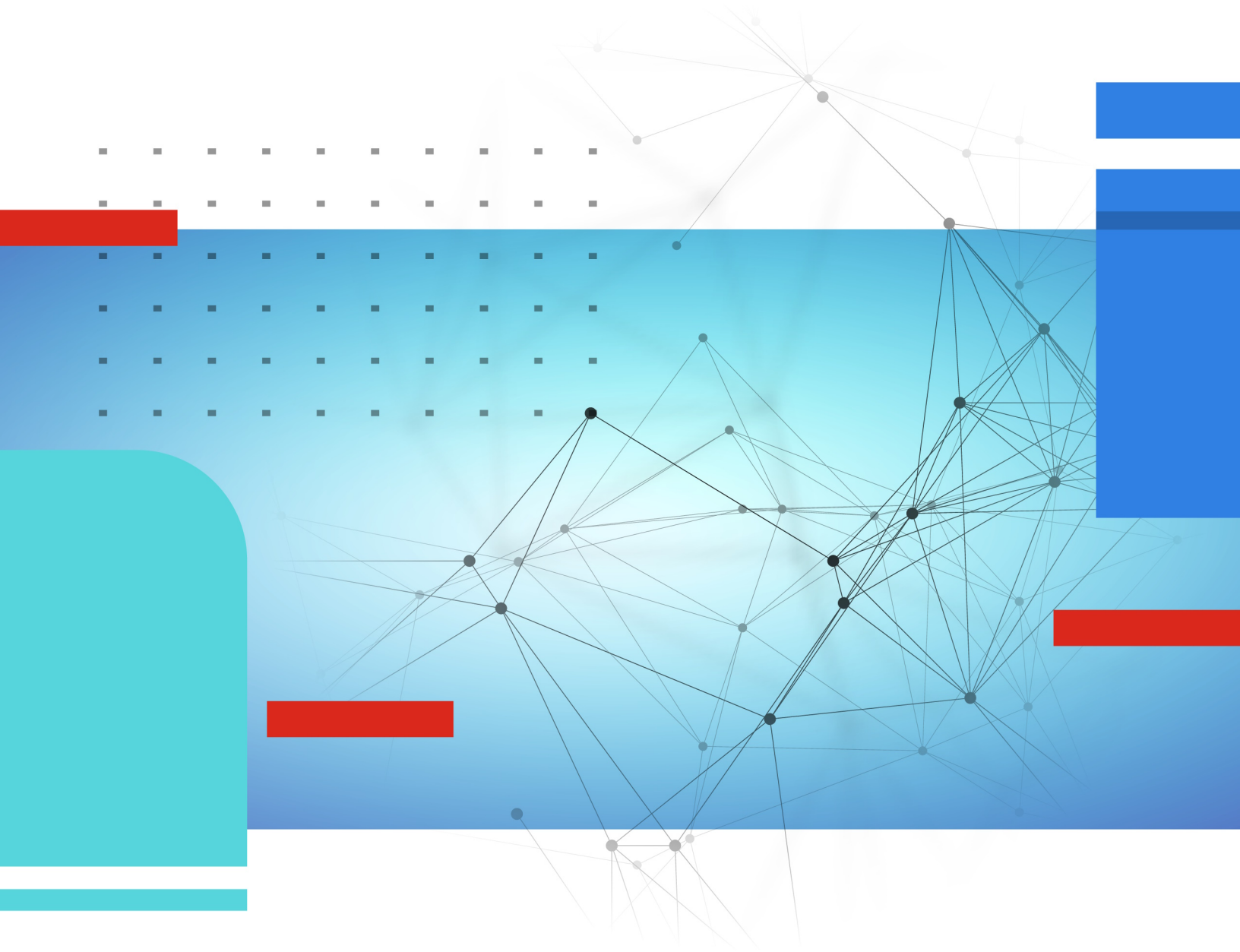
Getting Started

SOCaaS 24.4.c



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 5, 2026
SOCaaS 24.4.c Getting Started
00-244c-1077259-20260105

TABLE OF CONTENTS

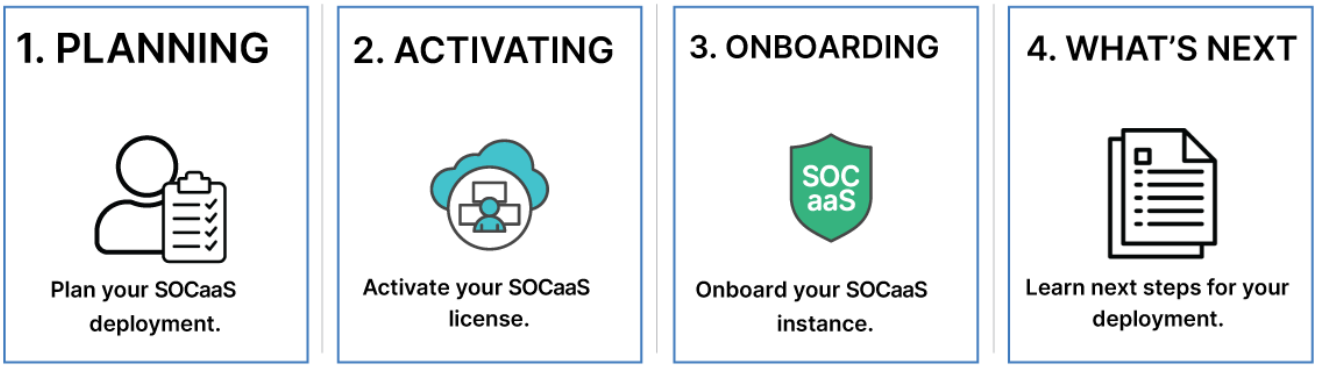
Change log

Date	Change description
2024-12-17	Initial release.
2025-09-11	Updated 1. Planning on page 6.
2026-01-05	Updated 4. What's next on page 11.

Getting started with SOCaaS

Steps to get started with SOCaaS

Getting started with SOCaaS consists of the following 4 steps:



1. PLANNING	**Plan your SOCaaS deployment by reviewing:** • **Team with a Fortinet partner or Fortinet account team on page 6** • **Asset monitoring on page 6** • **Licensing on page 7** • **Set up organizations and user profiles on page 7** • **Other requirements on page 8**
2. ACTIVATING	• **Register to activate your SOCaaS**
3. ONBOARDING	• **Complete the onboarding request from the FortiCloud SOCaaS portal** • **Generally takes 1-3 business days.**
4. WHAT'S NEXT	• **Subscribe to additional updates** • **Confirm SOCaaS release version - bottom left of portal** • **Learn more on page 11**

1. Planning

To ensure your SOCaaS deployment meets your business requirements and needs, plan your SOCaaS deployment by considering the following:

Team with a Fortinet partner or Fortinet account team

We highly recommend that you work with a Fortinet partner or your Fortinet account team to review how to fully leverage various Fortinet options to meet your target business and security goals. SOCaaS is provided as an easy add-on included with other product subscription to help you maximize investments. The collection team should be well versed in the SOCaaS offering as well as other products and services that work well with SOCaaS.

- **SOCaaS**—See the following to understand the scope of threat use cases covered by SOCaaS:
  - SOCaaS Datasheet
  - SOCaaS for Enterprise Handbook
  - SOCaaS for Partner and MSSP Handbook
- **FortiGuard**—See the FortiGate Subscriptions and FortiGuard Bundle Ordering Guide to select the service best suited for your needs. Enterprise protection bundle is recommended to enable the widest reach of threat use detections available through SOCaaS.

Asset monitoring

Plan a list of assets (log sources) to be monitored by SOCaaS by considering the following questions:

- What threats use cases are important?
- What critical applications need to be protected?
- What internal / external and user / system traffic is of interest?
- What Fortinet devices / controls are in place to protect the applications?
- What security and events logs are needed to monitor the threat use cases of interest?
- What events and alerts are to be filtered out?

- Which subnets / networks are to be filtered out?
- What threat visibility can be leveraged with other Fortinet deployed devices? See the SOCaaS Release Notes for a list of devices supported by SOCaaS.

If you are using on-premises FortiAnalyzer, perform a sizing exercise to determine the expected log rate and storage requirements to ensure continuous log collection and processing. Refer to the following topics in the SOCaaS User Guide for more details:

- Configuring log buffer cache size
- Estimating average log volume

Based on the answers to these questions, you can then determine the focused threat use cases. See the following handbooks to understand the scope of threat use cases covered by SOCaaS:

- SOCaaS for Enterprise Handbook
- SOCaaS for Partner and MSSP Handbook

Licensing

The SOCaaS portal enforces license requirements when you log in. SOCaaS requires the SOCaaS subscription. See Licensing for details.

Set up organizations and user profiles

Before submitting a SOCaaS onboarding request, set up proper user groups and permissions to ensure all users that will be using the service have the required permissions. Refer to the following resources for more details:

- For regular customers, see the FortiCloud Identity & Access Management (IAM) Guide for information about setting up user profiles.
- For MSSP customers, see the FortiCloud MSSP Deployment Guide (Organizations) and Asset Management for Partners Guide. To set up organizations in FortiCloud, see the following videos and guides:
  - FortiCloud Organizations - Overview video
  - FortiCloud Organizations – Getting Started video
  - FortiCloud Organization Portal Guide

  After your organization is set up, submit a SOCaaS Service Request to add your organization to SOCaaS. Our SOCaaS Operations team will help to confirm that your organization is ready to be used in SOCaaS.

If you have difficulty setting up your FortiCloud organizations and/or user access and require assistance, please open a ticket with Fortinet Customer Support.

Other requirements

After considering all the above, ensure that all the prerequisites listed in the Requirements section in the SOCaaS User Guide are met before proceeding to the next step: 2. Activating on page 9.

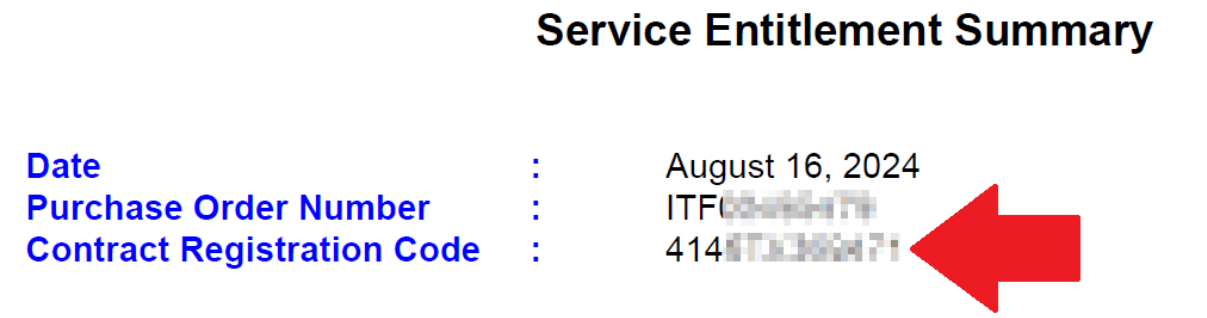
2. Activating

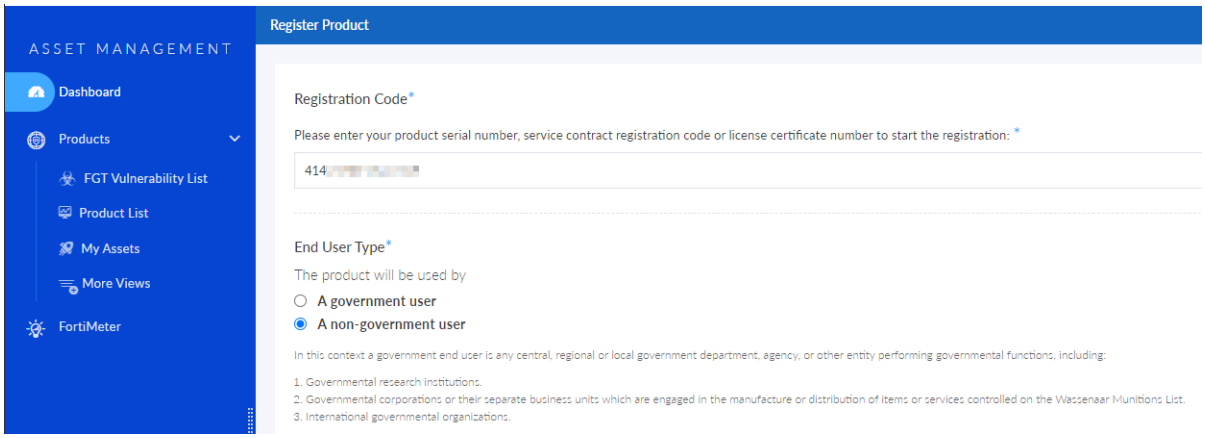
Activate your SOCaaS license by registering your devices and the SOCaaS license using your FortiCloud account.

To register your SOCaaS license:

1. Sign into your FortiCloud account, go to *Products*, and click *Register More*.
2. In the *FortiCloud Registration Code* field, enter the *Contract Registration Code* in the *Service Entitlement Summary* document that you received via email. In the example, the code is *414*....

   PLEASE REMEMBER TO REGISTER YOUR CONTRACT REGISTRATION CODE

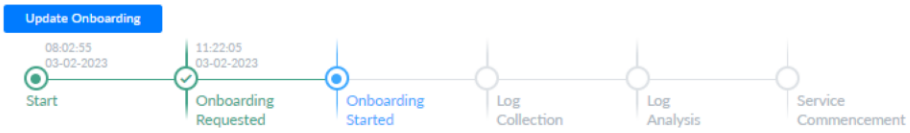




3. Continue with the remaining instructions to register your SOCaaS license. See Registering assets for details on the registration process.

3. Onboarding

Onboard your SOCaaS by completing the onboarding request from the FortiCloud SOCaaS portal:

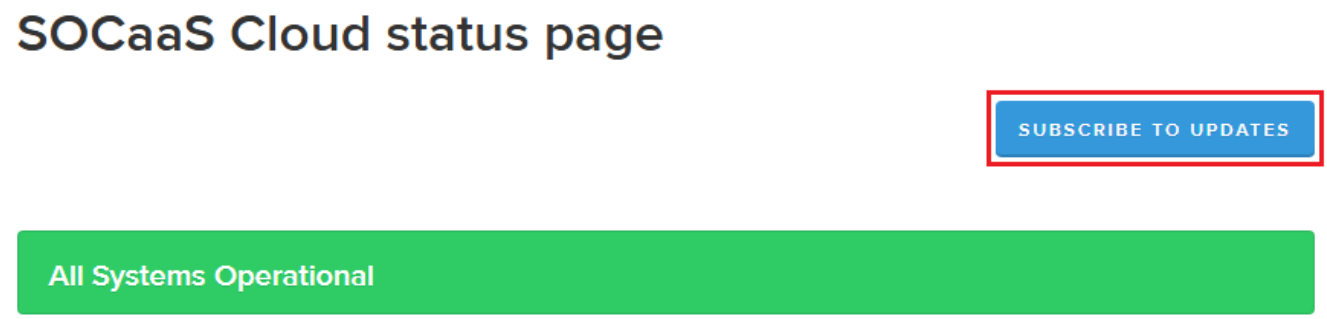


- Regular customer onboarding
- MSSP Onboarding

4. What's next

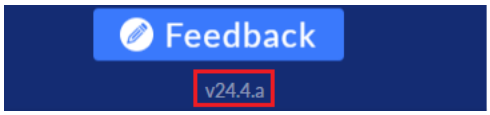
Subscribe to additional SOCaaS updates.

You can subscribe to SOCaaS system status notifications by going to https://status.socaas.forticloud.com/ and clicking *SUBSCRIBE TO UPDATES*.



Confirm your SOCaaS release version.

Log in to the SOCaaS portal and check the bottom left of the GUI to see the SOCaaS release version.



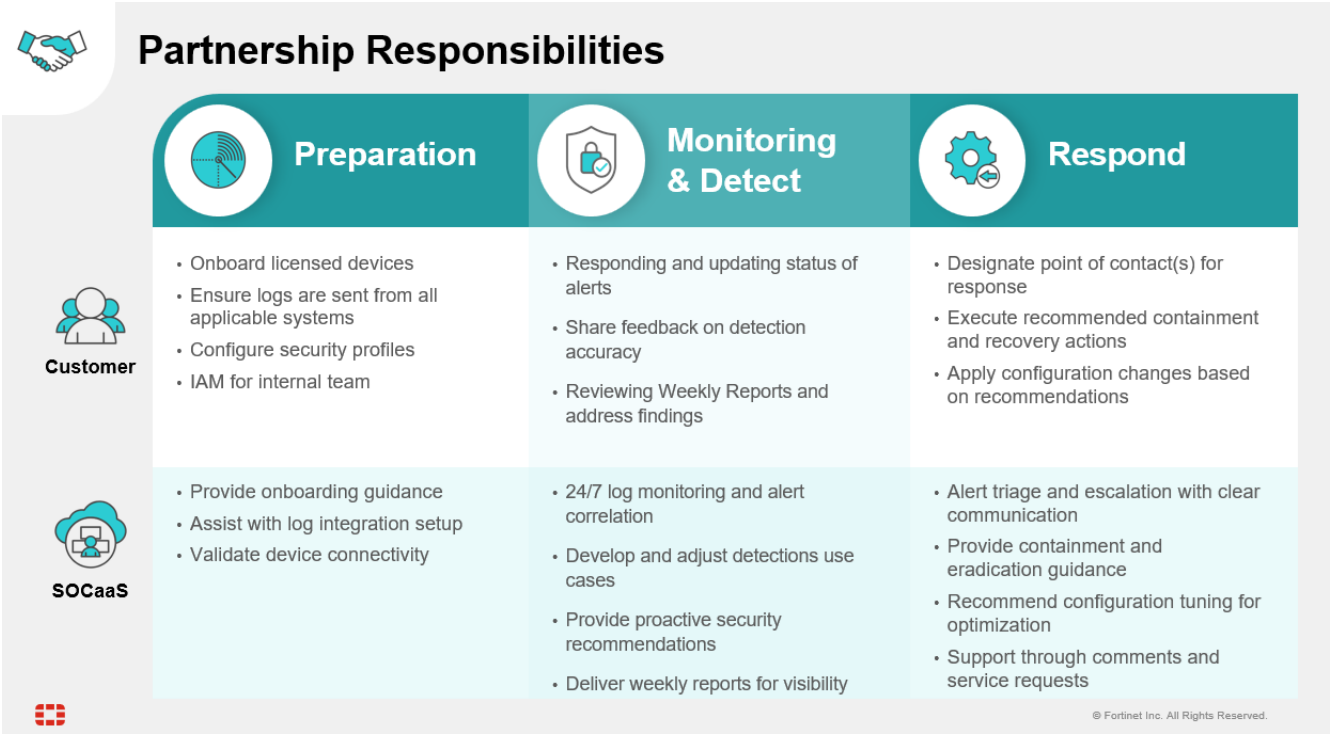
Learn more

Check out the following SOCaaS resources to learn more about SOCaaS:

- **SOCaaS documentation**
  - **Release Notes - New features and changes in your SOCaaS version**
  - **User Guide - Detailed information about using SOCaaS**
  - **SOC Portal training and other how-to Videos**
  - **FAQ - Frequently asked questions about SOCaaS**
- **FortiCompanion to Technical Support - requires FortiCloud account**
  - **Service requests**

Partnership responsibilities

Success with SOCaaS comes from collaboration. Together, proactive communication and timely action create a stronger security posture. The image below highlights the key responsibilities for both parties to ensure a successful SOCaaS relationship.


Partnership Responsibilities
Preparation
Monitoring & Detect
Respond
Customer
• Onboard licensed devices
• Ensure logs are sent from all applicable systems
• Configure security profiles
• IAM for internal team
• Responding and updating status of alerts
• Share feedback on detection accuracy
• Reviewing Weekly Reports and address findings
• Designate point of contact(s) for response
• Execute recommended containment and recovery actions
• Apply configuration changes based on recommendations
SOCaaS
• Provide onboarding guidance
• Assist with log integration setup
• Validate device connectivity
• 24/7 log monitoring and alert correlation
• Develop and adjust detections use cases
• Provide proactive security recommendations
• Deliver weekly reports for visibility
• Alert triage and escalation with clear communication
• Provide containment and eradication guidance
• Recommend configuration tuning for optimization
• Support through comments and service requests
© Fortinet Inc. All Rights Reserved.

www.fortinet.com