FortiBridge Release Notes

VERSION 4.1.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Wednesday, May 27, 2015

FortiBridge Release Notes Version 4.1.0

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-01-28	FortiBridge software version 4.0.0 release.
2015-05-01	FortiBridge software version 4.1.0 release.
2015-05-05	Added two additional known issues.
2015-05-27	Updated the instructions for upgrade from release 4.0 to 4.1

Introduction

This document provides upgrade instructions and information about open issues and caveats in FortiBridge v4.1.0. Please review all sections in this document prior to upgrading your device.

This document includes the following sections:

Supported models

This guide covers the following FortiBridge models:

- FBG-3002S (short-range) and FBG-3002L (long-range) - provides two 1G/10G network segments .
- FBG-3004S (short-range) and FBG-3004L (long-range) - provides four 1G/10G network segments.
- FBG-3041S (short-range) - provides one 40G network segment.

The FortiBridge 2000-series models (FBG-2001, FBG-2001F, FBG-2002, FBG-2002F, and FBG-2002X) are only supported on software version 3.1 and earlier.

Transceivers

The following transceivers are shipped with each product:

FortiBridge Model	Transceiver	Quantity
FBG-3002S	FTLX8571D3BCV / Finisar / 1G/10G 850nm Multimode Datacom SFP+ Transceiver	4
FBG-3002L	FTLX1471D3BCV / Finisar / 1G/10G 10km Single mode Datacom SFP+ Transceiver	4
FBG-3004S	FTLX8571D3BCV / Finisar / 1G/10G 850nm Multimode Datacom SFP+ Transceiver	8
FBG-3004L	FTLX1471D3BCV / Finisar / 1G/10G 10km Single mode Datacom SFP+ Transceiver	4
FBG-3041S	FTL410QE1C (40G Modules)	2

Summary of enhancements

The following is a list of enhancements in FortiBridge release 4.1.0:

- HTTP and Ping probes
- Statistics for CPU and memory
- Fortinet CLI
- Radius/TACACS+ authentication
- Admin GUI access via HTTPS

See FortiBridge Documentation for additional FortiBridge v4.1.0 documentation.

Upgrade Information

Upgrading from FortiBridge

FortiBridge release 4.1.0 supports the 3000-series product family. There is no upgrade path to this release for any of the 2000-series FortiBridge products.

The FortiBridge GUI and CLI support upgrade procedures starting with release 4.1.0. In addition, the CLI supports an upgrade path from release 4.0 to 4.1.

Firmware Upgrade Using the GUI

1. Go to **System > Status**.
2. On the **System Information** widget, next to the **Firmware Version** field, click **Update**
3. The web browser will open a pop-up window for you to select the image file.
4. Click **OK** to start the upgrade.
5. The system displays the upgrade progress in the text field of the pop-up window. When the upgrade is complete, the system displays a message indicating the success of the upgrade.
6. On the **Unit Operation** widget, click the **reboot** button.
7. After the restart, log in and verify the firmware version on the **System Information** widget.

Firmware Upgrade Using the CLI

Upgrade 4.0.0. to 4.1.x

Release 4.1 supports a different format for image files compared to 4.0. Upgrade from 4.0 requires two steps:

A. upgrade to the new file format.
B. upgrade to the latest 4.1 build.

A. Upgrade to the new file format

1. Copy the old-format firmware files and the matching 'update.desc' file to the /tftpboot directory of the TFTP server. These files are available to Fortinet support staff only, at the following location: http://172.30.71.240/images/misc/Old_file_format/
2. Enter the following CLI command: `update <tftp server IP address>`
3. When the upgrade is complete, enter the following CLI command:
   `reboot`

B. Upgrade to the latest 4.1 build.

1. Copy the latest release 4.1 firmware file to the /tftpboot directory of the TFTP server.
2. Enter the following CLI command: `update <tftp server IP address>`
3. When the upgrade is complete, enter the following CLI command:
   `reboot`

Upgrade 4.1.x to 4.1.x

1. Copy the latest release 4.1 firmware file to the /tftpboot directory of the TFTP server, or to a directory on the SCP server.
2. For a TFTP server, enter the following CLI command:
   `execute restore image tftp <image_file_name> <tftp-server_ipv4> [force]`
3. For an SCP server, enter the following CLI command:
   `execute restore image scp <image_file_name> <remote_path> <ssh-server_ipv4> <username> [force]`
4. When the upgrade is complete, enter the following CLI command:
   `reboot`

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select ***Download > Firmware Image Checksums***, enter the image file name including the extension, and select ***Get Checksum Code***.

Resolved Issues

The following issues have been resolved in Release 4.1.0:

Known issues

Defect ID	Description
0267572	Port LINK/ACT LED status is incorrect in the following cases: • For a link that is connected but idle (no traffic on the port), the LINK/ACT LED is yellow. The correct indication is solid green. • For a segment in failcutoff state, the network port LINK/ACT LED is yellow. The correct indication is for the LED to be turned off. Note: the Web admin GUI displays the indication correctly.
	In the system information display of the Web administration tool, the firmware version and the build number values are reversed. The build number field displays the firmware version. In the following example, the firmware version is 4.0.0: `Firmware Version 1.1.77.14 build 0.4.0.0 150119` Note: CLI commands (such as get_ver) display the firmware version correctly.
	In the system dashboard, the **administrators** panel displays the admin user name. If you change the user name using the CLI, the dashboard continues to display the old name. The correct behavior is to display the updated name.
	Syslog refers to Linkdropped mode rather than Failcutoff mode. When a segment transitions into failcutoff mode and later exits failcutoff mode, the Syslog entry displays "Linkdropped on" and "Linkdropped off" . The entries should refer to "Failcutoff".

	Some of the CLI commands are not supported in release 4.0.0:
	• Network and monitor link error thresholds and settings
	  • get/set_rx_tx_err_mode
	• Optional module/segment commands:
	  • get/set_m2n, get/set_2pl
	• Mail server commands:
	  • get/ set_mail_srv, get/set_mail_auth, get/set_mail_user, set_mail_psw, get/set_mail_mailto, get/set_alertmail
	• TACACS+ and Radius commands:
	  • get/set_tacacs_state, get/set_tacacs_server_ip, set_tacacs_key, get/set_tacacs_multi_users
	  • get/set_radius_auth_port, get/set_radius_acct_port

Known Issues

The 4.1.0 release includes the following known issues.

Known issues

Defect ID	Description
	The command **config probe probe_list heartbeat** provides sub-commands to set the source and destination MAC addresses. The equivalent unset commands should restore the default values (the MON0 MAC address for source and MON1 MAC address for destination). However, the unset_source_mac and unset_destination_mac commands do not reset the MAC addresses to their default values.
	Using the GUI interface, it is possible to create an SNMP community without a host ip address. The CLI works correctly.
	If a user is configured without an access profile, the user cannot log in into the GUI interface.
	When radius authentication enabled, the GUI login page incorrectly displays that TACACS is enabled.
	In the Unit Operation panel of the GUI, when a 40G module is selected, the status page displays two lines for the second segment. For this type of module, there is only one segment.
	If you use the CLI to define an SNMP community with a list of IP addresses, if location 2 contains an IP address and location 1 is empty, the GUI will show in location 1 IP of 0.0.0.0
	Get commands when in some sub-menu will not work correctly when doing get from a different get info.
	SNMP query is supported only for CPU usage and memory usage.
	If a user changes their password, and subsequently the system time is changed to a time which is prior to the password change time, the user may not be able to modify their password again. You may need to change the system time back to the original password change time.
	TACACS users that are not also defined as local users on the FortiBridge will have Read only permissions. A TACACS user that is also defined as a local user will get the privilege which is assigned to this user on the FortiBridge unit.

For inquires about a particular issue, please contact Customer Service & Support.