

# Release Notes

## FortiSOAR Cloud 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](mailto:techdoc@fortinet.com)



April, 2022

FortiSOAR Cloud 7.2.0 Release Notes

00-400-000000-20210416

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>FortiSOAR Cloud 7.2.0 Release</b> .....	<b>5</b>
<b>New features and enhancements</b> .....	<b>6</b>
<b>Special Notices</b> .....	<b>7</b>
FortiCloud Premium license .....	7
Introduction of the SOAR Framework Solution Pack .....	7
Change in the default role from T1 Analyst to SOC Analyst .....	8
<b>Upgrade Information</b> .....	<b>9</b>
Downgrading to previous versions .....	10
<b>Product Integration and Support</b> .....	<b>11</b>
Web Browsers & Recommended Resolution .....	11
<b>Limitations of FortiSOAR Cloud</b> .....	<b>12</b>

# Change Log

Date	Change Description
2022-04-21	Initial release of 7.2.0

# FortiSOAR Cloud 7.2.0 Release

FortiSOAR Cloud is a cloud-hosted Security Orchestration & Automated Response (SOAR) platform. It provides solutions for automating incident triaging & investigation; by seamlessly integrating with over 300+ security platforms resulting in faster responses, streamlined containment, and reduced mitigation times - from hours to seconds.

This document provides information about FortiSOAR Cloud version 7.2.0.

# New features and enhancements

## **Multi-Region support**

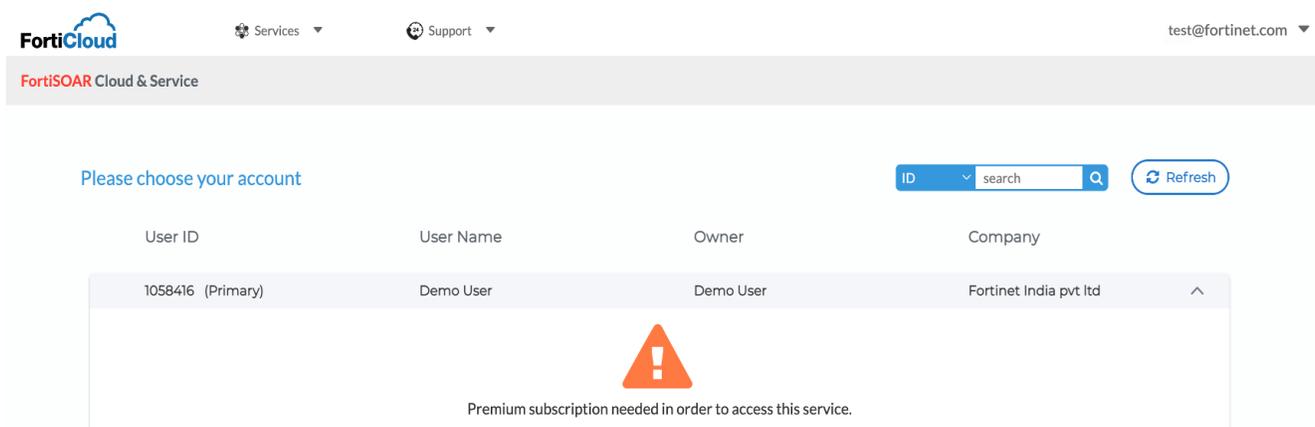
FortiSOAR Cloud 7.2.0 includes multi-region support.

## Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiSOAR Cloud version 7.2.0.

### FortiCloud Premium license

The FortiSOAR Cloud portal checks for the FortiCloud Premium license. If the FortiSOAR Cloud license is valid, but the FortiCloud Premium license is expired, a warning is displayed as shown in the following image:



To access the portal, renew the FortiCloud Premium license.

### Introduction of the SOAR Framework Solution Pack

Release 7.2.0 introduces the SOAR Framework Solution Pack (SP) which is the **Foundational** Solution Pack that creates the framework, including modules, dashboard, roles, widgets, etc., required for effective day-to-day operations of any SOC. The Incident Response modules have been removed from the FortiSOAR Cloud platform and moved to the SOAR Framework SP. Therefore, from release 7.2.0 the Incident Response modules, i.e., Alerts, Incidents, Indicators, and War Rooms are not part of the FortiSOAR Cloud platform, making it essential for users to install the SOAR Framework SP to optimally use and experience FortiSOAR Cloud's incident response. For detailed information about the SOAR Framework SP, see the SOAR Framework SP documentation.



In release 7.2.0 the SOAR Framework Solution Pack is installed by default on your FortiSOAR Cloud system.

## Change in the default role from T1 Analyst to SOC Analyst

When a new user logs in to their account, they are automatically assigned the SOC Analyst (earlier T1 Analyst) role on FortiSOAR, if they are added as a 'Limit Access' user in FortiCare.

# Upgrade Information

You can upgrade FortiSOAR Cloud using the Cloud portal.

1. Log onto the FortiSOAR Cloud Portal and navigate to your FortiSOAR Cloud VM page:

The screenshot displays the FortiSOAR Cloud & Service portal. At the top, there are navigation links for Services and Support, and a user profile for test@fortinet.com. Below the navigation, there are statistics for ACCOUNTS (1), REGIONS (0), ALARMS (0), and EXPIRING (0). A search bar and a REFRESH button are also visible. The main content area shows a table with columns for User ID, User Name, Owner, Company, and Region. Below the table, there are three gauges for VM resources: vCPU (8 vCPUs) at 100%, RAM (32 GB) at 23.6%, and Disk (1000 GB) at 0.2%. To the right, there is an INSTANCE INFORMATION section with details like Serial Number, Entitlement Expiry Date, Premium Expiry Date, Firmware Version, and Last updated on VM metrics. A sidebar on the right contains buttons for Reboot, Snapshot, Revert, WebSSH, and Enter.

2. To take a snapshot, click the **Snapshot** button.
3. Once your FortiSOAR Cloud VM has come up, go to the console of your FortiSOAR Cloud VM by clicking the **SSH** button.

4. Check that you are connected to a `screen` session. A `screen` session is needed for situations where network connectivity is less than favorable. You can check your `screen` session using the following command:

```
# screen -ls
```

This command returns an output such as the following example:

```
There is a screen on:
```

```
12081.upgrade (Detached)
```

Log back into the SSH console and run the following command to reattach the `screen` session:

```
screen -r 12081.upgrade
```

OR

```
screen -r upgrade
```

5. To upgrade your FortiSOAR Cloud, run the upgrade script as follows:

```
# sh upgrade-fortisoar-<version_number>.bin
```

OR

```
# chmod +x upgrade-fortisoar-<version_number>.bin
```

```
# ./upgrade-fortisoar-<version_number>.bin
```

For more information on the upgrade process, see the *FortiSOAR Upgrade Guide* in the [FortiSOAR Documentation Library](#).



In case the upgrade fails, collect the logs using the FortiSOAR UI. In the FortiSOAR UI, click the **FortiSOAR Version Number Build number** link to display the FortiSOAR dialog. Click the **Download Logs** link in the FortiSOAR dialog to download FortiSOAR logs. You can also use the `csadm log --collect` command to collect the logs.

Once you have collected the logs, revert the snapshot from the FortiCloud portal, and then open a support ticket with the logs attached so that Fortinet support can assist with the upgrade.

## Downgrading to previous versions

Downgrade to previous versions of FortiSOAR Cloud is not supported.

# Product Integration and Support

FortiSOAR Cloud version 7.2.0 supports the following item:

- Web browser support

## Web Browsers & Recommended Resolution

FortiSOAR Cloud 7.2.0 User Interface has been tested on the following browsers:

- Google Chrome version 100.0.4896.75
- Mozilla Firefox version 99.0
- Microsoft Edge version 99.0.1150.55
- The recommended minimum screen resolution for the FortiSOAR Cloud GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI might not get properly displayed.

## Limitations of FortiSOAR Cloud

- Only two SKUs are supported, one for the Enterprise edition and the other one for Multi-tenancy (master can be used for shared tenancy use cases only).
- High Availability (HA) is not supported. For HA, FortiCloud's intrinsic support will be leveraged.
- Only a single FortiSOAR Cloud VM is supported per FortiCare account.
- Upgrading FortiSOAR Cloud is a manual process as defined in the [Upgrade Information](#) chapter. Also, in case of an upgrade failure, the account owner needs to go to the FortiCloud portal and manually revert the snapshot.



[www.fortinet.com](http://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.