

Configure remote authentication through TACACS+

Published: 2024-04-02

The ExtraHop system supports Terminal Access Controller Access-Control System Plus (TACACS+) for remote authentication and authorization.

Ensure that each user to be remotely authorized has the [ExtraHop service configured on the TACACS+ server](#) before beginning this procedure.

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 **TACACS+**, and then click **Continue**.
4. On the Add TACACS+ Server page, type the following information:
 - **Host:** The hostname or IP address of the TACACS+ server. Make sure that the DNS of the ExtraHop system is properly configured if you are entering a hostname.
 - **Secret:** The shared secret between the ExtraHop system and the TACACS+ server. Contact your TACACS+ administrator to obtain the shared secret.



Note: The secret cannot include the number sign (#).

- **Timeout:** The amount of time in seconds that the ExtraHop system waits for a response from the TACACS+ server before attempting to connect again.
5. Click **Add Server**.
 6. Optional: Add additional servers as needed.
 7. Click **Save and Finish**.
 8. From the Permission assignment options drop-down list, choose one of the following options:
 - **Obtain privileges level from remote server**

This option allows remote users to obtain privilege levels from the remote server. You must also configure permissions on the TACACS+ server.
 - **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, NDR module access, and NPM module access.
 - **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, NDR module access, and NPM module access.
 9. 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**
 - **Packet slices only**
 - **Packets only**
 - **Packets and session keys**
 10. Optional: Configure NDR and NPM module access.
 - **No access**
 - **Full access**

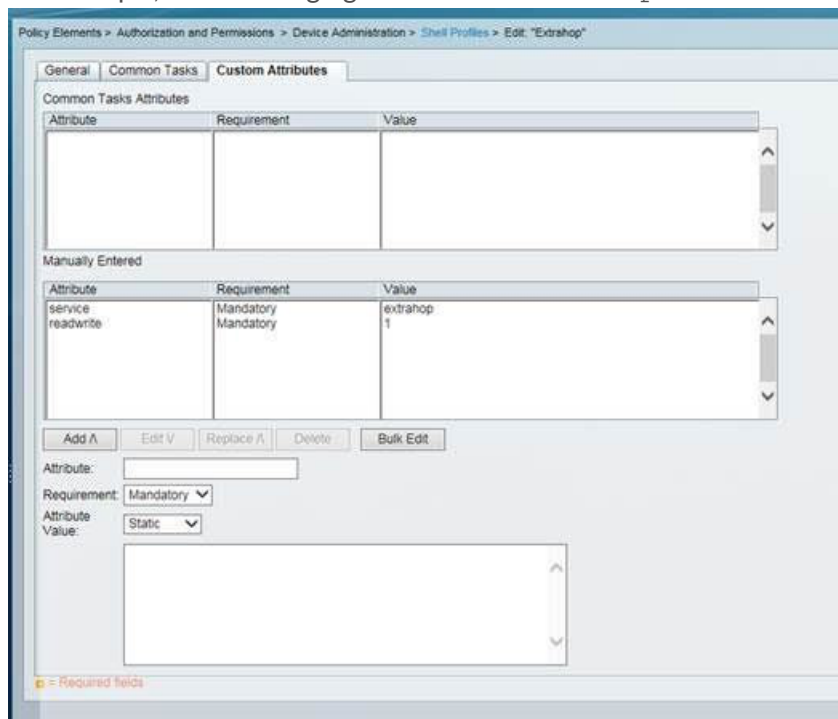
11. Click **Save and Finish**.
12. Click **Done**.

Configure the TACACS+ server

In addition to configuring remote authentication on your ExtraHop system, you must configure your TACACS+ server with two attributes, one for the ExtraHop service and one for the permission level. If you have an ExtraHop packetstore, you can optionally add a third attribute for packet capture and session key logging.

1. Log in to your TACACS+ server and navigate to the shell profile for your ExtraHop configuration.
2. For the first attribute, add `service`.
3. For the first value, add `extrahop`.
4. For the second attribute, add the privilege level, such as `readwrite`.
5. For the second value, add `1`.

For example, the following figure shows the `extrahop` attribute and a privilege level of `readwrite`.



Here is a table of available permission attributes, values, and descriptions:

Attribute	Value	Description
setup	1	Create and modify all objects and settings on the ExtraHop system and manage user access
readwrite	1	Create and modify all objects and settings on the ExtraHop system, not including Administration settings
limited	1	Create, modify, and share dashboards

Attribute	Value	Description
readonly	1	View objects in the ExtraHop system
personal	1	Create personal dashboards for themselves and modify any dashboards that have been shared with them
limited_metrics	1	View shared dashboards
ndrfull	1	View, acknowledge, and hide security detections
npmfull	1	View, acknowledge, and hide performance detections
packetsfull	1	View and download packets stored on a connected packetstore.
packetslicesonly	1	View and download packet slices on a connected packetstore.
packetsfullwithkeys	1	View and download packets and associated session keys stored on a connected packetstore.

6. Optional: Add the following attribute to allow users to view, acknowledge, and hide security detections

Attribute	Value
ndrfull	1

7. Optional: Add the following attribute to allow users to view, acknowledge, and hide performance detections that appear in the ExtraHop system.

Attribute	Value
npmfull	1

8. Optional: If you have an ExtraHop packetstore, add an attribute to allow users to download packet captures or packet captures with associated session keys.

Attribute	Value	Description
packetslicesonly	1	Users with any privilege level can view and download the first 64 bytes of packets.
packetsfull	1	Users with any privilege level can view and download packets stored on a connected packetstore.
packetslicesonly	1	View and download packet slices on a connected packetstore.

Attribute	Value	Description
packetsfullwithkeys	1	Users with any privilege level can view and download packets and associated session keys stored on a connected packetstore.