Connect to Reveal(x) 360 from self-managed sensors

Published: 2024-04-02

This guide provides instructions for connecting Reveal(x) 360 to the self-managed sensors and packetstores that are deployed on-premises or in AWS, Azure, and Google Cloud Platform (GCP) cloud service providers.

Before you begin

- You must have a user account with System Administration or System and Access Administration privileges to configure Reveal(x) 360. See the Reveal(x) 360 Setup and Administration Guide ⬈ to learn how to configure Reveal(x) 360 and create users before completing the steps in this guide.
- You must have a user account with system and access administration privileges on your sensors and packetstores.
- Your sensor and packetstore firmware should be the same firmware version as Reveal(x) 360.
- Your sensor and packetstores must be connected to ExtraHop Cloud Services before connecting to Reveal(x) 360. For more information, see Connect to ExtraHop Cloud Services ⬈.
- You should configure network traffic forwarding to your sensors after the sensors are connected to Reveal(x) 360.
- If you have a firewall, all traffic must be permitted outbound to TCP 443 to connect to ExtraHop Cloud Services and the ExtraHop Cloud Recordstore. For more information, see Configure your firewall rules ⬈.

    Note: For ExtraHop-managed sensors, see Deploy Reveal(x) 360 sensors for AWS ⬈.

    ▶ Video See the related training: Connect to the Reveal(x) 360 Console ⬈

Sensor sizing

When deploying self-managed sensors, consider the following sizing guidelines for allocating vCPUs and memory.

Guidelines

Deployment	Number of vCPUs	RAM (GB)
≤25 sensors AND ≤100K devices receiving Standard or Advanced Analysis	4	8
≤50 sensors AND ≤200K devices receiving Standard or Advanced Analysis	8	16
≤100 sensors AND ≤400K devices receiving Standard or Advanced Analysis	16	32
≤100 sensors AND ≤800K devices receiving Standard or Advanced Analysis	32	64
>100 sensors OR >800K devices receiving Standard or Advanced Analysis	Contact your ExtraHop sales representative	Contact your ExtraHop sales representative

Examples

- If you have 26 sensors and 5K devices receiving Standard or Advanced Analysis, configure the sensor deployment with 8 vCPUs, because this is greater than 25 sensors.

- If you have 7 sensors and 500K devices receiving Standard or Advanced Analysis, configure the sensor deployment with 32 vCPUs, because this is greater than 400K devices, but less than 800K devices.
- If you have 10 sensors and 1M devices receiving Standard or Advanced Analysis, contact your ExtraHop sales representative, because this is greater than 800K devices.

Generate a token

Generate a token for each sensor that you want to connect to Reveal(x) 360.

1. Log in to the Reveal(x) 360 Console.
2. Click the System Settings icon ⚙ at the top right of the page and then click **All Administration**.
3. Click **Sensors** in the left-hand pane.
4. Click **Connect Sensor**.
5. Copy the generated token.

   > **Note:** Each sensor or Trace appliance that you want to connect to Reveal(x) 360 requires a unique token.

6. Click **Done**.

Connect your sensor

1. Log in to the Administration settings on your self-managed sensor through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Console Settings section, click **Connect Console**.
3. Click **Connect Console**.
4. Paste the token you generated from the Reveal(x) 360 Console into the **Generated Token** field.
5. Type a name into the **Sensor Nickname** field to identify this sensor in the Reveal(x) 360 Console.
6. Click **Connect**.

Connect your packetstore

1. Log in to your self-managed packetstore through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Packetstore Cluster Settings section, click **Connect to Reveal(x) 360**.
3. Paste the token you generated from the Reveal(x) 360 Console into the **Generated Token** field.
4. Type a name into the **Packetstore Nickname** field to identify this appliance in the Reveal(x) 360 Console.
5. Click **Connect**.

Connect sensors to your Trace appliance

You must establish a connection from all of your sensors to your packetstores before you can query for packets.

1. Log in to the Administration settings on your self-managed sensor through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Packetstore Settings section, click **Connect Packetstores**.
3. Type the hostname or IP address of the packetstore in the Packetstore hostname field.
4. Click **Pair**.

5. Note the information listed in the Fingerprint field. Verify that the fingerprint listed on this page matches the fingerprint of the packetstore listed on the Fingerprint page in the Administration settings of the packetstore.
6. Type the password of the packetstore `setup` user in the Trace Setup Password field.
7. Click **Connect**.
8. To connect additional packetstores, repeat steps 2 through 7.

> **Note:** You can connect up to 4 packetstores to a sensor.

Test the configuration

Verify that you can view traffic from your connected sensors on the Reveal(x) 360 Console.

1. Log in to the Reveal(x) 360 Console.
2. Click **Dashboards** at the top of the page.
3. In the left pane, under System Dashboards, click **Network**. The charts should display data from the traffic.

> **Note:** It can take up to ten minutes after the traffic session is created before data appears.

Learn more about Reveal(x) 360

After traffic data appears, you can begin exploring Reveal(x) 360. Check out our documentation website ⧉, which includes general concepts ⧉, how-to guides ⧉, and walkthroughs ⧉. For example, you can learn how to create a dashboard ⧉ or activity map ⧉, prioritize the devices on your network for advanced analysis ⧉, and investigate security detections ⧉.