

OS Updates and Security Fixes

FortiSOAR[™] 7.2.0



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 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



June, 2022

FortiSOAR™ 7.2.0 OS Updates and Security Fixes

00-400-000000-20201124

TABLE OF CONTENTS

Change Log	4
FortiSOAR™ OS Update Process and Security Fixes	5
FortiSOAR™ OS Update Process	5
FortiSOAR™ CentOS 7 update server	5
FortiSOAR™ OS updates	5

Change Log

Date	Change Description
2022-06-29	Release of FortiSOAR™ 7.2.0 Security Patch 1 (SP1)

FortiSOAR™ OS Update Process and Security Fixes

FortiSOAR™ OS Update Process

The FortiSOAR™ 7.2.0 Security Patch delivers updated OS packages for the 7.2.0 release. This document provides you with the information you need about how you can get these updates without the need to upgrade FortiSOAR™.

FortiSOAR™ OS update process includes the following:

- [FortiSOAR™ CentOS 7 update server on page 5](#)
- [FortiSOAR™ OS updates on page 5](#)

FortiSOAR™ CentOS 7 update server

Whenever CentOS publishes an important OS update for CentOS, an announcement is made using the [CentOS-announce](#) mailing list. The FortiSOAR™ engineering team is subscribed to this mailing list. Once a new update is available, FortiSOAR™ Engineering first tests these updates on a FortiSOAR™ Virtual Appliance by performing vulnerability scan using Nessus™. If no reported vulnerabilities are seen sanity testing is done for stability and regression. After confirming that the update is safe, updates are pushed to the FortiSOAR™ CentOS 7 update server (repo.FortiSOAR.fortinet.com).

FortiSOAR™ OS updates

Before release, FortiSOAR™ is updated with the latest updates from the CentOS mirror servers. A FortiSOAR™ customer automatically receives an OS update when they upgrade to the latest FortiSOAR™.

If a customer needs to update CentOS 7 without upgrading the FortiSOAR™ product itself, they can do the following:

1. Ensure that repo.FortiSOAR.fortinet.com is reachable from your VM.
If you connect using a proxy, ensure that you set the proxy in the `/etc/wgetrc`, `/etc/profile`, and `yum.conf` files. This is required to download the OS updates file.
2. SSH to your FortiSOAR™ 7.2.0 VM and log in as a *root* user.
3. Download the OS update file (`security-update-fortisoar-7.2.0.bin`) for 7.2.0 by running the following command:

```
# wget https://repo.FortiSOAR.fortinet.com/7.2.0/security-update-fortisoar-7.2.0.bin
```

Note: If your instance can connect to repo.FortiSOAR.fortinet.com using only a proxy, then ensure that the proxy is set in the `/etc/wgetrc` file.
For example:

```
use_proxy=yes  
http_proxy=<proxy_server_ip:port>  
https_proxy=<proxy_server_ip:port>
```
4. Run the `security-update-fortisoar-7.2.0.bin` file to apply the security patch on your 7.2.0 system:

```
# sh security-update-fortisoar-7.2.0.bin
```
5. Reboot your host post-upgrade, if directed by the script.



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.