Configure remote authentication through LDAP

Published: 2021-08-28

The ExtraHop system supports the Lightweight Directory Access Protocol (LDAP) for authentication and authorization. Instead of storing user credentials locally, you can configure your ExtraHop system to authenticate users remotely with an existing LDAP server. Note that ExtraHop LDAP authentication only queries for user accounts; it does not query for any other entities that might be in the LDAP directory.

Before you begin

- This procedure requires familiarity with configuring LDAP.
- Ensure that each user is in a permission-specific group on the LDAP server before beginning this procedure.
- If you want to configure nested LDAP groups, you must modify the Running Configuration file. Contact ExtraHop Support for help.

When a user attempts to log onto an ExtraHop system, the ExtraHop system tries to authenticate the user in the following ways:

- Attempts to authenticate the user locally.
- Attempts to authenticate the user through the LDAP server if the user does not exist locally and if the ExtraHop system is configured for remote authentication with LDAP.
- Logs the user onto the ExtraHop system if the user exists and the password is validated either locally or through LDAP. The LDAP password is not stored locally on the ExtraHop system. Note that you must enter the username and password in the format that your LDAP server is configured for. The ExtraHop system only forwards the information to the LDAP server.
- If the user does not exist or an incorrect password is entered, an error message appears on the login page.

> **Important:** If you change LDAP authentication at a later time to a different remote authentication method, the users, user groups, and associated customizations that were created through remote authentication are removed. Local users are unaffected.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **Remote Authentication**.
3. From the Remote authentication method drop-down list, select **LDAP** and then click **Continue**.
4. On the LDAP Settings page, complete the following server information fields:
   a) In the Hostname field, type the hostname or IP address of the LDAP server. If you are configuring a hostname, make sure that the DNS entry of the ExtraHop system is properly configured.
   b) In the Port field, type the port number on which the LDAP server is listening.
   c) From the Server Type drop-down list, select **Posix** or **Active Directory**.
   d) Optional: In the Bind DN field, type the bind DN. The bind DN is the user credentials that allow you to authenticate with the LDAP server to perform the user search. The bind DN must have list access to the base DN and any OU, groups, or user account required for LDAP authentication. If this value is not set, then an anonymous bind is performed. Note that anonymous binds are not enabled on all LDAP servers.
   e) Optional: In the Bind Password field, type the bind password. The bind password is the password required when authenticating with the LDAP server as the bind DN specified above. If you are configuring an anonymous bind, leave this field blank. In some cases, an unauthenticated bind is possible, where you supply a Bind DN value but no bind password. Consult your LDAP administrator for the proper settings.
   f) From the Encryption drop-down list, select one of the following encryption options.

- **None:** This options specifies cleartext TCP sockets. All passwords are sent across the network in cleartext in this mode.
- **LDAPS:** This option specifies LDAP wrapped inside SSL.
- **StartTLS:** This option specifies TLS LDAP. (SSL is negotiated before any passwords are sent.)

g) Select **Validate SSL Certificates** to enable certificate validation. If you select this option, the certificate on the remote endpoint is validated against the root certificates as specified by the trusted certificates manager. You must configure which certificates you want to trust on the Trusted Certificates page. For more information, see Add a trusted certificate to your ExtraHop system.

h) Type a time value in the Refresh Interval field or leave the default setting of 1 hour. The refresh interval ensures that any changes made to user or group access on the LDAP server are updated on the ExtraHop system.

5. Configure the following user settings:

a) Type the base DN in the Base DN field. The Base DN is the point from where a server will search for users. The base DN must contain all user accounts that will have access to the ExtraHop system. The users can be direct members of the base DN or nested within an OU within the base DN if the **Whole Subtree** option is selected for the Search Scope specified below.

b) Type a search filter in the Search Filter field. Search filters enable you to define search criteria when searching the LDAP directory for user accounts.

Important: The ExtraHop system automatically adds parentheses to wrap the filter and will not parse this parameter correctly if you add parentheses manually. Add your search filters in this step and in step 5b, similar to the following example:

```
cn=atlas*
|(cn=EH-*)(cn=IT-*)
```

In addition, if your group names include the asterisk (*) character, the asterisk must be escaped as `\2a`. For example, if your group has a CN called `test*group`, type `cn=test\2agroup` in the Search Filter field.

c) From the Search Scope drop-down list, select one of the following options. Search scope specifies the scope of the directory search when looking for user entities.

- **Whole subtree:** This option looks recursively under the group DN for matching users.
- **Single level:** This option looks for users that exist in the base DN only; not any subtrees.

6. Optional: Import user groups. Select the **Import user groups from LDAP server** checkbox and configure the following settings.

Note: Importing LDAP user groups enables you to share dashboards with those groups. The imported groups appear on the User Group page in the Administration settings.

a) Type the base DN in the Base DN field. The Base DN is the point from where a server will search for user groups. The base DN must contain all user groups that will have access to the ExtraHop system. The user groups can be direct members of the base DN or nested within an OU within the base DN if the **Whole Subtree** option is selected for the Search Scope specified below.

b) Type a search filter in the Search Filter field. Search filters enable you to define search criteria when searching the LDAP directory for user groups.

Important: For group search filters, the ExtraHop system implicitly filters on the objectclass=group, and so objectclass=group should not be added to this filter.

c) From the Search Scope drop-down list, select one of the following options. Search scope specifies the scope of the directory search when looking for user group entities.

- **Whole subtree:** This option looks recursively under the base DN for matching user groups.
- **Single level:** This option looks for user groups that exist in the base DN; not any subtrees.

7. Click **Test Settings**. If the test succeeds, a status message appears near the bottom of the page. If the test fails, click **Show details** to see a list of errors. You must resolve any errors before you continue.
8. Click **Save and Continue**.

Next steps
Configure user privileges for remote authentication

Configure user privileges for remote authentication

You can assign user privileges to individual users on your ExtraHop system or configure and manage privileges through your LDAP server.

When assigning user privileges through LDAP, you must complete at least one of the available user privilege fields. These fields require groups (not organizational units) that are pre-specified on your LDAP server. A user account with access must be a direct member of a specified group. User accounts that are not a member of a group specified above will not have access. Groups that are not present are not authenticated on the ExtraHop system.

The ExtraHop system supports both Active Directory and POSIX group memberships. For Active Directory, `memberOf` is supported. For POSIX, `memberuid`, `posixGroups`, `groupofNames`, and `groupofuniqueNames` are supported.

1. Choose one of the following options from the Privilege assignment options drop-down list:
   - **Obtain privileges level from remote server**

     This option assigns privileges through your remote authentication server. You must complete at least one of the following distinguished name (DN) fields.

     • **Unlimited DN:** Create and modify all objects and settings on the ExtraHop system, including Administration settings.

     • **Full Write DN:** Create and modify objects on the ExtraHop system, not including Administration settings.

     • **Limited Write DN:** Create, modify, and share dashboards.

     • **Personal Write DN:** Create personal dashboards and modify dashboards shared with the logged-in user.

     • **Connected Appliances DN:** (Visible only on the Command appliance.) View a list of ExtraHop systems that are connected to the Command appliance.

     • **Full read-only DN:** View objects in the ExtraHop system.

     • **Restricted Read-only DN:** View dashboards shared with the logged-in user.

     • **Packet Access DN:** View and download packets captured through the ExtraHop Trace appliance.

     • **Packet and Session Keys Access DN:** View and download packets and any associated SSL session keys captured through the ExtraHop Trace appliance.

     • **Detections Access DN:** View, acknowledge, and hide detections that appear in the ExtraHop system.
   - **Remote users have full write access**

     This option grants remote users full write access to the ExtraHop system. In addition, you can grant additional access for packet downloads, SSL session keys, and detections.
   - **Remote users have full read-only access**

     This option grants remote users read-only access to the ExtraHop system. In addition, you can grant additional access for packet downloads, SSL session keys, and detections.
   - **Remote users can view connected appliances (Deprecated)**

This option, which only appears on the Command appliance, grants remote users log in access to the Administration page on the Command appliance to view any connected Discover, Explore, and Trace appliances. Note that this privilege is deprecated and will be unavailable in a future release.

2. Optional: Configure packet and session key access. Select one of the following options to allow remote users to download packet captures and SSL session keys.
   - **No access**
   - **Packets only**
   - **Packets and session keys**
3. Optional: Configure detections access. Select one of the following options to allow remote users to view detections. This setting is visible only when the global privilege policy for detections access control is set to **Only specified users can view detections**.
   - **No access**
   - **Full access**
4. Click **Save and Finish**.
5. Click **Done**.