SNMP Authentication

SNMP Policies

Cisco UCS Central supports:

- Global SNMP policies
- Defining SNMP traps and informs
- Defining SNMP users

You can define them with regular and privacy passwords, authentication types of MD5 or SHA, and encryption types DES and AES-128. Registered Cisco UCS domains choosing to define SNMP policies globally within that client's policy resolution control defer all SNMP policies to its registration with Cisco UCS Central.

The SNMP Agent functionality remotely monitors Cisco UCS Central. You can also change the Cisco UCS Central host IP, and then restart the SNMP agent on the new IP. SNMP is run on both the active and standby Cisco UCS Central servers. The configuration persists on both. Cisco UCS Central offers read-only access to only the operating system managed information base (MIB). Through the Cisco UCS Central CLI you can configure the community strings for SNMP v1, v2c, and create and delete the SNMPv3 users.

SNMP Functional Overview

The SNMP framework consists of three parts:

SNMP Manager

System used to control and monitor the activities of network devices using SNMP.

SNMP Agent

Software component within Cisco UCS Central. The managed device that maintains the data for Cisco UCS Central and reports the data, as needed, to the SNMP manager. Cisco UCS Central 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.

Managed Information Base (MIB)

Collection of managed objects in the SNMP agent. Cisco UCS Central supports only the OS MIBs.

For information about the specific MIBs available for Cisco UCS and where you can obtain them, see the MIB Reference for Cisco UCS Manager for B-series servers, and MIB Reference for Cisco UCS Standalone C-Series Servers C-series servers.

The following RFCs define the SNMP:

- 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 the SNMP manager send the requests. 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 Central generates SNMP notifications as traps. Traps are less reliable than Informs because the SNMP manager does not send any acknowledgment when it receives a trap. Therefore, Cisco UCS Central cannot determine if it received the trap.

An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If Cisco UCS Central does not receive the PDU, it can send the inform request again.

SNMP Security Features

SNMPv3 provides secure access to devices through a combination of authenticating and encrypting frames over the network. SNMPv3 authorizes management operations only by configured users 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 nothing has altered or destroyed any messages in an unauthorized manner. Also ensures that nothing has altered data sequences to an extent greater than can occur non-maliciously.

Message Origin Authentication

Confirms the claimed identity of the user who received the data.

Message Confidentiality and Encryption

Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMP Security Levels and Privileges

SNMPv1, SNMPv2c, and SNMPv3 each represent a different security model. A security model is an authentication strategy that is set up for a user and the role in which the user resides. The security model combines with the selected security level to determine the security mechanism applied when Cisco UCS Central processes the SNMP message.

The security level determines the privileges required to view the message associated with an SNMP trap. The security level determines whether Cisco UCS Central must protect the message from disclosure, or authenticate it. The supported security level depends upon which security model is implemented. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. 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.

SNMP Security Models and Levels

The following table describes the combinations of SNMP security models and levels supported in Cisco UCS Central.

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.

Model	Level	Authentication	Encryption	What Happens
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on: • Hash-based Message Authentication code (HMAC) • Message Digest 5 (MD5) algorithm • HMAC Secure Hash algorithm (SHA)
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on: • Hash-based Message Authentication code (HMAC) • Message Digest 5 (MD5) algorithm • HMAC Secure Hash algorithm (SHA) • Provides Data Encryption Standard (DES) 56-bit encryption. • Provides authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

SNMP Support in Cisco UCS Central

Support for MIBs

Cisco UCS Central supports read-only access to OS MIBs. No set operations are available for the MIBs. The following MIBs are supported by Cisco UCS Central:

- SNMP MIB-2 System
- HOST-RESOURCES-MIB
  - hrSystem
  - hrStorage
  - hrDevice
  - hrSWRun
  - hrSWRunPerf
- UCD-SNMP-MIB
  - Memory
  - dskTable
  - systemStats

    - fileTable
- SNMP MIB-2 Interfaces
    - ifTable
- IP-MIB
- SNMP-FRAMEWORK-MIB
    - snmpEngine
- IF-MIB
- DISMAN-EVENT-MIB
- SNMP MIB-2 snmp

Note Cisco UCS Central does not provide support for IPV6 and Cisco UCS Central MIBs.

Authentication Protocols for SNMPv3 Users

Cisco UCS Central supports the following authentication protocols for SNMPv3 users:

- HMAC-MD5-96 (MD5)
- HMAC-SHA-96 (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 Central 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.

Configuring an SNMP Policy

Before you begin

You can configure policies in the domain group root. You can also create new policies.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	(Optional) UCSC(policy-mgr) /domain-group # **create snmp**	If scoped into a domain group previously created, it creates the SNMP policy for that domain group.
Step 4	(Optional) UCSC(policy-mgr) /domain-group # **scope snmp**	If scoping into the domain group root previously created, it scopes the default SNMP policy's configuration mode from the domain group root.
Step 5	UCSC(policy-mgr) /domain-group/snmp* # **enable** | **disable snmp**	Enables or disable SNMP services for this policy.
Step 6	UCSC(policy-mgr) /domain-group/snmp* # **set snmp community** *snmp-community-name-text*	Enters a name for the SNMP community.
Step 7	UCSC(policy-mgr) /domain-group/snmp* # **set snmp syscontact** *syscontact-name-text*	Enters a name for the SNMP system contact.
Step 8	UCSC(policy-mgr) /domain-group/snmp* # **set snmp syslocation** *syslocation-name-text*	Enters a name for the SNMP system location.
Step 9	UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the domain group root
- Scopes the SNMP policy
- Enables SNMP services
- Sets the SNMP community name to SNMPCommunity01
- Sets the SNMP system contact name to SNMPSysAdmin01
- Sets the SNMP system location to SNMPWestCoast01
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # enable snmp
UCSC(policy-mgr) /domain-group/snmp* # set snmp community SNMPCommunity01
UCSC(policy-mgr) /domain-group/snmp* # set snmp syscontact SNMPSysAdmin01
UCSC(policy-mgr) /domain-group/snmp* # set snmp syslocation SNMPWestCoast01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
```

```
UCSC(policy-mgr) /domain-group/snmp #
```

The following example:

- Scopes into the domain group domaingroup01
- Creates the SNMP policy
- Enables SNMP services
- Sets the SNMP community name to SNMPCommunity01
- Sets the SNMP system contact name to SNMPSysAdmin01
- Sets the SNMP system location to SNMPWestCoast01
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create snmp
UCSC(policy-mgr) /domain-group/snmp* # enable snmp
UCSC(policy-mgr) /domain-group/snmp* # set snmp community SNMPCommunity01
UCSC(policy-mgr) /domain-group/snmp* # set snmp syscontact SNMPSysAdmin01
UCSC(policy-mgr) /domain-group/snmp* # set snmp syslocation SNMPWestCoast01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

The following example:

- Scopes into the domain group domaingroup01
- Scopes the SNMP policy
- Disables SNMP services
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # disable snmp
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

Configuring an SNMP Trap

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /domain-group # **scope snmp**	Scopes the default SNMP policy's configuration mode.
Step 4	(Optional) UCSC(policy-mgr) /domain-group/snmp # **create snmp-trap** *snmp-trap-ip*	If scoped into a domain group previously created, it creates the snmp-trap IP address for that domain group (in format 0.0.0.0), and enters SNMP trap configuration mode.
Step 5	(Optional) UCSC(policy-mgr) /domain-group/snmp # **scope snmp-trap** *snmp-trap-ip*	If scoped into the domain group root, it scopes the snmp-trap IP address for that domain group (in format 0.0.0.0), and enters SNMP trap configuration mode.
Step 6	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set community** *snmp-trap-community-host-config-string*	Enter the SNMP trap community string to configure the SNMP trap host.
Step 7	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set notificationtype traps**	Enter the notification type for the SNMP trap as SNMP trap notifications (traps).
Step 8	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set port** *port-number*	Enter the SNMP trap port number (1-65535).
Step 9	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set v3privilege auth** | **noauth** | **priv**	Enter a V3 privilege security level for the SNMP trap of authNoPriv security level (auth), noAuthNoPriv security level (noauth), or authPriv security level (priv).
Step 10	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set version v1** | **v2c** | **v3**	Enter a version for the SNMP trap of SNMP v1, v2c, or v3.
Step 11	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the domain group root
- Scopes the SNMP policy
- Creates the SNMP trap with IP address 0.0.0.0
- Sets the SNMP community host string to snmptrap01
- Sets the SNMP notification type to traps
- Sets the SNMP port to 1

- Sets the v3privilege to priv
- Sets the version to v1
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # create snmp-trap 0.0.0.0
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set community snmptrap01
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set notificationtype traps
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set port 1
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set v3privilege priv
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set version v1
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-trap #
```

The following example:

- Scopes into the domain group domaingroup01
- Scopes the SNMP policy
- Scopes the SNMP trap with IP address 0.0.0.0
- Sets the SNMP community host string to snmptrap02
- Sets the SNMP notification type to traps
- Sets the SNMP port to 65535
- Sets the v3privilege to auth
- Sets the version to v2c
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # scope snmp-trap 0.0.0.0
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set community snmptrap02
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set notificationtype traps
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set port 65535
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set v3privilege auth
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set version v2c
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-trap #
```

Configuring an SNMP User

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope snmp**	Scopes the SNMP policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/snmp # **create snmp-user** *snmp-user*	Enters a name for the SNMP user.
Step 5	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set aes-128 yes** | **no**	Uses AES-128 for the SNMP user (yes or no).
Step 6	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set auth md5** | **sha**	Uses MD5 or SHA authorization mode for the SNMP user.
Step 7	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set password** *password*	Enters and confirm a password for the SNMP user.
Step 8	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set priv-password** *private-password*	Enters and confirm a private password for the SNMP user.
Step 9	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the domain group root
- Scopes into the SNMP user named snmpuser01
- Sets aes-128 mode to enabled,
- Sets authorization to sha mode
- Sets password to userpassword01,
- Sets private password to userpassword02
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # scope snmp-user snmpuser01
UCSC(policy-mgr) /domain-group/snmp/snmp-user # set aes-128 yes
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set auth sha
```

```
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set password userpassword01
Enter a password: userpassword01
Confirm the password: userpassword01
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set priv-password userpassword02
Enter a password: userpassword02
Confirm the password: userpassword02
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-user #
```

The following example:

- Scopes into the domain group domaingroup01
- Scopes the SNMP policy
- Creates into the SNMP user named snmpuser01
- Sets aes-128 mode to enabled,
- Sets authorization to MD5 mode
- Sets password to userpassword01,
- Sets private password to userpassword02
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # create snmp-user snmpuser01
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set aes-128 yes
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set auth md5
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set password userpassword01
Enter a password: userpassword01
Confirm the password: userpassword01
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set priv-password userpassword02
Enter a password: userpassword02
Confirm the password: userpassword02
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-user #
```

The following example:

- Scopes into the domain group root
- Scopes the SNMP policy
- Scopes into the SNMP user named snmpuser01
- Sets aes-128 mode to disnabled
- Sets authorization to MD5 mode
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # scope snmp-user snmpuser01
UCSC(policy-mgr) /domain-group/snmp/snmp-user # set aes-128 no
```

```
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set auth md5
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-user #
```

Deleting an SNMP Policy

You can delete an SNMP policy from a sub-domain group of the domain group root. You cannot delete SNMP policies that reside in the domain group root.

Deleting an SNMP policy removes all SNMP trap and SNMP user settings within that policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a sub-domain group under the domain group root. **Note** Do not enter the domain group root. You cannot delete system default management interfaces monitoring policies in the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete snmp**	Deletes the SNMP policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the domain group domaingroup01
- Deletes the SNMP policy
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete snmp
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Deleting an SNMP Trap

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope snmp**	Scopes the default SNMP policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/snmp # **delete snmp-trap** *snmp-trap-ip*	Deletes the snmp-trap IP address for that domain group.
Step 5	UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the domain group root
- Scopes the SNMP policy
- Deletes the SNMP trap IP address 0.0.0.0
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp-trap 0.0.0.0
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

The following example:

- Scopes into the domain group domaingroup01
- Scopes the SNMP policy
- Deletes the SNMP trap IP address 0.0.0.0
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp-trap 0.0.0.0
```

```
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Deleting an SNMP User

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope snmp**	Scopes the SNMP policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/snmp # **delete snmp-user** *snmp-user*	Deletes the SNMP user.
Step 5	UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the domain group root
- Scopes the SNMP policy
- Deletes the SNMP user named snmpuser01
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp snmpuser01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

The followings example:

- Scopes into the domain group domaingroup01
- Scopes the SNMP policy
- Deletes the SNMP user named snmpuser02
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp snmpuser02
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```