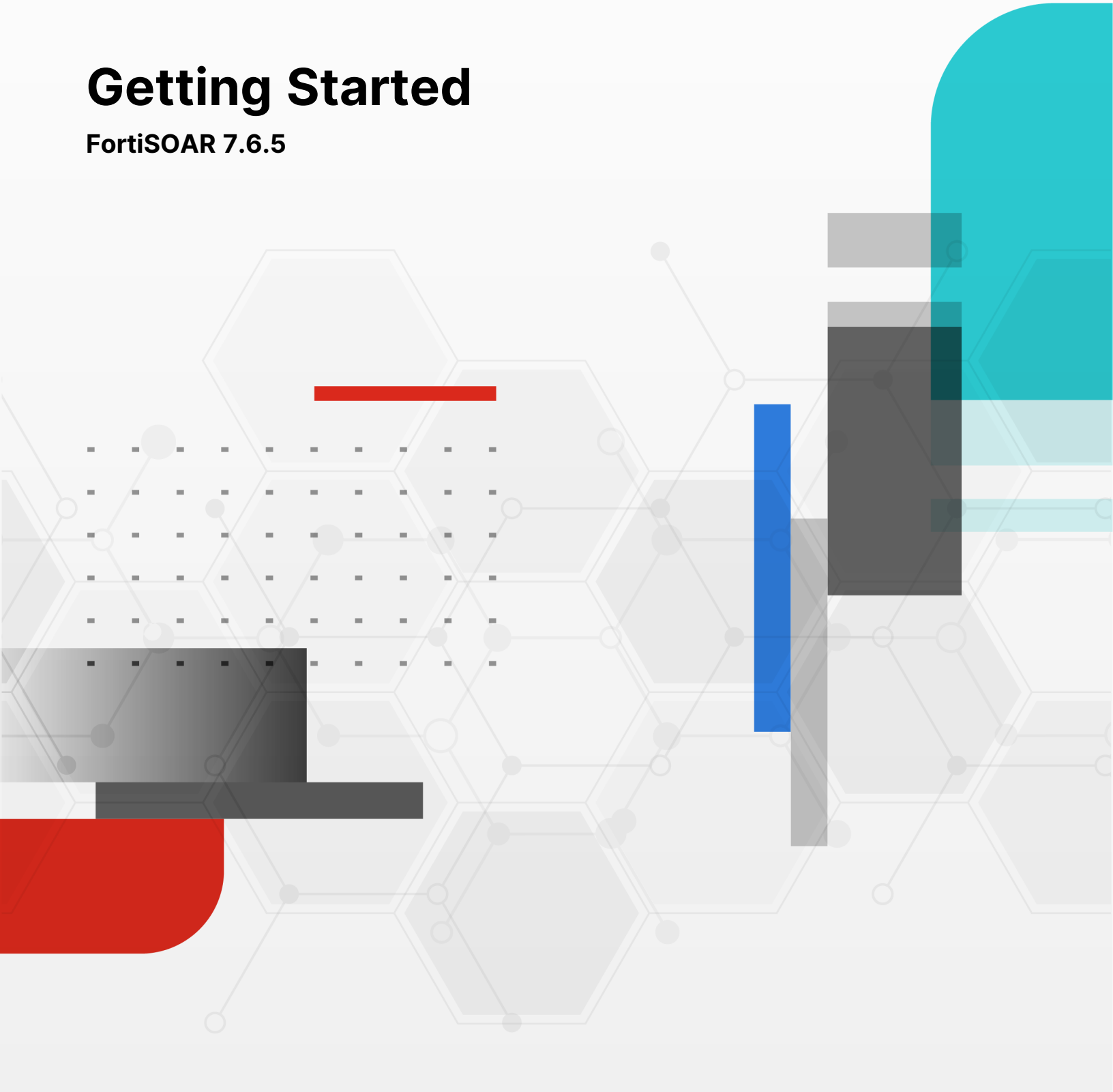
Getting Started

FortiSOAR 7.6.5



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

December, 2025
FortiSOAR 7.6.5 Getting Started
00-400-000000-20221031

TABLE OF CONTENTS

Change Log **4**
Overview **5**
Startup Steps **6**
Deployment and initial configuration **8**
Prepare to deploy FortiSOAR 8
Review the sizing and configuration 8
Choose the platform and specifications 8
Other Requirements 9
FortiSOAR Deployment and Initial Setup 9
Deploy FortiSOAR 9
Perform initial configuration 10
Activate your license 10
Accessing FortiSOAR 10
Setup Data Protection 12
Backing up data encryption keys 12
Scheduling data backups 12
Setting up HA clusters and DR 13
Perform additional configuration settings for FortiSOAR 13
Replace the self-signed certificates 13
Set up network proxy 13
Integrate FortiSOAR with your organization's Authentication systems 14
Additional settings 14
Create Users, Teams, and Roles 14
Set up a Segmented Network 14
Design your incident response platform **16**
Configure Indicator Extraction 17
Configure Enrichment and Mitigation Playbooks 17
Setup Data Ingestion 17
Configure your dashboards and reports 18
Define Notification Rules 18
Customize playbooks and solution packs **19**
Create custom investigation playbooks 19
Configure additional use-cases 19
Maintain your FortiSOAR system **20**
Set up system monitoring 20
Configure playbook and audit log purging 20
Set up CI-CD between your development and production environments 20
Retain data for audit 21

Change Log

Date	Change Description
2026-01-19	Enhanced the documentation related to disabling root shell access for `csadmin` users in the FortiSOAR Deployment and Initial Setup chapter.
2025-12-17	Initial release of 7.6.5

Overview

FortiSOAR is a platform designed to help organize records, actions, and workflows, allowing you to manage the entire lifecycle of a threat or breach within your organization.

This guide is intended to help new or experienced FortiSOAR administrators configure the system optimally using best practices, and also to familiarize you with the application and start exploring some of the core capabilities offered by FortiSOAR through detailed step-by-step instructions.

The guide focuses on setting up the 'Enterprise' flavor of FortiSOAR.

The guide includes a Startup Steps on page 6 to verify the completion of general deployment and configuration tasks. It is organized into the following sections:

- **Deploy** - Prepare your FortiSOAR system with the right hardware configuration, install FortiSOAR, and optimize your network and security settings for performance. For more information, see Deployment and initial configuration on page 8
- **Streamline** - Set up the incident response platform based on your record flow and automation of tasks such as ingestion, enrichment, and mitigation. For more information, see Design your incident response platform on page 16
- **Accelerate** - Leverage and customize various pre-defined playbooks and explore provided specialized Solution Packs. For more information, see Customize playbooks and solution packs on page 19.
- **Maintain** - Enable monitoring of your FortiSOAR system to ensure availability and optimal performance. For more information, see Maintain your FortiSOAR system on page 20.

For detailed information on FortiSOAR, see the FortiSOAR product documentation and visit the FortiSOAR user community.

Startup Steps

Use the following checklist to verify that all general deployment and configuration tasks have been completed.

	Task	Description
Deploy		
☐	Prepare the Environment	• Review sizing and resource configuration • Choose the deployment platform and specifications
☐	Deploy FortiSOAR	• Deploy FortiSOAR • Run the Configuration Wizard • Activate License • Log in to FortiSOAR • Set up a segmented network (*optional*)
☐	Configure Data Protection	• Back up encryption keys • Schedule data backups • Configure HA clusters and set up DR
☐	Perform Initial configuration	• Replace self-signed certificates (*recommended*) • Configure the network proxy (*recommended*)
☐	Set up Users and RBAC	• Add users, define teams, and assign roles and permissions
Streamline		
☐	Design the Incident Response Platform	• Configure indicator extraction • Setup enrichment and mitigation playbooks • Configure data ingestion • Design dashboards and reports • Define notification rules
Accelerate		
☐	Customize Playbooks and Solutions	• Develop custom investigation playbooks • Configure additional use cases
Maintain		
☐	Establish Operational Policies	• Set up system monitoring • Configure log purging

	• Implement CI/CD pipelines • Enable auditing and data archival

Deployment and initial configuration

This topic covers setting up a FortiSOAR server with the right hardware configuration, tuning network and security settings,and additional recommended configurations.

- Prepare to deploy FortiSOAR on page 8
- FortiSOAR Deployment and Initial Setup on page 9
- Setup Data Protection on page 12
- Perform additional configuration settings for FortiSOAR on page 13
- Create Users, Teams, and Roles on page 14
- Set up a Segmented Network on page 14

Prepare to deploy FortiSOAR

Before you begin the actual deployment of FortiSOAR, it is recommended that you complete the site preparations, including reviewing the sizing requirements and setting up the server with the appropriate hardware configuration.

Review the sizing and configuration

Use the FortiSOAR Sizing Guide to identify the right configuration for your anticipated workload. In release 7.6.1, a new CLI option for optimal resource configuration is added, which enables you to apply a configuration to tune all FortiSOAR services for the efficient use of available hardware resources, such as vCPU and RAM. For details, see the CLI Administration chapter in the "Administration Guide."

Choose the platform and specifications

If you are deploying FortiSOAR using the OVA, download the FortiSOAR Virtual Appliance and deploy it to VMware (via vSphere or vCenter) or AWS.
Alternatively, if you are installing FortiSOAR using the installation script, before deployment, ensure that you have setup a system with either Rocky Linux version 9.3/9.4/9.5/9.6 or RHEL version 9.3/9.4/9.5/9.6. Note that release 7.6.5 has been tested with RHEL 9.6 and Rocky Linux 9.6.

Virtual Machine (VM) recommended specifications:

- 12 available vCPUs
- 48 GB available RAM
- 1 TB available disk space: Recommended to have high-performance storage, preferably SSDs.
- 1 vNIC

Choose from the following supported hypervisors:

- On Premises
  - VMware ESXi versions 5.5, 6.0, 6.5, 7.0, and 8.0
  - Redhat KVM
- Cloud
  - FortiSOAR Cloud
  - AWS Cloud
- Docker

For any other virtualization or cloud hosting environment, such as GCP, Azure, OCI, or OCI DRCC, you can install Rocky Linux 9.3/9.4/9.5/9.6 or RHEL 9.3/9.4/9.5/9.6 and then install FortiSOAR using the FortiSOAR CLI installer. Note that release 7.6.5 has been tested with RHEL 9.6 and Rocky Linux 9.6. See the Deployment Guide for details.

Other Requirements

Internet access is highly recommended for FortiSOAR upgrades, license deployment, and installation of out-of-the-box connectors.

Add the following entries to the allowlist of your firewall or proxy servers:

For installing or upgrading (migrating) to FortiSOAR 7.3.0 or later: `*.rockylinux.org`

For upgrading FortiSOAR, installing connectors, and accessing the widget library: https://repo.fortisoar.fortinet.com/

For connector dependencies: https://pypi.python.org

For Ansible installation: https://files.pythonhosted.org

For FortiSOAR license synchronization: https://globalupdate.fortinet.net
Note: If SSL inspection is enabled on your proxy or firewall, ensure it is disabled for this URL to prevent connection issues.

For additional requirements such as port configurations, see the "Deployment Guide."

FortiSOAR Deployment and Initial Setup

Deploy FortiSOAR

After selecting the appropriate platform, sizing, and completing all prerequisites, deploy FortiSOAR using the process mentioned in the Deployment Guide.

Starting with release 7.6.5, the csadmin user's sudo privileges are restricted to only the commands required to work with FortiSOAR, instead of providing full 'root' access. This enhancement aligns with the principle of least privilege and reduces exposure to sensitive system files. Therefore, commands such as `yum`, `systemctl`, `csadm`, etc, must be prefixed with `sudo`, for example, `sudo csadm --help`.
To open or edit a file, prefix the command with '`sudo`' and specify the file's full path (`sudo vi <full path of file>`).
For example, `sudo vi /opt/cyops-auth/utilities/das.ini`.
Additionally note that for security reasons, '`root`' access is provided via the system console and is not available over SSH.

Perform initial configuration

Once installation is complete, use the 'Configuration Wizard' to bootstrap the appliance. This includes tasks such as automatically generating new keys and passwords unique to the FortiSOAR instance, generating the UUID for the device, and optionally changing the hostname and DNS of the FortiSOAR instance, etc.

Activate your license

After installing FortiSOAR, follow these steps to activate your license:

1. Login to your FortiCare account.
   Click **Asset** > **Register/Activate** to register your FortiSOAR product.
2. Generate license file.
   On the `Product Information` page, click **Edit**. In the **UUID** field, enter the Device UUID of your FortiSOAR installation, then click **Save**.
   For instructions on retrieving your Device UUID, see the Retrieving the FortiSOAR Device UUID topic in the "Deployment Guide."
3. Download and deploy the license.
   Download the generated license file, then upload it on the FortiSOAR logon page to activate your installation.
   For details on updating or renewing licenses, see the Licensing FortiSOAR chapter in the "Deployment Guide."

Before deploying your FortiSOAR license, ensure that the system can connect to https://globalupdate.fortinet.net. License deployment will fail without connectivity to this address, which is required to retrieve license entitlements and ensure proper product functionality after an upgrade.

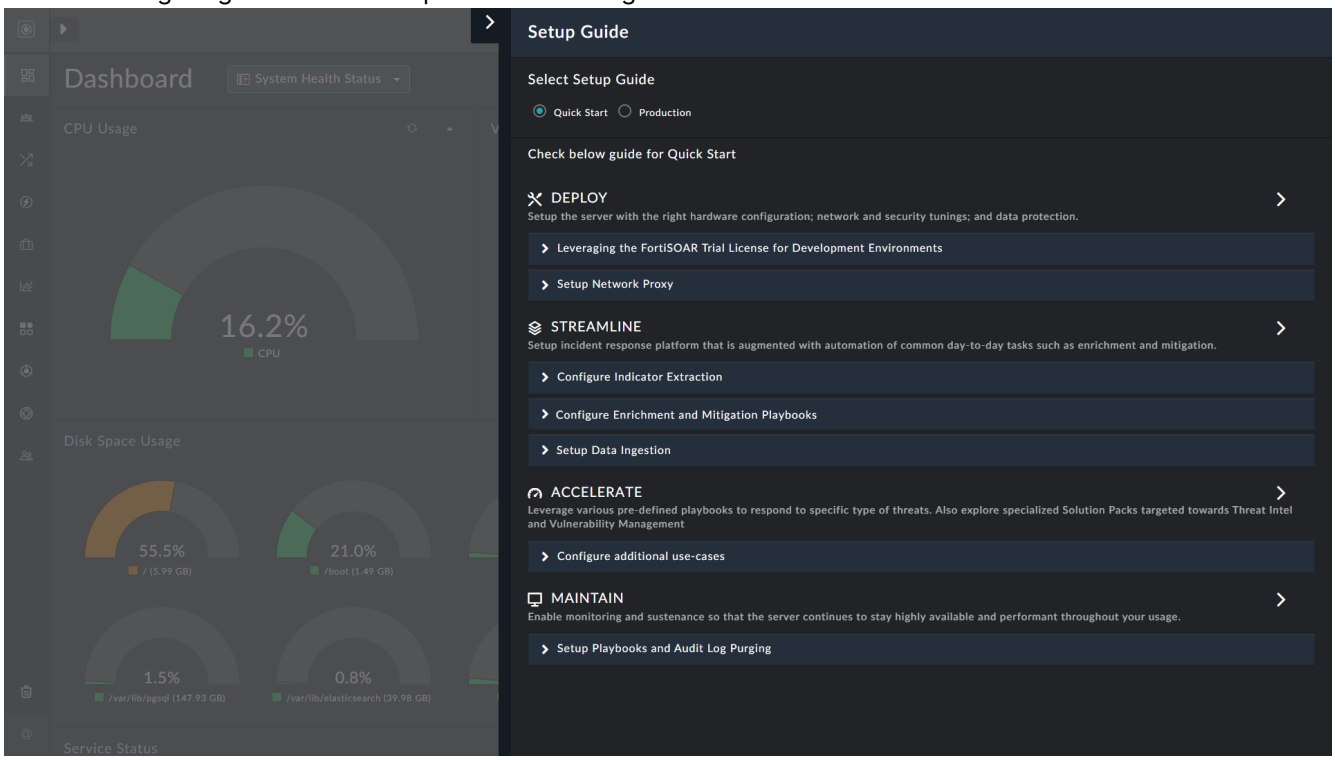
Accessing FortiSOAR

Once the license has been activated, you can log in to FortiSOAR and continue with the configuration process to complete the system setup.

When you log on to FortiSOAR for the first time as a csadmin user, you will be mandated to change your password. This enhances the security of your csadmin account and prevents unauthorized parties from accessing the administration account for FortiSOAR. New passwords that are set must contain at least 8 characters, one lower-case alphabet, one upper-case alphabet, one digit, and any one of the following special characters ~!@#$%^&*|?_

Ensure that you note down your csadmin password since if you forget your initial csadmin password, then you have to request FortiSOAR to reset this password. Also, when you are changing your csadmin password, you must ensure that you also update the email ID that is specified for csadmin, which by default is set to `soc@fortinet.com` (which is not a valid email ID). You can change the email ID by clicking the **User Profile** icon ( ) to open the `User Profile` page and change the email address in the **Email** field. Once you set a valid email ID in the user profile, then you would be able to reset your password, whenever required, by clicking the **Forgot Password** link on the login page.

When administrators log into FortiSOAR for the first time, they are presented with a 'Setup Guide' that assists them in configuring FortiSOAR for optimal functioning:



The minimum permissions required to view and use the 'Setup Guide' are 'Read' and 'Update' permissions for both `Security` and `Application` and 'Read' permission for `Widget` and `Solution Pack`. Additionally, ensure that the **Enable Setup Guide** option is selected on the `System Configuration` page (see the System Configuration and Management chapter in the "Administration Guide" for details), which is the default setting. For more information, see the Setup Guide Widget documentation.

To minimize the Setup Guide, click the **>** arrow. To reopen the Setup Guide, click the **Setup Guide** icon in the top-right corner of FortiSOAR:

To hide the Setup Guide icon, clear the **Enable Setup Guide** option on the `System Configuration` page.

Setup Data Protection

FortiSOAR offers a variety of data protection strategies, including scheduled data backups to Highly Available (HA) Clusters and Disaster Recovery (DR) options. Review the available options and, based on your Recovery Time Objective (RTO) and Recovery Point Objective (RPO), configure the appropriate strategy.

Backing up data encryption keys

Encryption keys are used to secure data within FortiSOAR. When FortiSOAR is installed for the first-time default encryption keys are generated automatically. These keys are unique to each instance, so you typically do not need to change them.
Important: It is highly recommended that you back up the encryption keys: `.Defuse.key` and `PASSWORD_ENCRYPTION_KEY`. For more information, see Backing up the data encryption keys.

Scheduling data backups

Use FortiSOAR's optimized backup and restore process to schedule regular data backups. This ensures data security and allows seamless restoration of data to a new FortiSOAR system when needed.

Setting up HA clusters and DR

FortiSOAR supports the creation of HA clusters using either an internal or external PostgreSQL database, and also provides various Disaster Recovery solutions. For detailed information, refer to High Availability Configuration and Maintenance.

Perform additional configuration settings for FortiSOAR

After running the FortiSOAR Configuration Wizard, you can enhance system security for production deployment based on your specific requirements. This includes tasks such as replacing the default self-signed certificates, configuring a network proxy, integrating FortiSOAR with authentication systems, and updating the FortiSOAR default database passwords.

Replace the self-signed certificates

FortiSOAR comes with default self-signed certificates for the web server, which are valid for two years from the time of FortiSOAR instance creation. For steps to regenerate these certificates, see the Regenerating Self-Signed certificates topic in the *Monitoring & Optimization* chapter in the "Best Practices Guide." For a production environment, it is strongly recommended to replace the default certificates with valid organization-signed certificates.

Set up network proxy

If your server accesses the internet and other intranet zones through a proxy, ensure that the proxy details are configured for the solution packs and connectors to establish the necessary outbound connections. This configuration is necessary to ensure that FortiSOAR can service all external requests. Additionally, ensure the following URLs are added to your organization's firewall or proxy server allowlist:

- Product software repository: https://repo.fortisoar.fortinet.com
- For connector dependencies: https://pypi.python.org
- License synchronization: https://globalupdate.fortinet.net
  Note: If SSL inspection is enabled on your proxy or firewall, make sure it disabled for this URL to prevent connection issues.

Integrate FortiSOAR with your organization's Authentication systems

You can integrate FortiSOAR with your organization's authentication systems to enable centralized and secure user access. Supported authentication methods include:

- SSO (Single Sign-On): FortiSOAR supports SSO integration with various identity providers, including FortiAuthenticator (FAC), Google, Microsoft Entra ID (formerly Azure AD), Okta, and others.
- LDAP: Enable LDAP or Active Directory authentication to allow user access through your organization's directory services. You can add users by mapping user attributes or by searching the directory and importing selected users.
- Radius: FortiSOAR supports authentication via a RADIUS server. Users can log in using their RADIUS credentials.

Additional settings

You can also apply additional, recommended settings such as changing the system hostname and updating the FortiSOAR default database passwords, to align with your organization's security and deployment standards.

Create Users, Teams, and Roles

After setting up your FortiSOAR system, the next step is to configure teams, users, and roles and assign appropriate permissions using FortiSOAR's Role-Based Access Control (RBAC) features. You can also configure authentication settings, such as setting session and idle timeouts, user account options, and access key management.

Set up a Segmented Network

FortiSOAR supports segmented networks, enabling secure remote execution of connector actions in multi-segmented environments. If you need to remotely run connector actions, you can use 'FortiSOAR Agents'. These agents support a deployment model that spans across network segments, allowing FortiSOAR—whether hosted on-premises or in the cloud—to securely connect to applications located in other network segments.

To set up an FSR agent, you need to:

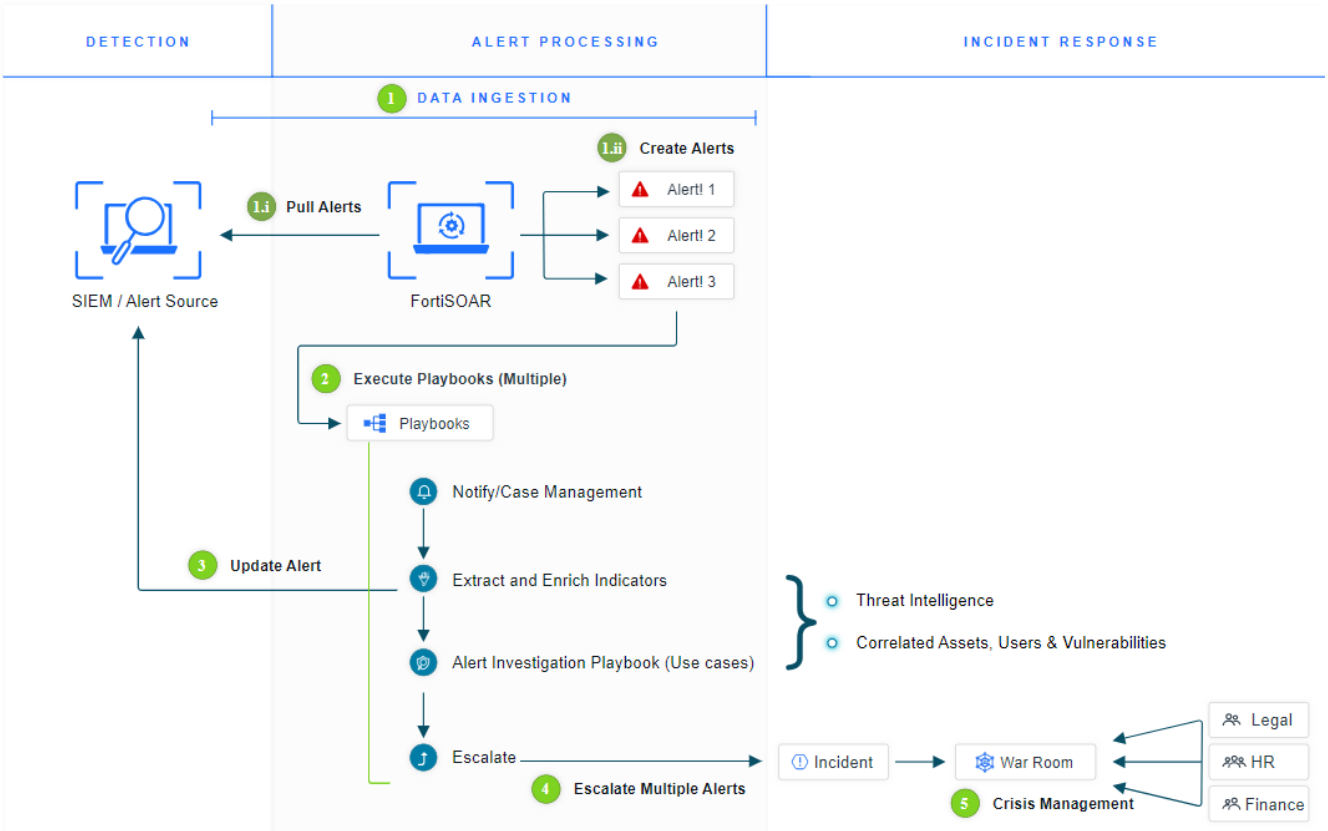
1. Add a Secure Message Exchange (SME).
   An SME establishes a secure channel to relay information to agents or tenant nodes. You can use an externally deployed SME, the default (embedded) SME, or both.
2. Add the agents to your FortiSOAR instance.
3. Install the agents.

For details, see the Deploying FSR Agents topic in the "Deployment Guide."

Design your incident response platform

When designing your incident response platform, it is important to understand your information flow and determine the sources from which alerts are generated. Typically, alerts are ingested into FortiSOAR using SIEMs, Emails, EDRs, and other sources. Once the alerts are ingested, multiple automated playbooks are run to extract and enrich the alerts. Extraction means the indicators such as source IP and destination IP that are associated with the alerts are created into indicator records. After extraction, the indicators need to be enriched using various threat intelligence platforms such as, VirusTotal and AlientVault, to add additional context to the indicator. This provides analysts with enough information to determine whether a given alert is a false positive or true positive. In the case of a true positive, the related alerts are escalated into an incident and automated playbooks can be used to mitigate the threat. Playbooks provide consistency in the complete incident response process, ensuring a consistent method of extracting, enriching, and investigating alerts. Additionally, if required crisis management can be leveraged by creating war rooms and using other utilities to respond to the incident. This is how FortiSOAR streamlines the complete incident response into a single console, eliminating the need for analysts to open multiple applications and saving a significant amount of time and frustration.

The following flowchart helps you understand the default flow of records through FortiSOAR based on the SOAR Framework Solution Pack; the flow can be changed to meet your requirements.



The streamline phase includes the following activities:

- Configure Indicator Extraction on page 17
- Configure Enrichment and Mitigation Playbooks on page 17
- Setup Data Ingestion on page 17
- Configure your dashboards and reports on page 18
- Define Notification Rules on page 18

Configure Indicator Extraction

The SOAR Framework Solution Pack (SFSP) includes indicator extraction playbooks that are triggered automatically when an alert or incident is created. These playbooks extract indicators from alert or incident fields and enrich them using predefined enrichment playbooks based on the indicator type.

To optimize the extraction process, you can configure the indicator extraction logic to match specific alert or incident types, add custom indicator types, or include additional fields of interest in the playbook to capture more data beyond the default fields, etc.

You can also exclude certain indicators from enrichment by adding them to an exclusion list, which helps reduce false positives and improve overall efficiency.

For more information, see the Indicator Extraction Configuration widget.

Configure Enrichment and Mitigation Playbooks

Playbooks in FortiSOAR allow you to automate security processes across external systems while aligning with your organization's business processes. You can customize the included playbooks to match your organization's procedures and take advantage of FortiSOAR's automation capabilities.

The SOAR Framework Solution Pack includes extraction and enrichment playbooks that are automatically triggered on indicator creation. Ensure that you configure the required threat intelligence integrations such as VirusTotal and IBM X-Force, for automatic enrichment. Similarly, the SOAR Solution pack also contains mitigation playbooks that should be configured to mitigate threats, such as blocking specific types of indicators, disabling specific users, and isolating hosts, based on your containment strategies.

Setup Data Ingestion

FortiSOAR is integrated with over 650 connectors to help you connect to various data sources. Use the 'Content Hub' in your FortiSOAR instance to configure connectors and set up data ingestion. This will ensure actionable events from your SIEMs, email servers, ticketing solutions, and other data sources are pulled at regular intervals to create alert records in your FortiSOAR system.

Most connectors come with pre-populated standard field mapping from the source data into the FortiSOAR alert record is pre-populated by most connectors. However, it's important to verify that the fields of your interest are

correctly mapped. See the FortiSOAR Connectors page to view the list of supported integrations and the data ingestion content for details.

Configure your dashboards and reports

The SOAR Framework Solution Pack installs a variety of dashboards, reports, and widgets to provide a comprehensive solution. The included dashboards and reports help you to effectively monitor your FortiSOAR setup and include key performance indicators(KPIs) such as Mean Time To Respond (MTTR).

Widgets visually display information based on your requirements. For example, the incident correlations widget shows the correlation graph of an incident, and the record distribution widget visualizes items/records and their correlations in different levels based on a given grouping context.

It is recommended that you configure the required reports and the dashboards such as the 'Overview' dashboard that displays total alerts received, escalation ratio, time saved, and closure reasons among many other things, and the 'SOC Admin' dashboard that shows recent incident, alerts, and assigned tasks. You can also customize these dashboards and reports or create new ones based on your needs.

Define Notification Rules

FortiSOAR is designed to involve humans in the investigation process, so generating timely action-centric (or informational) notifications is crucial. To achieve this goal, FortiSOAR includes a common framework for diverse notifications, such as email notifications, UI notifications from various services (like alerts/incidents/tasks assignments), Comments @mentions, and workflow failures. This notification framework allows users to have complete control over the setup and consumption of notifications, including how and when they want to receive notifications and what notifications they want to receive.

You should review notification rules to ensure they match your requirements, such as how and when teams and users are notified when an alert is assigned, or the notification generated when a user is mentioned in a comment. You must also provide the necessary details to configure the notification channel such as specifying the SMTP or Exchange configuration to be used for sending out the notifications.

Customize playbooks and solution packs

You can customize pre-defined playbooks to address to threats specific to your organization. Additionally, you can explore specialized Solution Packs for threat intelligence management, vulnerability and risk management, case and ticket management, and other areas.

The accelerate phase includes the following activities:

- Create custom investigation playbooks on page 19
- Configure additional use-cases on page 19

Create custom investigation playbooks

Build investigation playbooks tailored to your organization's needs and to assist in investigations or respond to threats specific to your organization. For guidance on building playbooks, refer the "Playbooks Guide."

Configure additional use-cases

Explore the packaged solutions available on FortiSOAR Content Hub, which automate various SOC use-cases, such as Phishing Email Response, Malware Response Using SIEM & EDR Solutions, and more. Additionally, the content hub also contains solution packs focused on specialized functions such as Brute Force Attack Response, Bi-Directional Jira Sync, MITRE ATT&CK Enrichment Framework, OT - Vulnerability Management, and others. Leverage these solution packs and integrations to create your own incident response solutions.

Maintain your FortiSOAR system

To ensure optimal performance of your FortiSOAR system, it is important to establish policies for monitoring, purging logs at regular intervals, auditing, and other related activities.

The maintain phase can contain the following activities:

- Set up system monitoring on page 20
- Configure playbook and audit log purging on page 20
- Set up CI-CD between your development and production environments on page 20
- Retain data for audit on page 21

Set up system monitoring

Setup system monitoring for your FortiSOAR instance to receive email notifications for server health including notifications for any service failures or if any monitored threshold exceeds the set threshold. This ensures that you can take preemptive actions for any issues with your FortiSOAR server.

You can also leverage FortiSOAR's integration with FortiMonitor to monitor system-level metrics on your instances, including CPU, RAM, disk usage, network bandwidth, and services such as Nginx and PostgreSQL.

Configure playbook and audit log purging

Setup log purging to rotate logs at regular intervals to prevent disk space issues and system slowdowns caused by excessive log volumes.

Set up CI-CD between your development and production environments

Use the FortiSOAR Continuous Delivery solution pack to automate your content development workflows and deploy quality code using a continuous and iterative process of building, testing, and deploying content through source control. You can test new FortiSOAR solution packs and your customizations to them into your staging environment, and then setup continuous delivery to streamline the process of implementing these changes in your production environment.

Retain data for audit

FortiSOAR offers various options for archiving data, allowing you to retain historical data for audit and compliance purposes, as well as for occasional reference. You can choose to enable log forwarding, which forwards logs to an external log management server (syslog server) to centralize and manage all logs in one location. Additionally, you can set up data archival for primary data if you need to retain it for longer periods in your data lake.

www.fortinet.com

Copyright© 2026 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 Chief Legal Officer, 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.