Users and user groups

Published: 2024-04-02

Users can access the ExtraHop system 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, SAML, Radius, and TACACS+.

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 systems 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 to the browser-based user interface and to the ExtraHop command-line interface (CLI). On physical sensors, the default password for this account is the service tag number on the front of the appliance. On virtual sensors, the default password is `default`.

shell

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

Note: The default ExtraHop password for either account when deployed in Amazon Web Services (AWS) and Google Cloud Platform (GCP) is the instance ID of the virtual machine.

Next steps

- Add a local user account

Remote Authentication

The ExtraHop system supports remote authentication for user access. Remote authentication enables organizations that have authentication systems such as LDAP (OpenLDAP or Active Directory, for example) to enable all or a subset of their users to log in to the system 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 user 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 SAML
- Configure remote authentication through TACACS+
- Configure remote authentication through RADIUS

Remote users

If your ExtraHop system is configured for SAML or LDAP remote authentication, you can create an account for those remote users. Preconfiguring accounts on the ExtraHop system for remote users enables you to share system customizations with those users before they log in.

If you choose to auto-provision users when you configure SAML authentication, then the user is automatically added to the list of local users when they log in for the first time. However, you can create a remote SAML user account on the ExtraHop system when you want to provision a remote user before that user has logged in to the system. Privileges are assigned to the user by the provider. After the user is created, you can add them to local user groups.

Next steps

- Add an account for a remote user

User groups

User groups enable you to manage access to shared content by group instead of by individual user. Customized objects such as activity maps can be shared with a user group, and any user who is added to the group automatically has access. You can create a local user group—which can include remote and local users. Alternatively, if your ExtraHop system is configured for remote authentication through LDAP, you can configure settings to import your LDAP user groups.

- Click **Create User Group** to create a local group. The user group appears in the list. Then, select the checkbox next to the user group name and select users from the **Filter users...** drop-down list. Click **Add Users to Group**.
- (LDAP only) Click **Refresh All User Groups** or select multiple LDAP user groups and click **Refresh Users in Groups**.
- Click **Reset User Group** to remove all shared content from a selected user group. If the group no longer exists on the remote LDAP server, the group is removed from the user group list.
- Click **Enable User Group** or **Disable User Group** to control whether any group member can access shared content for the selected user group.
- Click **Delete User Group** to remove the selected user group from the system.
- View the following properties for listed user groups:

  Group Name

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

  Type

  Displays Local or Remote as the type of user group.

  Members

  Displays the number of users in the group.

  Shared Content

  Displays the number of user-created objects that are shared with the group.

  Status

  Displays whether the group is enabled or disabled on the system. 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 content.

  Members Refreshed (LDAP only)

  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 **Refresh Users in Group**, or programmatically through the REST API. You can refresh a group from the User Group page or from within the Member List page.
- A remote user logs in to the ExtraHop system for the first time.
- A user attempts to load a shared dashboard that they do not have access to.

User privileges

Administrators determine the module access level for users in the ExtraHop system.

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

For information about remote user privileges, see the configuration guides for LDAP, RADIUS, SAML, and TACACS+.

Privilege Levels

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

Module Access privileges

These privileges determine the features that users can access in the ExtraHop system. Administrators can grant users role-based access to one or all of the NDR, NPM, and Packet Forensics modules. A module license is required to access module features.

Network Detection and Response (NDR)

Allows the user to access security features such as attack detections, investigations, and threat briefings.

Network Performance and Monitoring (NPM)

Allows the user to access performance features such as operations detections and the ability to create custom dashboards.

Packet Forensics

Allows the user to view and download packets and session keys, packets only, or packet slices only.

System Access privileges

These privileges determine the level of functionality users have within the modules where they have been granted access.

For Reveal(x) Enterprise, users with system access and administration privileges can access all features, packets, and session keys for their licensed modules.

For Reveal(x) 360, system access and administration privileges, access to licensed modules, packets, and session keys must be assigned separately. Reveal(x) 360 also offers an additional System Administration account that grants full system privileges except for the ability to manage users and API access.

The following table contains ExtraHop features and their required privileges. If no module requirement is noted, the feature is available in both the NDR and NDM modules.

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
Activity Maps							
Create, view, and	Y	Y	Y	Y	Y	Y	N

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
load shared activity maps							
Save activity maps	Y	Y	Y	Y	Y	N	N
Share activity maps	Y	Y	Y	Y	N	N	N
Alerts	NPM module license and access required.						
View alerts	Y	Y	Y	Y	Y	Y	Y
Create and modify alerts	Y	Y	Y	N	N	N	N
Analysis Priorities							
View Analysis Priorities page	Y	Y	Y	Y	Y	Y	N
Add and modify analysis levels for groups	Y	Y	Y	N	N	N	N
Add devices to a watchlist	Y	Y	Y	N	N	N	N
Transfer priorities management	Y	Y	Y	N	N	N	N
Bundles							
Create a bundle	Y	Y	Y	N	N	N	N
Upload and apply a bundle	Y	Y	Y	N	N	N	N
View list of bundles	Y	Y	Y	Y	Y	Y	N
Dashboards	NPM module license and access required to create and modify dashboards.						

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
View and organize dashboards	Y	Y	Y	Y	Y	Y	Y
Create and modify dashboards	Y	Y	Y	Y	Y	N	N
Share dashboards	Y	Y	Y	Y	N	N	N
Detections	NDR module license and access required to view and tune security detections and create investigations. NPM module license and access required to view and tune performance detections.						
View detections	Y	Y	Y	Y	Y	Y	Y
Acknowledge Detections	Y	Y	Y	Y	Y	N	N
Modify detection status and notes	Y	Y	Y	Y	N	N	N
Create and modify investigations	Y	Y	Y	Y	N	N	N
Create and modify tuning rules	Y	Y	Y	N	N	N	N
Device Groups	Administrators can configure the Device Group Edit Control global policy to specify whether users with limited write privileges can create and edit device groups.						
Create and modify device groups	Y	Y	Y	Y (If the global privilege policy is enabled)	N	N	N
Metrics							
View metrics	Y	Y	Y	Y	Y	Y	N
Notification Rules	NDR module license and access required to create and modify notifications for security detections and threat briefings. NPM module license and access required to create and modify notifications for performance detections.						
Create and modify	Y	Y	Y	N	N	N	N

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
detection notification rules							
Create and modify threat briefing notification rules	Y	Y	Y	N	N	N	N
Create and modify system notification rules (Reveal(x) only)	Y	Y	N	N	N	N	N
Records	Recordstore required.						
View record queries	Y	Y	Y	Y	Y	Y	N
View record formats	Y	Y	Y	Y	Y	Y	N
Create, modify, and save record queries	Y	Y	Y	N	N	N	N
Create, modify, and save record formats	Y	Y	Y	N	N	N	N
Dashboard Reports	Console required.						
Create, view, and manage scheduled reports	Y	Y	Y	Y	N	N	N
Threat Intelligence	NDR module license and access required.						
Manage threat collections	Y	Y	N	N	N	N	N

	System and Access Administrati	System Administrati (Reveal(x) 360 only)	Full Write	Limited Write	Personal Write	Full Read-Only	Restricted Read-Only
View threat intelligence information	Y	Y	Y	Y	Y	Y	N
Triggers							
Create and modify triggers	Y	Y	Y	N	N	N	N
Administrative Privileges							
Access the ExtraHop Administration settings	Y	Y	N	N	N	N	N
Connect to other appliances	Y	Y	N	N	N	N	N
Manage other appliances (Console)	Y	Y	N	N	N	N	N
Manage users and API access	Y	N	N	N	N	N	N