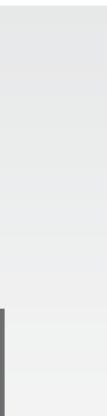


r1 Administration Guide

FortiSOAR MEA 7.0.0



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://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



April, 2021

FortiSOAR MEA 7.0.0 r1 Administration Guide

00-400-000000-20210113

TABLE OF CONTENTS

Change Log	4
Introduction	5
Key Concepts	5
How FortiSOAR MEA works with FortiAnalyzer	5
Quick Start	6
Enabling the FortiSOAR MEA	6
Licensing FortiSOAR MEA	7
Accessing FortiSOAR MEA using SSH	7
Backing up and restoring FortiSOAR MEA configurations	8
More Information	9

Change Log

Date	Change Description
2021-04-23	Initial release of 7.0.0

Introduction

This document provides information about FortiSOAR MEA version 7.0.0. FortiSOAR MEA is a management extension application (MEA) that can be enabled with FortiAnalyzer.

Key Concepts

Fortinet Security Orchestration, Automation, and Response Platform (**FortiSOAR™**) is a centralized hub for all of your security operations. Our platform provides customizable mechanisms for prevention, detection, and response that work across tools in your environment. The FortiSOAR MEA gets installed on FortiAnalyzer and allows you to manage your security operations using FortiAnalyzer and without the need of having a separate FortiSOAR instance.

How FortiSOAR MEA works with FortiAnalyzer

When enabled, the FortiSOAR MEA gets installed on FortiAnalyzer. An MEA is a management extension application that is released and signed by Fortinet to run on FortiAnalyzer. An MEA is full-fledged running instance of product in form of a docker container, enabling you to use and monitor different solutions from Fortinet using a single pane of glass.



From FortiAnalyzer version 7.0.0, there is a capping of 50% on RAM and CPU for MEAs. This means if FortiAnalyzer has 8 CPUs and 16 GB RAM, then only 4 CPUs and 8 GB RAM will be available to MEAs. Note that this 4 CPUs and 8 GB RAM will be used for all the MEAs, and not just for the FortiSOAR MEA. Therefore, users need to ensure that they provision FortiAnalyzer with sufficient resources to meet the minimum (default) FortiSOAR MEA configuration of 4 CPU cores and 8 GB RAM, which would mean that FortiAnalyzer should be deployed with a minimum of 8 CPUs and 16 GB RAM. However, to use FortiSOAR MEA at a production volume, you should provide the standard configuration of 8 CPUs and 32 GB RAM and depending on the number of running applications, the FortiAnalyzer resources should be increased. **For example, if you are running only the FortiSOAR MEA at a production volume, i.e., at the standard configuration of 8 CPUs and 32 GB RAM on FortiAnalyzer, then ensure that the FortiAnalyzer has a minimum configuration of 16 CPUs and 64 GB RAM.**

You must also specify the ElasticSearch and Celeryd configuration follows, if your FortiSOAR MEA is running at a production volume of 8 CPUs and 32 GB RAM:

- /etc/elasticsearch/jvm.options (within the FortiSOAR running container):
-Xms8g
-Xmx8g
- /etc/celeryd/celeryd.conf (within the FortiSOAR running container):
CELERYD_OPTS="--autoscale=16, 8"

Quick Start

This section includes the following information to help you get started with using FortiSOAR MEA:

- [Enabling the FortiSOAR MEA](#)
- [Accessing FortiSOAR MEA using SSH](#)
- [Backing up and restoring FortiSOAR MEA configurations](#)

Enabling the FortiSOAR MEA

FortiAnalyzer provides access to a FortiSOAR MEA application that is released and signed by Fortinet.



Only *root* users or users with sudo permissions can enable management extensions.

Enabling the FortiSOAR MEA using the FortiAnalyzer GUI

1. Ensure you are using ADOM version 6.4 or later.
 2. Log on to FortiAnalyzer and navigate to **Administration > System Settings > Management Extensions**.
 3. Click the grayed-out tile for **FortiSOAR MEA** to enable the application.
 4. Click **OK** on the confirmation dialog to install and open the FortiSOAR MEA .
- Note:** It may take some time to install the application. Also, note that on the first boot of FortiSOAR MEA, the Configuration Wizard runs automatically and performs the initial configuration steps for FortiSOAR MEA, such as enabling the embedded (default) Secure Message Exchange (SME), installing the trial license, etc. All of these steps take some time for completion.

Enabling the FortiSOAR MEA using the CLI

1. Login to FortiAnalyzer using SSH.
2. Enable the FortiSOAR MEA using the following commands:

```
FAZ-VM64 # config system docker  
(docker) # set status enable  
(docker) # set fortisoar enable  
(docker) # end
```

You can check the status of the FortiSOAR MEA using the following command:

```
FAZ-VM64 # diagnose docker status
```

Once the FortiSOAR MEA extension is enabled, a trial FortiSOAR experience gets activated. For the trial mode, you do not require a license, a **Trial(Extension)** license is already included. The trial mode is limited by 2 users that can use FortiSOAR MEA for a maximum of 300 actions a day.

Also, by default, the IR Content Pack is installed. For more information on the IR Content Pack, see the [FSR-IR-CONTENT-PACK](#) article present in the Fortinet Knowledge Base.

Licensing FortiSOAR MEA

The FortiSOAR MEA is shipped with a Trial (Extension) license by default and you do not need to install any additional license to use FortiSOAR MEA on FortiAnalyzer. The trial mode is limited by 2 users that can use FortiSOAR MEA for a maximum of 300 actions a day.



Important steps such as "Create Records", "Update Records", "Find Records", "Connection Actions", etc., are counted towards the maximum action count limit of 300. However, steps used for data manipulation such as "Wait", "Approval", "Loops", "Reference a Playbook", etc. are not counted towards the action count restriction.

For a more extensive usage without action count limit and to enable more users, you can update the trial license at any time to a FortiSOAR license. However, since the trial license is an "Enterprise" type license, you can only deploy a FortiSOAR license of type "Enterprise" using the FortiSOAR UI.

To update the Trial (Extension) license to a FortiSOAR license:

1. Log onto FortiSOAR.
2. Click **Settings > License Manager** to open the **License Manager** page as shown in the following image:

The screenshot shows the FortiSOAR License Manager interface. On the left, there's a sidebar with icons for System, Configuration, Audit Log, License Manager (which is selected), Agent Configurations, Secure Message Exchange, Agents, and Security Management. The main panel has a title 'System' and a sub-section 'License Manager'. It displays the following information in a table:

Serial Number	FSRVMPTM20000061
Type	Extension
Edition	Enterprise
Total Users	2 Users
Device UUID	dfe727eabb50fc08c27ee895ae048c2
Allowed Actions Per Day	200 (Consumed: 23/200)

At the bottom of the main panel, there's a button labeled 'Update License' with a file icon.

3. To update your license, click **Update License** and either drag-and-drop your updated license or click and browse to the location where your license file is located, then select the file and click **Open**.

Accessing FortiSOAR MEA using SSH

If you SSH to FortiSOAR MEA on FortiAnalyzer for the first time, then you must accept the FortiSOAR MEA EULA. To accept the EULA on the FortiAnalyzer CLI, do the following:

1. Login to FortiAnalyzer using SSH.
2. Ensure that the FortiSOAR MEA Extensions is enabled. For more information, see [Enabling the FortiSOAR MEA MEA using the CLI](#) section.
3. Get the FortiAnalyzer root prompt by running the `execute shell` command.
4. Run the following command:
`docker exec -ti -u csadmin fortisoar_fortisoar_1 bash -l`

This command will ask you to accept the EULA. You must accept the EULA before you can proceed to the FortiSOAR MEA Configuration Wizard.

After you accept the EULA and the Configuration Wizard is run, you can perform various operations on the FortiAnalyzer CLI such as checking the statuses of the FortiSOAR MEA using the FortiSOAR Admin CLI (csadm). For example, to check the status of services run the `csadm services --status` command. For more information on 'csadm' see the see the *FortiSOAR™ Administration Guide*.

Backing up and restoring FortiSOAR MEA configurations

When FortiSOAR MEA is enabled, and you perform a backup of FortiAnalyzer using its UI, then the FortiSOAR MEA configurations also get backed up. You can then use these backed up configurations to restore the FortiSOAR MEA configuration.



Only FortiSOAR MEA configurations are backed up, FortiSOAR MEA data is not backed up. To backup and restore both the configurations and data of FortiSOAR MEA, use the `csadm db` command. For more information, see the *Backing up and Restoring FortiSOAR* chapter in the "Administration Guide."

More Information

FortiSOAR is available as follows:

- As a management extension application with FortiAnalyzer called FortiSOAR MEA. For information about FortiSOAR MEA, see the [FortiAnalyzer Documentation](#).
- As a stand-alone product called FortiSOAR. For information about stand-alone FortiSOAR, see the [FortiSOAR Documentation](#).

This guide includes information about enabling FortiSOAR MEA in FortiAnalyzer. It also provides information about how FortiSOAR MEA works with FortiAnalyzer.

After FortiSOAR MEA is enabled with FortiAnalyzer, you can configure and use features, such as authentication and log management, which are the same in FortiSOAR MEA and stand-alone FortiSOAR. For more information about configuring FortiSOAR features, see the *FortiSOAR Administration Guide* and for using FortiSOAR, see the *FortiSOAR User Guide*.



www.fortinet.com

Copyright© 2021 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.