Syslog Integration

https://campus.barracuda.com/doc/96023053/

Syslog Integration supports syslog version 3 and is available with Email Protection Advanced Plan.

Syslog Integration enables you to export your message log data to a syslog server or a security information and events management (SIEM) system. With Syslog Integration, you can store your information beyond 30 days and use it for tracking, analysis, and troubleshooting.

To configure Syslog Integration:

1. Log into Email Gateway Defense and navigate to the **Account Management** tab.
2. Open any firewall ports needed for communication with your syslog server/SIEM system. Refer to Email Gateway Defense IP Ranges for information on IP ranges.
3. Enter the **IP Address/Hostname** and **Port** for your syslog server/SIEM system. The default port is 6514.
4. Click **Test** to ensure that Email Gateway Defense can connect with your syslog server/SIEM system.
    - If the test works, your message log data begins transferring to your syslog server/SIEM system.
    - If the test fails, check the IP Address/Hostname and Port information and reenter it if needed. Then perform the test again.

To delete the syslog server, click **Delete**.

Notes:

- Most syslog server/SIEM systems can be configured to check client certificates. Barracuda Networks syslog clients currently use a self-signed client certificate. Thus, if the syslog server/SIEM system validates client certificates, syslog messages can be rejected. To avoid this error, turn off syslog client certificate validation for Email Gateway Defense or add the certificate to a trusted certificate configuration. **Note** that a syslog server that accepts a CA-signed client certificate is not required; a syslog server that accepts self-signed client certificates can also be used.
- 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 is transferred at the account level, not at the domain level.

Data Sent

Sample of JSON sent to sys log:

```
account_id: ESS12345
   attachments: null
   domain_id: 121111
   dst_domain: realty.com
   env_from: Moore@gvt.net.br
   geoip: BRA
   hdr_from: "Mena" <Moore@gvt.net.br>
   hdr_to: "Eric" <mike@realty.com>
   message_id: 1634567131-112064-5307-8715-1
   ptr_record: 179.181.231.191.static.gvt.net.br
   recipient_count: 1
   recipients: [ [-]
     { [-]
       action: blocked
       delivered: not_delivered
       delivery_detail:
       email: mike@realty.com
       reason: bbl
       reason_extra: 179.181.231.191, in Domain Settings: realty.com
       taxonomy: spam
     }
   ]
   size: 3609
   src_ip: 179.181.231.191
   subject: I could not resist and pass by!
   timestamp: 2021-10-18T14:25:43+0000
   tls: false
```

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. For information on the Message Log field names, refer to the help file on the Message Log page.