Troubleshoot an Atlas connection

Published: 2018-07-16

Atlas Remote Analysis services provide monthly customized reports about your ExtraHop data.

You can establish a connection to the Atlas server from the Admin UI of your ExtraHop Discover appliance. However, if the connection fails, this guide explains how to troubleshoot common connectivity issues.

For information on how to connect to the Atlas server through the Admin UI, see the Atlas section of the ExtraHop Admin UI Guide.

Important: The procedures in this guide require access to the ExtraHop Admin UI and require that you modify the Running Config file. You can view and modify the code in the Running Config file, which specifies the default system configuration and saves changes to the current running configuration so the modified settings are enabled after a system restart. For more information, see the Running Config section of the ExtraHop Admin UI Guide.

Configure your firewall rules

Before you can connect to the Atlas server, you must allow access to the Atlas public IP server through any firewalls.

Connection to the Atlas server requires that your environment meets the following conditions:

- The ability to do a DNS lookup of an *.a.extrahop.com
- The ability to connect to the Atlas server through HTTPS (port 443)

ExtraHop Networks can change the Atlas server IP address at any time, but you can identify the current IP address by selecting from one of the following options:

When connecting from EMEA, run the following command:

```
dig +short atlas-eu.a.extrahop.com
```

When connecting from all other locations, run the following command:

```
dig +short example.a.extrahop.com
```

Connect to Atlas through a proxy

If you want to connect to Atlas services through a proxy, add the following lines to the Running Config file in each ExtraHop system that you want to connect to the Atlas server.

Note: The username and password might be optional for your proxy.

1. Log into the ExtraHop Admin UI.
2. In the System Configuration section, click **Running Config**.
3. Click **Edit config**.
4. Search through the Running Config file to see if an `http_proxy` entry already exists for `atlas`.
   - If the entry already exists, modify the lines to match the example below.
   - If the entry does not exist, add the example lines to the end of the Running Config file.

```
"http_proxy": {
    "atlas": {
```

```
        "host": "proxyhost",
        "port": "8080",
        "username": "username",
        "password": "password"
    }
},
```

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

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, which decrypts and re-encrypts the traffic before sending the packets to the Atlas server .

The ExtraHop appliance cannot connect to the Atlas server, because the certificate validation has failed. To bypass certificate validation and connect to the Atlas server, you must modify the Running Config file.

1. Log into the ExtraHop Admin UI.
2. In the System Configuration section, click **Running Config**.
3. Click **Edit config**.
4. Add the following lines to the end of the Running Config file:

```
"ecm": { "atlas_verify_cert": false }
```

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