How to Enable Integration with Barracuda XDR

https://campus.barracuda.com/doc/98207840/

The Barracuda CloudGen Firewall allows administrators to stream relevant security events to the Barracuda XDR platform to detect and provide an incident response to malicious events. A 24x7 SOC Team streamlines responses to incidence, which reduces the damage of the attack. For more information on the Barracuda XDR solution, please refer to:
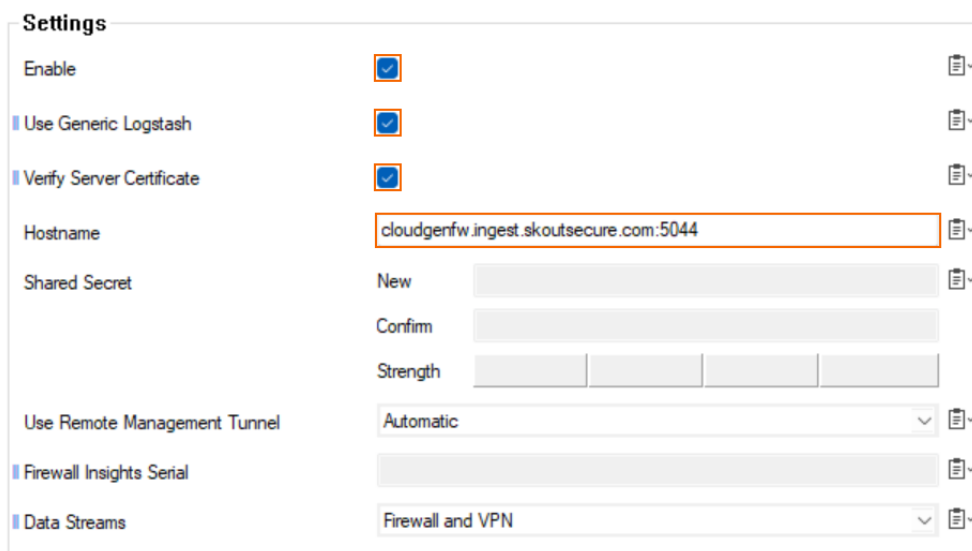https://barracudamsp.com/product-details/extended-detection-and-response-xdr/

Streaming events to Barracuda XDR requires a Firewall Insights subscription assigned to the box. The license is provided by the Barracuda XDR team.

> When using Barracuda XDR with CloudGen Firewall firmware 8.3.1, you must install hotfix 1088. Please reach out to Barracuda Networks Technical Support to receive the custom hotfix.

Enable Streaming to Barracuda XDR Platform for Standalone Firewalls

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, click **Firewall Insights**.
3. Expand the **Configuration Mode** menu and select **Switch to Advanced**.
4. Click **Lock**.
5. Enable the service and select **Use Generic Logstash**.
6. Enable **Verify Server Certificate**.
7. In the **Hostname** field, enter the endpoint FQDN:
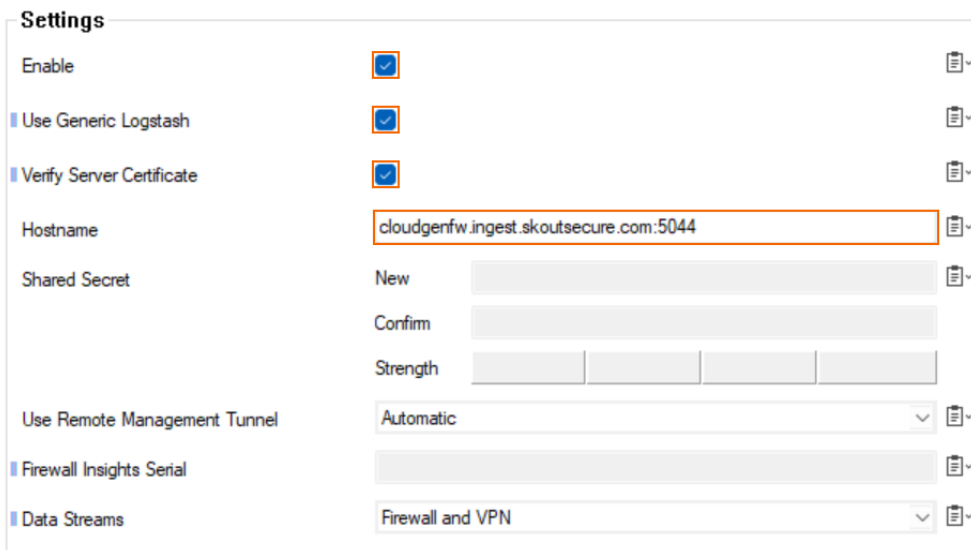   cloudgenfw.ingest.skoutsecure.com:5044

8. Click **Send Changes** and **Activate**.

Enable Streaming to Barracuda XDR Platform for Managed Firewalls

1. Go to **CONFIGURATION > Configuration Tree > Range > Cluster > Boxes > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, click **Firewall Insights**.
3. Expand the **Configuration Mode** menu and select **Switch to Advanced**.
4. Click **Lock**.
5. Enable the service and select **Use Generic Logstash**.
6. Enable **Verify Server Certificate**.
7. In the **Hostname** field, enter the endpoint FQDN: `cloudgenfw.ingest.skoutsecure.com:5044`

8. Set **Use Remote Management Tunnel** to **N**o.
   > If the box has Internet access via remote management tunnel, set this parameter to **Automatic**.
9. Click **Send Changes** and **Activate**.

(Optional) Link the Syslog Streaming node to a Repository

1. Make sure repositories are enabled, for more information, see [Repositories](#).
2. Within the **Configuration Tree**, right click on the **Syslog Streaming** node that has been configured, and select **Copy to Repository**.
3. Select the repository and enter appropriate object name.
4. Right-click the created repository object and select **Multiple Object Action**.
5. Select all firewalls in your Control Center you want to activate the integration for.
6. Select **Link to Repository** as the **Action on selected Nodes**, and click **Go**.
7. Click **OK**.
8. On the top-right of the window, click **Activate**.

Figures

1. xdr_int.png
2. xdr_int.png