Oracle® Communications Session Monitor

FIPS Compliance Guide

Release 5.2

G14536-03

October 2024

Oracle Communications Session Monitor FIPS Compliance Guide, Release 5.2

G14536-03

Contents

About This Guide

This document presents information about the Oracle Communications Session Monitor product family. The Session Monitor platform supports the following products:

- Oracle Communications Operations Monitor
- Oracle Enterprise Operations Monitor
- Oracle Communications Control Plane Monitor
- Oracle Communications Fraud Monitor

Documentation Set

Table 1   Documentation Suite for Session Monitor Release 5.2

Document Name	Document Description
Backup and Restore Guide	Provides instructions for backing up and restoring Session Monitor.
FIPS 140-2 Compliance Guide	Provides conceptual and procedural information about the Federal Information Processing Standard (FIPS) functionality in Session Monitor.
Developer Guide	Contains information for using the Session Monitor SAU Extension.
Fraud Monitor User Guide	Contains information for installing and configuring Fraud Monitor to monitor calls and detect fraud.
Installation Guide	Contains information for installing Session Monitor
Mediation Engine Connector User Guide	Contains information for configuring and using the Mediation Engine Connector.
Operations Monitor User Guide	Contains information for monitoring and troubleshooting IMS, VoLTE, and NGN networks using the Operations Monitor.
Release Notes	Contains information about the Session Monitor Release 5.2, including new features.
Security Guide	Contains information for securely configuring Session Monitor.
Upgrade Guide	Contains information for upgrading Session Monitor.

Revision History

This section provides a revision history for this document.

Date	Description
October 2024	Initial release

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

1
Session Monitor FIPS 140-2 Compliance

The Federal Information Protection Standards, or FIPS 140-2, are security standards for federal and defense cyber security compliance, focusing on data encryption created by the National Institute of Standards and Technology (NIST).

The FIPS 140-2 standards are used in designing, implementing, and operating cryptographic modules. A cryptographic module is the set of hardware, software, and (or) firmware that implements security functions, such as algorithms and key generation. The standards also define the methods for testing and validation of the modules.

The Oracle Communications Session Monitor supports cryptographic libraries and algorithms that has been validated against **FIPS 140-2** requirements.

As part of the FIPS 140-2 compliance, Session Monitor leverages the cryptographic libraries validated by the underlying Operating system (Oracle Linux 8) as well as MySQL cryptographic libraries to ensure that the offering is FIPS 140-2 compliant. When you use Session Monitor in the FIPS 140-2 mode, it provides an enhanced layer of security.

> **Note:**
>
> FIPS mode is not enabled by default and you must configure it.

2
Prerequisites

For Session Monitor to work in the FIPS mode, enable the FIPS mode in both Oracle Linux as well as MySQL. You can enable the FIPS mode on Session Monitor using the Operating System and MySQL versions:

- Session Monitor Release 5.2 p3 or later releases (Upgrade /Fresh install both possible)
- Oracle Linux 8.10
- "BaseOS Latest", "AppStream Latest" and "Security Validation (Update 8)" yum repositories enabled
- MySQL 8.0.39
- MySQL Connector Version 8.0.33

The versions of Oracle Linux that were FIPS 140-2 validated was version 8.4. It is recommend that you use the latest version of Oracle Linux 8.x and MySQL 8.0.x to maintain security. Also, you cannot use FIPS 140-2 cryptographic modules on Oracle Linux 8 systems that are running an update earlier than Oracle Linux 8.4.

> **Note:**
>
> Session Monitor only supports FIPS 140-2 based on the Linux versions listed above.

Also, RHEL (or any other flavor of Linux outside of Oracle Linux) based installation is out of scope of FIPS 140-2.

Cryptographic Modules

FIPS 140-2 compliance requires the clear definition of modules that perform cryptographic functions. The following cryptographic modules are required for the FIPS mode to be working on Session Monitor Release 5.2 :

- openssl-1.1.1k-12.el8_9.x86_64.rpm [4215]
- gnutls-3.6.16-8.el8_9_fips.x86_64.rpm [4229]
- libgcrypt-1.8.5-7.el8_6_fips.x86_64.rpm [4232]

> **Note:**
>
> The list above shows the latest versions available as part of Oracle Linux 8.x, the link provided in brackets specify the security certificate corresponding to the versions which was validated for FIPS 140-2. For more information, visit the Oracle Security Evaluations website (FIPS 140 | External Security Evaluations | Secure Development | Oracle) and download the latest security policy. The Security Policy document explains how to verify that the package is FIPS 140-2 validated, as well as how to configure the module for FIPS mode. Use the Search bar to gather all Oracle Linux listings and download security policy for the same.

FIPS 140-2 Approved Cipher Algorithms

After enabling the FIPS mode, Session Monitor sends out only the following listed FIPS 140-2 approved Cipher Suites for all external interfaces where TLS is enabled:

1. Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
2. Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
3. Cipher Suite: TLS_AES_128_CCM_SHA256 (0x1304)
4. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
5. Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
6. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CCM (0xc0ad)
7. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
8. Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
9. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CCM (0xc0ac)
10. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
11. Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
12. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
13. Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
14. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
15. Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
16. Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
17. Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f)
18. Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
19. Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e)
20. Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
21. Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
22. Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
23. Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
24. Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

The following Cipher Suites are NOT FIPS 140-2 compliant and cannot be used by Session Monitor when the FIPS mode enabled:

1. TLS_CHACHA20_POLY1305_SHA256 (0x1303)
2. TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
3. TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
4. TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
5. TLS_RSA_WITH_AES_256_CCM (0xc09d)
6. TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
7. TLS_RSA_WITH_AES_128_CCM (0xc09c)
8. TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
9. TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
10. TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
11. TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
12. TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa)

3 Single RPM for Session Monitor

Session Monitor has only a single RPM, which works irrespective of whether the FIPS mode is enabled OR not in Oracle Linux/MySQL. This ensures major convenience for the customers, as it avoids the necessity to look for specific versions of the RPM file just for enabling FIPS.

Session Monitor also allows disabling the FIPS mode (if enabled) from Oracle Linux/MySQL without reinstalling the Session Monitor RPM.

However, if you are toggling between FIPS mode (Enabled/Disabled), then any key not created in the FIPS Mode must be regenerated. Hence, you must choose if you want to disable FIPS after enabling it. It is recommended that you avoid toggling the FIPS mode between Enable and Disable multiple times.

4 Installing Session Monitor with the FIPS Mode Enabled

This section contains instructions to install Session Monitor with the FIPS mode enabled.

Install the following versions of Oracle Linux and MySQL before enabling the FIPS Mode at Oracle Linux or MySQL. For information on how to install Session Monitor, see Installing Session Monitor.

- Oracle Linux 8.10
- MySQL 8.0.39
- MySQL Connector: 8.0.33

For more information, see:

- Installing Session Monitor with the FIPS Mode Enabled
- Offline Installation of Session Monitor with the FIPS Mode Enabled

Installing Session Monitor with the FIPS Mode Enabled

This section contains instructions to install Session Monitor with the FIPS mode enabled.

Before enabling the FIPS mode, ensure that you read the section Known Limitations and Caveats

1. Ensure that the Oracle Linux 8 system is configured with "BaseOS Latest", "AppStream Latest" and "Security Validation (Update 8)" yum repositories enabled:

   - Execute the following commands at the console:

     ```
     # yum install yum-utils
     # yum-config-manager --enable ol8_baseos_latest ol8_appstream
     ol8_u4_security_validation
     ```

2. Verify that the openssl version `openssl-1.1.1k-12.el8_9.x86_64.rpm` is installed. If not, install the same from the **BaseOS Latest** repository.
3. Verify that the libraries in this listed are installed. If not, install the same from the **Security Validation (Update 8) yum** repositories:
   - gnutls-3.6.16-8.el8_9.3_fips.x86_64.rpm
   - libgcrypt-1.8.5-7.el8_6_fips.x86_64.rpm
4. Execute this command at the console to enable the FIPS mode in Oracle Linux 8.10:

   ```
   fips-mode-setup --enable
   ```

5. Reboot the server after enabling the FIPS mode at Oracle Linux.

   ```
   reboot
   ```

6. After rebooting the server, execute the following command to verify FIPS status:

   ```
   fips-mode-setup --check
   ```

   The result looks like: `FIPS mode is enabled`.

7. Execute the following steps to enable FIPS mode at MySQL:

   ```
   Open the my.cnf file using the following command.
   vi /etc/my.cnf
   Add the following line at the end of my.cnf file.
   ssl_fips_mode=1
   Restart the mysql services using the following command.
   systemctl restart mysqld
   ```

8. Use the following commands to install the Session Monitor

   ```
   yum install “ocsm-x.x.x.x.x.x86_64.rpm”
   ```

9. After installing Session Monitor, execute the following command to verify the status of FIPS at MySQL:

   ```
   mysql vsp -e 'select md5(8);show warnings;';
   ```

   The output looks like:

   ```
   +---------+------
   +------------------------------------------------------------------------+
   | Level   | Code |
   Message                                                                |
   +---------+------
   +------------------------------------------------------------------------+
   | Warning | 4073 | SSL fips mode error: FIPS mode ON/STRICT: MD5 digest is
   not supported. |
   +---------+------
   +------------------------------------------------------------------------+
   1 row in set (0.00 sec)
   ```

Offline Installation of Session Monitor with the FIPS Mode Enabled

This section contains instructions to perform offline installation of Session Monitor with the FIPS mode enabled.

Before enabling the FIPS mode, ensure that you read the section Known Limitations and Caveats

1. Download the latest version of the following libraries required for FIPS from the yum.oracle.com Oracle Linux 8 Repository manually

   a. Oracle Linux 8 Repository - BaseOS Latest

      openssl-1.1.1k-12.el8_9.x86_64.rpm - https://yum.oracle.com/repo/OracleLinux/OL8/baseos/latest/x86_64/getPackage/openssl-1.1.1k-12.el8_9.x86_64.rpm.

b. Oracle Linux 8 Repository - Security Validation (Update 4)

   - gnutls-3.6.16-8.el8_9.3_fips.x86_64.rpm - https://yum.oracle.com/repo/OracleLinux/OL8/4/security/validation/x86_64/getPackage/gnutls-3.6.16-8.el8_9.3_fips.x86_64.rpm
   - libgcrypt-1.8.5-7.el8_6_fips.x86_64.rpm - https://yum.oracle.com/repo/OracleLinux/OL8/4/security/validation/x86_64/getPackage/libgcrypt-1.8.5-7.el8_6_fips.x86_64.rpm

   > **Note:**
   >
   > If openssl version openssl-1.1.1k-12.el8_9.x86_64.rpm is already installed as part of your Oracle Linux 8.10 installation, you can skip the installation of openssl package.

2. Copy the downloaded RPMs to `/var/ftp/pub/ocsm/` location of the Repo Server.
3. On the Repo Server, execute the following command:

   ```
   createrepo /var/ftp/pub/ocsm/
   ```

4. On the Session Monitor Server, execute the following command:

   ```
   yum clean all
   ```

5. Install the required libraries for FIPS one by one on the Session Monitor Server using the commands:

   ```
   yum install openssl-1.1.1k-12.el8_9.x86_64
   yum install gnutls-3.6.16-8.el8_9.3_fips.x86_64
   yum install libgcrypt-1.8.5-7.el8_6_fips.x86_64
   ```

6. Execute this command at the console to enable the FIPS mode in Oracle Linux 8.10:

   ```
   fips-mode-setup --enable
   ```

7. Reboot the server after enabling the FIPS mode at Oracle Linux.

   ```
   reboot
   ```

8. After rebooting the server, execute the following command to verify FIPS status:

   ```
   fips-mode-setup --check
   ```

   The result looks like: `FIPS mode is enabled`.
9. Execute the following steps to enable FIPS mode at MySQL.

   a. Open the my.cnf file using the following command.

   ```
   vi /etc/my.cnf
   ```

b. Add the following line at the end of the my.cnf file.

```
ssl_fips_mode=1
```

c. Restart the MySQL services using the following command.

```
systemctl restart mysqld
```

10. Use the following commands to install the Session Monitor:

```
yum install ocsm
```

11. After installing Session Monitor, execute this command to verify the status of FIPS on the MySQL server:

```
mysql vsp -e 'select md5(8);show warnings;';
```

The output looks like:

```
+---------+------
+---------------------------------------------------------------------------+
| Level   | Code |
Message                                                                   |
+---------+------
+---------------------------------------------------------------------------+
| Warning | 4073 | SSL fips mode error: FIPS mode ON/STRICT: MD5 digest is
not supported. |
+---------+------
+---------------------------------------------------------------------------+
1 row in set (0.00 sec)
```

5 Upgrading Session Monitor and Enabling the FIPS Mode

Use the instructions in this procedure to upgrade Session Monitor Release 5.2:

Ensure that the following versions of Oracle Linux and MySQL have been installed before enabling the FIPS mode on the Oracle Linux Server/MySQL:

- Oracle Linux 8.10
- MySQL Version 8.0.39
- MySQL Connector: 8.0.33

Upgrading Session Monitor and Enabling the FIPS Mode

Use the instructions in this procedure to upgrade Session Monitor Release 5.2:

Before you upgrade, see the Known Limitations and Caveats.

1. Use the following commands to upgrade Session Monitor.

   ```
   pld-systemctl stop
   yum upgrade “ocsm-x.x.x.x.x.x.x86_64.rpm”
   ```

2. Ensure that the Oracle Linux 8 system is configured with "BaseOS Latest", "AppStream Latest" and "Security Validation (Update 8)" yum repositories enabled:

   - Execute the following commands at the console:

     ```
     # yum install yum-utils
     # yum-config-manager --enable ol8_baseos_latest ol8_appstream
     ol8_u4_security_validation
     ```

3. Verify that openssl version “openssl-1.1.1k-12.el8_9.x86_64.rpm” is installed. If not, install the same from “BaseOS Latest” repository.

4. Verify that these libraries are installed. If not, install the same from Security Validation (update 8) yum repositories:

   - gnutls-3.6.16-8.el8_9.3_fips.x86_64.rpm
   - libgcrypt-1.8.5-7.el8_6_fips.x86_64.rpm

Offline - Upgrading Session Monitor with the FIPS Mode Enabled

Use the instructions in this procedure to offline upgrade Session Monitor Release 5.2:

Before you upgrade, see the Known Limitations and Caveats.

1. Use the following commands to offline upgrade Session Monitor. The latest Session Monitor RPM and dependencies must be present in the repository server. For more information, see Configuring the Repository Server.

   ```
   pld-systemctl stop
   yum clean all
   yum upgrade ocsm-x.x.x.x.x
   ```

2. Download the latest versions of following libraries required for FIPS from the yum.oracle.com Oracle Linux 8 repository manually.

   a. Oracle Linux 8 Repository - Base OS latest:

   Table 5-1 Links for the Latest Version of Libraries

Library	Link
openssl-1.1.1k-12.el8_9.x86_64.rpm	https://yum.oracle.com/repo/OracleLinux/OL8/baseos/latest/x86_64/getPackage/openssl-1.1.1k-12.el8_9.x86_64.rpm

   b. Oracle Linux 8 Repository - Security Validation (Update 4)

   Table 5-2 Links for the Latest Version of Libraries

Library	Link
gnutls-3.6.16-8.el8_9.3_fips.x86_64.rpm	https://yum.oracle.com/repo/OracleLinux/OL8/4/security/validation/x86_64/getPackage/gnutls-3.6.16-8.el8_9.3_fips.x86_64.rpm
libgcrypt-1.8.5-7.el8_6_fips.x86_64.rpm	https://yum.oracle.com/repo/OracleLinux/OL8/4/security/validation/x86_64/getPackage/libgcrypt-1.8.5-7.el8_6_fips.x86_64.rpm

   > **Note:**
   >
   > If the openssl version openssl-1.1.1k-12.el8_9.x86_64.rpm is already installed as part of your Oracle Linux 8.10 installation, you can skip the installation of openssl package.

3. Copy the downloaded RPMs to /var/ftp/pub/ocsm/ location of the Repo Server.

4. On the Repo Server, execute the following command:

   ```
   createrepo /var/ftp/pub/ocsm/
   ```

5. On the Session Monitor Server, execute the following command:

   ```
   yum clean all
   ```

6. Install the required libraries for FIPS one by one on the Session Monitor Server using the commands:

   ```
   yum install openssl-1.1.1k-12.el8_9.x86_64
   yum install gnutls-3.6.16-8.el8_9.3_fips.x86_64
   yum install libgcrypt-1.8.5-7.el8_6_fips.x86_64
   ```

Enabling the FIPS Mode

Enable the FIPS mode on the Oracle Linux server/ MySQL server using the commands given in this section.

Ensure that you have upgraded to Session Monitor Release 5.2.

Enabling the FIPS Mode on the Oracle Linux Server

Enable the FIPS mode on the Oracle Linux server using the commands given in this section.

Ensure that you have upgraded to Session Monitor Release 5.2.

1. Execute the following command at the console to enable FIPS mode in Oracle Linux 8.10:

   ```
   fips-mode-setup --enable
   ```

2. Reboot the server once FIPS mode is enabled at Oracle Linux.

   ```
   reboot
   ```

3. Verify the FIPS status, after rebooting. Execute the following command:

   ```
   fips-mode-setup --check
   ```

   The output should look like:

   ```
    “FIPS mode is enabled”
   ```

Enabling the FIPS Mode on the MySQL Server

Enable the FIPS mode on the MySQL server using the commands given in this section.

Ensure that you have upgraded to Session Monitor Release 5.2.

1. Execute the following steps to enable FIPS mode at MySQL
   - Stop Session Monitor services using command:

     ```
     “source /opt/oracle/ocsm/ocsm_env.sh”
     “pld-systemctl stop"
     ```

   - Open the my.cnf file using the following command:

     ```
     vi /etc/my.cnf
     ```

- Add the following line at the end of my.cnf file.

  ```
  ssl_fips_mode=1
  ```

- Restart the mysql services using the following command.

  ```
  systemctl restart mysqld
  ```

- Restart the OCSM services again using the following command

  ```
  pld-systemctl start
  ```

2. After enabling the FIPS mode at MySQL execute the following command at MySQL to verify FIPS status.

   ```
   mysql vsp -e 'select md5(8);show warnings;';
   ```

   Output should be:

   ```
   +---------+------
   +-------------------------------------------------------------------------+
   | Level   | Code |
   Message                                                                 |
   +---------+------
   +-------------------------------------------------------------------------+
   | Warning | 4073 | SSL fips mode error: FIPS mode ON/STRICT: MD5 digest is
   not supported. |
   +---------+------
   +-------------------------------------------------------------------------+
   1 row in set (0.00 sec)
   ```

6

Disabling the FIPS Mode

The following procedures describe how to disable FIPS mode in Session Monitor:

Disabling the FIPS Mode on the Oracle Linux Server

The following procedure describes how to disable the FIPS mode in Session Monitor on the Oracle Linux server:

Steps to disable the FIPS mode at the Oracle Linux version 8.10 server:

1. Execute the following command at console.

   ```
   fips-mode-setup --disable
   ```

2. Reboot the server using following command at console:

   ```
   reboot
   ```

3. Execute the following command to check the FIPS mode status on the Oracle Linux 8.10 server:

   ```
   fips-mode-setup --check
   ```

   The output should be:

   ```
   FIPS mode is disabled
   ```

Disabling the FIPS Mode on the MySQL Server

The following procedure describes how to disable the FIPS mode in Session Monitor on the MySQL server:

Steps to disable the FIPS mode at MySQL server:

1. Stop the Session Monitor services first using these commands:

   ```
   source /opt/oracle/ocsm/ocsm_env.sh
   pld-systemctl stop
   ```

2. Open the `my.cnf` file using this command:

   ```
   vi /etc/my.cnf
   ```

3. Remove the following line at the end of the `my.cnf` file:

   ```
   ssl_fips_mode=1
   ```

4. Restart the MySQL services using the following command:

   ```
   systemctl restart mysqld
   ```

5. Start the Session Monitor services using command:

   ```
   pld-systemctl start
   ```

6. After disabling the FIPS mode at the MySQL server, execute the following command at MySQL to verify FIPS status.

   ```
   mysql vsp -e 'select md5(8);show warnings;'


   Output should be (there shouldn’t be any warning):
   +----------------------------------+
   | md5(8)                           |
   +----------------------------------+
   | c9f0f895fb98ab9159f51fd0297e236d |
   +----------------------------------+
   ```

> **Note:**
>
> If you toggle between enable/disable the FIPS mode, then you must regenerate any keys not created in the FIPS mode. So, you must be careful if you want to disable the FIPS mode after enabling.

7

Session Monitor Password Policies

Versions of Session Monitor prior to Release 5.2 p3, support values of 1, 2, and 3 for **Setting Secure password policy**.

Secure Passwords Policy

The **Setting Secure password policy** option takes 3 numerical values from 1 to 3, each value enables a specific secure password hashing policy. Following is a short description of each.

> **Note:**
>
> When a new user is created OR a password expires for an existing user, the password is generated as per policy value set in **System Settings**:

Table 7-1 Setting Secure password policy

Value	Description
1	Use of Legacy password hashing only. This is the minimum value. If the password policy is set to 1, the new password is generated using bcrypt (based on Blowfish algorithm based hash).
2	Employs new, more secure password hashing policy, but keeps compatibility with legacy algorithm. In this case, both authentication modes, new and old will be attempted. This is the default value. If the password policy is set to 2, the new password is generated based on SHA-256 hash. However, with the password policy set to 2, it would still allow users having password encrypted using bcrypt.
3	Adheres only to new password algorithms policy. Be careful with this value, as users that have old type of password hashing will not be able to authenticate. This is the maximum value. If the password policy is set to 3, the new password will be a SHA-256 hash and bcrypt based passwords are not allowed.

Password Policy Changes

Password policy changes have been introduced after Session Monitor Release 5.2 P3. The main changes are that password policies 1 and 2 are now removed from the system as they were not secure. Only password policy 3 has been retained and this is the only and default option.

For existing users, if there are any users whose password is encrypted using password policy 1, then Session Monitor does not allow upgrade for such systems.

During the upgrade, a pre-test runs to check if any user has password encrypted using password policy 1 – the upgrade fails with the message:

```
Below users have an insecure password hash created using policy 1
Please change 'Secure password policy' to 3 in the 'System Settings' and change
the passwords accordingly...
```

If the above situation arises, then perform the following steps:

1. Set the Secure password policy to 3 in the **System Settings**.
2. Manually change the passwords of the users whose names appear in the message.
3. Try to upgrade again. This time it should be successful. Post a successful upgrade, **System Settings** > **Secure Password Policy** is set to 3.

For a fresh installation, the **Secure Password Policy** is set to 3 by default, and there is no option to change it.

The above changes will be in place irrespective of the FIPS mode in Oracle Linux or MySQL. This particular implementation is applicable for savepoints as well.

Savepoint Restore on Session Monitor Release 5.2 P3 will fail if any user has password encrypted using password policy 1. Perform the fix as given below:

1. Perform Step 1 and Step 2 given above.
2. Re-create the Savepoint.
3. Try to restore.

8
SNMP V3 Enhancements

By default, Session Monitor supports HMAC as an authentication protocol and AES as encryption protocol for User Based Security Model for SNMP v3. In particular, below HMAC/AES modes are supported:

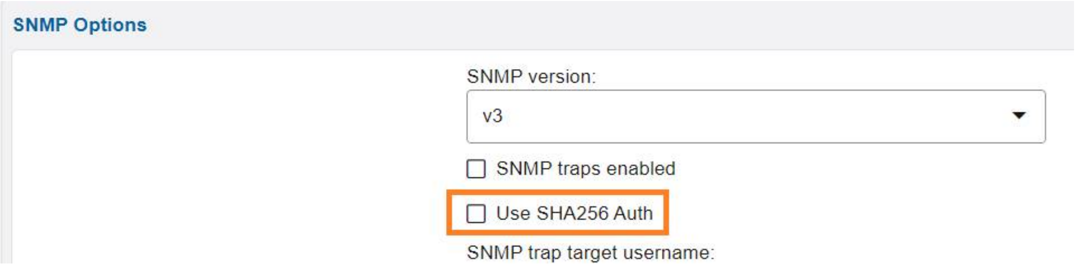
1. usmHMACSHAAuthProtocol (per RFC 3414)
2. usmAesCfb128Protocol

As part of FIPS 140-2 compliance enhancements, Session Monitor has introduced support for SHA-2 hash functions in the HMAC mode as defined in RFC 7630 for SNMP v3. **usmHMAC192SHA256AuthProtocol** HMAC authentication protocol is now supported: : **usmHMAC192SHA256AuthProtocol** uses SHA-256 and truncates the output to 192 bits (24 octets).

To enable **usmHMAC192SHA256AuthProtocol** Authentication protocol in SNMP v3,

1. In the GUI, go to **Settings**, **SNMP Options**.
2. Select the configuration option **Use SHA256 Auth**.

Figure 8-1 Use SHA256 Auth Configuration Option



SNMP Options

SNMP version:

v3

□ SNMP traps enabled

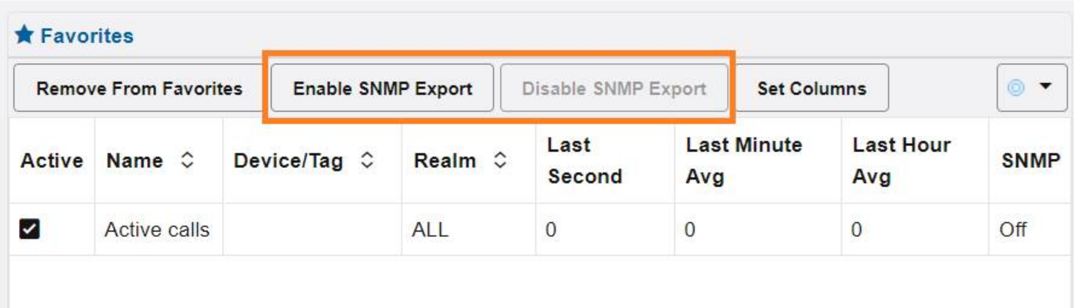
□ Use SHA256 Auth

SNMP trap target username:

> **Note:**
>
> It is recommended to select the option **Use SHA256 Auth** when the FIPS mode is enabled in Oracle Linux /MySQL.

Enabling the **Use SHA256 Auth** option does not have any impact **Enable/Disable SNMP Export** for a particular KPI from the **Favorites** bar in the **KPI/Metrics** page. The **Enable/ Disable SNMP Export** feature continues to work as before.

Figure 8-2   Enable/Disable SNMP Export



Active	Name	Device/Tag	Realm	Last Second	Last Minute Avg	Last Hour Avg	SNMP
☑	Active calls		ALL	0	0	0	Off

9 Known Limitations and Caveats

Session Monitor does not support Internal Radius functionality if you have enabled the FIPS mode.

When the FIPS mode is enabled, then Session Monitor sends out only FIPS 140-2 approved Cipher Suites for External Authentication with LDAP connection, as defined in the section FIPS 140-2 Approved Cipher Algorithms. Hence, the LDAP server may need to be updated to support at least one of the FIPS approved security algorithm.

An additional option to send SNMP traps with SHA256 encoding is available with R5.2p3, irrespective of whether FIPS mode enabled or not. It is recommended to use that option when the FIPS mode is enabled. This also means that the SNMP server may need to be upgraded to support SNMP Traps with SHA 256 encoding.

10 Secure Setup and Initialization

The operator sets up the device as defined in the Oracle Communications Session Monitor User Guide. The admin user also makes sure that:

- All traffic is encapsulated in a TLS.
- HTTPS is enabled and the web server certificate is configured before connecting to the Web GUI over TLS.
- SNMP V3 is configured with AES-128/HMAC only: For more information, see SNMP v3 Enhancements.
- SSH is configured to use AES CTR mode for encryption
- SSH only uses Diffie-Hellman group 14 in the FIPS approved mode.
- Telnet is not used in the FIPS mode of operation.
- All operator passwords are a minimum of 8 characters in length
- Internal RADIUS is not used in the FIPS approved mode.