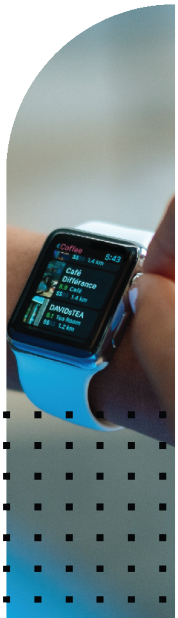
Release Notes

FortiSOAR Cloud 7.0.2



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

October, 2021
FortiSOAR Cloud 7.0.2 Release Notes
00-400-000000-20210416

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-10-11	Initial release of 7.0.2

FortiSOAR Cloud 7.0.2 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 7.0.2.

The recommended minimum screen resolution for the FortiSOAR Cloud GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

New features and enhancements

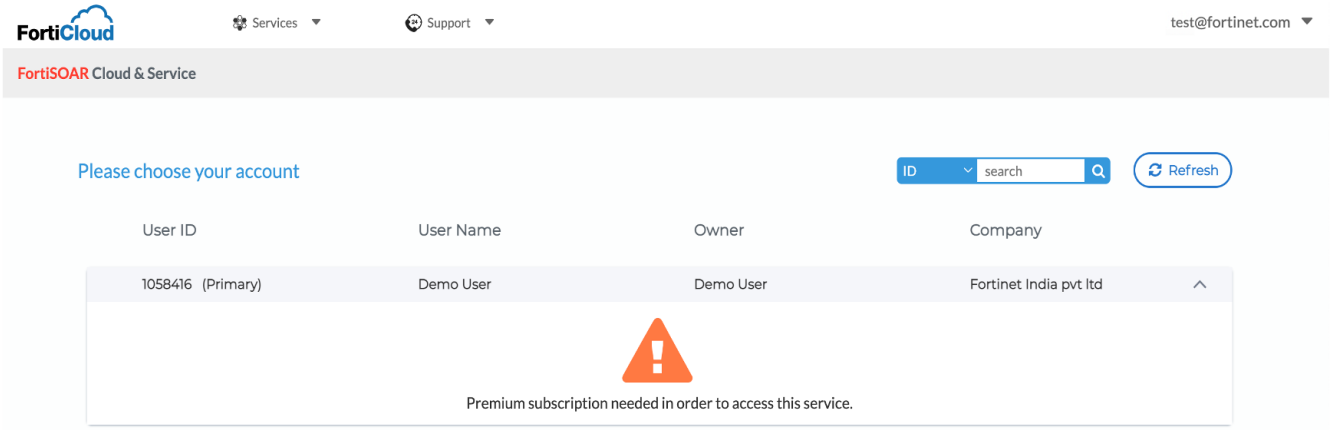
Feature	Details
Added support for client-based certificate authentication to Secure Message Exchange	FortiSOAR Cloud version 7.0.2 supports client-based certificate authentication to create connections between FSR agents or tenants and secure message exchange. Thereby enhancing security by ensuring that only trusted clients can connect to the secure message exchange. Prior to the 7.0.2 release, only basic authentication using username and password was used to create connections between FSR agents or tenants and secure message exchange was supported. Now, the following types of authentications are supported: • **Basic Authentication with Peer Verification**: Uses username and password to create connections between FSR agent or tenant and secure message exchange, and also performs 'Certificate Verification'. • **Client Certificate Authentication**: Presents a certificate to the server which is signed by a trusted CA, and which uses the Common Name (CN) as the username when an agent or tenant tries to connect with the secure message exchange.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiSOAR Cloud version 7.0.2.

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.

Client Certificate Authentication

From version 7.0.2 onwards, you can use client certificate based authentication to create connections between the distributed tenants or FSR agents and the secure message exchange. Prior to the 7.0.2 release, basic authentication using username and password was used to create connections between distributed tenants and secure message exchange. Going forward, you can configure the following types of authentications in FortiSOAR Cloud to connect distributed tenants or FSR agents and secure message exchange:

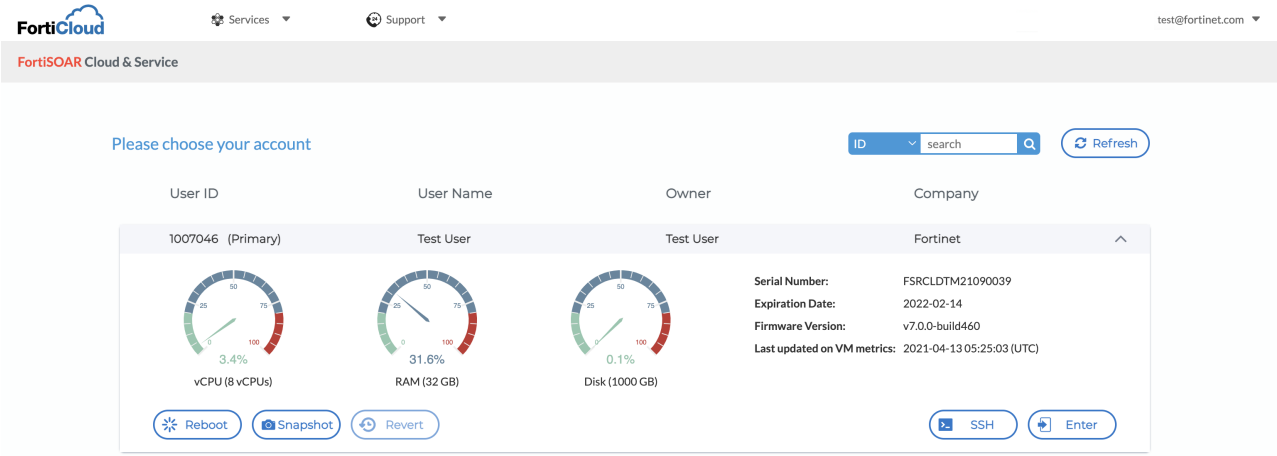
- **Basic Authentication with Peer Verification**: Uses username and password to create connections between FSR agents or distributed tenants and secure message exchange, and also performs 'Certificate Verification'. This process will verify that the clients which are attempting to connect can be trusted by presenting a certificate that is signed by a CA and trusted by the server; thereby ensuring that only trusted clients can connect to the secure message exchange.
- **Client Certificate Authentication**: Presents a certificate to the server which is signed by a trusted CA. It is recommended that you create the certificate with the common name as the name of your agent or tenant. This provides enhanced security as this gives the facility to connect only to trusted clients.

In case of FortiSOAR Cloud you always require that clients that want to connect to secure message exchange must present the client certificate to the secure message exchange for verification, i.e., the `mutual TLS (mTLS)` is always enabled. In case of FortiSOAR Cloud, client certificates for secure message exchange and FSR agents are added by default, so you do not require to explicitly add the certificates. Also, in case of FSR agents, you need to reconfigure FSR agents by downloading the installer; however, the installer will contain auto-generated certificates. For more information, see the *Deploying* FortiSOAR chapter in the "FortiSOAR Deployment Guide" and the *FortiSOAR Admin CLI* chapter in the "FortiSOAR Administration Guide".

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:



2. To take a snapshot, click the **Snapshot** button.
   Note: Your FortiSOAR Cloud VM stops while the snapshot is in progress. Once the snapshot is completed the FortiSOAR Cloud VM restarts.
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 7.0.2 supports the following item:

- Web browser support

Web browser support

FortiSOAR Cloud version 7.0.2 supports the following web browsers:

- Chrome version 93.0.4577.63
- Firefox version 92.0
- Internet Explorer Edge version 93.0.961.47

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