

# What standards are covered by SNMP4J (i.e., RFCs, FIPS 140-2)?

## IETF RFC Compliance

SNMP4J / SNMP4J-Agent implements the following IETF RFCs:

| RFC #                                              | Title                                                                                                         | Coverage          | Versions (SNMP4J)                              |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------|-------------------|------------------------------------------------|
| <a href="#">3410</a>                               | Introduction and Applicability Statements for Internet Standard Management Framework                          | ✓                 | ★                                              |
| <a href="#">3411</a>                               | An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks                | ✓                 | ★                                              |
| <a href="#">3412</a>                               | Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)                          | ✓                 | ★                                              |
| <a href="#">3413</a>                               | Simple Network Management Protocol Applications                                                               | ✓                 | ★                                              |
| <a href="#">3414</a>                               | User Based Security Model (USM) for SNMPv3                                                                    | ✓                 | ★                                              |
| <a href="#">3415</a>                               | View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)                      | ✓                 | ★                                              |
| <a href="#">3416</a>                               | Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)                        | ✓                 | ★                                              |
| <a href="#">3417</a>                               | Transport Mappings for the Simple Network Management Protocol (SNMP)                                          | UDP and TCP only  | ★                                              |
| <a href="#">3418</a>                               | Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)                           | ✓                 | ★                                              |
| <a href="#">3584</a>                               | Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework | ✓                 | ★                                              |
| <a href="#">3826</a>                               | The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model                 | ✓                 | ★                                              |
| <a href="#">4088</a>                               | Uniform Resource Identifier (URI) Scheme for the Simple Network Management Protocol (SNMP)                    | ✓                 | >= 2.2                                         |
| <a href="#">5343</a>                               | Simple Network Management Protocol (SNMP) Context EngineID Discovery                                          | ✓                 | >= 2                                           |
| <a href="#">6353</a>                               | Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)              | ✓ TLS 1.0, 1.2    | >= 2 (TLS 1.2 with Java SE 8 or later)         |
|                                                    |                                                                                                               | ✓ DTLS            | >= 3.0                                         |
| <a href="#">5590</a>                               | Transport Subsystem for the Simple Network Management Protocol (SNMP)                                         | ✓                 | >= 2                                           |
| <a href="#">5591</a>                               | Transport Security Model for the Simple Network Management Protocol (SNMP)                                    | ✓                 | >= 2<br>CRL, OSCP revocation checking >= 3.6.0 |
| <a href="#">5592</a>                               | Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)                                | ✗                 |                                                |
| <a href="#">7630</a>                               | HMAC-SHA-2 Authentication Protocols in the User-based Security Model (USM) for SNMPv3                         | ✓                 | >= 2.4                                         |
| <a href="#">draft-reeder-snmpv3-usm-3desede-00</a> | Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in "Outside" CBC Mode              | ✓                 | ★                                              |
| <a href="#">draft-blumenthal-aes-usm-04</a>        | The AES Cipher Algorithm in the SNMP's User-based Security Model                                              | ✓ (AES 192 + 256) | ★                                              |

SNMP4J-AgentX implements the follow IETF RFCs:

| RFC # | Title                                                     | Coverage     | Versions |
|-------|-----------------------------------------------------------|--------------|----------|
| 2741  | Agent Extensibility (AgentX) Protocol Version 1           | ✓ (TCP only) | ★        |
| 2742  | Definitions of Managed Objects for Extensible SNMP Agents | ✓            | ★        |

## FIPS 140-2 Compliance

SNMP4J uses standard JCE hashing and encryption algorithms as provided through the Java Cryptography Extension (JCE) as listed in the table below. Thus, by using a FIPS 140-2 certified JCE provider, SNMP4J becomes FIPS 140-2 compliant:

| Message Digest / Cipher Suite Name | SNMP4J Class Name                                                                                          | SNMPv3 Protocol                                                 | Protocol Type  |
|------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|----------------|
| SHA-1                              | AuthSHA                                                                                                    | SHA                                                             | Authentication |
| MD5                                | AuthMD5                                                                                                    | MD5                                                             | Authentication |
| DES/CBC/NoPadding                  | PrivDES                                                                                                    | DES                                                             | Privacy        |
| AES/CFB/NoPadding                  | PrivAES128<br>PrivAES192<br>PrivAES256<br>PrivAES192With3DESKeyExtension<br>PrivAES256With3DESKeyExtension | AES 128<br>AES 192<br>AES 256<br>(nonstandard)<br>(nonstandard) | Privacy        |
| DESede/CBC/NoPadding               | Priv3DES                                                                                                   | 3DES                                                            | Privacy        |