

Understanding Barracuda Message Archiver Syslog Data

<https://campus.barracuda.com/doc/42047885/>

This article refers to the Barracuda Message Archiver firmware version 5.0 or higher.

If remote logging servers are configured, you can designate a Syslog server to which to send Barracuda Message Archiver web interface and mail syslog data on the **Advanced > Syslog** page in the web interface.

Click **Monitor Syslog** in the web interface to open a new browser window and view data as it is generated.

Web Interface Syslog

The Web Interface Syslog includes information related to configuration changes made from the web interface, as well as any user login activities. The data appears on the local facility with login information at the info priority level, and configuration changes at the debug priority level on the specified Syslog server.

Example 1. User Login.

```
Dec  5 09:44:41 2014 barracuda web: [192.168.1.42] LOGIN (auditor1)
```

Diagram illustrating the components of the User Login Syslog message:

- Date/Time Stamp:** Dec 5 09:44:41 2014
- Barracuda Message Archiver Name:** barracuda
- Indicates this is a Web Log:** web:
- Barracuda Message Archiver IP Address:** [192.168.1.42]
- Action:** LOGIN
- User Login Name:** (auditor1)

Example 2. Failed Login Attempt.

```
Dec  5 07:18:30 2014 barracuda web: [192.168.1.42] FAILED_LOGIN (admin)
```

Diagram illustrating the components of the Failed Login Attempt Syslog message:

- Action:** FAILED_LOGIN
- User Login Name:** (admin)

Example 3. Virus Scanning Disabled by Admin.

```
Dec 5 09:28:53 2014 barracuda web: [192.168.1.42] global[] CHANGE scana_filter_virus_check (No) [admin]
```

Action

Mail Syslog

The Mail Syslog includes mail-related data such as timestamp, mail type, unique message identifier, message size, envelope 'From' and 'To' addresses, and any additional information related to the message (for example, the uncompressed message size and size occupied on disk). The data appears on the mail facility at the debug priority level on the specified mail server.

Example 1. New Message from **jae.black@enron.com** to **david.forster@enron.com** and **larry.valderrama@enron.com** with Timestamp **1411416561**.

```
Sep 22 16:09:21 2014 barracuda [worker] - new_mail: fc49e66f5889785eb723c634f4061b88 1411416561 <jae.black@enron.com> david.forster@enron.com 0 inbound 10581 4096
Sep 22 16:09:21 2014 barracuda [worker] - new_mail: fc49e66f5889785eb723c634f4061b88 1411416561 <jae.black@enron.com> larry.valderrama@enron.com 0 inbound 10581 4096
```

Reserved
Uncompressed Message Size
Size Occupied on Disk

Example 2. Two Separate New Messages from **lynn.blair@enron.com**.

In this example, the IDs after `new_mail` are different, showing that these are different messages.

```
Sep 22 16:09:17 2014 barracuda [worker] - new_mail: afdd42d518ab9b0ec4929ce35bee9a58 1411416557 lynn.blair@enron.com rick.dietz@enron.com 0 inbound 4038 4096
Sep 22 16:09:17 2014 barracuda [worker] - new_mail: 709771f3fd82a6204eeefa0dd425b6276 1411416557 lynn.blair@enron.com center.ets@enron.com 0 inbound 3568 4096
```

Figures

1. user_login.png
2. failed_login.png
3. scan_disable.png
4. example1.png
5. example2.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.