Configure remote authentication through RADIUS

Published: 2019-02-10

The ExtraHop appliance supports Remote Authentication Dial In User Service (RADIUS) for remote authentication and local authorization only. For remote authentication, the ExtraHop appliance supports unencrypted RADIUS and plaintext formats.

1. In the Access Settings section, click **Remote Authentication**.
2. Select **RADIUS** from the Remote authentication method drop-down, then click **Continue**.
3. On the Add RADIUS Server page, type the following information:

   Host

   The hostname or IP address of the RADIUS server. Make sure that the DNS of the ExtraHop appliance is properly configured if you specify a hostname.

   Secret

   The shared secret between the ExtraHop appliance and the RADIUS server. Contact your RADIUS administrator to obtain the shared secret.

   Timeout

   The amount of time in seconds that the ExtraHop appliance waits for a response from the RADIUS server before attempting the connection 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:
   - **Remote users have full write access**

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