How to Enable Integration with Barracuda XDR

https://campus.barracuda.com/doc/98207863/

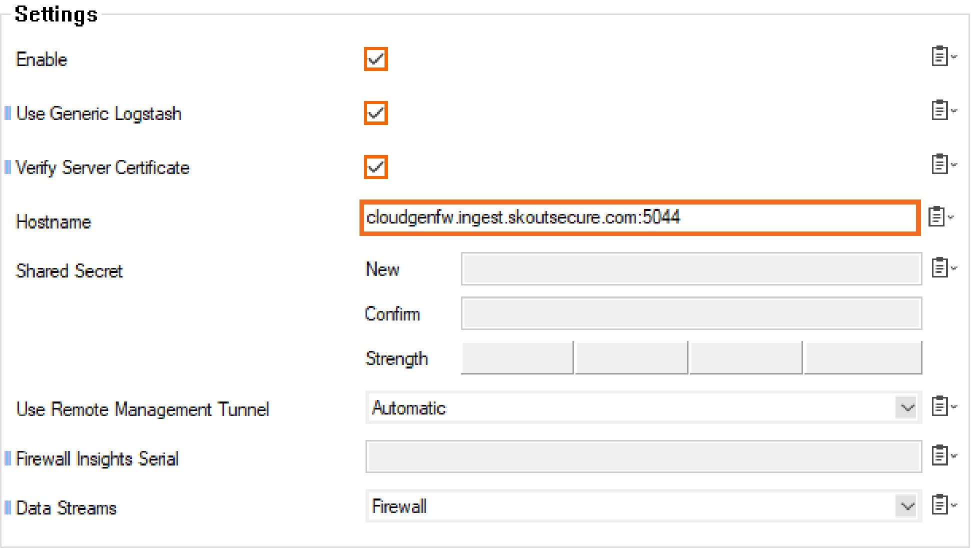
The Barracuda CloudGen Firewall allows administrators to stream relevant security events to the Barracuda XDR platform to detect and provide an incident response to malicious events. A 24x7 SOC Team streamlines responses to incidence, which reduces the damage of the attack. For more information on the 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 license 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 contact 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`



Settings

Enable ☑

Use Generic Logstash ☑

Verify Server Certificate ☑

Hostname: cloudgenfw.ingest.skoutsecure.com:5044

Shared Secret: New / Confirm / Strength

Use Remote Management Tunnel: Automatic

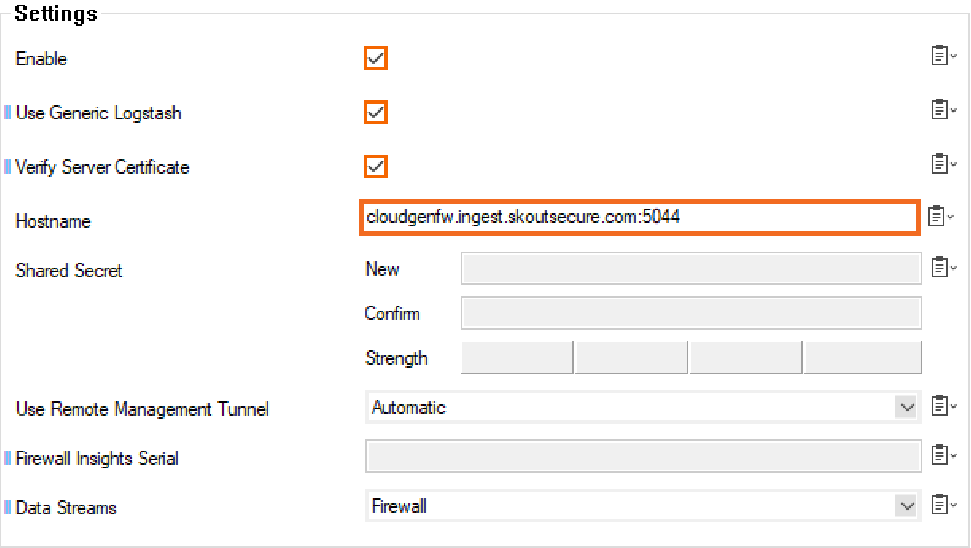
Firewall Insights Serial:

Data Streams: Firewall

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`



Settings

Enable	☑
Use Generic Logstash	☑
Verify Server Certificate	☑
Hostname	cloudgenfw.ingest.skoutsecure.com:5044
Shared Secret	New Confirm Strength
Use Remote Management Tunnel	Automatic
Firewall Insights Serial	
Data Streams	Firewall

8. Click **Send Changes** and **Activate**.
9. Make sure repositories are enabled, for more information, see Repositories.
10. Within the **Configuration Tree**, right click on the **Syslog Streaming** node that has been configured, and select **Copy to Repository**.
11. Select the repository and enter appropriate object name.
12. Right-click the created repository object and select **Multiple Object Action**.
13. Select all firewalls in your Control Center you want to activate the integration for.
14. Select **Link to Repository** as the **Action on selected Nodes**, and click **Go**.
15. Click **OK**.
16. On the top-right of the window, click **Activate**.

Figures