



FortiADC - Admin Password Recovery Guide

Version 6.0.0

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 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



August 3, 2020

FortiADC 6.0.0 Admin Password Recovery Guide

01-600-650988-20200803

TABLE OF CONTENTS

Change Log	4
How to reset admin password	5
Required items	5
Configuration	5
Caveats	5
Steps	6

Change Log

Date	Change Description
2020-08-03	Admin Password Recovery Guide initial release.

How to reset admin password

Note: This functionality is only available on versions 5.3.6, 5.4.4, and 6.0.0 or newer.

Periodically a situation arises when FortiADC needs to be accessed or the admin account's password needs to be changed but no one with the existing password is available. If physical access to the device is possible, this feature enables the admin password to be reset.

A new *maintainer* user account is made available after a *cold boot* for 60 seconds after the system clock starts to tick. This account only has access to reset admin accounts' password and a few other commands to execute as detailed below. A maintainer user login is limited to console access and cannot log in via any other method.

Once logged into FortiADC as a maintainer user, FortiADC can be reset to factory default settings. This can be useful if the admin administrator account was deleted.

Maintainer user access is **enabled** by default.

Required items

- Console cable
- Terminal software (e.g. Putty.exe for Windows, Terminal for MacOS)
- Serial number of the FortiADC unit

Configuration

To enable/disable maintainer user account access:

CLI:

```
config system global
  set admin-maintainer enable/disable
end
```

Caveats

- Maintainer user account is only available after a cold reboot.
- Maintainer user account is not available after a warm reboot or upgrade.
- Maintainer user account is only available for 60s after the device powers up. In some cases, this may translate to less than 15s after the login prompt is displayed.
- Maintainer user has console access only.
- Maintainer user can only be used to reset admin password.
- For some VM platforms, cold reboot is labeled "Reset".
- For hardware systems, physical access is required. To cold reboot in cases when power switch is not available, unplug power cable and plug back in after 10s.
- For security purposes, using the maintainer account and resetting a password will cause a log to be created, making these actions traceable.

Steps

1. Connect to the ADC console port or access the VM console.

2. Cold reboot the ADC as described above.

3. Wait for ADC login prompt to appear.

```
FortiBootLoader
FortiADC-200F ( 0:56-09.26.2017)
```

```
FortiADC-200F (17:05-06.08.2017)
Ver:00010002
```

```
Serial number:FAD2HF3A17000103
Total RAM: 8192MB
Boot up, boot device capacity: 1968MB.
Press any key to display configuration menu...
```

```
Reading boot image 6393140 bytes.
Initializing FortiADC...
```

```
System is started.
```

```
FAD2HF3A17000103 login:
```

4. Type in username: *maintainer*

5. The password is *bcpb<serial number>* (e.g. *bcpbFAD2HF3A17000103*)

6. Now logged in as maintainer, type the following commands to change the admin password.

- a. In a FortiADC unit where VDOMs are not enabled:

```
# config system admin
  edit admin
    set password
  end
```

- b. in a FortiADC unit where VDOMs are enabled:

```
# config global
  config system admin
    edit admin
      set password
  end
```

7. If the admin account was deleted, execute factory reset to recover.

```
# execute factoryreset
```

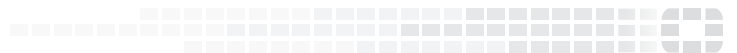
8. If the admin account was not deleted, then reboot.

```
# execute reboot
```

9. New admin password should now be in effect.



FORTINET[®]



Copyright© 2020 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.