Reveal(x) 360 Setup and Administration Guide

Published: 2021-08-31

After you receive your initial email from ExtraHop Networks, there are a few procedures you must complete before you can start analyzing your traffic. This guide provides procedures for basic setup and administration of the Reveal(x) 360 system.

Activate your Okta administrator account

The Okta administrator role is granted to the email address that you provided during sign up.

1. Open your Welcome to ExtraHop Reveal(x) 360 email.
2. Click **Activate Now**.
   The user setup page appears.
3. Type your desired password in the password fields.
4. Select a forgotten password question from the drop-down list and then type your answer.
5. Select a security image.
6. Click **Create My Account**.
   You are redirected to the Okta User Home page and can begin adding users.

Note: The ExtraHop Okta implementation includes a subset of Okta features. Some features, such as removing users, are not available.

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`
- `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.

Manage Users in ExtraHop Okta

Before users can log in to Reveal(x) 360, the Okta administrator must create users and assign them to groups that determine their privileges.

Here are some important considerations about users and user groups:

- You cannot remove a user. Deactivate the user to remove their ability to access the Reveal(x) 360 system.
- You cannot create your own user groups. You must assign users to the built-in ExtraHop groups.
- You cannot modify the built-in groups.

Note: Optionally, you can configure Reveal(x) 360 to manage users through an existing supported SAML 2.0 identity provider.

Add a user

1. Log in to Okta through https://extrahop-cloud.okta.com with the Okta administrator account credentials.
2. At the top of the user home page, click **Admin**.
3. From the Directory drop-down menu, select **People**.
4. Click **Add Person** and complete all fields. The Secondary email field is optional.
5. In the Groups field, start by typing your customer-specific domain name and select one of the following groups. A user can only be a member of one group.

   Note: Each group is preceded by your customer-specific domain name and customer ID, similar to the following example: `example_company-a001E00001Lfn4LUAR-FullReadOnly-NoPackets`. For more information about privileges, see User privileges.

Privilege	Description
OktaAdmin	Add, activate, deactivate, unlock users, and reset passwords in ExtraHop Okta. Create and modify all objects and settings, including Administration pages in Reveal(x) 360.
ApplianceAdmin	Create and modify all objects and settings, including Administration pages.
FullWrite-NoPackets	Create and modify all objects and settings, excluding Administration pages.
FullWrite-FullPackets	FullWrite privileges, plus view and download packets. Requires Ultra package.
FullWrite-FullPacketsWithKeys	FullWrite privileges, plus view and download packets and any associated stored SSL session keys. Requires Ultra package.
LimitedWrite-NoPackets	Create, modify, and share dashboards.
LimitedWrite-FullPackets	LimitedWrite privileges, plus view and download packets. Requires Ultra package.
LimitedWrite-FullPacketsWithKeys	LimitedWrite privileges, plus view and download packets and any associated stored SSL session keys. Requires Ultra package.
PersonalWrite-FullPackets	Create personal dashboards and modify dashboards shared with the logged-in user, view

Privilege	Description
	and download packets captured through triggers and the ExtraHop Trace Appliance.
PersonalWrite-NoPackets	Create personal dashboards and modify dashboards shared with the logged-in user.
FullReadOnly-NoPackets	View objects in the ExtraHop system.
FullReadOnly-FullPackets	FullReadOnly privileges, plus view and download packets. Requires Ultra package.
RestrictedReadOnly-NoPackets	View dashboards shared with the logged-in user.

6. Select the **Send user activation email now** checkbox.
7. Click **Save**. Alternatively, click **Save and Add Another** to add additional users. The user is sent an activation email with instructions about how to complete their account setup. After the account is set up, the user can log in to Reveal(x) 360 through `https://extrahop-cloud.okta.com` with their email address.

Deactivate a user

You cannot remove a user, but you can deactivate a user to remove their ability to access the Reveal(x) system.

1. In the Okta Admin Console, from the Directory drop-down menu, select **People**.
2. From the More Actions drop-down menu, click **Deactivate**.
3. Select the checkbox next to the name of the user or users you want to deactivate.
4. Click **Deactivate Selected**.
5. In the Deactivate Person dialog box, click **Deactivate**.

Manage sensors

After you have configured your users in Okta, click **My Apps** and then click your Reveal(x) 360 application icon under the Work tab. You are forwarded to your Reveal(x) 360 environment where you can add sensors to monitor your network traffic.

ExtraHop-managed Reveal(x) sensors for AWS can be selected and deployed from within the Reveal(x) 360 Console.

- Deploy Reveal(x) 360 sensors for AWS

Self-managed sensors and Trace appliances can also be connected from within the Reveal(x) 360 Console. Note that if you have an existing Command appliance, you must disconnect the Command appliance before connecting your self-managed sensors to Reveal(x) 360.

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