

OS Update Lifecycle

FortiSIEM 6.3.1



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



01/27/2022

FortiSIEM 6.3.1 OS Update Lifecycle

Change Log

Date	Change Description
01/25/2019	Initial version of the guide.
11/20/2019	CentOS Upgrade Guide released for 5.2.6.
03/30/2020	CentOS Upgrade Guide released for 5.3.0.
11/30/2020	Upgrade to CentOS 8.
03/31/2021	Updated for 6.1.x and 6.2.0.
05/06/2021	CentOS Upgrade Guide released for 6.2.1.
07/06/2021	CentOS Upgrade Guide released for 6.3.0.
08/10/2021	Updated FortiSIEM OS updates for 6.3.0.
08/26/2021	CentOS Upgrade Guide released for 6.3.1.
10/15/2021	CentOS Upgrade Guide released for 6.3.2.
12/22/2021	CentOS Upgrade Guide released for 6.3.3.

FortiSIEM OS Update Process

FortiSIEM OS update process includes the following:

- [FortiSIEM CentOS 8 update server](#)
- [FortiSIEM OS updates](#)

FortiSIEM CentOS 8 update server

Whenever Redhat/CentOS publishes an important OS update for CentOS 8, an announcement is made via [CentOS-announce](#) mailing list. FortiSIEM engineering team subscribes to this mailing list. Once a new update is available, FortiSIEM engineering first tests these updates on FortiSIEM Virtual Appliance for stability and regression. After confirming that the update is safe, FortiSIEM CentOS 8 update server updates the OS packages from CentOS mirror servers.

FortiSIEM OS updates

Before release, FortiSIEM is updated with latest updates from **FortiSIEM CentOS 8 update server**. FortiSIEM customer automatically receives an OS update when they upgrade to the latest FortiSIEM.

If a customer needs to update CentOS 8 without upgrading FortiSIEM product itself, they can execute the script on demand: `yum upgrade -y`. For this, FortiSIEM instance needs port 443 access to:

- os-pkgs-cdn.fortisiem.fortinet.com
- os-pkgs.fortisiem.fortinet.com

Note: If you wish to set up an offline repository server instead of directly using Fortinet servers os-pkgs-cdn.fortisiem.fortinet.com and os-pkgs-c8.fortisiem.fortinet.com, check the Offline Upgrade guide in 6.3 [Reference Manuals](#).



www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.