Configure remote authentication through TACACS+

Published: 2021-08-31

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, 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.
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**
   - **Packets only**
   - **Packets and session keys**

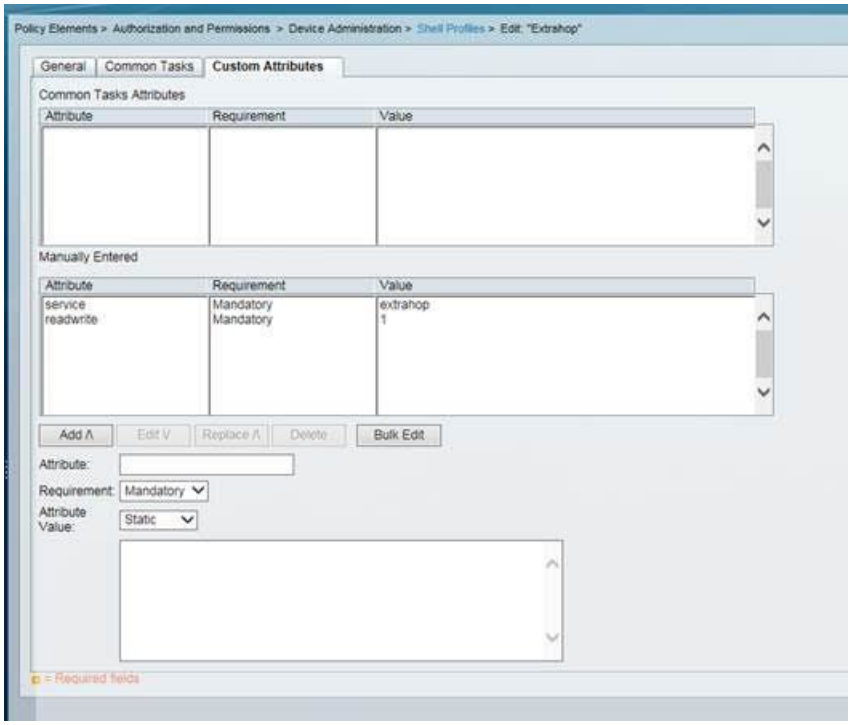
10. Optional: Configure detections access. Select one of the following options to allow remote users to view detections. This setting is visible only when the global privilege policy for detections access control is set to **Only specified users can view detections**.
    - **No access**
    - **Full access**
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 a Trace appliance, 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 list of available permission attributes, values, and descriptions:

- `setup = 1`, which allows the user to create and modify all objects and settings on the ExtraHop system, including Administration settings
- `readwrite = 1`, which allows the user to create and modify all objects and settings on the ExtraHop system, not including Administration settings
- `limited = 1`, which allows the user to create, modify, and share dashboards
- `readonly = 1`, which allows the user to view objects in the ExtraHop system
- `personal = 1`, which allows the user to create dashboards for themselves and modify any dashboards that have been shared with them

- `limited_metrics = 1`, which allows the user to view shared dashboards

6. Optional: Add the following attribute to allow users to view, acknowledge, and hide detections that appear in the ExtraHop system.
   - `detectionsaccessfull = 1`
7. Optional: If you have a Trace appliance, add an attribute to allow users to download packet captures or packet captures with associated session keys.

   Here is a list of the available packet capture attributes and values:

   - `packetsfull = 1`, which allows users with any privilege level to view and download packets
   - `packetsfullwithkeys = 1`, which allows users with any privilege level to view and download packets and associated session keys stored on the Trace appliance