



# FortiAnalyzer - Cookbook

Version 5.2.0

**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 COOKBOOK**

<https://cookbook.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



May 06, 2019

FortiAnalyzer 5.2.0 Cookbook

05-520-556116-20190506

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Expanding storage for FortiAnalyzer 5.2.x units</b> .....	<b>5</b>

# Change Log

Date	Change Description
2019-05-06	Initial release.

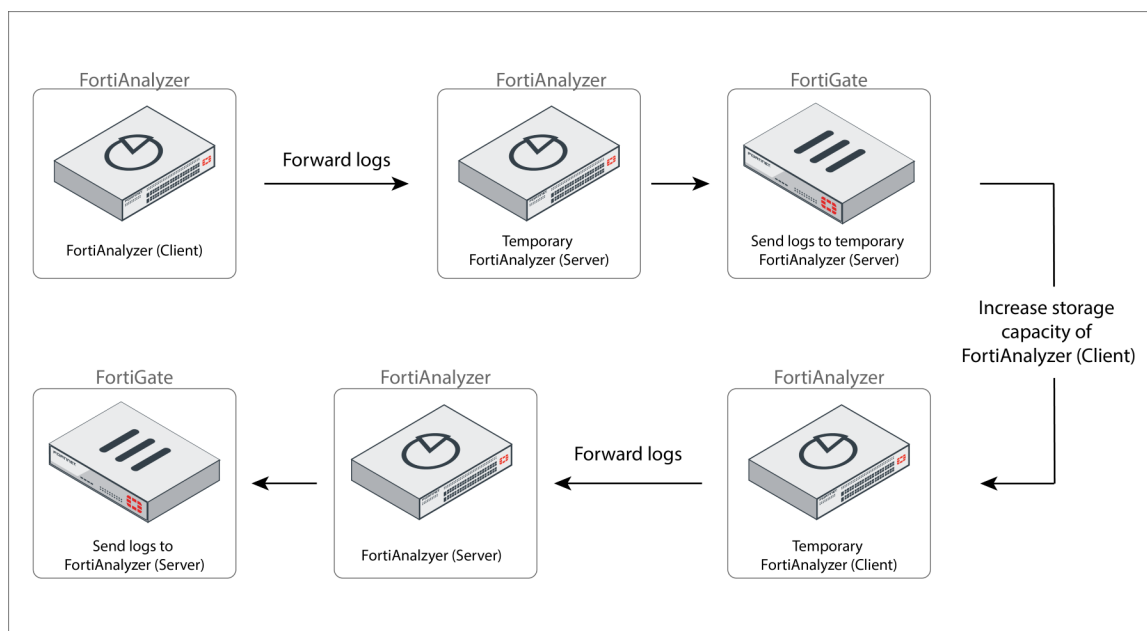
## Expanding storage for FortiAnalyzer 5.2.x units

This example illustrates how to expand storage capacity to over 16 TB for a FortiAnalyzer 5.2.x VM or device.

You can use the *Log Aggregation* feature in aggregation mode to temporarily forward logs from one FortiAnalyzer unit to a temporary FortiAnalyzer unit while you increase the storage capacity of the FortiAnalyzer unit to over 16 TB.

You should also reconfigure FortiGate to send logs to the temporary FortiAnalyzer unit to avoid losing any logs while you increase the storage capacity of your FortiAnalyzer unit.

After you increase storage capacity, you can use the *Log Aggregation* feature to return the logs from the temporary FortiAnalyzer to the FortiAnalyzer unit that now has increased storage capacity. Don't forget to reconfigure FortiGate to send logs to the FortiAnalyzer unit again.



You can use this procedure when upgrading the default 12 HDD (hard disk drive) for FAZ-4000B or FAZ-3500E to the maximum 24 HDD.

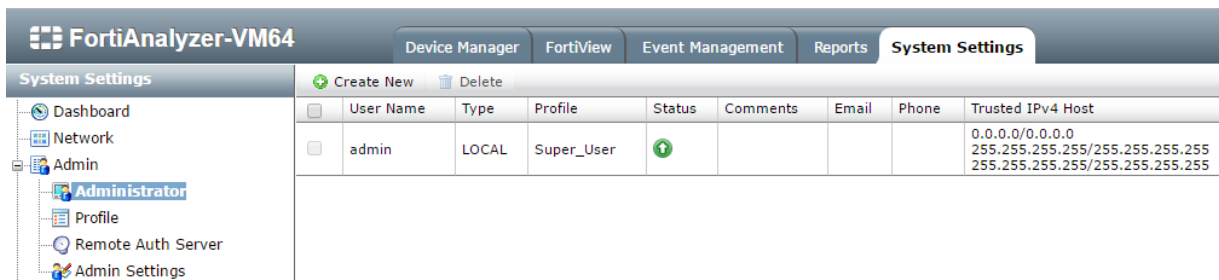
### To configure expanded storage for your FortiAnalyzer 5.2.x devices:

1. Configure the temporary FortiAnalyzer to receive logs (server).
2. Configure log forwarding on the unit for which you want to increase storage capacity (client).
3. Reconfigure FortiGate to send logs to the temporary FortiAnalyzer unit.
4. Increase storage capacity for the FortiAnalyzer unit.
5. Return logs to the unit with increased storage capacity.
6. After log aggregation completes, rebuild the SQL database on the unit with increased storage capacity.
7. Reconfigure FortiGate to send logs to the unit with increased storage capacity.

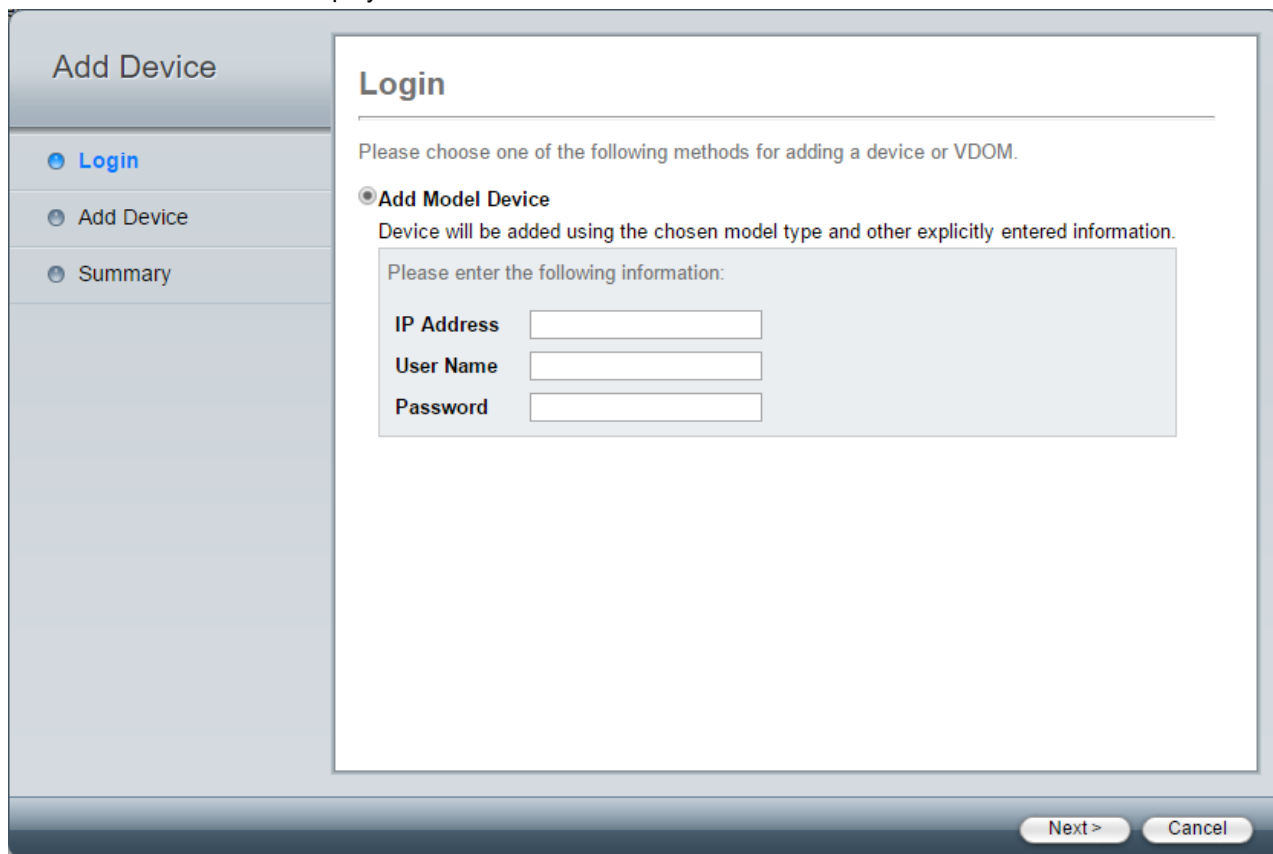
## Configuring the temporary FortiAnalyzer to receive logs (server)

To configure the temporary FortiAnalyzer to receive logs:

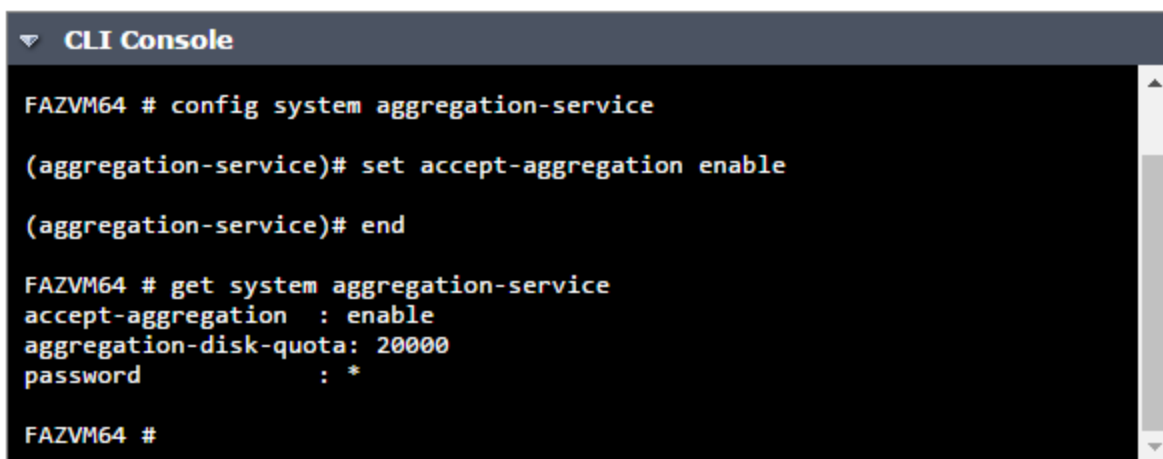
1. Configure an administrator account with a *Super\_User* profile. The client will need to provide the login credentials of this Administrator account to get authenticated by the server.
  - You can use the default admin account, which is assigned the Super\_User profile.
  - Alternatively, you can create a custom administrator account by going to *System Settings > Admin > Administrator*.



2. Add the FortiAnalyzer unit for which you want to increase storage capacity to the temporary FortiAnalyzer by going to *Device Manager > Add Device*. The *Add Device* wizard is displayed. Follow the wizard to add the device.



3. Enable the log aggregation service by going to *System Settings > Dashboard*.

A screenshot of a CLI console window titled "CLI Console". The terminal shows the following commands and output:

```
FAZVM64 # config system aggregation-service
(aggregation-service)# set accept-aggregation enable
(aggregation-service)# end

FAZVM64 # get system aggregation-service
accept-aggregation : enable
aggregation-disk-quota: 20000
password           : *
```

4. In the CLI Console widget, enter the following commands.

```
config system aggregation-service
    set accept-aggregation enable
end
```

```
get system aggregation-service
    accept-aggregation: enable
    aggregation-disk-quota: 20000
    password: *    <-- set for password
```

```
config system interface
    edit port<number>
        set ip <ip address> <netmask>
        set allowaccess ping https ssh snmp telnet http webservice aggregator fgfm
    end
```

## Configuring the FortiAnalyzer unit for which you want to increase storage capacity (client)

### To configure FortiAnalyzer for increased storage:

1. Go to *System Settings > Dashboard*.
2. In the CLI Console widget, enter the following commands:

```
config system aggregation-client
    edit 1
        set mode aggregation
        set server-ip <ip address>
        set agg-password <password>
```

## Increasing storage capacity for the FortiAnalyzer unit

### To increase storage capacity for FortiAnalyzer:

1. Add new hard disks with a total size greater than 16 TB to FortiAnalyzer.
2. Format the FortiAnalyzer disks to have more than 16 TB of storage capacity.

## Returning logs to the FortiAnalyzer unit with increased storage capacity

### To set up log forwarding to return the logs to the FortiAnalyzer:

1. Configure the FortiAnalyzer unit with the new storage capacity as the log-forwarding server.
2. Configure the temporary FortiAnalyzer as the log-forwarding client.  
The log forwarding client sends all of the logs to the log-forwarding server. As a result, the log-forwarding feature returns all of the logs to the FortiAnalyzer unit with increased storage capacity.

## Rebuilding the SQL database on the FortiAnalyzer unit with increased storage capacity

### To rebuild the SQL database on FortiAnalyzer:

On FortiAnalyzer, run the following CLI command:

```
exec sql-local rebuild-db
```

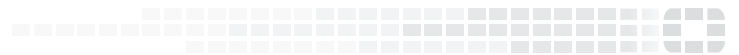
## Reconfiguring FortiGate to send logs to the FortiAnalyzer unit with increased storage capacity

You can perform this step while the FortiAnalyzer database is rebuilding. FortiAnalyzer can still receive new logs and insert them into the SQL database while the database is rebuilding.





**FORTINET®**



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.