

Bomgar Base 3 Syslog Message Reference

Index

Introduction	2
Message Format	2
Message Segmentation	2
Payload Format	3
Old/New Nomenclature	4
Events	5
Fields	6
Change Password Fields	6
Change Username Fields	6
Login Fields	6
Network Fields	7
Network Address Fields	8
Network Route Descriptor	8
Setting Fields	9

Introduction

This document is intended to provide a reference for the syslog messages that are generated by the **/appliance** interface of the Bomgar Box. It is assumed that the reader is familiar with the syslog concept and functionality. This document lists the different events that are logged by the syslog service that resides on the appliance and describes what the events mean as well as what triggers them.

Message Format

All syslog messages follow a specific format. Below is an example of a message as well as an explanation of its parts.

```
Oct 12 14:58:35 example_host BG: 1234:01:01:site=support.example.com/appliance;
who=John Smith(jsmith);who_ip=192.168.1.1;event=login;target=web/appliance;status=success
```

The example above represents one message on one line. Messages can be broken down into two parts: a header followed by a payload of fields and values.

The header is made up of the date, time, hostname, and the characters **BG:**, which designate that this message is a Bomgar-specific syslog message. The remaining header information is made up of a unique 4-digit site ID, a segment number, and the total number of segments. If your appliance has only one site installed, all messages will have the same site ID. All three of these data are followed by colons. So from the example above, the entire header is simply:

Oct 12 14:58:35	example_host	BG:	1234:	01:	01:
└──────────┘			└──┘	└──┘	└──┘
Date/Time			Site ID	Segment Number	Total Segments

Following the header is the payload. The format of the payload is essentially **field1=value1;field2=value2;...** This format is better suited to provide an order-independent set of data than a comma-separated format would provide, since some of the messages may contain upwards of 70 fields of data.

Finally, note also the escaping of “=”, “;”, and “\” characters. If any payload values include any of these characters, those characters will be prefixed with a backslash character (“\”) to indicate that the next character is part of the value data, not a delimiter. For example, if a username were changed to **user;s=name\id** in the web interface, then the payload field/value pair in the syslog message would read **...new_username=user\s=name\id;**

Message Segmentation

As mentioned above, certain syslog messages can be much larger than others. As a result, the syslog service will segment any messages that are larger than 1KB into multiple messages. In this guide, these messages will be referred to as segments.

Since the message example above is less than 1024 bytes, the header shows a value of **01:01:**, indicating that this is the first segment and that there is only one segment in this message. A larger example message which does show segmentation is used in the **Old/New Nomenclature** section on page 4 of this guide.

Payload Format

Examination of the payload shows that there are several standard data fields in every message. Messages will also contain non-standard data fields that provide more information about the syslog message. For the moment, the standard data fields will be discussed.

site	The hostname for which the Bomgar software was built.
who	The username associated with this event.
who_ip	The IP address of the system that caused the event.
event	The name of the event that occurred

Again, each of these fields will be present somewhere within the payload, but the order is not specifically set. Of these four fields, the most significant is the **event** field. The value associated with the **event** field indicates what actually occurred.

```
Oct 12 14:58:35 example_host BG: 1234:01:01:site=support.example.com/appliance;
who=John Smith(jsmith);who_ip=192.168.1.1;event=login;target=web/appliance;status=success
```

From the example, it can be determined that this particular message was generated by a login attempt. The remaining payload provides information about that event. In this case, the login attempt was for the **/appliance** administrative interface (**target=web/appliance**), and it was a successful attempt (**status=success**).

Syslog messages stack in order of occurrence. In the example below, a user attempts to log in but is required to change his or her password. The user tries to use an invalid password before setting one that matches the site's security policy and then log in successfully. Where the string **...<data truncated>...** occurs, extraneous data was removed to make the example messages more readable.

```
Oct 12 14:53:24 example_host BG: 1234:01:01:site=support.example.com; ...<data truncated>...
event=login;status=failure;reason=change_password
```

```
Oct 12 14:53:43 example_host BG: 1234:01:01:site=support.example.com; ...<data truncated>...
event=change_password;status=failure;reason=invalid_password
```

```
Oct 12 14:54:02 example_host BG: 1234:01:01:site=support.example.com; ...<data truncated>...
event=change_password;status=success
```

```
Oct 12 14:54:03 example_host BG: 1234:01:01:site=support.example.com; ...<data truncated>...
event=login;status=success
```

Old/New Nomenclature

One important note should be made concerning a common nomenclature that is frequently used within syslog messages. When a change is made to an existing setting, the change is often notated by prefixing the original setting with **old_** and the new setting with **new_**. The example below demonstrates a display name change. Note that this example message is split into two segments because the amount of data exceeds 1KB.

```
Oct 12 14:53:24 example_host BG: 1234:01:02:site=support.example.com; ...<data truncated>...  
event=user_changed;old_username=jsmith;old_display_name=John Smith;old_permissions:support
```

```
Oct 12 14:53:24 example_host BG: 1234:02:02:t=1;old_permissions:support:canned_messages=1;  
...<data truncated>... new_display_name=John D. Smith
```

This event shows that the display name was changed. The syslog process takes a snapshot of the user's current settings and prefixes those settings with **old_**. It then takes a snapshot of only the changes that are about to take effect and prefixes those settings with **new_**. Because, in this example, only the **display_name** setting has been changed, only that setting will have both an **old_** entry and a **new_** entry. However, all of the other unchanged settings will also be listed, prefixed with **old_**.

Events

Each syslog message contains the name of an event that triggered the message to be logged in the first place. Events are triggered by actions such as login attempts, defining network settings, and so forth.

Below is a comprehensive list of the possible events included with this version of the Bomgar base software, accompanied by a brief description of each event. Note that some events may be caused by multiple triggers. In those cases, the triggers are identified below.

Event	Trigger
admin_password_reset_to_factory_default	The Reset Admin Account button has been clicked, reverting a site's administrative account to its default credentials.
change_password	A user has attempted to change the administrative password.
change_username	A user has attempted to change the administrative username.
default_site_changed	The default support site for this Bomgar Box has been changed to another site, and the change has been saved.
login	A login attempt has been made.
network_address_added	A new IP address has been added and saved.
network_address_changed	An existing IP address has been modified and saved.
network_address_removed	An existing IP address has been deleted. Note that you cannot delete the default route.
network_changed	The global network configuration has been changed, and the change has been saved.
network_route_changed	A static route has been added, modified, or removed.
reboot	The Bomgar Box has been rebooted.
setting_added	A setting has been defined and saved for the first time.
setting_changed	A setting has been modified and saved.
starting_support_tunnel	A support tunnel has been initiated from the Bomgar Box.
syslog_server_changed	The remote syslog server setting has been changed and saved.

Fields

Many of the events listed above will have additional fields. These fields are defined below.

Change Password Fields

These fields apply to the **change_password** event.

Field	Value	Explanation
status	success failure	Whether the password change attempt succeeded or failed.
reason	failed invalid_password	Indicates whether the old password supplied was incorrect or the new password failed to meet complexity requirements.

Change Username Fields

These fields apply to the **change_username** event.

Field	Value	Explanation
status	success failure	Whether the username change attempt succeeded or failed.
reason	failed invalid_username	Indicates whether the supplied password was incorrect or the new username failed to meet formatting requirements.

Login Fields

These fields apply to the **login** event.

Field	Value	Explanation
status	success failure	Whether the login attempt succeeded or failed.
reason	failed exceeded_failed_login_attempts change_password	Indicates the reason for the failure, such as the number of failed login attempts having exceeded the permissible amount or the password requiring reset.

Network Fields

These fields apply to the **network_changed** event.

Field	Value	Explanation
default_route	string	The default network route for the Bomgar Box.
dns:1	string	The IP address of the primary DNS server.
dns:2	string	The IP address of the secondary DNS server.
dns:3	string	The IP address of the tertiary DNS server.
dns:opendns	1 or 0	1: The Bomgar Box should fall back to OpenDNS servers if the configured DNS servers fail to reply. 0: The Bomgar Box should never fall back to OpenDNS servers.
gateway:interface	string	The interface to use as the default gateway.
gateway:ip	string	The IP address of the default gateway.
hostname	string	The hostname of the Bomgar Box.
icmp_echo	1 or 0	1: The interface will respond to ICMP echoes. 0: The interface will not respond to ICMP echoes.
ntp_server	string	The IP address of the NTP server.
ssl:ciphers	comma-delimited list	The set of ciphersuites supported by the Bomgar Box for HTTPS/SSL traffic.
ssl:v2	1 or 0	1: SSLv2 is enabled. 0: SSLv2 is not enabled.
ssl:v3	1 or 0	1: SSLv3 is enabled. 0: SSLv3 is not enabled.

Network Address Fields

These fields apply to the **network_address_added**, **network_address_changed**, and **network_address_removed** events.

Field	Value	Explanation
enabled	1 or 0	1: This IP address is enabled. 0: This IP address is disabled.
interface	string	The NIC to use as the interface.
ip	string	The IP address of the interface.
netmask	string	The netmask for this IP address.
permit:http	1 or 0	1: Permit HTTP traffic through this IP and interface. 0: Do not permit HTTP traffic through this IP and interface.
permit:https	1 or 0	1: Permit HTTPS traffic through this IP and interface. 0: Do not permit HTTPS traffic through this IP and interface.
permit:session	1 or 0	1: Permit Bomgar session traffic, such as a representative console and customer client connections, through this IP and interface. 0: Do not permit Bomgar session traffic through this IP and interface.

Network Route Descriptor

This field applies to the **network_route_changed** event.

Field	Value	Explanation
[ip/bit=gw@NIC]	string	The IP address and CIDR bitmask, along with the gateway address at a particular interface. Examples: 10.0.0.0/8=10.0.0.1@NIC1 192.168.0.0/16=192.168.0.1@NIC2

Setting Fields

These fields apply to the **setting_added** and **setting_changed** events.

Field	Value	Explanation
alerts:email	string	The list of email addresses to which to send email alerts.
email:encryption	none ssl tls	The type of encryption used for the SMTP email server.
email:host	string	The SMTP server through which to send emails.
email:password	* * * *	Indicates if the password has changed. The actual string is never supplied.
email:port	integer	The SMTP server port through which to connect.
email:user	string	The username used to authenticate with the SMTP server.
networks:list	string	A list of IP addresses which should be allowed or denied.
networks:type	allow_all allow_list deny_list	Whether to allow all IP addresses, to allow only specified IP addresses, or to deny specified IP addresses access to the /appliance administrative interface of the Bomgar Box.
ports:http	comma-delimited list	A list of ports that will respond to HTTP traffic.
ports:https	comma-delimited list	A list of ports that will respond to HTTPS traffic.
ports:management:allowed	comma-delimited list	A list of ports that are allowed to access the /appliance interface.
ports:management:denied	comma-delimited list	A list of ports that are not allowed to access the /appliance interface.
ports:management:http	integer	The port to use when generating a URL that should be viewed over HTTP.
ports:management:https	integer	The port to use when generating a URL that should be viewed over HTTPS.
syslog	string	The address of the remote syslog server to which to send messages.
timezone	string	The time zone in which this Bomgar Box renders system times.

You can configure your Bomgar Box to send these log message to an existing syslog server. Bomgar Box logs are sent using the **local0** facility.

For more information on Bomgar administration, visit www.bomgar.com/documentation.