

Migrate from ExtraHop Okta

Published: 2022-03-15

The following procedures are for the administrators of Reveal(x) 360 systems that are configured with a custom identity provider. You must update your identity provider settings as part of a one-time update to a new authentication service that enables simpler user management.


Update User Access settings

Complete the following steps in the system and then click **Update Now**. There will be a brief outage while your Reveal(x) 360 system is migrated to the new environment. The update can take several minutes to complete. Users will not be able to log in to the system during this time.

Step 1

If your Reveal(x) 360 system is configured with a custom identity provider, you must update the access attributes for System and Access Administration and System Administration users as well as the Entity ID in the SAML settings of your identity provider.

Users assigned the OktaAdmin or Cloud Setup user privilege are automatically assigned the System and Access Administration privilege. Only users with the System and Access Administration privilege can edit user access settings.

1. From the Reveal(x) 360 Overview page, click **System Settings**  and then click **All Administration**.
2. Click **User Access**.
3. In the **System and Access Administration** field, enter an attribute value for this privilege level. The value should be the same as the value you configure on your identity provider.
4. In the **System Administration** field, enter an attribute value for this privilege level. The value should be the same as the value you configure on your identity provider.

Step 2


By default, you are configured for at least one built-in user. We recommend multi-factor authentication (MFA) for all built-in users. Clear the checkbox to remove MFA for built-in users.

Select the Require multi-factor authentication checkbox to require that users who log in through the built-in identity provider configure multi-factor authentication. See the section below on [multi-factor authentication](#) to learn more.

Step 3

You must enter at least one email address.

In the **Email Recipients** field, enter the email address of users you want to receive a notification that the update is complete.

 **Important:** The notification email includes an Entity ID value that you must update in your custom identity provider SAML settings. Users cannot log in to the ExtraHop system through the identity provider until the Entity ID is updated.


Step 4

Select the **I am ready to complete this update** checkbox and then click **Update Now**. During the update, all user sessions on the ExtraHop system are terminated.

Multi-factor authentication

If any existing users are configured for multi-factor authentication, their migrated user account will still be configured for MFA; however, they must reconfigure their authentication app when they log in.

For users that do not have MFA enabled or for users added after migration, we recommend that you enable MFA on their account for increased security.

1. From the Reveal(x) 360 Overview page, click **System Settings**  and then click **Administration**.
2. Click **User Access**.
3. In the Users section, click **View Users**.
4. Click on the name of the user you want to modify MFA settings for.
5. In the Multi-Factor Authentication (MFA) section, select the **Require multi-factor authentication** checkbox.
6. Click **Save**.

The user is prompted to configure MFA when they log in.