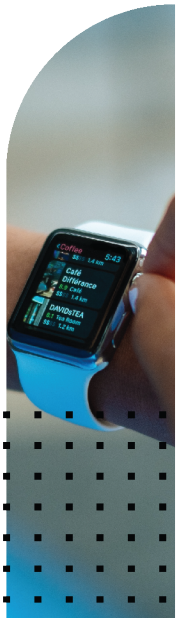
FIPS Support

FortiSIEM 6.3.1



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

01/27/2022
FortiSIEM 6.3.1 FIPS Support

TABLE OF CONTENTS

Change Log

Date	Change Description
06/30/2020	Initial version of this manual.
03/23/2021	6.2.0 release.
05/06/2021	6.2.1 release.
07/06/2021	6.3.0 release.
08/26/2021	6.3.1 release.
10/15/2021	6.3.2 release.
12/22/2021	6.3.3 release.

FIPS Support

Erasing Disk Contents

One of the requirements for FIPS compliance is the ability to erase the contents of any disk. The Disk Zerioization feature removes the contents of the disk by replacing it with zeros (0).

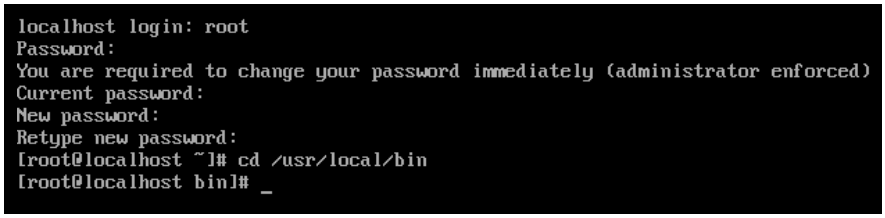
The shell scripts `prepare_boot_loader.sh` and `boot_loader_operations.sh` erase all of the data from all of the disks in the FortiSIEM system. The `prepare_boot_loader.sh` script loads the FortiSIEM boot loader. The `boot_loader_operations.sh` script automatically reads all the disks, including OS disk, and iteratively fills them with zeros twice to ensure that no data remains on the disk.

Only the root user can run the `prepare_boot_loader.sh` and `boot_loader_operations.sh` scripts. Once the scripts complete the erasing, the user will not be able to login into the system. No utilities will be able to fetch data from the erased disks.

Run the prepare_boot_loader Script

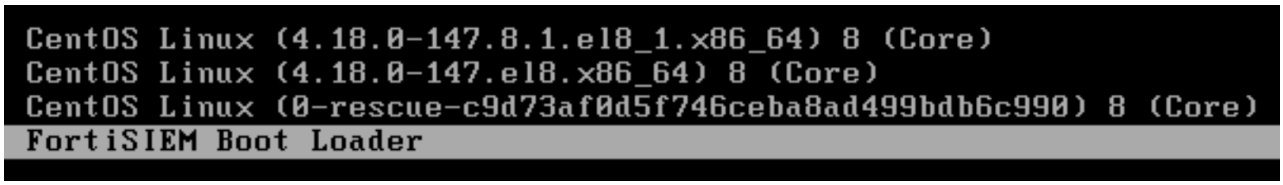
Follow these steps to run the `prepare_boot_loader.sh` script:

1. Log in to the system as user `root` and password `ProspectHills`. **Note:** you might be required to change your password after logging in.
2. Navigate to `/usr/local/bin` in the FortiSIEM server.

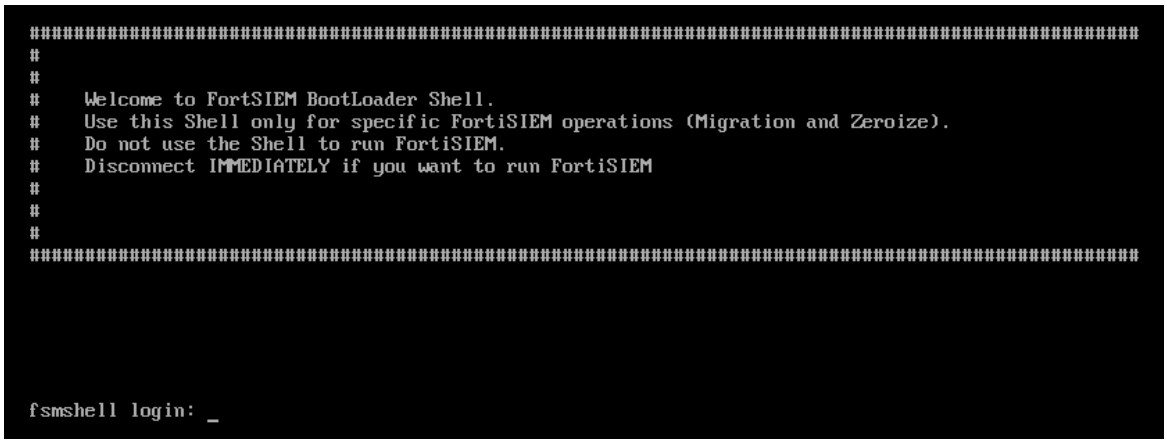


3. Run the script `prepare_boot_loader.sh`. The system will be rebooted.
   `# prepare_boot_loader.sh`

4. Use the arrow keys on the keyboard to select **FortiSIEM Boot Loader** from the boot menu. Press **Enter**.



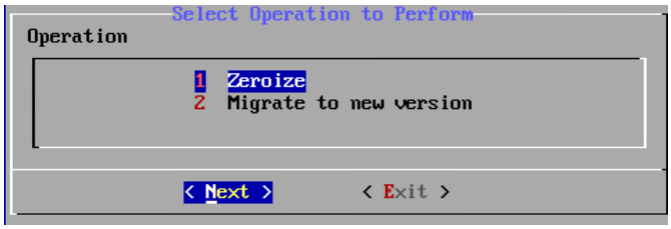
5. After some minutes, the Boot Loader shell will appear.



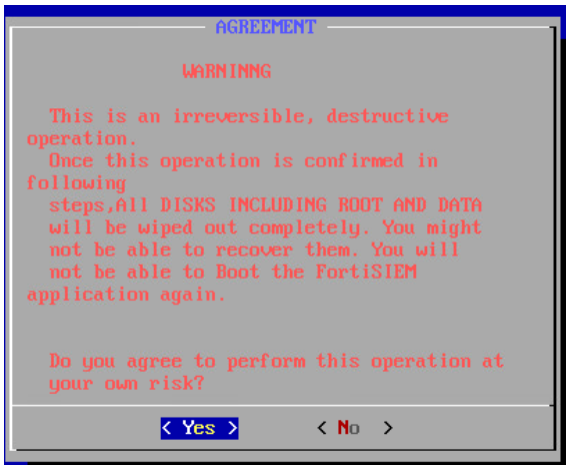
Run the boot_loader_operations Script

Follow these steps to run the `boot_loader_operations.sh` script:

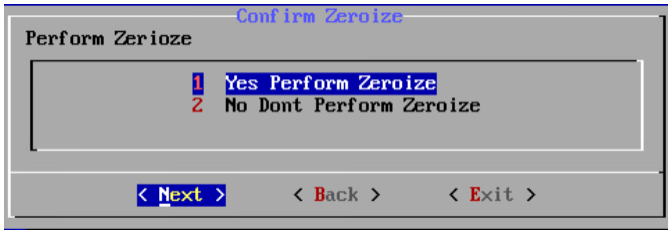
1. Log in to the Boot Loader shell as user `root`, with the default password. If you changed the password above, use the new password instead.
2. Navigate to `/usr/bin`.
3. Run the `boot_loader_operations.sh` script.
   ```
   # boot_loader_operations.sh
   ```
   A simple UI will open where you can initiate the Zeroize operation.
4. In the **Select Operations to Perform** dialog box, select **1 Zerioze**. Select **Next** and press **Enter** to continue.



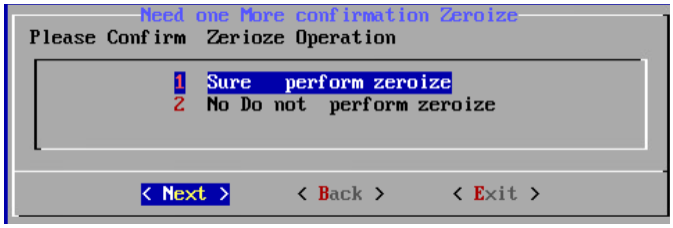
5. Read the contents In the **AGREEMENT** dialog box carefully. Select **Yes** and press **Enter** to continue. Otherwise, select **No** and press **Enter** to exit the script.



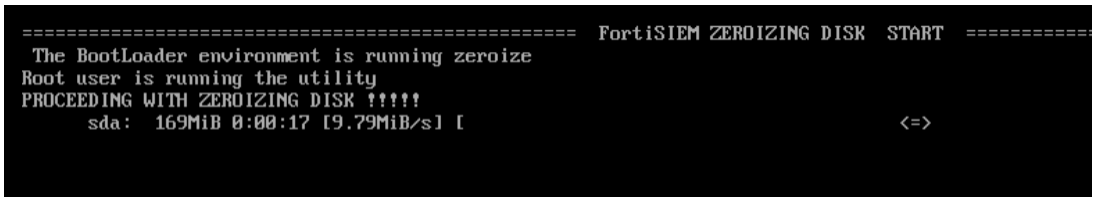
6. If you click **Yes**, a dialog box to confirm Zeroize appears. Click **1 Yes Perform Zeroize**. Select **Next** and press **Enter** to continue.



7. If you click **Next**, another dialog box to reconfirm Zeroize appears. Click **1 Sure perform zeroize**. Select **Next** and press **Enter** to continue.



8. The Zeroize process starts:



Depending on the size of disks and amount of data present, it may take a long time to complete the Zeroize operation. After the script completes, you should not be able to boot the system.

Verify the Disk is Erased

Run the following command for each disk to verify that the script has erased all of the data. The purpose of the command is to determine if any non-zero characters exist.

```
dd if=/dev/sdX 2>/dev/null | /iszero >sdX-nonzerochars.txt
```

Where **x** represents the name of the disk you attached. The contents of the `sd`**`x`**`-nonzerocharars.txt` file should be empty.

For example, if you attached a disk `b`:

```
dd if=/dev/sdb 2>/dev/null | /iszero >sdb-nonzerochars.txt
```

If you attached a disk `c`:

```
dd if=/dev/sdc 2>/dev/null | /iszero >sdc-nonzerochars.txt
```

Cryptographic Algorithms

The following table displays the certificate numbers for Red Hat Enterprise Linux 7, because Red Hat Enterprise Linux 8 is under certification.

CentOS 8.1 Module	Version in FortiSIEM 6.3.1
NSS	nss-3.44.0-8.el8.x86_64
OpenSSL	openssl-1.1.1c-2.el8_1.1.x86_64
OpenSSH and OpenSSH Server	openssh-8.0p1-3.el8.x86_64 openssh-server-8.0p1-3.el8.x86_64
libSSH	libssh-0.9.0-4.el8.x86_64 libssh-0.9.0-4.el8.i686
OpenJDK	java-1.8.0-openjdk-1.8.0.252.b09-2.el8_1.x86_64

The following table displays the cryptographic algorithms and their use in various CentOS 8.1 modules used by FortiSIEM 6.3.1.

Algorithm	Used By CentOS8 Module
SHA256	NSS, OpenSSL
SHA384	NSS, OpenSSL
SHA512	NSS,
HMAC-SHA1	NSS, OpenSSH
HMAC-SHA1-ETM	OpenSSH, libSSH
HMAC-SHA256	NSS,
HMAC-SHA2-256	OpenSSH
HMAC-SHA2-256-ETM	OpenSSH, libSSH
HMAC-SHA2-512	OpenSSH, libSSH
HMAC-SHA2-512-ETM	OpenSSH, libSSH

Algorithm	Used By CentOS8 Module
HMAC-SHA384	NSS
HMAC-SHA512	NSS
HMAC-SHA2-512	OpenSSH
SECP256R1	NSS,
SECP384R1	NSS,
SECP521R1	NSS,
aes128-gcm	NSS, OpenSSL, OpenSSH
aes128-ctr	NSS, OpenSSH
aes128-cbc	OpenSSH
aes256-gcm	NSS, OpenSSL, OpenSSH
aes256-ctr	OpenSSH
aes256-cbc	NSS, OpenSSH
ECDHE-RSA	NSS
ECDHE-ECDSA	NSS
ecdh-sha2-nistp256	OpenSSH
ecdh-sha2-nistp384	OpenSSH
ecdh-sha2-nistp521	OpenSSH
DHE-RSA	NSS
diffie-hellman-group-exchange-sha256	OpenSSH, libSSH
diffie-hellman-group14-sha256	OpenSSH
diffie-hellman-group16-sha512	OpenSSH, libSSH
diffie-hellman-group18-sha512	OpenSSH, libSSH
rsa-sha2-256	OpenSSH, libSSH
rsa-sha2-256-cert-v01	OpenSSH, libSSH
rsa-sha2-512	OpenSSH, libSSH
rsa-sha2-512-cert-v01	OpenSSH, libSSH
ecdsa-sha2-nistp256	OpenSSH, libSSH
ecdsa-sha2-nistp256-cert-v01	OpenSSH, libSSH
ecdsa-sha2-nistp384	OpenSSH, libSSH
ecdsa-sha2-nistp384-cert-v01	OpenSSH, libSSH

Algorithm	Used By CentOS8 Module
ecdsa-sha2-nistp521	OpenSSH, libSSH
ecdsa-sha2-nistp512-cert-v01	OpenSSH, libSSH

www.fortinet.com