# SNMP Configuration



# SNMP Overview

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language for monitoring and managing devices in a network.

## SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within Cisco UCS, the managed device that maintains the data for Cisco UCS, and reports the data as needed to the SNMP manager. Cisco UCS includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP in Cisco UCS Manager.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent. Cisco UCS release 1.4(1) and higher supports a larger number of MIBs than earlier releases.

Cisco UCS supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. SNMP is defined in the following:

- RFC 3410 (http://tools.ietf.org/html/rfc3410)
- RFC 3411 (http://tools.ietf.org/html/rfc3411)
- RFC 3412 (http://tools.ietf.org/html/rfc3412)
- RFC 3413 (http://tools.ietf.org/html/rfc3413)

- RFC 3414 (http://tools.ietf.org/html/rfc3414)
- RFC 3415 (http://tools.ietf.org/html/rfc3415)
- RFC 3416 (http://tools.ietf.org/html/rfc3416)
- RFC 3417 (http://tools.ietf.org/html/rfc3417)
- RFC 3418 (http://tools.ietf.org/html/rfc3418)
- RFC 3584 (http://tools.ietf.org/html/rfc3584)

# SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

Cisco UCS Manager generates SNMP notifications as either traps or informs. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap, and Cisco UCS Manager cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response Protocol Data Unit (PDU). If the Cisco UCS Manager does not receive the PDU, it can send the inform request again.

# SNMP Security Levels and Privileges

SNMPv1, SNMPv2c, and SNMPv3 each represent a different security model. The security model combines with the selected security level to determine the security mechanism applied when the SNMP message is processed.

The security level determines the privileges required to view the message associated with an SNMP trap. The privilege level determines whether the message requires protection from disclosure or whether the message is authenticated. The supported security level depends on which security model is implemented. SNMP security levels support one or more of the following privileges:

- noAuthNoPriv—No authentication or encryption
- authNoPriv—Authentication but no encryption
- authPriv—Authentication and encryption

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

# Supported Combinations of SNMP Security Models and Levels

The following table  identifies the combinations of security models and levels.

*Table 1: SNMP Security Models and Levels*

| Model | Level | Authentication | Encryption | What Happens |
|---|---|---|---|---|
| v1 | noAuthNoPriv | Community string | No | Uses a community string match for authentication. |
| v2c | noAuthNoPriv | Community string | No | Uses a community string match for authentication. |
| v3 | noAuthNoPriv | Username | No | Uses a username match for authentication. |
| v3 | authNoPriv | HMAC-MD5 or HMAC-SHA | No | Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA). |
| v3 | authPriv | HMAC-MD5 or HMAC-SHA | DES | Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard. |

# SNMPv3 Security Features

SNMPv3 provides secure access to devices through a combination of authenticating and encrypting frames over the network. SNMPv3 authorizes only configured users to perform management operations and encrypts SNMP messages. The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages are not altered or destroyed in an unauthorized manner, and that data sequences are not altered beyond what can occur non-maliciously.
- Message origin authentication—Ensures that the identity of a message originator is verifiable.
- Message confidentiality and encryption—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

# SNMP Support in Cisco UCS

Cisco UCS provides the following support for SNMP:

### Support for MIBs

Cisco UCS supports read-only access to MIBs.

For information about the specific MIBs available for Cisco UCS and where you can obtain them, see the http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html for B-series servers, and http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/c-series/b_UCS_Standalone_C-Series_MIBRef.html C-series servers.

### Authentication Protocols for SNMPv3 Users

Cisco UCS supports the following authentication protocols for SNMPv3 users:

- HMAC-MD5-96 (MD5)
- HMAC-SHA-96 (SHA)

Cisco UCS Manager Release 3.2(3) and later releases do not support MD5 authentication if SNMPv3 is in Federal Information Processing Standards (FIPS) mode. Hence, any existing or newly created SNMPv3 users with MD5 authentication will not be deployed with these releases and the following fault message will appear:

```
Major     F1036    2018-02-01T14:36:32.995     99095 SNMP User testuser can't be
deployed. Error: MD5 auth is not supported
```

To deploy such a user, modify the authentication type to **SHA**.

### AES Privacy Protocol for SNMPv3 Users

Cisco UCS uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The privacy password, or priv option, offers a choice of DES or 128-bit AES encryption for SNMP security encryption. If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, Cisco UCS Manager uses the privacy password to generate a 128-bit AES key. The AES privacy password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters.

Cisco UCS Manager Release 3.2(3) and later releases do not support SNMPv3 users without AES encryption. Hence, any existing or newly created SNMPv3 users without AES encryption will not be deployed with these releases, and the following fault message will appear:

```
Major     F1036    2018-02-01T14:36:32.995     99095 SNMP User testuser can't be
deployed. Error: AES is not enabled
```

To deploy such a user, enable **AES-128** encryption.

# Enabling SNMP and Configuring SNMP Properties

SNMP messages from a Cisco UCS domain display the fabric interconnect name rather than the system name.

### Procedure

**Step 1** In the **Navigation** pane, click **Admin**.

**Step 2** Expand **All** > **Communication Management** > **Communication Services**.

**Step 3** Select the **Communication Services** tab.

**Step 4** In the **SNMP** area, complete the following fields:

| Name | Description |
|---|---|
| **Admin State** field | This can be one of the following:<br>• **Enabled**<br>• **Disabled**<br>Enable this service only if your system includes integration with an SNMP server.<br>If **Admin State** is enabled, Cisco UCS Manager GUI displays the remaining fields in this section. |

**Step 5** Click **Save Changes**.

### What to do next

Create SNMP traps and users.

# Creating an SNMP Trap

### Procedure

**Step 1** In the **Navigation** pane, click **Admin**.

**Step 2** Expand **All** > **Communication Management** > **Communication Services**.

**Step 3** Select the **Communication Services** tab.

**Step 4** In the **SNMP Traps** area, click +.

**Step 5** In the **Create SNMP Trap** dialog box, complete the following fields:

| Name | Description |
|---|---|
| **Hostname (or IP Address)** field | The host name or IP address of the SNMP host to which Cisco UCS Manager should send the trap.<br>You can use an IPv4 address, or an IPv6 address for the SNMP host. The host name can also be a fully qualified domain name of an IPv4 address. |
| **Community/Username** field | The SNMP v1 or v2c community name or the SNMP v3 username Cisco UCS Manager includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service.<br>Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark), & (ampersand), or an empty space. |

| Name | Description |
|---|---|
| **Port** field | The port on which Cisco UCS Manager communicates with the SNMP host for the trap.<br>Enter an integer between 1 and 65535. The default port is 162. |
| **Version** field | The SNMP version and model used for the trap. This can be one of the following:<br>• **V1**<br>• **V2c**<br>• **V3** |
| **Type** field | The type of trap to send. If you select **V2c** or **V3** for the version, the type of trap to be sent can be one of the following:<br>• **Traps**<br>• **Informs** |
| **v3 Privilege** field | If you select **V3** for the version, the privilege associated with the trap. This can be one of the following:<br>• **Auth**—Authentication but no encryption<br>• **Noauth**—No authentication or encryption<br>• **Priv**—Authentication and encryption |

**Step 6** Click **OK**.

**Step 7** Click **Save Changes**.

# Deleting an SNMP Trap

### Procedure

**Step 1** In the **Navigation** pane, click **Admin**.

**Step 2** Expand **All** > **Communication Management** > **Communication Services**.

**Step 3** Select the **Communication Services** tab.

**Step 4** In the **SNMP Traps** area, click the row in the table that corresponds to the user you want to delete.

**Step 5** Click the **Delete** icon to the right of the table.

**Step 6** If a confirmation dialog box displays, click **Yes**.

**Step 7** Click **Save Changes**.

# Creating an SNMPv3 user

**Procedure**

**Step 1** In the **Navigation** pane, click **Admin**.

**Step 2** Expand **All** > **Communication Management** > **Communication Services**.

**Step 3** Select the **Communication Services** tab.

**Step 4** In the **SNMP Users** area, click +.

**Step 5** In the **Create SNMP User** dialog box, complete the following fields:

| Name | Description |
|---|---|
| **Name** field | The username assigned to the SNMP user.<br>Enter up to 32 letters or numbers. The name must begin with a letter and you can also specify _ (underscore), . (period), @ (at sign), and - (hyphen).<br>**Note** You cannot create an SNMP username that is identical to a locally authenticated username. |
| **Auth Type** field | The authorization type. This can be only be **SHA**. |
| **Use AES-128** field | Whether the user uses AES-128 encryption. |
| **Password** field | The password for this user. |
| **Confirm Password** field | The password again for confirmation purposes. |
| **Privacy Password** field | The privacy password for this user. |
| **Confirm Privacy Password** field | The privacy password again for confirmation purposes. |

**Step 6** Click **OK**.

**Step 7** Click **Save Changes**.

# Deleting an SNMPv3 User

**Procedure**

**Step 1** In the **Navigation** pane, click **Admin**.

**Step 2** Expand **All** > **Communication Management** > **Communication Services**.

**Step 3** Select the **Communication Services** tab.

**Step 4** In the **SNMP Users** area, click the row in the table that corresponds to the user you want to delete.

**Step 5** Click the **Delete** icon to the right of the table.

**Step 6** If a confirmation dialog box displays, click **Yes**.

**Step 7** Click **Save Changes**.