway server components already support TLS 1.3, and we will slowly transition installed customer equipment to using the new protocol via incremental software upgrades over time.

In cases where a firewall or security devices prevent access via TLS 1.3, we will continue to support fallback to TLS 1.2 for some time.