Configure remote authentication through RADIUS

Published: 2020-06-08

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. Log in to the Administration page 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 **RADIUS** and then click **Continue**.
4. 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.
5. Click **Add Server**.
6. Optional: Add additional servers as needed.
7. Click **Save and Finish**.
8. From the Privilege assignment options drop-down list, choose one of the following options:
   - **Remote users have full write access**

     This option grants remote users full write access to the ExtraHop Web UI. 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 Web UI. In addition, you can grant additional access for packet downloads, SSL session keys, and detections.
   - **Remote users can view connected appliances**

     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.
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**.