FortiSIEM - ISO Installation Guide

Version 5.3.2

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

07/31/2020
FortiSIEM 5.3.2 ISO Installation Guide

TABLE OF CONTENTS

Change Log **4**
Installing FortiSIEM From an ISO **5**
Hardware Requirements for Collector Nodes 5
ISO Installation 5

Change Log

Date	Change Description
09/20/2019	Initial release of the ISO Installation Guide.
11/20/2019	Release of the ISO Installation Guide for 5.2.6.
03/30/2020	Release of the ISO Installation Guide for 5.3.0.

Installing FortiSIEM From an ISO

This topic covers installation of FortiSIEM from an ISO under a native file system, also known as installing "on bare metal."

- Hardware Requirements for Collector Nodes
- ISO Installation

Hardware Requirements for Collector Nodes

Component	Quantity	Host SW	Processor	Memory	OS/App Storage
Collector	1	ESX	2 Core 2 GHz, 64-bit	4 GB	40 GB
Collector	1	Native Linux Suggested Platform: Dell PowerEdge R210 Rack Server	2 Core, 64-bit	4GB	40 GB

ISO Installation

You can install Collectors on bare metal hardware (without a Hypervisor layer). Be sure to read the section on **Hardware Requirements for Collector Nodes** before starting the installation process.

1. Download the ISO image from: https://support.fortinet.com.html
2. Burn the ISO to a DVD so that you can boot from it to begin the setup.
3. Before you begin the installation, make sure the host where you want to install the Collector has an Internet connection. Once the ISO DVD boots up, it will prompt you for installation-specific input such as the following:
   - Keyboard type
   - Language
   - Timezone
   - Whether to re-initialize (i.e. reformat) the disk where it will install collector
   - root password
4. Log in to the server where you want to install the Collector as user `root` with the password you created at installation time.
5. Make sure your boot DVD is loaded.
6. Run the following script to configure the IP and hostname: `/opt/vmware/share/vami/vami_config_net`.

- The machine will reboot and `yum` update itself.
- Make sure the collector can reach the `os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs.fortisiem.fortinet.com` URLs on port 443 for OS updates.

7. Once the machine reboots, log in again as user `root` with password with the password you created at installation time.
8. Run the following command to install the i686 packages required by `phCheckpoint`:
   - `yum -y install libcurl.i686 net-snmp-libs.i686 libesmtp.i686 libstdc++.i686 pam.i686 libicu.i686`
9. Register the Collector with Supervisor using the following command:
   - `phProvisionCollector`

     For example:
     `phProvisionCollector --add <Organization-user-name> <Organization-user-password> <Supervisor-IP> <Organization-name> <Collector-name>`

Copyright© (Undefined variable: FortinetVariables.Copyright Year) 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.