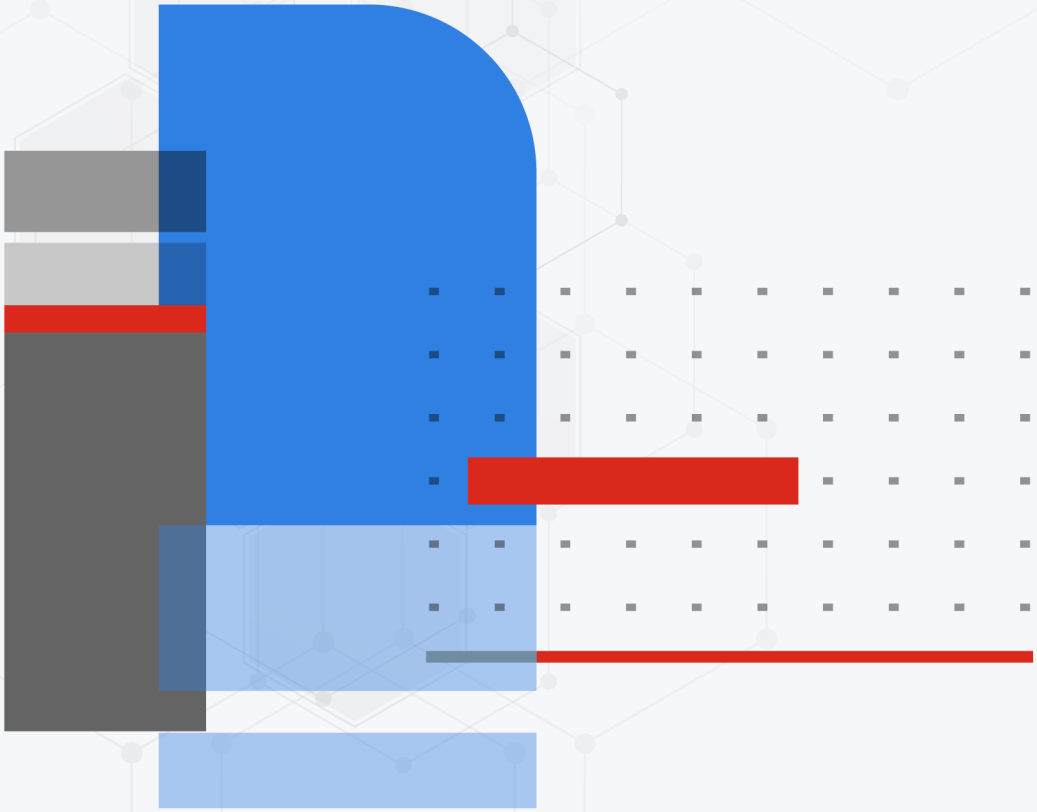
Hardening Guide

FortiSIEM 6.7.3



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

02/06/2024
FortiSIEM 6.7.3 Hardening Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
12/02/2020	Initial release of FortiSIEM Hardening Guide.
03/23/2022	FortiSIEM Hardening Guide released for 6.4.0.
05/09/2022	FortiSIEM Hardening Guide released for 6.5.0.
05/18/2022	Updated Change HTTPS and SSH Ports to Non-standard Ports section.
07/19/2022	Updated Modify Lockout Frequency section.
07/26/2022	FortiSIEM Hardening Guide released for 6.6.0.
09/12/2022	FortiSIEM Hardening Guide released for 6.5.1.
09/14/2022	FortiSIEM Hardening Guide released for 6.6.1.
09/19/2022	FortiSIEM Hardening Guide released for 6.6.2.
01/03/2023	FortiSIEM Hardening Guide released for 6.7.0.
02/13/2023	FortiSIEM Hardening Guide released for 6.7.1.
03/07/2023	FortiSIEM Hardening Guide released for 6.7.2.
03/28/2023	FortiSIEM Hardening Guide released for 6.7.3.
04/11/2023	FortiSIEM Hardening Guide released for 6.7.4.
04/18/2023	Note added to Change HTTPS and SSH Ports to Non-standard Ports section.
05/22/2023	FortiSIEM Hardening Guide released for 6.7.5.
06/16/2023	FortiSIEM Hardening Guide released for 6.7.6.
07/13/2023	FortiSIEM Hardening Guide released for 6.7.7.
09/12/2023	FortiSIEM Hardening Guide released for 6.7.8.
09/29/2023	Audit FortiSIEM User Activity section updated.
02/05/2024	FortiSIEM Hardening Guide released for 6.7.9.

Hardening FortiSIEM Security

This guide describes some of the techniques used to harden and improve the security of FortiSIEM.

OS Security

FortiSIEM 6.4.x runs on Rocky Linux. The following sections describe how to enable various features of FortiSIEM 6.x.

Ensure Strong Cryptographic Algorithms are Enabled

FortiSIEM 6.x can run in two modes: FIPS and non-FIPS. In both modes, secure cipher suites are chosen by default and pass vulnerability scanner tests. Check the release notes for specific FIPS limitations.

In the FIPS mode:

- FortiSIEM uses only FIPS-compliant cryptographic algorithms. For a full list of supported cryptographic algorithms, see Cryptographic Algorithms.
- During startup and reboot, FortiSIEM will run self-tests to ensure that proper FIPS-compliant algorithms are being used. If a non-FIPS compliant algorithm is chosen, then FortiSIEM will not startup.

To turn on FIPS mode, follow these steps:

1. SSH to the FortiSIEM node.
2. Run the `configFSM.sh` script and select the FIPS option.

Note that a FIPS-compliant node will only communicate with a FIPS-compliant node. If FortiSIEM needs to communicate with an older device that does not support FIPS, then that communication will break.

In non-FIPS mode, FortiSIEM supports only TLS 1.2 and 1.3.

For TLS 1.2, the following Cipher suites are supported:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519)
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 4096)
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 4096)

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519)
- TLS_DHE_RSA_WITH_AES_256_CCM_8 (dh 4096)
- TLS_DHE_RSA_WITH_AES_256_CCM (dh 4096)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 4096)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519)
- TLS_DHE_RSA_WITH_AES_128_CCM_8 (dh 4096)
- TLS_DHE_RSA_WITH_AES_128_CCM (dh 4096)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 4096)

For TLS 1.3, the following Cipher suites are supported:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_CCM_SHA256

Enable Public CA Signed SSL Certificates

In FortiSIEM 6.x, all external communication is via SSL, unless collecting data from a devices forces the use of another protocol (for example, NetFlow or SNMP). Protect all SSL communication with public CA signed certificates.

For details on configuring public certificates, see Configuring CA Certificates.

Enable Disk Encryption

You can encrypt disks to prevent a malicious user from attaching them to an external system to read their content.

FortiSIEM does not recommend encrypting the root disk which presents an operational challenge during boot up to provide a passphrase. There are three additional disks:

- `/cmdb`: holds the Postgres database
- `/svn`: holds the device configuration and monitored files
- `/data`: holds the logs

Any of these disks can be encrypted by following the steps here.

Network Security

- Close Unused Ports
- Change HTTPS and SSH Ports to Non-standard Ports
- Disable Unused Interfaces

Close Unused Ports

FortiSIEM only permits the ports it needs for communicating with external systems and for communicating with its cluster members. See Appendix A for details on ports which are open by default.

You may want to close some ports that are not applicable for your environment, for example, SNMP Trap on port 162. There is extensive literature on configuring `firewalld` to block ports using `firewall-cmd`.

Change HTTPS and SSH Ports to Non-standard Ports

Note: Currently, changing SSL default ports will fail, and it is not recommended at this time.

By default, HTTPS port is opened on port 443.

To change this, follow these steps:

1. SSH to the FortiSIEM node.
2. Open `/etc/httpd/conf.d/ssl.conf` for writing.
3. Change Listen 443 to Listen `<your port>`.
4. Change `<VirtualHost _default_:443>` to use `<your port>`.
5. Restart the service by running `systemctl reload httpd`.
6. Check the status by running `systemctl status httpd`.

For each port change, please open the port in the FortiSIEM firewall in order to allow for the inbound connection.

To change, add the port to be allowed from the firewall by running the following commands as root:

```
# firewall-cmd --add-port <your port>/tcp --permanent
# firewall-cmd --reload
```

By default, the SSH port is opened on port 22.

To change this, follow these steps:

1. SSH to the FortiSIEM node.
2. Open `/etc/ssh/sshd_config` for writing.
3. Change Port 22 to Port `<your port>`.
4. Restart service by running `systemctl reload sshd`.
5. Check status by running `systemctl status sshd`.

For each port change, please open the port in the FortiSIEM firewall in order to allow for the inbound connection.

To change, add the port to be allowed from the firewall by running the following commands as root:

```
# firewall-cmd --add-port <your port>/tcp --permanent
# firewall-cmd --reload
```

Disable Unused Interfaces

In VM deployments, only one network interface is used.

In hardware appliances, an interface may become live if a cable is plugged into it. To administratively disable an interface, follow these steps:

1. SSH to the FortiSIEM node.
2. Run `sudo ifconfig <your interface> down`.

Application Security

Change Default Passwords

FortiSIEM has the following default user accounts for installation and configuration:

- SSH: user = admin, default password = ProspectHills
- GUI: user = admin, default password = admin*1

In FortiSIEM 6.1.0 and later, the user is forced to change these default passwords during installation.

For older installations which are migrating to 6.1.x, the user must manually change the GUI password, if it has not been changed already.

Choose Strong Passwords

In FortiSIEM 6.1.0 and later, both SSH and GUI passwords must contain between 8 and 64 characters, and must include 1 letter, 1 numeric character and 1 special character.

FortiSIEM enforces this during user creation. For older installations migrating to 6.1.x, the user must manually change the GUI password to meet the above restrictions, if it has not been changed already.

The minimum password length is 8 characters (maximum password length is 64 characters) chosen from the set of ninety five (95) characters. New passwords are required to include 1 letter, 1 numeric character, and 1 special character. The odds of guessing a password are 1 in {95^8}, which is significantly lower than one in a million.

Setup External User Authentication

For GUI users, external authentication provides greater security. FortiSIEM supports three external authentication mechanisms:

- LDAP, LDAPS, or LDAPTLS, such as Active Directory
- RADIUS, such as FortiAuthenticator and Cisco ISE

- SAML, such as Okta

Follow the procedures here for setting up external authentication.

Use Password Vaults for Device Communication

FortiSIEM supports CyberArk password vault where device communication passwords may be stored. FortiSIEM does not store a password locally, instead, it pulls in a password when it needs it.

Currently, FortiSIEM supports the following credentials from CyberArk password vault:

- SNMP
- SSH
- WMI
- HTTP and HTTP(S)
- FTP and FTP Over SSL
- LDAP and LDAPS
- POP3 and POP3 over SSL
- IMAP and IMAP over SSL
- SMTP and SMTP over SSL

To configure CyberArk password vault integration, set Password config to CyberArk during credential definition in **ADMIN > Setup > Credentials > Step 1: Create Credentials** in the FortiSIEM GUI.

Set up Two Factor Authentication

FortiSIEM 6.1.0 and later supports Cisco Duo for 2 factor GUI user authentication. Follow the procedures documented here for setup.

Shorten Idle Timeout

A GUI user will be logged out after a certain period of time, if the keyboard or mouse and is inactive and is not in any of these GUI areas:

- **Dashboard**
- **ADMIN > Setup > Test Connectivity**
- **ADMIN > Setup > Discovery**
- **ANALYTICS > Export Report**

The **Idle Timeout** is configured on a per user basis from **CMDB > Users** as part of user attributes. When a user is created by default, **Idle Timeout** is not set and not required. However, administrators can set this option for tighter security.

Modify Lockout Frequency

A GUI user is locked out if the user fails 5 consecutive logins. You can specify the time duration for which the user remains locked out in **CMDB > Users** when editing or creating a new user by going to **User Lockout**, selecting **Delay next login for <##> minutes**, and changing the value. By default, this value is 15 minutes.

Locking out after 5 consecutive logins is sufficient to throttle brute force login.

Force Password Reset After a Certain Number of Days

You can force a FortiSIEM GUI user to change password after a certain number of days. You can set this value in **CMDB > User > Password Reset**.

Avoid Shared Accounts

Always associate a specific user to a specific account.

Map Users to Specific Roles Using RBAC

FortiSIEM provides fine-grained Role based access control (RBAC) at four levels:

- GUI access – restrict users to certain parts of the GUI
- Data visibility – restrict users to only see certain logs from certain devices
- Obfuscation – restrict users from seeing certain log fields like IP, user, host name, etc.
- Workflow permission – restrict users from sensitive operations such as deploying rules, scheduling reports, obfuscation, and remediation

Assigning users to a specific FortiSIEM admin role based on their job function provides tighter control over the information in FortiSIEM.

First, use one of the existing system-defined roles or define a custom role in **ADMIN > Settings > Role > Role Management**. You can then associate users to roles in two ways:

- Locally defined users – Go to **CMDB > User > Set System Admin** and associate a user to a role
- Externally authenticated users - Go to **ADMIN > Settings > Role > AD Group Role** and define mappings from Active Directory groups to FortiSIEM Roles. When the user logs in, FortiSIEM looks up the user role in Active Directory and dynamically associates the user to the mapped FortiSIEM role.

For details see here.

Restrict SSH Access to Administrators

SSH access to FortiSIEM nodes must be restricted to admin users who install, upgrade, and troubleshoot issues. Most user operations like analyzing logs and creating dashboards, rules and reports can be done from the GUI.

Audit FortiSIEM User Activity

FortiSIEM provides extensive out of the box audit reports. To find these reports, go to **RESOURCES > Reports**, expand the Reports folder and inspect the FortiSIEM Audit sub-folder. The following use cases are covered, with each report containing fine-grained details including the user who performed the activity and the Source IP from which the user logged in.

- FortiSIEM successful/failed GUI and SSH log on
- Account lockouts and unlock activity
- User creation, deletion, role assignment, and password modification
- User Role creation, deletion and modification
- Rule creation, deletion, modification, activation, and deactivation
- Report creation, deletion, modification, export, and schedule
- Dashboard creation, deletion, modification, and sharing
- CMDB Device creation, deletion and modification
- External threat intelligence update
- Notification policy creation, deletion and modification
- Incident clearing and closing history
- Case creation, update and closure history
- Incident remediation history
- Event database archive and purge history

A full list of audit events can be found here:

- Changes made via the GUI
- Analytic query execution
- Authentication

General Best Practices

- Install in a Secure Location
- Keep FortiSIEM Up to Date
- Network Segmentation & Protection
- Register with Fortinet Support
- Run Authenticated Vulnerability Scans
- Patch Newly Discovered Rocky Linux Level Vulnerabilities

Install in a Secure Location

A good place to start is with physical security. Install your FortiSIEM in a secure location, such as a locked room or one with restricted access. A restricted location prevents unauthorized users from getting physical access to the device.

If unauthorized users have physical access, they can disrupt your organization's Security Operations Center (SOC) by shutting down your FortiSIEM (either by accident or on purpose), or disconnecting the network cable to prevent it from receiving logs or storing events to external storage. Unauthorized users can also connect a console cable and attempt to log into the CLI. Additionally, when a FortiSIEM reboots, a person with physical access can interrupt the boot process and install different firmware.

Keep FortiSIEM Up to Date

Always keep FortiSIEM up to date. The most recent version is the most stable and has the most bugs fixed and vulnerabilities removed. Fortinet periodically updates the FortiSIEM software and firmware to include new features and resolve important issues.

Network Segmentation & Protection

FortiSIEM should be in a protected network segment accessible to hosts that require access only. In most deployments, FortiSIEM is restricted to certain networks and hosts where accounting and auditing is enabled, especially for remote terminal access such as SSH.

Network Firewall and Web Application Firewalls can also provide an additional level of protection along with the detection of malicious activity targeting FortiSIEM.

FortiSIEM should be considered an attack target as it provides key detection and accounting of audit information that an attacker would wish to disable and compromise the integrity of.

Register with Fortinet Support

You need to register your FortiSIEM with Fortinet Support to receive customer services, such as software updates, new log parsers, rules, reports, and customer support.

It is also recommended that you purchase FortiGuard IOC service so that FortiSIEM can detect malware IP, domain, URL, and file hashes in your network. To register your product go to the Fortinet Support website.

Run Authenticated Vulnerability Scans

FortiSIEM periodically releases software updates that address severe and medium vulnerabilities. As a defense in depth strategy, you can also run vulnerability scanners against FortiSIEM to look for newly found unpatched vulnerabilities.

Vulnerability scanners may produce false positives. To reduce such occurrences, always run authenticated scans and validate against Redhat websites to determine that the patch is included in your release. You can follow the instructions here for details.

Patch Newly Discovered Rocky Linux Level Vulnerabilities

If you determine that Rocky Linux has released a patch, which is either not yet available in FortiSIEM, or it is available but you are not willing to upgrade, then you can run a `yum` update and apply the patch on your FortiSIEM node. See here for detailed steps.

Appendix A: Open Ports and Protocols

The FortiSIEM External Ports in the External Systems Configuration Guide specifies the ports and protocols that FortiSIEM needs for its operation.

Appendix B: Reference Architecture

The Fortinet FortiSIEM Reference Design Guide provides a more general architecture overview with good practice considerations:

www.fortinet.com