FortiController-5000 - Release Notes

Version 5.2.11

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 31, 2022
FortiController-5000 5.2.11 Release Notes
11-5211-708049-20221031

TABLE OF CONTENTS

Change log

Date	Changed description
October 31, 2022	Added known issue to 854652 to Known issues on page 11.
March 4, 2022	Added the following sections: • FortiController 5.2.11 trusted host limitation on page 6. • Known issues on page 11.
May 3, 2021	Included more information about supported FortiOS versions in Product integration and support on page 9.
April 22, 2021	Initial release.

Introduction

This document provides the following information for FortiController-5000 5.2.11 build 0191:

See the Fortinet Document Library for FortiController-5000 documentation.

Supported models

FortiController-5000 5.2.11 supports the following models:

FortiController	FCTL5103B, FCTL5903C, and FCTL5913C.

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for FortiController-5000 5.2.11 build 0191.

FortiController 5.2.11 supports FortiOS 5.6.6 or later or 6.0.3 or later

Before you upgrade your FortiController firmware to 5.2.11, you must upgrade the FortiOS firmware running on the FortiGates in the SLBC cluster to FortiOS 5.6.6 or later or FortiOS 6.0.3 or later. Running older versions of FortiOS may cause IPsec VPN issues. FortiController 5.2.11 is not compatible with FortiOS 6.0.0, 6.0.1, or 6.0.2.

FortiController-5103B and ESP fragmented SIP traffic

If your FortiController-5103B SLBC cluster is processing ESP fragmented SIP traffic, Fortinet recommends running FortiController-5000 5.2.10 build 0189 instead of upgrading to 5.2.11 build 0191.

FortiController-5000 5.2.10 build 0189 disables IP fragment broadcasting when the load balancing method is set to `src-dst-ip` (L3 load balancing).

```
config load-balance session-setup
   set ipsec-session load-balance
   set load-distribution-method src-dst-ip
end
```

FortiController 5.2.11 trusted host limitation

FortiController 5.2.11 supports creating a maximum of 140 trusted hosts. Creating more than 140 trusted hosts is allowed by the CLI, but creating more than 140 trusted hosts can block management access over special management ports to the FortiController and FortiGates in the secondary chassis in an FGCP HA configuration.

FortiGates in an SLBC cluster can go out of sync after a FortiGuard update

When operating normally, FortiOS uses a collection of CAs (called a CA bundle) for various certificate-related functions. FortiOS normally gets the latest CA bundle from FortiGuard.

FOS firmware images come with their own CA bundle. Immediately after a firmware upgrade, all of the FortiGates in a Session-aware Load Balancing Cluster (SLBC) will have the CA bundle that comes with the firmware image. When the first automatic or manual FortiGuard update occurs, the primary FortiGate in the SLBC downloads the latest CA bundle from FortiGuard and synchronizes it to the other FortiGates in the cluster. Due to a known issue with FortiOS 5.6.7 and earlier, this synchronization step may fail, resulting in a synchronization problem with the cluster.

You can avoid this issue by using the following steps to upgrade the firmware of the FortiGates in an SLBC cluster, perform a FortiGuard update, and manually re-synchronize the configuration:

1. Log in to the primary FortiGate and enter the following command to disable graceful-upgrade.
   ```
   config system elbc
      set graceful-upgrade disable
   end
   ```
2. Use the normal firmware upgrade procedure to upgrade the SLBC firmware.
3. After all of the FortiGates have restarted and joined the cluster, log into the primary FortGate and use the `diagnose sys confsync status` command to verify that the primary FortiGate can communicate with all of the FortiGates in the cluster.
4. Enter `diagnose autoupdate versions | grep -A2 'Bundle'` to check the version of CA bundle on the primary FortiGate (for example, for FOS v5.6.7, the version should be 1.00012).
5. Start a FortiGuard update on the primary FortiGate. For example, use the `execute update-now` command.
6. Wait a few minutes, then enter `diagnose autoupdate versions | grep -A2 'Bundle'` to verify that a new CA bundle has been installed.
7. Backup the configuration of the primary FortiGate.
8. Restore the configuration of the primary FortiGate.
   The primary FortiGate synchronizes its configuration to all of the FortiGates in the cluster. After a few minutes, all of the FortiGates should restart and the cluster configuration should be synchronized.
9. Use the `diagnose sys confsync status` command to verify that the cluster is synchronized.

Upgrade Information

You can find FortiController-5000 5.2.11 firmware images on the Fortinet Support Download Firmware Images page by selecting the **FortiSwitchATCA** product.

Upgrading from FortiController-5000 5.2.7

FortiController-5000 5.2.11 build 0191 supports upgrading from FortiController-5000 5.2.7 and above.

Downgrading to previous firmware versions

Downgrading from FortiController-5000 5.2.11 to previous releases is not supported.

Firmware image checksums

You can find MD5 checksums of FortiController-5000 5.2.11 firmware images on the Fortinet Support Firmware Image Checksums page by entering the firmware image file name including the extension, and selecting **Get Checksum Code**.

Product integration and support

The following table lists FortiController-5000 5.2.11 build 0191 product integration and support information.

Web browser	• Microsoft Internet Explorer version 10. • Mozilla Firefox version 33. • Google Chrome version 37. Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS	• 5.6.11 and later. • 6.0.3 and later. • 6.4.0 and later. • 7.0.0 and later.

Resolved issues

The following issues have been fixed in FortiController-5000 5.2.11 build 0191. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
674840	Resolved an issue that caused front panel interfaces of secondary FortiControllers in an active-passive SLBC cluster to operate in a forward state and incorrectly forward packets, possibly causing an HA split-brain scenario.
685724	The FortiController-5103B now load balances fragmented packets correctly when the load balancing method is set to `src-ip`.

Known issues

The following known issues have been found in FortiController-5000 5.2.11 build 0191. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
854652	When using the `config switch fabric-channel trunk` command to create a new trunk (or aggregate interface) or edit a trunk that has been previously added, the configuration change is implemented when you press the Enter key after entering the `set` command to change the configuration. Normally, in the FortiController CLI, configuration changes are not implemented until you enter `end` to save your changes. This also means that if you make a configuration change to a trunk and enter `abort`, the change has already been made and entering `abort` has no effect. If you need to revert a trunk configuration change that you wanted to cancel with the `abort` command, you can use the `config switch fabric-channel trunk` command to manually revert to the correct configuration. Changing the trunk (aggregate interface) configuration from the GUI is not affected by this issue. On the GUI, changes are not implemented until you select OK to save your changes and you can cancel a configuration change without saving it.
781093	FortiController 5.2.11 supports creating a maximum of 140 trusted hosts. Creating more than 140 trusted hosts is allowed by the CLI, but creating more than 140 trusted hosts can block management access over special management ports to the FortiController and FortiGates in the secondary chassis in an FGCP HA configuration.