r1 Administration Guide

FortiSOAR MEA 7.0.1
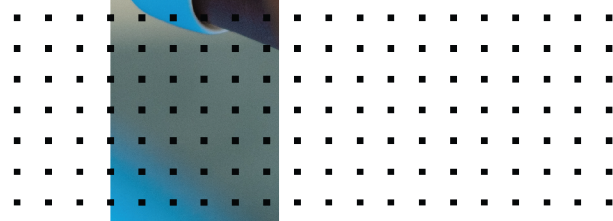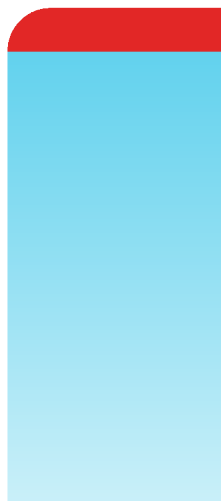
FORTINET DOCUMENT LIBRARY

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/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

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-07-23	Initial release of 7.0.1

Introduction

This document provides information about FortiSOAR MEA version 7.0.1. FortiSOAR MEA is a management extension application (MEA) that can be enabled with some FortiManager models.

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 FortiManager and allows you to manage your security operations using FortiManager and without the need of having a separate FortiSOAR instance.

How FortiSOAR MEA works with FortiManager

When enabled, the FortiSOAR MEA gets installed on FortiManager. An MEA is a management extension application that is released and signed by Fortinet to run on FortiManager. 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 FortiManager version 7.0.0 onwards, there is a capping of 50% on RAM and CPU for MEAs. This means if FortiManager 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 FortiManager with sufficient resources to meet the minimum (default) FortiSOAR MEA configuration of 4 CPU cores and 8 GB RAM, which would mean that FortiManager 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 FortiManager 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 FortiManager, then ensure that the FortiManager 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

FortiManager 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 FortiManager GUI

1. Ensure you are using ADOM version 6.4 or later.
2. Log on to FortiManager 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 FortiManager using SSH.
2. Enable the FortiSOAR MEA using the following commands:
   ```
   FMG-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:
```
FMG-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 FortiManager. 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 (Extenstion) 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:
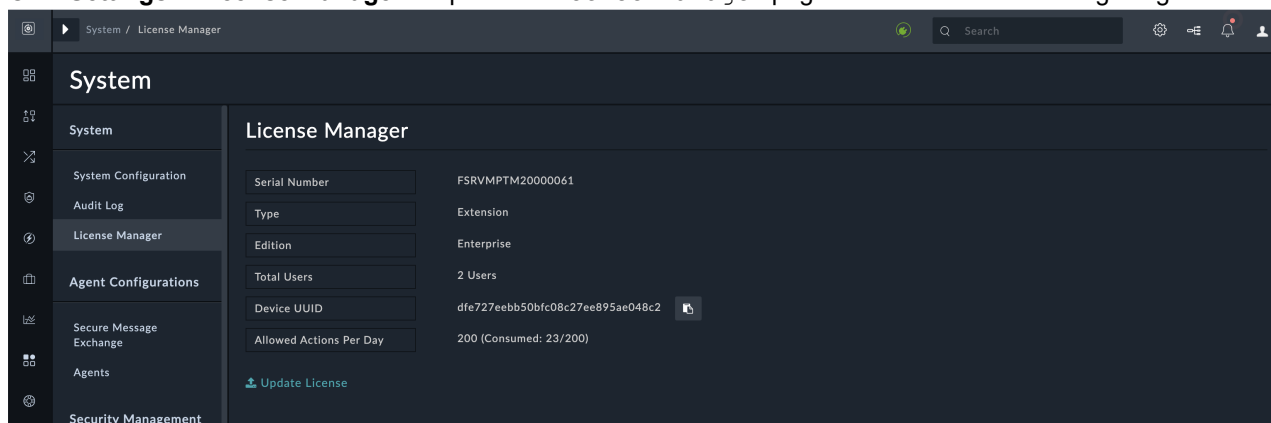
3. To update your license, click **Update License** and either drag-and-drop your updated license or click and browse to the location where your license file is located, then select the file and click **Open**.

Accessing FortiSOAR MEA using SSH

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

1. Login to FortiManager 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 FortiManager 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 FortiManager 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 FortiManager 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."

Troubleshooting issues faced in FortiSOAR MEA

The default Trial(Extension) license does not get installed

There might be cases when your default Trial(Extension) does not get installed or you face an issue with license synchronization during deployment.

Resolution

Upload your license using the FortiSOAR UI and once the license is uploaded, you can install the license. If you are still facing a synchronization issue, click the **Retry Sync** button on the UI.

More Information

FortiSOAR is available as follows:

- As a management extension application with FortiManager called FortiSOAR MEA. For information about FortiSOAR MEA, see the FortiManager 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 FortiManager. It also provides information about how FortiSOAR MEA works with FortiManager.

After FortiSOAR MEA is enabled with FortiManager, 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*.

FORTINET

www.fortinet.com