Migrate to SAML from LDAP through the Admin UI

Published: 2020-02-24

Secure, single sign-on (SSO) authentication to the Command and Discover appliances is easy to configure. However, if you have configured your ExtraHop appliance for remote authentication through LDAP, TACACS+, or RADIUS, changing to SAML permanently deletes all existing remote users and their customizations, such as saved dashboards, activity maps, reports (for Command appliances), and record queries (for Explore appliances).

Migration is a multi-step process; in each section we provide the steps to safely migrate a single user and their customizations from LDAP to SAML through the Admin UI. If you need to migrate a large volume of remote users with customizations, we strongly recommend that you migrate to SAML through the REST API. If you prefer to engage a turn-key solution for migration, contact your ExtraHop sales representative.

Important: Customizations must be saved from the appliance where remote users have created them. For example, if a remote user has a critical dashboard on a Command appliance and a Discover appliance, you must complete these procedures on both appliances for that remote user.

Procedure overview

Migrating to a new remote authentication method is a complex process. Be sure you understand all of the steps before you begin and be sure to schedule a maintenance window to avoid disrupting users.

Before you begin

1. Enable exception files on your Discover and Command appliances. If the ExtraHop system unexpectedly stops or restarts during the migration process, the exception file is written to disk. The exception file can help ExtraHop Support diagnose the issue that caused the failure.
2. Create a backup of your Discover and Command appliances. Backup files include all users, customizations, and shared settings. Download and store the backup file off-appliance to a local machine.

Because changing the remote authentication method on the appliance effectively deletes all remote users, you must first create a (mirrored) local user for each remote user where you can temporarily transfer customizations and sharing settings. After transferring these settings once, you must configure SAML for the appliance, and then transfer the settings a second time from the local users to the SAML users. Finally, you can delete the temporary local users from the appliance.

Here is an explanation of each step:

1. If you plan on migrating only a select few accounts through the Admin UI, review existing remote user accounts to identify users with customizations that you want to preserve, and identify the user groups that have been given shared permissions to customizations.
2. Create a temporary local user account for each remote user that you want to preserve.
3. (Optional for Explore appliance users) Save record queries created by remote users to the setup user account.
4. Delete remote users and transfer their customizations to the local account.
5. Configure SAML. (All remaining remote users and user groups are deleted along with their customizations.)
6. Create an account for the SAML user on the appliance. After the appliance is configured for SAML, you can create a remote account for your users before they log into the appliance for the first time.
7. Delete the local user account and transfer the customizations again, this time from the temporary local account to the SAML user account. When your SAML users log in for the first time, their customizations will be available.

Identify critical remote users and user groups

Because migration is a time-consuming process through the Admin UI, we recommend that you limit the number of user accounts that you preserve to only those with complex or business critical customizations. In addition, if you have imported LDAP user groups, any dashboards or activity maps shared with those groups will no longer be shared after you configure SAML. While user groups cannot be imported from SAML, you can configure and share customizations with a local user group on the appliance.

- Make a list of remote users with critical dashboards, activity maps, saved record queries (Explore appliance only), and scheduled reports (Command appliance only)
- View LDAP user groups and their shared settings, create a local user group, and then manually share dashboards and activity maps with the local user group after migrating to SAML.

Dashboard associations

You must retrieve information about dashboard ownership and sharing before you configure SAML on your appliance.

Because dashboards are only visible to the users who created them or to users who have shared permissions, we recommend that you complete this step through the REST API.

If you must complete this step through the Admin UI, each remote user must manually share their dashboard with a local user.

Activity map associations

You can retrieve information about activity map ownership and sharing before you configure SAML on your appliance.

All activity maps are visible to users with Unlimited privileges.

1. Log into the ExtraHop appliance with the setup user account, and then click **Assets** at the top of the page.
2. Click **Activity** in the left pane and then click the group of clients, servers, or devices for the protocol you want.
3. Click **Activity Map**, located near the upper right corner of the page.
4. Click the **Load** icon in the upper right corner.
5. Make a note of each activity map owner.
6. Identify the activity map properties and sharing options for each activity map.
   a) Click the name of the activity map.
   b) Click the command menu in the upper right corner and then select **Share**.
   c) Make a note of any users or groups the activity map is shared with.

(Command appliance only) Scheduled report associations

You must retrieve information about scheduled report ownership before you configure SAML on your appliance.

All reports are visible to users with Unlimited privileges.

1. Log into the Command appliance as a user with Unlimited privileges.
2. Click the System Settings icon, and then click **Scheduled Reports**.
3. Identify any scheduled reports that you want to preserve, and note the user listed in the Owners column.

(Explore appliance only) Save record queries

In the following steps, you will learn how to preserve record queries saved by a remote user.

Because saved queries can be accessed by all system users, you can export all saved queries to a bundle and then upload them after migrating to SAML. Imported record queries are assigned to the user that uploads the bundle. (For example, if you import queries from a bundle while logged in as the setup user, all of the queries list setup as the query owner.) After migration, remote users can view the saved record queries and save a copy for themselves.

This procedure must be completed from the Admin UI.

1. Log into the ExtraHop appliance with the setup user account.
2. Click the System Settings icon and then select **Bundles**.
3. From the Bundles page, select **New**.
4. Type a name to identify the bundle.
5. Click the arrow next to Queries in the Contents table and select the checkboxes next to the saved queries you want to export.
6. Click **OK**. The bundle appears in the table on the Bundles page.
7. Select the bundle and click **Download**. The queries are saved to a JSON file.

Next steps
After migration, upload the bundle to restore the saved record queries.

Create a temporary local account

In the following steps, you will learn how to create a local user account as a mirror of a remote user account.

We recommend that you create a local username that appends _local to the existing remote username. For example, for LDAP user `john_smith`, create a local user named `john_smith_local`.

1. Log into the Admin UI on the ExtraHop appliance.
2. In the Access Settings section, click **Users**.
3. Click **Add User**.
4. In the Personal Information section, type the following information:
   a) Login ID: The username that for the temporary users, which cannot contain any spaces.
   b) Full Name: A display name for the user, which can contain spaces.
   c) Password: The password for this account.
   d) Confirm Password: Re-type the password from the Password field.
5. In the Authentication Type section, select **Local**.
6. In the User Type section, select the type of privileges for the user.
7. Click Save.

Delete remote users and transfer customizations

In the Admin UI, this step calls for a specific delete-user procedure, which includes the option to transfer ownership for a single user account. This option is best if you only have a few user customizations that must be preserved. Note that in the REST API, you must transfer each customization first, and then delete the user separately. If you delete all users by switching the remote authentication method to SAML, ownership cannot be transferred.)

In the following steps, you will learn how to transfer customizations to the temporary local account you created while deleting the related remote user.

1. Log into the Admin UI on the ExtraHop appliance.
2. In the Access Settings section, click **Users**.
3. Scroll to the remote user you want to delete and click the **X** to the far right.

a) An option appears to transfer dashboards and activity maps. (On a Command appliance, you can also transfer scheduled reports in this step.)

4. Select **Transfer dashboards, activity maps, and scheduled reports owned by a to the following user** *<remote user>* and then select the temporary local user account you created. For example, when deleting remote user `john_smith` you can transfer customizations to local user `john_smith_local`.
5. Repeat for each user whose customizations you want to preserve.

Configure SAML on the appliance

Depending on your environment, configure SAML. Guides are available for both Okta and Google. After you configure SAML on your ExtraHop appliance, you are able to create accounts on the appliance for your remote users, and transfer their customizations before they log in for the first time.

Create SAML accounts on the appliance

In the following steps, you will learn how to create a SAML user on the appliance.

Note: Verify the required format for usernames that are entered in the Login ID field with the administrator of your Identity Provider. If the usernames do not match, the remote user will not be matched to the user created on the appliance.

1. Log into the Admin UI on the ExtraHop appliance.
2. In the Access Settings section, click **Users**.
3. Click **Add User**.
4. In the Login ID field, type the SAML username. (SAML usernames are case-sensitive.)
5. In the Full Name field, type the first and last name of the user.
6. In the Authentication Type section, select **Remote**.
7. Click **Save**.
8. Repeat for each user whose customizations you want to preserve.

Delete local users and transfer customizations

In the following steps, you will learn how to delete the temporary local user accounts that are storing remote user customizations and transfer the customizations to the final SAML user accounts.

1. Log into the Admin UI on the ExtraHop appliance.
2. In the Access Settings section, click **Users**.
3. Scroll to the local user you want to delete and click the **X** to the far right.
   a) An option appears to transfer dashboards and activity maps. (On a Command appliance, you can also transfer scheduled reports in this step.)
4. Select **Transfer dashboards, activity maps, and scheduled reports owned by a to the following user** *<local user>* and then select the SAML user account you created. For example, when deleting local user `john_smith_local` you can transfer customizations to SAML user `johnsmith`.
5. Repeat for each user whose customizations you want to preserve.