Configure remote authentication through TACACS+

Published: 2018-11-09

The ExtraHop appliance 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. In the Access Settings section, click **Remote Authentication**.
2. In the Methods section, select **TACACS+** from the Remote authentication method drop-down, then click **Continue**.
3. 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 appliance is properly configured if you are entering a hostname.

   • Secret**:** The shared secret between the ExtraHop appliance and the TACACS+ server. Contact your TACACS+ administrator to obtain the shared secret.

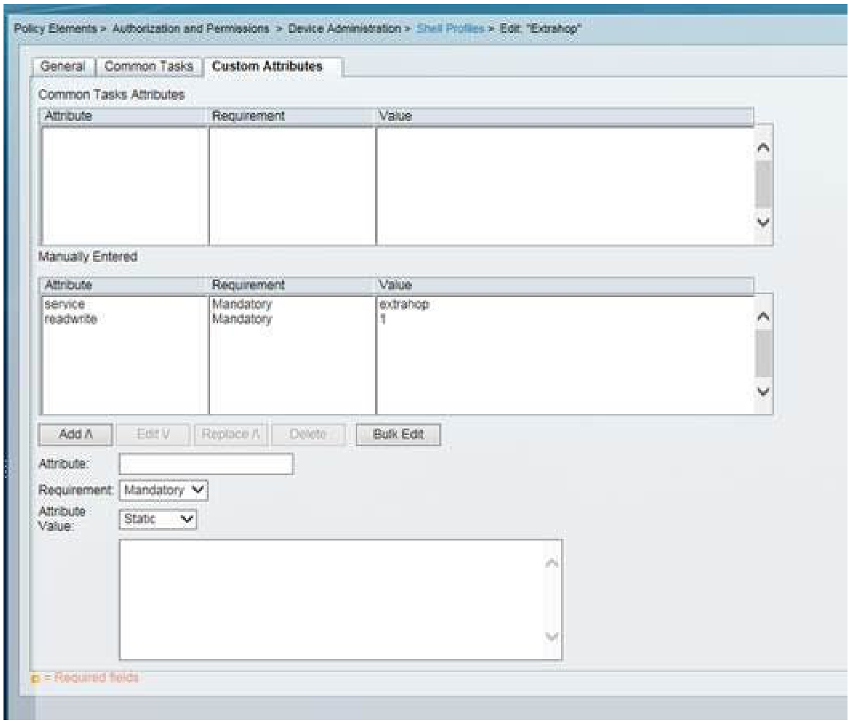
   • Timeout**:** The amount of time in seconds that the ExtraHop appliance waits for a response from the TACACS+ server before attempting to connect again.
4. Click **Add Server**.
5. Optional: Add additional servers as needed.
6. Click **Save and Finish**.
7. Choose one of the following options from the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

     This option allows remote users to obtain permission levels from the remote server.

     You must also configure the TACACS+ server with two attributes, one for the ExtraHop service and one for the permission level.

     1. For the Attribute, add `service`.
     2. For the Value, add `extrahop`.
     3. For the Attribute, add the permission level, such as `readwrite`.
     4. For the Value, add `1`.

For example, the following figure shows a configured permission level of `readwrite`.


Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "Extrahop"
General
Common Tasks
Custom Attributes
Add ∧
Edit ∨
Replace ∧
Delete
Bulk Edit
= Required fields

Common Tasks Attributes

Attribute	Requirement	Value

Manually Entered

Attribute	Requirement	Value
service	Mandatory	extrahop
readwrite	Mandatory	1

Attribute:

Requirement: Mandatory

Attribute Value: Static

The following list shows the different permission levels and the access they provide to users.

- `setup = 1`, which allows the user to create and modify all objects and settings on the ExtraHop Web UI and Admin UI
- `readwrite = 1`, which allows the user to create and modify all objects and settings on the ExtraHop Web UI
- `limited = 1`, which allows the user to create, modify, and share dashboards
- `readonly = 1`, which allows the user to view objects in the ExtraHop Web UI
- `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
- `packetsfull = 1`, which allows the user to view and download packets for any of the above user permission levels

- **Remote users have full write access**

  This option allows remote users to have full write access to the ExtraHop Web UI.

- **Remote users have full read-only access**

  This option allows remote users to have read-only permissions to the ExtraHop Web UI.

  Note: You can add read-write permissions on a per-user basis later through the Users page in the Admin UI.

- **Remote users have command cluster access**

  This option, which only appears on the Command appliance, allows remote users to log into the Admin UI on the Command appliance and view any connected Discover, Explore, and Trace appliances.

8. Optional: To allow remote users to view and download packet captures, select the Remote users can view and download packets checkbox.
9. Click **Save and Finish**.
10. Click **Done**.