

Connect to ExtraHop Cloud Services

Published: 2024-05-01

ExtraHop Cloud Services provides access to ExtraHop cloud-based services through an encrypted connection. The services you are connected to are determined by your system license.

After the connection is established, information about the available services appear on the ExtraHop Cloud Services page.

- By sharing data with ExtraHop Machine Learning Service, you can enable features that enhance the ExtraHop system and your user experience.
 - Enable AI Search Assistant to find devices with natural language user prompts, which are shared with ExtraHop Cloud Services for product improvement. See the [AI Search Assistant FAQ](#) for more information. AI Search Assistant cannot currently be enabled for the following regions:
 - Asia Pacific (Singapore, Sydney, Tokyo)
 - Europe (Frankfurt, Paris)
 - Opt in to Expanded Threat Intelligence to enable the Machine Learning Service to review data such as IP addresses and hostnames against threat intelligence provided by CrowdStrike, benign endpoints, and other network traffic information. See the [Expanded Threat Intelligence FAQ](#) for more information.
 - Contribute data such as file hashes and external IP addresses to Collective Threat Analysis to improve the accuracy of detections. See the [Collective Threat Analysis FAQ](#) for more information.
- ExtraHop Update Service enables automatic updates of resources to the ExtraHop system, such as ransomware packages.
- ExtraHop Remote Access enables you to allow ExtraHop account team members and ExtraHop Support to connect to your ExtraHop system for configuration help. See the [Remote Access FAQ](#) for more information about remote access users.

 [View the related training: Connect to ExtraHop Cloud Services](#)

Before you begin

- Reveal(x) 360 systems are automatically connected to ExtraHop Cloud Services, however, you might need to [allow access through network firewalls](#).
- You must apply the relevant license on the ExtraHop system before you can connect to ExtraHop Cloud Services. See the [License FAQ](#) for more information.
- You must have setup or [system and access administration privileges](#) to access Administration settings.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **ExtraHop Cloud Services**.
3. Click **Terms and Conditions** to read the content.
4. Read the terms and conditions, and then select the checkbox.
5. Click **Connect to ExtraHop Cloud Services**.

After you are connected, the page updates to show status and connection information for each service.

6. Optional: In the Machine Learning Service section, select one or more enhanced features:
 - Enable AI Search Assistant by selecting **I agree to enable AI search assistant and send natural language searches to ExtraHop Cloud Services**. (NDR module required)
 - Enable Expanded Threat Intelligence by selecting **I agree to send IP addresses, domain names, hostnames, file hashes, and URLs to ExtraHop Cloud Services**.

- Enable Collective Threat Analysis by selecting **I agree to contribute domain names, hostnames, file hashes, and external IP addresses to ExtraHop Cloud Services.**

If the connection fails, there might be an issue with your firewall rules.

Configure your firewall rules

If your ExtraHop system is deployed in an environment with a firewall, you must open access to ExtraHop Cloud Services. For Reveal(x) 360 systems that are connected to self-managed sensors, you must also open access to the ExtraHop Cloud Recordstore.

Open access to Cloud Services

For access to ExtraHop Cloud Services, your sensors must be able to resolve DNS queries for *.extrahop.com and access TCP 443 (HTTPS) from the IP address that corresponds to your sensor license:

- 35.161.154.247 (Portland, U.S.A.)
- 54.66.242.25 (Sydney, Australia)
- 52.59.110.168 (Frankfurt, Germany)

Open access to Cloud Recordstore

For access to the ExtraHop Cloud Recordstore, your sensors must be able to access outbound TCP 443 (HTTPS) to these fully-qualified domain names:

- bigquery.googleapis.com
- bigquerystorage.googleapis.com
- oauth2.googleapis.com
- www.googleapis.com
- www.mtls.googleapis.com
- iamcredentials.googleapis.com

You can also review the public guidance from Google about [computing possible IP address ranges](#) for googleapis.com.

In addition to configuring access to these domains, you must also configure the [global proxy server settings](#).

Connect to ExtraHop Cloud Services through a proxy

If you do not have a direct internet connection, you can try connecting to ExtraHop Cloud Services through an explicit proxy.

Before you begin

Verify whether your proxy vendor is configured to perform machine-in-the-middle (MITM) when tunneling SSH over HTTP CONNECT to localhost:22. ExtraHop Cloud Services deploys an encrypted inner SSH tunnel, so traffic will not be visible to MITM inspection. We recommend that you create a security exception and disable MITM inspection for this traffic.

- ❗ **Important:** If you are unable to disable MITM on your proxy, you must disable certificate validation in the ExtraHop system running configuration file. For more information, see [Bypass certificate validation](#).

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **Connectivity**.
3. Click **Enable ExtraHop Cloud Proxy**.

4. Type the hostname for your proxy server, such as `proxyhost`.
5. Type the port for your proxy server, such as `8080`.
6. Optional: If required, type a user name and password for your proxy server.
7. Click **Save**.

Bypass certificate validation

Some environments are configured so that encrypted traffic cannot leave the network without inspection by a third-party device. This device can act as an SSL/TLS endpoint that decrypts and re-encrypts the traffic before sending the packets to ExtraHop Cloud Services.

If an appliance is connecting to ExtraHop Cloud Services through a proxy server and the certificate validation fails, disable certificate validation and attempt the connection again. The security provided by ExtraHop system authentication and encryption ensures that communication between appliances and ExtraHop Cloud services cannot be intercepted.



Note: The following procedure requires familiarity with modifying the ExtraHop running configuration file.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Appliance Settings section, click **Running Config**.
3. Click **Edit config**.
4. Add the following line to the end of the running configuration file:

```
"hopcloud": { "verify_outer_tunnel_cert": false }
```

5. Click **Update**.
6. Click **View and Save Changes**.
7. Review the changes and click **Save**.
8. Click **Done**.