Integrate RevealX Enterprise with Netskope

Published: 2025-02-10

This integration enables you to configure one or more ExtraHop sensors to ingest packets from your Netskope solution to detect threats, discover and monitor devices, and gain insight into traffic.

Note: See the blog post "Zero Trust Integration from ExtraHop and Netskope" to learn more about how this integration works.

Enable Netskope packet ingest

You can enable Netskope packet ingest on one or more sensors on the ExtraHop system.

Note: We recommend that you enable this integration on sensors deployed in the same cloud storage type that you configure for Netskope Cloud TAP, which receives packets in Microsoft Azure, Google Cloud Platform (GPS), or Amazon Web Services (AWS).

Before you begin

- You must configure Cloud TAP in your Netskope environment.
- Your user account must have System and Access Administration privileges.
- For each ExtraHop sensor that will ingest Netskope packets:
  - Your ExtraHop sensor must be running firmware version 9.4 or later.
  - Your ExtraHop sensor must be dedicated to ingesting Netskope packets.
  - You must configure at least one interface on your ExtraHop sensor that specifies a mode that includes GENEVE encapsulation.
  - You cannot configure any interfaces on your ExtraHop sensor for Monitoring mode.

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. From the Network Settings section, click **Connectivity**.
4. From the Netskope Settings section, select **Enable Netskope packet ingest**.
5. Click **Save**, and then return to the main page.
6. From the Appliance Settings section, click **Services**.
7. Select **TLS Session Key Receiver**.
8. Click **Save**, and then return to the main page.
9. From the System Configuration section, click **Capture**.
10. Select **Enable SSL Session Key Storage**.
11. Click **Save**, and then return to the main page.
12. From the Appliance Settings section, click **Running Config**.
13. Click **Edit Config**, and then specify the following entries under `netskope_decap`:

```
"ssl_sharing_secret_timeout_msec": 300000,
"ssl_test_agents_connected": true,
"ssl_secret_map_size": 131072,
"ssl_secret_map_max_secrets": 1048576,
"ssl_secret_max_per_bucket": 32,
```

14. Click **Update**.

Next steps

© 2025ExtraHop Networks, Inc. All rights reserved.

- Log into Administration settings on the connected RevealX Enterprise console to check the status of sensors integrated with Netskope.
- From the Assets page, you can search for devices on sensors integrated with Netskope to view traffic and detections observed from the Netskope data.