Configure and Troubleshoot SNMP in SWA

Contents

Introduction

This document describes the steps to troubleshoot Simple Network Monitoring Protocol (SNMP) in Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Access To**Command Line Interface (CLI)**of SWA
- Administrative Access to the SWA.
- Basic knowledge of SNMP.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

How SNMP Works

SNMPis an applicationâ€“layer communication protocol that allows network devices to exchange management information among these systems and with other devices outside the network.

Through SNMP, network administrators can manage network performance, find and solve network problems, and plan network growth.

SNMP makes network monitoring more cost effective and allows your network to be more reliable. (For more information aboutSNMP, see RFCs 1065, 1066, and 1067.)

An SNMPâ€“managed network consists of a Manager, Agents, and Managed devices.

- The Manager provides the interface between the human network manager and the management system.
- The Agent provides the interface between the manager and the device being managed
- Management systems execute most of the management processes and provide the bulk of memory resources used for network management.

An agent resids on each managed device translates local management information data (such as performance information or event and error information) caught in software traps, into a readable form for the management system.

The SNMP agent captures data from Management Information Base (MIB) (device parameter and network data repositories) or from error or change traps.

MIB

The MIB, is a data structure that describes SNMP network elements as a list of data objects. The SNMP manager must compile the MIB file for each equipment type in the network to monitor SNMP devices.

The manager and agent use a MIB and a relatively small set of commands to exchange information. The MIB is organized in a tree structure with individual variables being represented as leaves on the branches.

A long numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages. The MIB associates each OID with a readable label and various other parameters related to the object.

The MIB then serves as a data dictionary or codebook that is used to assemble and interpret SNMP messages.

When the SNMP manager wants to know the value of an object, such as the state of an alarm point, the system name, or the element uptime, it assemble a GET packet that includes the OID for each object of interest.

The element receives the request and looks up each OID in its code book (MIB). If the OID is found (the object is managed by the element), a response packet is assembled and sent with the current value of the object included.

If the OID is not found, a special error response is sent that identifies the un-managed object

SNMP Trap

SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited

SNMP message.

SNMPv1 and SNMPv2c, along with the associated MIB, encourage trap-directed notification.

The idea behind trap-directed notification is that if a manager is responsible for a large number of devices, and each device has a large number of objects, it is impractical for the manager to poll or request information from every object on every device.

The solution is for each agent on the managed device to notify the manager without solicitation. It does this by send a message known as a Trap of the event.

After the manager receives the event, the manager displays it and can choose to take an action based on the event. For instance, the manager can poll the agent directly, or poll other associated device agents to understand the event better.

Trap-directed notification can result in substantial savings of network and agent resources by eliminate the need for frivolous SNMP requests. However, it is not possible to totally eliminate SNMP polls.

SNMP requests are required for discovery and topology changes. In addition, a managed device agent can not send a trap, if the device has had a catastrophic outage.

SNMPv1 traps are defined in RFC 1157, with these fields:

- ***Enterprise:***Identifies the type of managed object that generates the trap.
- ***Agent address:*** Provides the address of the managed object that generates the trap.
- ***Generic trap type:***Indicates one of a number of generic trap types.
- ***Specific trap code:***Indicates one of a number of specific trap codes.
- ***Time stamp:*** Provides the amount of time that has elapsed between the last network reinitialization and generation of the trap.
- ***Variable bindings:*** The data field of the trap that contains PDU. Each variable binding associates a particular MIB object instance with its current value.

SNMPv3

SNMPv3 supports the SNMP "Engine ID" Identifier, uniquely identifying each SNMP entity. Conflicts can occur if two SNMP entities have duplicate EngineIDs.

The EngineID is used to generate the key for authenticated messages. (For more information onSNMPv3, see RFCs 2571-2575.)

Many SNMP products remain fundamentally the same under SNMPv3 but are enhanced by these new features:

Security

- Authentication
- Privacy

Administration

- Authorization and access control

- Logical contexts
- Naming of entities, identities, and information
- People and policies
- User names and key management
- Notification destinations and proxy relationships
- Remote configuration via SNMP operations

SNMPv3 security models come primarily in two forms as Authentication and Encryption.

Authentication is used to ensure that only the intended recipient reads traps. As messages are created, they are given a special key based on the entity EngineID. The key is shared with the intended recipient and used to receive the message.
Encryption, privacy encrypts the payload of the SNMP message to ensure that unauthorized users cannot read it. Any intercepted traps filled with garbled characters and is unreadable. Privacy is especially useful in applications where SNMP messages must be routed over the Internet.
There are three security levels in an SNMP Group:

noAuthnoPriv â€“ Communication without authentication and privacy.
authNoPriv â€“ Communication with authentication and without privacy. The protocols used for Authentication are Message-Digest algorithm 5 (MD5) and Secure Hash Algorithm (SHA).
authPriv â€“ Communication with authentication and privacy. The protocols used for Authentication are MD5 and SHA, and for Privacy, Data Encryption Standard (DES) and Advanced Encryption Standard (AES) protocols can be used.

SNMP in SWA

The AsyncOS operating system supports system status monitoring viaSNMP.

Please note:

- SNMPis**off**by default.
- SNMPSET operations (configuration) are not implemented.
- AsyncOS supportsSNMPv1, v2, and v3.
- Message authentication and encryption are mandatory when enablingSNMPv3. Passphrases for authentication and encryption must be different.
- The encryption algorithm can be AES (recommended) or DES.
- The authentication algorithm can be SHA-1 (recommended) or MD5.
- The**snmpconfig** command â€œremembersâ€ your passphrases the next time you run the command.
- For AsyncOS releases prior to 15.0, TheSNMPv3 username is: **v3get**.
- For AsyncOS release 15.0 and later, The defaultSNMPv3 username is: v3get. As an admin, you can opt for any other username.
- If you use onlySNMPv1 orSNMPv2, you must set a community string. The community string does not default to **public**.
- ForSNMPv1 andSNMPv2, you must specify a network from whichSNMPGET requests are accepted.

- To use traps, anSNMPmanager (not included in AsyncOS) must be running and its IP address entered as the trap target. (You can use a host name, but if you do, traps only work if DNS is working.)

ConfiguringSNMPMonitor

To configureSNMPto gather system status information for the appliance, use the**snmpconfig** command in the CLI. After you choose and configure values for an interface, the appliance responds to**SNMPv3 GET** requests.

When you useSNMP, please consider these points:

- In SNMP version 3 requests must include a matching passphrase.
- By default, version 1 and 2 requests are rejected.
- If enabled, version 1 and 2 requests must have a matching community string.

```
SWA_CLI> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP

Do you want to enable SNMP? [Y]> Y

Please choose an IP interface for SNMP requests.
1. Management (10.48.48.184/24 on Management: wsa125to15-man.amojarra.calo)
2. P1 (192.168.13.184/24 on P1: wsa1255p1.amojarra.calo)
3. P2 (192.168.133.184/24 on P2: wsa1255p2.amojarra.calo)
[1]> 1

Which port shall the SNMP daemon listen on?
[161]> 161

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2

Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2

Enter the SNMPv3 username or press return to leave it unchanged.
[w3get]> SNMPMUser

Enter the SNMPv3 authentication passphrase.
[]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[]>

Enter the SNMPv3 privacy passphrase.
[]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[]>
```

```
Service SNMP V1/V2c requests? [N]> N

Enter the Trap target as a host name, IP address or list of IP addresses
separated by commas (IP address preferred). Enter "None" to disable traps.
[10.48.48.192]>

Enter the Trap Community string.
[ironport]> swa_community

Enterprise Trap Status
1. CPUUtilizationExceeded       Enabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. connectivityFailure          Disabled
7. keyExpiration                Enabled
8. linkUpDown                   Enabled
9. memoryUtilizationExceeded    Enabled
10. updateFailure               Enabled
11. upstreamProxyFailure        Enabled
Do you want to change any of these settings? [N]> Y

Do you want to disable any of these traps? [Y]> N

Do you want to enable any of these traps? [Y]> Y

Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 6

Please enter the URL to check for connectivity failure, followed by the
checking interval in seconds, separated by a comma:
[http://downloads.ironport.com,5]>

Enterprise Trap Status
1. CPUUtilizationExceeded       Enabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. connectivityFailure          Enabled
7. keyExpiration                Enabled
8. linkUpDown                   Enabled
9. memoryUtilizationExceeded    Enabled
10. updateFailure               Enabled
11. upstreamProxyFailure        Enabled
Do you want to change any of these settings? [N]>

Enter the System Location string.
[location]>

Enter the System Contact string.
[snmp@localhost]>

Current SNMP settings:
Listening on interface "Management" 10.48.48.184/24 port 161.
SNMP v3: Enabled.
SNMP v3 UserName: SNMPMUser
SNMP v3 Authentication type: SHA
SNMP v3 Privacy protocol: AES
SNMP v1/v2: Disabled.
```

```
Trap target: 10.48.48.192
Location: location
System Contact: snmp@localhost

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>

SWA_CLI> commit
```

SWA MIB files

MIB files are available from URL: https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html

Use the latest version of each MIB file.

There are multiple MIB files:

- **asyncoswebsecurityappliance-mib.txt** is anSNMPv2 compatible description of the Enterprise MIB forSecure Web Appliances.
- **ASYNCOS-MAIL-MIB.txt** is anSNMPv2 compatible description of the Enterprise MIB for Email Security appliances.
- **IRONPORT-SMI.txt** This â€œStructure of Management Informationâ€ file defines the role of the **asyncoswebsecurityappliance-mib**.

This release implements a read-only subset of MIB-II as defined in RFCs 1213 and 1907.

Seehttps://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.htmlto know more about CPU usage monitoring on the appliance withSNMP.

SWA SNMP TRAP

SNMPprovides the ability to send traps, or notifications, to advise an administration application when one or more conditions have been met.

Traps are network packets that contain data relating to a component of the system sending the trap.

Traps are generated when a condition has been met on theSNMPagent (in this case, the CiscoSecure Web Appliance).

After the condition has been met, theSNMPagent then forms anSNMPpacket and sends it to the host running theSNMPmanagement console software.

You can configureSNMPtraps (enable or disable specific traps) when you enableSNMPfor an interface.

> **Note**: To specify multiple trap targets: when prompted for the trap target, you can enter up to 10 comma separated IP addresses.

The **connectivityFailure** trap is intended to monitor your appliance connection to the Internet. It does this

by attempting to connect and send an HTTP GET request to a single external server every 5 to 7 seconds. By default, the monitored URL is **downloads.ironport.com** on port 80.

To change the monitored URL or port, run the **snmpconfig** command and enable the **connecivityFailure** trap, even if it is already enabled. You can see a prompt to change the URL.

> **Tip**: To simulate **connectivityFailure** traps, you can use the **dnsconfig** CLI command to enter a non-working DNS server. Lookups for downloads.ironport.com fails, and traps are sent every 5-7 seconds. Be sure to change the DNS server back to a working server after your test is over.

Recommended Monitoring OIDs

This is a list of the recommended MIBs to monitor and not an exhaustive list:

Hardware OID	Name
1.3.6.1.4.1.15497.1.1.1.18.1.3	raidID
1.3.6.1.4.1.15497.1.1.1.18.1.2	raidStatus
1.3.6.1.4.1.15497.1.1.1.18.1.4	raidLastError
1.3.6.1.4.1.15497.1.1.1.10	fanTable
1.3.6.1.4.1.15497.1.1.1.9.1.2	degreesCelsius

This is OIDs map directly to the output of the**status detail**CLI command:

OID	Name	Status detail field
System Resources		
1.3.6.1.4.1.15497.1.1.1.2.0	perCentCPUUtilization	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	perCentMemoryUtilization	RAM
Transactions per Second		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThruputNow	Average transactions per second in last minute.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheThruput1hrPeak	Maximum transactions per second in last hour.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThruput1hrMean	Average transactions per second in last hour.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	Maximum transactions per second since proxy restart.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheThruputLifeMean	Average transactions per second since proxy restart.
Bandwidth		

1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBwidthTotalNow	Average bandwidth in last minute.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	Maximum bandwidth in last hour.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hrMean	Average bandwidth in last hour.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBwidthTotalLifePeak	Maximum bandwidth since proxy restart.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBwidthTotalLifeMean	Average bandwidth since proxy restart.
Response time		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheHitsNow	Average cache hit rate in last minute.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	Maximum cache hit rate in last hour.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMean	Average cache hit rate in last hour.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	Maximum cache hit rate since proxy restart.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheHitsLifeMean	Average cache hit rate since proxy restart.
Cache hit rate		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheHitsNow	Average cache hit rate in last minute.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	Maximum cache hit rate in last hour.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMean	Average cache hit rate in last hour.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	Maximum cache hit rate since proxy restart.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheHitsLifeMean	Average cache hit rate since proxy restart.
Connections		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	Idle client connections.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerIdleConns	Idle server connections.
1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClientTotalConns	Total client connections.
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheServerTotalConns	Total server connections.

Troubleshoot SNMP

To view the connectivity between SWA and your SNMP manager it is best to capture packets, you can put the packet capture filter to: **(port 161 or port 162)**

Note: This filter is due to default SNMP ports, if you have changed the ports, please put the configured port numbers in the packet capture filter.

Steps to capture packets from SWA:

Step 1. log in to GUI

Step 2. on top right choose Support and Help

Step 3. select Packet Capture

Step 4. choose Edit settings

Step 5. Make sure correct interface has been selected

Step 6. Enter the filter conditions.

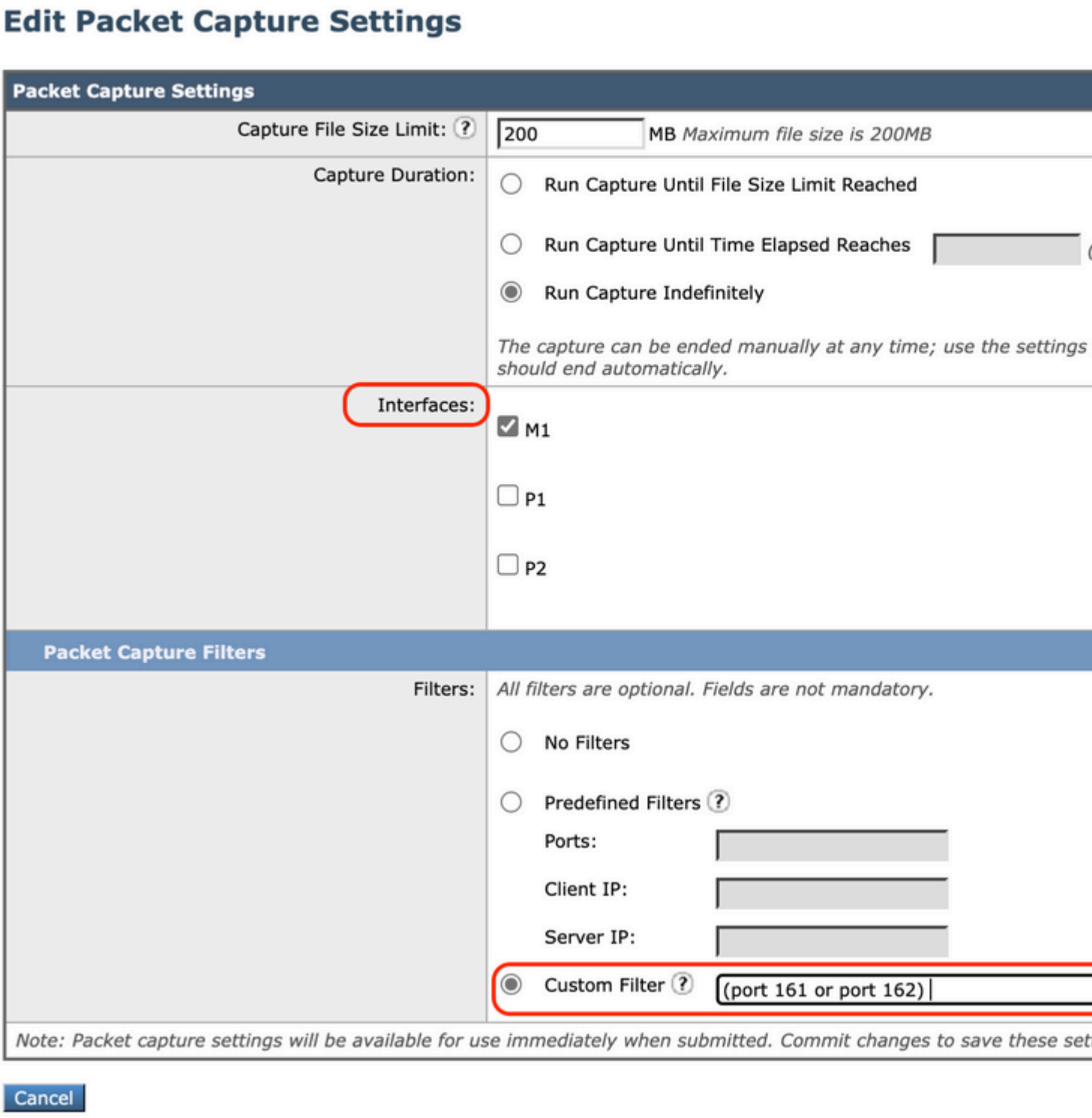

Image- Configure Packet Capture Filters

Step 7. Choose **Submit**

Step 8. Choose Start Capture.

> **Tip**: you can decrypt SNMPv3 packet captures with Wireshark. for more information please visit this link : [How-to-decrypt-snmpv3-packets-using-wireshark]

SNMPWALK

snmpwalk

is the name given to an SNMP application that runs multiple GET-NEXT requests automatically. The SNMP GET-NEXT request is used to query an enabled device and take SNMP data from a device. The **snmpwalk** command is used because it allows the user to chain GET-NEXT requests together without having to enter unique commands for each and every OID or node within a sub-tree

Install SNMPWALK on Windows Operating Systems

For Microsoft Windows users, you first need to download the tool.

Install SNMPWALK on Linux kernel

```
#For Redhat, Fedora, CentOs:
yum install net-snmp-utils

#For Ubuntu:
apt-get install snmp
```

Install SNMPWALK on MacOS

By default snmpwalk is installed on MacOS

To generate SNMP GET request, you can use **snmpwalk** command from another computer in your network which has connectivity to SWA, here are some samples of **snmpwalk** command:

```
snmpwalk -v2c -c <Community Name>  <SWA IP Address>
```

```
snmpwalk -v3 -l authPriv  -u v3get  -a SHA -A <Password>  -x AES -X <Password>  <SWA IP Address>
```

> **Note**: You can choose set security level to noAuthNoPriv or authNoPriv or authPriv depends on your SWA configurations.

SNMPTRAP

snmptrap is hidden CLI command which required SNMP be enabled on the SWA. You can generate SNMP trap by selecting the object, and trap, here is an example:

```
SWA_CLI>nmptrap

1. CPUUtilizationExceeded
2. FIPSModeDisableFailure
3. FIPSModeEnableFailure
4. FailoverHealthy
5. FailoverUnhealthy
6. connectivityFailure
```

```
7. keyExpiration
8. linkUpDown
9. memoryUtilizationExceeded
10. updateFailure
11. upstreamProxyFailure
Enter the number of the trap you would like to send.
[]> 8

1. CPUUtilization
2. FIPSApplicationName
3. FailoverApplicationName
4. RAIDEvents
5. RAIDID
6. connectionURL
7. ifIndex
8. ip
9. keyDescription
10. memoryUtilization
11. raidStatus
12. updateServiceName
Enter the number of the object you would like to send.
[]> 8

Enter the trap value.
[]> 10.20.3.15

Enter the user name
[admin]> SNMPuser

Please select Trap Protocol version:
1. 2c
2. 3
[1]> 2
```

SNMP logs in SWA

SWA has two logs related to SNMP, Some log types related to the web proxy component are not enabled. you can enable them from:

- In GUI :System Administration > Log subscriptions
- In CLI : **logconfig** > **new**

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
SNMP Logs	Records debug messages related to the SNMP network management engine.	Yes	Yes
SNMP Module Logs	Records Web Proxy messages related to interacting with the SNMP monitoring system.	No	No

Common Issues With SNMP

Some OIDS fail (either no value or wrong value).

This issue is related to SNMP pull. here are two samples of expected output and output with error:

```
Sample Output without Error:
$ snmpwalk -O a -v 3 -M "/var/lib/mibs/" -m "ALL" -l authPriv -a MD5 -x DES -u v3get -A xxx -X xxx proxy
iso.3.6.1.4.1.15497.1.1.1.9.1.1.1 = INTEGER: 1
iso.3.6.1.4.1.15497.1.1.1.9.1.2.1 = INTEGER: 22
iso.3.6.1.4.1.15497.1.1.1.9.1.3.1 = STRING: "Ambient"

Sample Output with Error:
$ snmpwalk -O a -v 3 -M "/var/lib/mibs/" -m "ALL" -l authPriv -a MD5 -x DES -u v3get -A xxx -X xxx proxy
iso.3.6.1.4.1.15497.1.1.1.9 = No Such Instance currently exists at this OID
```

You can check for "Application Faults" in snmp_logs

You can check the snmp_logs from **CLI** > **grep** > choose the number associated with snmp_logs:

```
SWA_CLI> grep

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
37. "snmp_logs" Type: "SNMP Logs" Retrieval: FTP Poll
...
Enter the number of the log you wish to grep.
[]> 37

Enter the regular expression to grep.
[]>

Do you want this search to be case insensitive? [Y]>

Do you want to search for non-matching lines? [N]>

Do you want to tail the logs? [N]> y

Do you want to paginate the output? [N]>
```

Reference

User Guide for AsyncOS 15.0 for Cisco Secure Web Appliance - LD (Limited Deployment) - Troubleshooting [Cisco Secure Web Appliance] - Cisco

Calculating Proxy CPU Utilization on the WSA Using SNMP - Cisco

snmpcmd(1) (freebsd)

snmptrap (freebsd)