Oracle® Communications Session Monitor

FIPS Compliance Guide

Release 6.0
G35181-01
May 2025

ORACLE

Oracle Communications Session Monitor FIPS Compliance Guide, Release 6.0

G35181-01

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

Documentation Set

Table 1 Documentation Suite for Session Monitor Release 6.0

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.
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 6.0, 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
May 2025	• Initial release for Session Monitor Release 6.0.0.0.1

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 6.0 P1 (6.0.0.0.1) 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 8.4.5
- MySQL Connector Version 8.4.0

The versions of Oracle Linux that were FIPS 140-2 validated was version 8.4. It is recommended that you use the latest version of Oracle Linux 8.x and MySQL 8.4.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 the minimum versions required for the FIPS mode to be working on Session Monitor Release 6.0 :

- openssl-1.1.1k-12.el8_9.x86_64.rpm or higher [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. The following list includes the minimum versions required for FIPS to be enabled. For information on how to install Session Monitor, see Installing Session Monitor.

- Oracle Linux 8.10
- MySQL 8.4.5
- MySQL Connector: 8.4.0

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. Login to the Session Monitor server installed with Oracle Linux 8.10 as a root user or root privileged user.
2. Navigate to the directory where the Session Monitor zip file was extracted and ensure the FIPS scripts have executable permission. If not, use the following command to set the execute permission.

   ```
   chmod +x ./scripts/FIPS_Scripts/*.sh
   ```

3. Enable FIPS mode in Oracle Linux 8.10 using the following command.

   ```
   ./scripts/FIPS_Scripts/Enable_FIPS_on_OL_6.0.sh <mode of install>
   ```

> **Note:**
>
> In this command, the **<mode of install>** is either **online** or **offline** based on the type of installation being done. For example, `./scripts/FIPS_Scripts/Enable_FIPS_on_OL_6.0.sh online`.

4. After enabling FIPS mode on Oracle Linux, execute the following command to verify FIPS status:

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

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

5. Install the Session Monitor using ZIP files downloaded from MOS/OSDC. For more information, see the *Installation Guide*.

6. Once Session Monitor is installed, navigate to the directory where the Session Monitor zip file was extracted. Provide permissions and execute the following commands to enable FIPS at MySQL.

   ```
   chmod +x ./scripts/FIPS_Scripts/*.sh
   ./scripts/FIPS_Scripts/Enable_FIPS_on_MySQL_6.0.sh
   ```

7. 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
The following libraries are the minimum versions required for FIPS, which are downloaded as part of the Session Monitor zip file.

- 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.
- 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:**
>
> The minimum version required for the openssl package is openssl-1.1.1k-12.el8_9.x86_64.rpm or higher.

1. Login to the Session Monitor server installed with Oracle Linux 8.10 as a root user or root privileged user.
2. Install the Session Monitor in an Offline Mode using the zip bundle.

> **Note:**
>
> For more information, see the *Installation Guide*.

3. Once the Session Monitor is installed, navigate to the /tmp/ocsm directory where the RPM files and scripts have been downloaded for offline installation and ensure the FIPS scripts have executable permissions. If not, use the following command to set the execute permission:

```
chmod +x ./scripts/FIPS_Scripts/*.sh
```

4. Enable FIPS mode in Oracle Linux 8.10 by executing the following command.

```
./scripts/FIPS_Scripts/Enable_FIPS_on_OL_6.0.sh <mode of install>
```

> **Note:**
>
> In this command, the **<mode of install>** is either **online** or **offline** based on the type of installation being done. For example, `./scripts/FIPS_Scripts/Enable_FIPS_on_OL_6.0.sh offline`.

5. Execute the following command to verify FIPS status on Oracle Linux

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

6. Execute the following command to enable FIPS at MySQL.

```
./scripts/FIPS_Scripts/Enable_FIPS_on_MySQL_6.0.sh
```

7. Execute the following 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 6.0:

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 8.4.5 Version
- MySQL Connector: 8.4.0

Upgrading Session Monitor and Enabling the FIPS Mode

Use the instructions in this procedure to upgrade Session Monitor Release 6.0:

Before you upgrade, see the Known Limitations and Caveats.

1. Use the following commands to stop Session Monitor services.

   ```
   pld-systemctl stop
   ```

2. Upgrade the Session Monitor using the Session Monitor zip file downloaded from MOS/OSDC. For more information, see the *Upgrade Guide*.

Offline - Upgrading Session Monitor with the FIPS Mode Enabled

Use the instructions in this procedure to offline upgrade Session Monitor Release 6.0:

Before you upgrade, see the Known Limitations and Caveats.

1. Use the following command to stop the Session Monitor services.

   ```
   pld-systemctl stop
   ```

2. Offline Upgrade the Session Monitor using the Session Monitor zip file downloaded from MOS/OSDC. For more information, see the *Upgrade Guide*.
3. The latest versions of following libraries are required for FIPS from the yum.oracle.com Oracle Linux 8 repository, which is downloaded as part of the Session Monitor zip file.
   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

> **Note:**
>
> The minimum version required for the openssl package is openssl-1.1.1k-12.el8_9.x86_64.rpm or higher.

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

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 6.0.

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 6.0.

1. Navigate to the directory where the Session Monitor zip file was extracted and ensure the FIPS scripts have executable permission. If not, set the execute permission using the following command:

   ```
   chmod +x ./scripts/FIPS_Scripts/*.sh
   ```

2. Enable the FIPS mode in Oracle Linux 8.10 by executing the following command at the console:

   ```
   ./scripts/FIPS_Scripts/Enable_FIPS_on_OL_6.0.sh <mode of install>
   ```

   > **Note:**
   >
   > In this command, the **<mode of install>** is either **online** or **offline** based on the type of installation being done. For example, `./scripts/FIPS_Scripts/Enable_FIPS_on_OL_6.0.sh online`.

3. Verify the FIPS status, after running the script. 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 6.0.

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"
     ```

   - Navigate to the directory where the Session Monitor zip file was extracted and ensure the FIPS scripts have executable permission. If not, set the execute permission using the following command:

     ```
     chmod +x ./scripts/FIPS_Scripts/*.sh
     ```

   - Enable the FIPS mode at MySQL by executing the following command:

     ```
     ./scripts/FIPS_Scripts/Enable_FIPS_on_MySQL_6.0.sh
     ```

   - 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. Navigate to the directory where the Session Monitor zip file was extracted and ensure the FIPS scripts have executable permission. If not, set the execute permission using the following command:

   ```
   chmod +x ./scripts/FIPS_Scripts/*.sh
   ```

2. Enable FIPS mode in Oracle Linux 8.10 by executing the following command:

   ```
   ./scripts/FIPS_Scripts/Disable_FIPS_on_OL_6.0.sh
   ```

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. Navigate to the directory where the Session Monitor zip file was extracted and ensure the FIPS scripts have executable permission. If not, set the execute permission using the following command:

   ```
   chmod +x ./scripts/FIPS_Scripts/*.sh
   ```

3. Enable the FIPS mode at MySQL by executing the following command:

```
./scripts/FIPS_Scripts/Disable_FIPS_on_MySQL_6.0.sh
```

4. Start the Session Monitor services using command:

```
pld-systemctl start
```

5. 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
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:

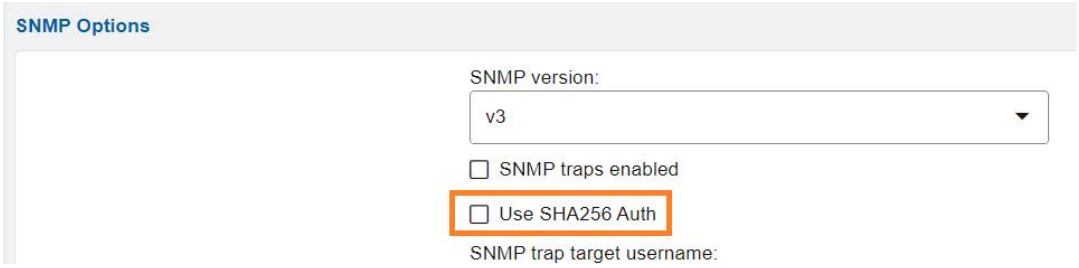
1. usmHMACSHAAuthProtocol (per RFC 3414)
2. usmAesCfb128Protocol

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**.

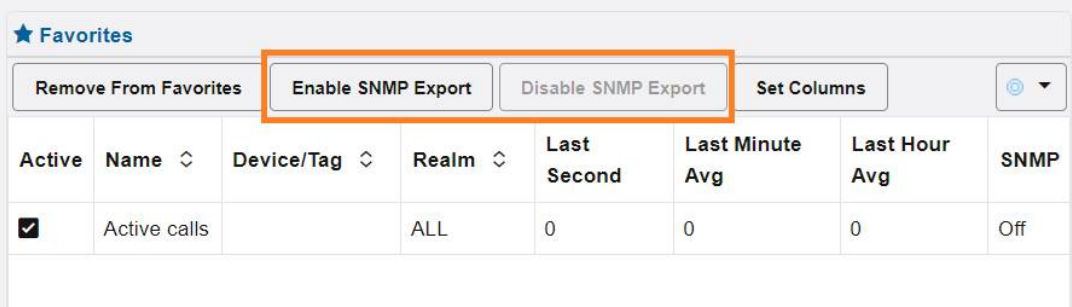
Figure 7-1 Use SHA256 Auth Configuration Option



> **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 7-2 Enable/Disable SNMP Export



8
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 Session Monitor Release 6.0 P1 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.

9
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.