Remote Access FAQ

Published: 2021-08-31

Here are some answers to frequently asked questions about remote access.

What is remote access?

Remote access enables designated ExtraHop teams to connect to an ExtraHop system and provide troubleshooting and configuration help. Remote access is disabled by default; administrators must configure remote access settings on their system before access is allowed.

How is the connection for remote access established and secured?

Remote access is part of ExtraHop Cloud Services. All communication from the ExtraHop system is sent over an encrypted and authenticated HTTPS connection, secured with mutual authentication, TLS 1.2, and perfect forward secrecy, to a dedicated, per-customer cloud-computing instance that is provisioned and maintained by ExtraHop.

Read more about ExtraHop security policies in ExtraHop Security, Privacy and Trust Overview.

How does ExtraHop ensure that only authorized ExtraHop users connect to my system?

ExtraHop authenticates remote access users through two checkpoints managed by independent teams. Each team authenticates the ExtraHop employee account through a SAML SSO provider that requires two-factor authentication.

Who can connect to my system through these remote access groups, what data can they see, and what operations can they perform?

Remote access is disabled by default. The level of access for remote access users is determined by the remote access group and selected privilege level.

Note: Disabling ExtraHop Support remote access on the Reveal(x) 360 User Access page does not disable remote access to the ExtraHop-managed sensors.

Remote Access Group	Users and Privileges
ExtraHop Account Team	ExtraHop Account team members that you specifically add by username with the level of privileges you grant.
ExtraHop Support	ExtraHop Support staff can access your system through the level of privileges you grant: • **ExtraHop System and Administration Access** provides unlimited (or setup user level) access to the system user interfaces through a web browser.

Remote Access Group	Users and Privileges
	• **Remote Shell Access** provides SSH access to the system and should only be selected when requested by ExtraHop Support or Escalations Teams for troubleshooting complex issues. This option requires that you generate and send an encrypted SSH key from the ExtraHop appliance to ExtraHop Support. The SSH key is first decrypted by the ExtraHop IT team and then granted to the Support or Escalations team as needed.
Atlas Analysts	If you have signed up for Atlas Reports, the ExtraHop analysts who provide your reports can access the ExtraHop system with Unlimited system privileges.

Can ExtraHop download packets from my network?

Only the remote access options for **ExtraHop System and Administration Access** and **Remote Shell** enable packet downloads. However, you can also specify packet download privileges for your specified Account Team users.

What operations are recorded in the audit log for remote access?

The audit log records the following types of operations, identified by the specific user or user group:

- Any login attempt
- Changes made in the main user interface
- Changes made in the Administration settings

See the following topic for a list of audit log events.

Note: You cannot see which parts of the system were viewed by a user because the system does not collect that data.

Can I send audit log data from the ExtraHop system to a third-party system?

Yes, you can send audit logs to a remote syslog server.