SNMP

Guidelines and Limitations for SNMP

We recommend that you do not have the SNMP management station in the subnet of dynamic interface or service port of the controller.

If the SNMP management station subnet is the same as that of the dynamic interface, we recommend that you set the SNMP queries to the IP address of the dynamic interface of the controller. Similarly, if the SNMP management station subnet is the same as that of the service port, we recommend that you set the SNMP queries to the IP address of the service port of the controller.

Controller has a limitation where, even if the queries are made to the management IP address, SNMP response packets are sent with the source IP address as the dynamic interface or the service port respectively. For more information, see CSCvk38081.

To avoid AP data mismatch, we recommend retrieving the AP-related details sent to DNA Center from the controller only after all the APs are in **Run** state.

Configuring SNMP (CLI)

Procedure

- Create an SNMP community name by entering this command:
  config snmp community create *name*
- Delete an SNMP community name by entering this command:
  config snmp community delete *name*
- Configure an SNMP community name with read-only privileges by entering this command:
  config snmp community accessmode ro *name*
- Configure an SNMP community name with read-write privileges by entering this command:

config snmp community accessmode rw *name*

- For IPv4 configuration—Configure an IPv4 address and subnet mask for an SNMP community by entering this command:

  config snmp community ipaddr *ip-address ip-mask name*

Note This command behaves like an SNMP access list. It specifies the IP address from which the device accepts SNMP packets with the associated community. An AND operation is performed between the requesting entity's IP address and the subnet mask before being compared to the IP address. If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches to all IP addresses. The default value is 0.0.0.0.

Note The controller can use only one IP address range to manage an SNMP community.

- For IPv6 configuration—Configure an IPv6 address and prefix-length for an SNMP community by entering this command:

  config snmp community ipaddr *ipv6-address ip-mask name*

- Enable or disable a community name by entering this command:

  config snmp community mode {**enable** | **disable**}

- Enable or disable a community name by entering this command:

  config snmp community ipsec {**enable** | **disable**}

- Configure the IKE authentication methods by entering this command:

  config snmp community ipsec ike auth-mode {**certificate** | **pre-shared-key** *ascii/hex secret*}

  Authentication mode can be configured per trap receiver. By default, the authentication mode is set to certificate.

- Configure a destination for a trap by entering this command:

  config snmp trapreceiver create *name ip-address*

- Delete a trap by entering this command:

  config snmp trapreceiver delete *name*

- Change the destination for a trap by entering this command:

  config snmp trapreceiver ipaddr *old-ip-address name new-ip-address*

- Configure the trap receiver IPSec session entering this command:

  config snmp trapreceiver ipsec {**enable** | **disable**} *community-name*

  Trap receiver IPSec must be in the disabled state to change the authentication mode.

- Configure the IKE authentication methods by entering this command:

  config snmp trapreceiver ipsec ike auth-mode {**certificate** | **pre-shared-key** *ascii/hex secret community-name*}

Authentication mode can be configured per trap receiver. By default, the authentication mode is set to certificate.

- Enable or disable the traps by entering this command:

  config snmp trapreceiver mode {**enable** | **disable**}

- Configure the name of the SNMP contact by entering this command:

  config snmp syscontact *syscontact-name*

  Enter up to 31 alphanumeric characters for the contact name.

- Configure the SNMP system location by entering this command:

  config snmp syslocation *syslocation-name*

  Enter up to 31 alphanumeric characters for the location.

- Verify that the SNMP traps and communities are correctly configured by entering these commands:

  show snmpcommunity

  show snmptrap

Note Related issue: CSCvr33858.

Read-only community does not get snmpEngineID. As per RFC 2575, the recommendation is such that, some of the OIDs are to be restricted and one of them is SnmpEngineId(engineId). For more information, see https://tools.ietf.org/html/rfc2575.

- See the enabled and disabled trap flags by entering this command:

  show trapflags

  If necessary, use the **config trapflags** command to enable or disable trap flags.

- Configure when the warning message should be displayed after the number of clients or RFID tags associated with the controller hover around the threshold level by entering this command:

  config trapflags {**client** | **rfid**} max-warning-threshold {*threshold-between-80-to-100* | **enable** | **disable**}

  The warning message is displayed at an interval of 600 seconds (10 minutes).

- Configure the SNMP engine ID by entering this command:

  config snmp engineID *engine-id-string*

Note The engine ID string can be a maximum of 24 characters.

- View the engine ID by entering this command:

  show snmpengineID

- Configure the SNMP version by entering this command:

  config snmp version {**v1** | **v2c** | **v3**} {**enable** | **disable**}

SNMP Community Strings

The controller has commonly known default values of "public" and "private" for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. If you use the default community names, and since these are known, the community names could be used to communicate to the controller using SNMP. Therefore, we strongly advise that you change these values.

Changing the SNMP Community String Default Values (GUI)

Procedure

Step 1 Choose **Management** and then **Communities** under SNMP. The SNMP v1 / v2c Community page appears.

Step 2 If “public” or “private” appears in the Community Name column, hover your cursor over the blue drop-down arrow for the desired community and choose **Remove** to delete this community.

Step 3 Click **New** to create a new community. The SNMP v1 / v2c Community > New page appears.

Step 4 In the Community Name text box, enter a unique name containing up to 16 alphanumeric characters. Do not enter “public” or “private.”

Step 5 In the next two text boxes, enter the IPv4/IPv6 address and IP Mask/Prefix Length from which this device accepts SNMP packets with the associated community and the IP mask.

Step 6 Choose **Read Only** or **Read/Write** from the Access Mode drop-down list to specify the access level for this community.

Step 7 Choose **Enable** or **Disable** from the Status drop-down list to specify the status of this community.

Step 8 Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your settings.

Step 10 Repeat this procedure if a “public” or “private” community still appears on the SNMP v1 / v2c Community page.

Changing the SNMP Community String Default Values (CLI)

Procedure

Step 1 See the current list of SNMP communities for this controller by entering this command:

show snmp community

Step 2 If "public" or "private" appears in the SNMP Community Name column, enter this command to delete this community:

config snmp community delete *name*

The *name* parameter is the community name (in this case, “public” or “private”).

Step 3 Create a new community by entering this command:

config snmp community create *name*

Enter up to 16 alphanumeric characters for the *name* parameter. Do not enter “public” or “private.”

Step 4 For IPv4 specific configuration, enter the IPv4 address from which this device accepts SNMP packets with the associated community by entering this command:

config snmp community ipaddr *ip_address ip_mask name*

Step 5 For IPv6 specific configuration, enter the IPv6 address from which this device accepts SNMP packets with the associated community by entering this command:

config snmp community ipaddr *ip_address prefix_length name*

Step 6 Specify the access level for this community by entering this command, where **ro** is read-only mode and **rw** is read/write mode:

config snmp community accessmode {**ro** | **rw**} *name*

Step 7 Enable or disable this SNMP community by entering this command:

config snmp community mode {**enable** | **disable**} *name*

Step 8 Enable or disable SNMP IPSec sessions for all SNMP communities by entering this command:

config snmp community ipsec {**enable** | **disable**} *name*

By default SNMP IPSec session is disabled. SNMP IPSec session must be disabled state to change the authentication mode.

Step 9 Configure the IKE authentication methods by entering this command:

config snmp community ipsec ike auth-mode {**certificate** | **pre-shared-key** *ascii/hex secret*}

- If authentication mode is configured as pre-shared-key, then enter a secret value. The secret value can either be an ASCII or a hexadecimal value. If auth-mode configured is certificate, then WLC will use the ipsecCaCert and ipsecDevCerts for SNMP over IPSEC.
- If authentication mode is configured as certificate, then controller uses the IPSEC CA and IPSEC device certificates for SNMP sessions. You need to download these certificates to the controller using the **transfer download datatype** {**ipseccacert** | **ipsecdevcert**} command.

Step 10 Save your changes by entering this command:

save config

Step 11 Repeat this procedure if you still need to change the default values for a “public” or “private” community string.

Configuring Real Time Statistics (CLI)

SNMP traps are defined for CPU and memory utilization of AP and controller. The SNMP trap is sent out when the threshold is crossed. The sampling period and statistics update interval can be configured using SNMP and CLI.

Note To get the right value for the current memory usage, you should configure either sampling interval or statistics interval.

- Configure the sampling interval by entering this command:

  config service statistics sampling-interval *seconds*

- Configure the statistics interval by entering this command:

  config service statistics statistics-interval *seconds*

- See sampling and service interval statistics by entering this command:

  show service statistics interval

SNMP Trap Enhancements

This feature provides soaking of SNMP traps and resending of traps after a threshold that you can configure called the hold time. The hold time helps in suppressing false traps being generated. The traps that are supported are for CPU and memory utilization of AP and controller. The retransmission of the trap occurs until the trap is cleared.

Procedure

- Configure the hold time after which the SNMP traps are to be resent by entering this command:

  config service alarm hold-time *seconds*

- Configure the retransmission interval of the trap by entering this command:

  config service alarm trap retransmit-interval *seconds*

- Configure debugging of the traps by entering this command:

  debug service alarm {**enable** | **disable**}

Configuring SNMP Trap Receiver (GUI)

Procedure

Step 1 Choose **Management** > **SNMP** > **Trap Receivers**.

Step 2 Click **New**.

The **SNMP Trap Receiver > New** page is displayed.

Step 3 In the **SNMP Trap Receiver Name** box, enter the SNMP trap receiver name.

Step 4 In the **IP Address (IPv4/IPv6)** box, enter the IP address of the trap receiver. Both IPv4 and IPv6 address formats are supported.

Step 5 From the **Status** drop-down list, choose to **Enable** or **Disable** the trap receiver.

Step 6 Check the **IPSec** check box if you want to enable IPSec parameters for the trap receiver.

Step 7 (Optional) If you enable the IPSec for the trap receiver, choose an **IPSec Profile Name** from the drop-down list.

Step 8 Save the configuration.

You can create a maximum of 6 such SNMP trap receivers.