How to Connect to a Syslog

https://campus.barracuda.com/doc/93192797/

Syslog Integration supports syslog version 3.

Syslog Integration enables you to export your event data to a syslog server or a security information and events management (SIEM) system. With Syslog Integration, you can store your information and use it for tracking, analysis, and troubleshooting.

Setting Up Syslog Integration

To configure Syslog Integration:

1. Click the Settings icon to access the administrative functions.
2. Select the **Syslog Integration** tab.
3. Open any firewall ports needed for communication with your syslog server/SIEM system. Barracuda Sentinel public IP addresses are: 3.232.50.116 and 52.202.236.132
4. Enter the **IP Address/Hostname** and **Port** for your syslog server/SIEM system. The default port is 6514.
5. Click **Save**.
6. Click **Test** to ensure that Barracuda Sentinel can connect with your syslog server/SIEM system.
    - *If the test is successful*, your message log data begins transferring to your syslog server/SIEM system.
    - *If the test is not successful*, check the IP Address/Hostname and Port information and reenter it if needed. Then perform the test again.

To deactivate the syslog server, clear the **Active** checkbox, then click **Save**.

Notes:

- You can only connect one syslog server/SIEM system at a time. You can delete an existing entry and replace it, but you cannot have multiple entries.
- This feature is available only for Transmission Control Protocol (TCP) with Transport Layer Security (TLS).
- If your syslog server/SIEM system stops responding, data will not spool until the communication is re-established.
- After you enable or disable syslog integration, it can take up to 10 minutes for message transmission to either start or stop.

Data Sent

Barracuda Sentinel sends the following objects to syslog:

- Spear Phishing Threat


```
{
 "sender":"user@example.com",
 "recipient":"user@barracuda.com",
 "subject":"YOUR FUND NOTIFICATION",
 "date":"2020-06-22 - 16:34:34",
 "category":"Spear Phishing Threat",
 "type":"spam"
}

{
 "sender":"user@example.com",
 "recipient":"user@barracuda.com",
 "subject":"Lily, Shop Gifts for Grads & Dads",
 "date":"2020-06-23 - 15:42:58",
 "category":"Spear Phishing Threat",
 "type":"phishing"
}
```


- Account Takeover Alert
  - Email


```
{
 "user_email":"user@barracuda.com",
 "user_display_name":"Internal, User",
 "subject":"HW#22.pdf",
 "sender_email":"user@example.com",
 "sender_display_name":"John, User",
 "date":"2020-06-23 - 21:45:27",
 "category":"Account Takeover Alert",
 "type":"Email"
}
```


  - Sign Ins


```
{
 "user_email":"user@barracuda.com",
 "user_display_name":"Internal, User",
 "login_ip":"189.210.116.245",
 "login_user_agent":"Windows/10 - Chrome",
 "login_country":"Mexico",
 "date":"2020-06-21 - 00:40:00",
 "category":"Account Takeover Alert",
 "type":"Sign Ins"
}
```


  - Inbox Rules


```
{
 "user_email":"user@barracuda.com",
 "user_display_name":"Internal, User",
 "rule_name":"Forward mail to John",
```

```
 "rule_sequence":"1"",
 "date":"2020-06-21 - 00:40:00",
 "category":"Account Takeover Alert",
 "type":"Inbox Rules"
}
```


Data Format

Data is sent to the syslog in JSON format. You can parse the data any way you choose to meet the needs of your organization.

Figures