Users and user groups

Published: 2018-11-29

Users can access the ExtraHop appliance in three ways: through a set of pre-configured user accounts, through local user accounts configured on the appliance, or through remote user accounts configured on existing authentication servers, such as LDAP, Radius, and TACACS+.

If you are providing users access from an LDAP server, you can also import and manage the members of an existing user group.

Local users

This topic is about default and local accounts. See Remote Authentication to learn how to configure remote accounts.

The following accounts are configured by default on ExtraHop appliances but do not appear in the list of names on the Users page. These accounts cannot be deleted and you must change the default password upon initial login.

setup

This account provides full system read and write privileges on the Web UI, Admin UI, and Shell, which is the ExtraHop command-line interface (CLI). On physical appliances, the default password for this account is the service tag number on the front of the appliance. On virtual appliances, the default password is `default`.

shell

The `shell` account, by default, has access to non-administrative shell commands in the ExtraHop CLI. On physical appliances, the default password for this account is the service tag number on the front of the appliance. On virtual appliances, the default password is `default`.

Note: The default ExtraHop password for either account when deployed in Amazon Web Services (AWS) is the string of numbers after the -i in the instance ID.

Next steps

- Add a local user account

Remote Authentication

ExtraHop appliances supports remote authentication for user authentication. Remote authentication enables organizations that have authentication systems such as LDAP (such as OpenLDAP or Active Directory), RADIUS, or TACACS+ to enable all or a subset of their users to log on to the appliance with their existing credentials.

Centralized authentication provides the following benefits:

- User password synchronization.
- Automatic creation of ExtraHop accounts for users without administrator intervention.
- Management of ExtraHop privileges based on LDAP groups.
- Administrators can grant access to all known users or restrict access by applying LDAP filters.

Next steps

- Configure remote authentication through LDAP
- Configure remote authentication through TACACS+
- Configure remote authentication through RADIUS

User groups

On Discover and Command appliances, the User Groups page provides controls to view, enable, and disable user groups that are imported from a configured LDAP server. User groups allow for easier sharing of dashboards to all members in the group. Only remote user accounts and groups can be members of remote user groups.

Remote user groups are automatically discovered in the distinguished name (DN) specified as part of the remote authentication settings. See the Remote Authentication section about configuring LDAP authentication.

After you enable LDAP user groups through the remote authentication settings, the following user group properties appear in the table:

Group Name

Displays the name of the remote LDAP group. To view the members in the group, click the group name.

Members

Displays the number of users in the group that are associated with a dashboard and that have logged into the ExtraHop Discover or Command appliance.

Associations

Displays the number of dashboards that are shared with the group.

Status

Displays whether the group is enabled or disabled on the appliance. When the status is `Disabled`, the user group is considered empty when performing membership checks; however, the user group can still be specified when sharing a dashboard.

Last Refresh

Displays the amount of time elapsed since the group membership was refreshed. User groups are refreshed under the following conditions:

- Once per hour, by default. The refresh interval setting can be modified on the **Remote Authentication** > **LDAP Settings** page.
- An administrator refreshes a group by clicking **Refresh All User Groups** or selecting a specific user group and clicking **Refresh Users in Group**. You can refresh a group from the User Group page or from within the Member List page.
- A remote user logs into the ExtraHop Web UI or Admin UI for the first time.
- A user attempts to load a shared dashboard that they do not have access to.

Reset a user group

When you reset a user group, all shared dashboard associations are removed from the group. If the group no longer exists on the remote LDAP server, the group is removed from the user group list.

Select one or more user groups in the list and click **Reset User Groups**.

Enable or disable a user group

You can share custom dashboards with a remote user group so that every member of the group can view the associated dashboard. If a user group is disabled, no group member can view the associated dashboard, even if the dashboard is still shared with the group.

Select one or more user groups in the list and click **Disable User Groups**.

User privileges

Administrators determine the level of access and functionality users have with the ExtraHop Web and Admin UIs. In addition to setting the privilege level for the user, you can add certain options that can apply to any user privilege level.

For information about user privileges for the REST API, see the REST API Guide.

Privilege Levels

Set the privilege level for your user to determine which areas of the ExtraHop appliance they can access.

	Unlimited	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
Activity Maps						
Create, view, and load shared activity maps	Y	Y	Y	Y	Y	N
Save activity maps	Y	Y	Y	Y	N	N
Share activity maps	Y	Y	Y	N	N	N
Alerts						
View alert history	Y	Y	Y	Y	Y	N
Create and modify alerts	Y	Y	N	N	N	N
Custom Pages						
Create and modify custom pages	Y	Y	N	N	N	N
Dashboards						
View and organize dashboards	Y	Y	Y	Y	Y	Y
Create and modify dashboards	Y	Y	Y	Y	N	N
Share dashboards	Y	Y	Y	N	N	N
Detections	**Note:** Detections require a connection to the cloud-based ExtraHop Machine Learning Service.					
View detections	Y	Y	Y	Y	Y	N

and provide feedback						
Analysis Priorities						
View Analysis Priorities page	Y	Y	Y	Y	Y	N
Add and modify analysis levels for groups	Y	Y	N	N	N	N
Add devices to a watchlist	Y	Y	N	N	N	N
Transfer priorities management	Y	Y	N	N	N	N
Device Groups						
Create and modify device groups	Y	Y	N	N	N	N
Metrics						
View metrics	Y	Y	Y	Y	Y	N
Records (Explore appliance)						
View record queries	Y	Y	Y	Y	Y	N
View record formats	Y	Y	Y	Y	Y	N
Create, modify, and save record queries	Y	Y	N	N	N	N
Create, modify, and save record formats	Y	Y	N	N	N	N
Scheduled Reports (Command appliance)						
Create, view, and manage	Y	Y	Y	N	N	N

scheduled reports						
Triggers						
Create and modify triggers	Y	Y	N	N	N	N
Administrative Privileges						
Access the ExtraHop Admin UI	Y	N	N	N	N	N
Connect to other appliances	Y	N	N	N	N	N
Manage other appliances (Command appliance)	Y	N	N	N	N	N

Privilege Options

The following privilege options can be assigned to users with any privilege level.

- View and download packets
- View and download packets and session keys
- View connected appliances (Command appliance only)