18 May 2016

SNMP

All Versions

Best Practices

Check Point
SOFTWARE TECHNOLOGIES LTD.

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=31396

To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

Revision History

Date	Description
18 May 2016	Updated OID for traps in General Purpose Appliances (on page 17)
16 August 2015	Updated VSX OIDs ("VSX" on page 23) Added section for Recommended Custom Traps
01 June 2014	Fixed typo ("Sample Configuration File" on page 34)
11 February 2014	First release of this document

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments
mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on SNMP All Versions Best Practices.

Contents

Introduction to SNMP

In This Section:

SNMP (Simple Network Management Protocol) is an Internet standard protocol. SNMP is used to send and receive management data, protocol data units (PDUs), to network devices. SNMP-compliant devices, called agents, keep data about themselves in Management Information Bases (MIBs) and resend this data to the SNMP requesters.

Network management applications use SNMP and the supported MIB to query a management agent. The Check Point SNMP implementation lets an SNMP manager monitor the system and modify selected objects only. You can define and change one read-only community string and one read-write community string. You can set, add, and delete trap receivers and enable or disable various traps. You can also enter the location and contact strings for the system.

Check Point platforms support SNMP v1, v2, and v3. An SNMP manager can monitor a device using `GetRequest`, `GetNextRequest`, `GetBulkRequest`, and a specified number of traps. The Check Point implementation also supports `SetRequest` to change these attributes: `sysContact`, `sysLocation`, and `sysName`. You must configure read-write permissions for `set` operations to work.

Check Point MIBs

Check Point products use these MIB files:

MIB	Location
Standard MIBs Note: Not all standard MIBs are supported for Check Point products.	`/usr/share/snmp/mibs`
Check Point MIBs	`$CPDIR/lib/snmp`
Gaia specific trap MIBs (`GaiaTrapsMIB`)	`/etc/snmp`

SNMP and Network Security

In This Section:

"SNMP is not a particularly simple protocol (despite its name)."

David Blank-Edelman, author of *Automating System Administration with PERL*

SNMP can help you monitor and manage network objects, such as: appliances, servers and other components. However, make sure that you configure SNMP correctly to prevent possible security vulnerabilities. Enable SNMP only for network objects that you are managing with the NMS (Network Management System).

- Third-party servers and components usually enable SNMP by default. Disable SNMP on servers and components that you are not managing.
- SNMP v1 and v2 use community strings (passwords) that are sent in clear-text. It is possible to use a packet-sniffer to detect these strings and gain control of objects that are managed with SNMP.
- SNMP v3 uses the MD5 hashing algorithm for authentication and DES for encryption. We recommend that you use SNMP v3 authentication and message encryption whenever possible.
- SNMP is disabled by default on Check Point appliances, Security Gateways, and Security Management Servers.

Note - SNMP is enabled by default on the IPSO operating system. If SNMP is enabled when you upgrade from IPSO to Gaia, it is also enabled for Gaia.

Recommendations for SNMP v1 and SNMPv2

These are some recommendations to maximize network security when you are using SNMP v1 and SNMPv2:

- Use complex passwords for community strings: upper and lower case with at least 15 characters
- Make sure that the read-only and read-write community strings are unique
- Send SNMP traffic over a secure internal network

Implementing SNMP

In This Section:

Check Point SNMP References

For more about how to configure SNMP, see the appropriate guide for your operating system and version:

- *Gaia Administration Guide*
- *SecurePlatform Administration Guide*
- *Voyager Reference Guide for IPSO*

The Check Point Support Center http://supportcenter.checkpoint.com contains many SKs that explain how to configure SNMP. Search for SNMP or MIBs.

Preparing to Implement SNMP

These are some general recommendations to help you implement SNMP in your network:

- Make sure that the authority (NMS) can communicate with appliances, servers, and MIBs
- For 3rd party servers and components, use the manufacturer's documentation to configure them for SNMP management
- Make sure that the Firewall Rule Base allows the applicable SNMP traffic
- Use the NMS to test SNMP communications and connectivity

Implementing SNMP for Gaia

This is a high-level workflow to enable and configure SNMP for Gaia with the WebUI.

1. Log in to the WebUI of the appliance or server.
2. Enable the SNMP Agent.
3. Select the SNMP Versions that the network supports.
4. Select the interfaces and the SNMP Agent Addresses that SNMP traffic can use.
5. Configure the SNMP security settings:
   - For SNMP v1 and v2, configure the Community Strings.
   - For SNMP v3 configure the USM Users.
6. Configure the Enabled Traps.
7. Configure the Trap Receivers.
8. Add a rule to the Rule Base to allow SNMP traffic.
9. Install the policy on the applicable Security Gateways and servers.

Configuring SNMP - Gaia

The Gaia implementation of SNMP is built on net-snmp 5.4.2.1. Changes have been made to the first version to address security and other fixes. For more information, see Net-SNMP (http://www.net-snmp.org).

Warning - If you use SNMP, it is recommended that you change the community strings for security purposes. If you do not use SNMP, disable SNMP or the community strings.

You can use Gaia to do these SNMP-related tasks:

- Define and change one read-only community string
- Define and change one read-write community string
- Enable and disable the SNMP daemon
- Create SNMP users
- Change SNMP user accounts
- Add or delete trap receivers
- Enable or disable the various traps
- Enter the location and contact strings for the device

User-Based Security Model (USM)

Gaia supports the User-based Security Model (USM), a component of SNMP v3, for message-level security. With USM (see RFC 3414 http://tools.ietf.org/search/rfc3414), access to the SNMP service is controlled by user identities. Each user has a name, an authentication password and an optional encryption password for SNMP messages.

SNMP users are maintained separately from system users. You can create SNMP user accounts with the same names as system user accounts or create SNMP user accounts with different names. When you delete a system user account, you must also delete the SNMP user account.

Configuring SNMP - WebUI

Enabling SNMP

After you enable SNMP for the Security Gateway or Security Management Server, configure the SNMP traps ("Managing Traps" on page 28).

To enable SNMP:

1. In the tree view, click System Management > SNMP.
2. Select Enable SNMP Agent.
3. In Version drop down list, select the version of SNMP to run:
   - v1/v2/v3 (any)

     Select this option if your management station does not support SNMP v3.
   - v3-Only

     Select this option if your management station supports v3.

4. Optional: In SNMP Location String, enter a string that contains the location for the system. The maximum length for the string is 128 characters. That includes letters, numbers, spaces, special characters. For example: `Bldg 1, Floor 3, WAN Lab, Fast Networks, Speedy, CA`.
5. Optional: In SNMP Contact String, enter a string that contains the contact information for the device. The maximum length for the string is 128 characters. That includes letters, numbers, spaces, special characters. For example: `John Doe, Network Administrator, (111) 222-3333`.

To configure the SNMP agent interface:

In the Agent Interfaces or Agent Addresses section:

- Select Interface to enable SNMP for all interfaces on a computer.

  or

- Select one or more interfaces in the list to enable SNMP only for the selected interfaces.

To configure the community strings:

1. In the V1/V2 Settings section, in Read Only Community String, enter a string other than public.

   This is a basic security precaution that you must always use.
2. Optional: Set a Read-Write Community String.

   

   Warning - Define a read-write community string only if it is necessary to enable set operations, and the network is secure.

Configuring USM

To add a USM user:

1. In the tree view, click System Management > SNMP.
2. Below V3 - User-Based Security Model (USM), click Add.

   The Add New USM User window opens.
3. Enter the User Name.

   The range is 1 to 31 alphanumeric characters with no spaces, backslash, or colon characters. This can be the same as a user name for system access.
4. In Security Level, select from the drop down list:
   - authPriv—The user has authentication and privacy pass phrases and can connect with privacy encryption.
   - authNoPriv—The user has only an authentication pass phrase and can connect only without privacy encryption.
5. In User Permissions, select the privileges for the user:
   - Read-only
   - Read-write
6. In Authentication Pass Phrase, enter a password for the user that is between 8 and 128 characters in length.

7. In Privacy Pass Phrase, enter a pass phrase that is between 8 and 128 characters in length.
   This phrase is used to secure SNMP message payloads.
8. Click Save.
   The new user shows in the table.

To delete a USM user:

1. In the tree view, click System Management > SNMP.
2. Below V3 - User-Based Security Model (USM), select the user and click Remove.
   The Deleting USM User Entry window opens.
3. The window shows this message: Are you sure you want to delete "username" entry? Click Yes.

To edit a USM user:

1. In the tree view, click System Management > SNMP.
2. Below V3 - User-Based Security Model (USM), select the user and click Edit.
   The Edit USM User window opens.
3. In the window you can change the Security Level, User Permissions, the Authentication Passphrase, or the Privacy Passphrase.
4. Click Save.

Configuring SNMP Traps

To enable or disable trap types:

1. In the tree view, click System Management > SNMP.
2. In the Enabled Traps section, click Set.
   The Add New Trap Receiver window opens.
   - To enable a trap: select from the Disabled Traps list, and click Add
   - To disable a trap: select from the Enabled Traps list, and click Remove
3. Click Save.
4. Add a USM user: in Trap User, select an SNMP user.
   You must do this even if using SNMPv1 or SNMPv2.
5. In Polling Frequency, specify the number of seconds between polls.
6. Click Apply.

To configure trap receivers (management stations):

1. In the tree view, click System Management > SNMP.
2. In the Trap Receivers Settings section, click Add. The Add New Trap Receiver window opens.
3. In IP Address, enter the IP address of a receiver.
4. In Version, select the Trap SNMP Version for the trap receiver from the drop down menu.
5. For SNMPv1 and SNMPv2, in Community String, enter the community string for the specified receiver.
6. Click Save.

To edit trap receivers:

1. In the tree view, click System Management > SNMP.
2. In the Trap Receivers Settings section, select the trap and click Edit.
   The Edit Trap Receiver window opens.
3. You can change the version or the community string.
4. Click Save.

To delete trap receivers:

1. In the tree view, click System Management > SNMP.
2. In the Trap Receivers Settings section, select the trap and click Remove.
   The Deleting Trap Receiver Entry window opens.

Using Common Counters

In This Section:

This chapter lists common SNMP counters and traps that are commonly used in networks.

System

CPU

Counters

Counter	OID	Format	Description
CPU usage	Overall: procUsage .1.3.6.1.4.1.2620.1.6.7.2.4 Per Core: multiProcUsage .1.3.6.1.4.1.2620.1.6.7.5.1.5.x *	Integer 0-100	Percentage of CPU utilization
User Time	Overall: procUsrTime .1.3.6.1.4.1.2620.1.6.7.2.1 Per Core: multiProcUserTime .1.3.6.1.4.1.2620.1.6.7.5.1.2.x *	Integer 0-100	Percentage of CPU utilization for user mode processes
System Time	Overall: procSysTime .1.3.6.1.4.1.2620.1.6.7.2.2 Per Core: multiProcSystemTime .1.3.6.1.4.1.2620.1.6.7.5.1.3.x *	Integer 0-100	Percentage of CPU utilization for kernel mode processes
Idle time	Overall: procIdleTime .1.3.6.1.4.1.2620.1.6.7.2.3 Per Core: multiProcIdleTime .1.3.6.1.4.1.2620.1.6.7.5.1.4.x *	Integer 0-100	Percentage of CPU idle time
Interrupts per second	Overall: procInterrupts .1.3.6.1.4.1.2620.1.6.7.2.6 Per Core: multiProcInterrupts .1.3.6.1.4.1.2620.1.6.7.5.1.7.x *	Integer	Number of CPU interrupts per second Note: Not supported on IPSO operating system
Number of Cores	procNum .1.3.6.1.4.1.2620.1.6.7.2.7	Integer	Number of machine cores

* Replace the letter "x" with the core number. Do not use the last digit to get a report for all cores.

Traps

Trap	OID	Format	Description
Core utilization alert	chkpntCPUCoreUtilTrap .1.3.6.1.4.1.2620.1.2000.3.1	String	Trap sent when core utilization exceeds the threshold. Trap includes core name.
Core interrupts alert	chkpntCPUCoreInterruptsTrap .1.3.6.1.4.1.2620.1.2000.3.2	String	Trap sent when the number of core interrupts exceeds the threshold. Trap includes core name.

Memory

Counters

Counter	OID	Format	Description
Total real RAM	memTotalReal64 .1.3.6.1.4.1.2620.1.6.7.4.3	String	Total real memory in bytes. Memory used by applications.
Active real RAM	memActiveReal64 .1.3.6.1.4.1.2620.1.6.7.4.4	String	Active real memory (memory used by applications that is not cached to the disk) in bytes.
Free real RAM	memFreeReal64 .1.3.6.1.4.1.2620.1.6.7.4.5	String	Free memory available for applications in bytes.
Total virtual RAM	memTotalVirtual64 .1.3.6.1.4.1.2620.1.6.7.4.1	String	The size in BYTES of the virtual-memory working segment pages.
Active virtual RAM	memActiveVirtual64 .1.3.6.1.4.1.2620.1.6.7.4.2	String	The size in bytes of the virtual-memory working segment pages that have actually been touched.
Hmem fails	fwPerfStat.fwHmem. fwHmem-failed-alloc .1.3.6.1.4.1.2620.1.1.26.1.21	Integer	Memory allocation failure.
Kmem fails	fwPerfStat.fwHmem. fwKmem-failed-alloc .1.3.6.1.4.1.2620.1.1.26.2.15	Integer	Insufficient free memory.

Traps

Trap	OID	Format	Description
Real memory utilization alert	chkpntRealMemoryTrap .1.3.6.1.4.1.2620.1.2000.4.2	String	Alert sent when real memory exceeds the threshold % of total memory.
Swap memory utilization alert	chkpntSwapMemoryTrap .1.3.6.1.4.1.2620.1.2000.4.1	String	Alert sent when swap memory exceeds the threshold % of virtual (swap) memory.

Disk

The following table shows the disk partition counters:

Counters

Counter	OID	Format	Description
Index	multiDiskIndex .1.3.6.1.4.1.2620.1.6.7.6.1.1.x *	Integer	Partition index
Name	multiDiskName .1.3.6.1.4.1.2620.1.6.7.6.1.2.x *	String	Partition name
Size	multiDiskSize .1.3.6.1.4.1.2620.1.6.7.6.1.3.x *	String	Total partition size in bytes
Used	multiDiskUsed .1.3.6.1.4.1.2620.1.6.7.6.1.4.x *	String	Disk used in partition in bytes
Total Free Bytes	multiDiskFreeTotalBytes .1.3.6.1.4.1.2620.1.6.7.6.1.5.x *	String	Total free disk in partition in bytes
Total Free Percentage	multiDiskFreeTotalPercent .1.3.6.1.4.1.2620.1.6.7.6.1.6.x *	Integer	Percentage of total free disk in partition
Available free Bytes	multiDiskFreeAvailableBytes .1.3.6.1.4.1.2620.1.6.7.6.1.7.x *	String	Available free disk in partition (not reserved by the OS) in bytes
Available free Percentage	multiDiskFreeAvailablePercent .1.3.6.1.4.1.2620.1.6.7.6.1.8.x *	Integer	Percentage of available free disk in partition
RAID disk state	raidDiskState .1.3.6.1.4.1.2620.1.6.7.7.2.1.9	Integer	RAID disk status
RAID physical state	raidDiskTable .1.3.6.1.4.1.2620.1.6.7.7.2	Table	Physical RAID storage status: Limitation: Raid counters are not supported on Smart-1 appliances.

Counter	OID	Format	Description
RAID logical state	raidVolumeTable .1.3.6.1.4.1.2620.1.6.7.7.1	Table	Logical RAID storage status: Limitation: Raid counters are not supported on Smart-1 appliances.

* Replace the letter "x" with the partition number. Do not use the last digit to get a report for all partitions.

Traps

Trap	OID	Format	Description
Disk full alert	chkpntDiskSpaceTrap .1.3.6.1.4.1.2620.1.2000.2.1	String	Available space on RAID partition is less than the specified threshold. Trap includes file system name.
RAID disk state alert	chkpntRAIDDiskTrap .1.3.6.1.4.1.2620.1.2000.2.3	Integer	RAID disk is in one of these states: 1-Degraded 2-Failed 255 Unknown Trap includes disk and volume ID.
RAID disk flag alert	chkpntRAIDDiskFlagsTrap .1.3.6.1.4.1.2620.1.2000.2.4	Integer	RAID disk sends on of these flags: OUT_OF_SYNC(0x01) QUIESCED(0x02) Trap includes disk and volume ID.

Operating System

Traps

Trap	OID	Format	Description
Configuration changed	chckpntSystemConfiguration ChangeTrap .1.3.6.1.4.1.2620.1.3000.10.1.1		Shows when a change to the system configuration is applied in Gaia
Configuration Saved	chckpntSystemConfiguration SaveTrap .1.3.6.1.4.1.2620.1.3000.10.1.2		Shows when a permanent change to the system configuration occurs in Gaia
Boot / Cold start	coldStart .1.3.6.1.6.3.1.1.5.1		Shows when the SNMP agent is re-initialized

Appliances

General Purpose Appliances

Counters

Counter	OID	Format	Description
Power supply	powerSupplyInfo .1.3.6.1.4.1.2620.1.6.7.9	Table	Status table of power supply: • Index .1.3.6.1.4.1.2620.1.6.7.9.1.1.1 Power supply index • Status .1.3.6.1.4.1.2620.1.6.7.9.1.1.2 Up or Down
Fan rotation	fanSpeedSensorTable .1.3.6.1.4.1.2620.1.6.7.8.2	Table	Status table of fan rotation: • Index fanSpeedSensorIndex .1.3.6.1.4.1.2620.1.6.7.8.2.1.1 Fan index • Name fanSpeedSensorName .1.3.6.1.4.1.2620.1.6.7.8.2.1.2 Fan sensor name • Value fanSpeedSensorValue .1.3.6.1.4.1.2620.1.6.7.8.2.1.3 Fan rotations per minute • Status fanSpeedSensorStatus .1.3.6.1.4.1.2620.1.6.7.8.2.1.6: 0 = OK Otherwise = problem

Counter	OID	Format	Description
Temperature	tempartureSensorTable .1.3.6.1.4.1.2620.1.6.7.8.1	Table	Appliance temperature status: • Index tempertureSensorIndex .1.3.6.1.4.1.2620.1.6.7.8.1.1.1 Sensor index • Name tempertureSensorName .1.3.6.1.4.1.2620.1.6.7.8.1.1.2 Sensor name • Value (tempertureSensorValue .1.3.6.1.4.1.2620.1.6.7.8.1.1.3 Temperature in Celsius • Status (tempertureSensorStatus .1.3.6.1.4.1.2620.1.6.7.8.1.1.6 0 =OK Other = Problem
Appliance model	svnApplianceProductName .1.3.6.1.4.1.2620.1.6.16.7	String	Appliance model name Supported for R77.10 and higher.
Appliance serial number	svnApplianceSerialNumber .1.3.6.1.4.1.2620.1.6.16.3	String	Appliance serial number Supported for R77.10 and higher on 2012 Appliances.
Manufacturer	svnApplianceManufacturer .1.3.6.1.4.1.2620.1.6.16.9	String	Returns "Check Point" Supported for R77.10 and higher.

Traps

Trap	OID	Format	Description
Temperature sensor alert	chkpntTempertureTrap .1.3.6.1.4.1.2620.1.3000.5.1.1	String	Temperature sensor alert. Sensor name provided in trap.
Fan speed sensor alert	chkpntFanSpeedTrap .1.3.6.1.4.1.2620.1.3000.5.2.1	String	Fan speed sensor alert. Sensor name provided in trap.
Voltage sensor alert	chkpntVoltageTrap .1.3.6.1.4.1.2620.1.3000.5.3.1	String	Voltage sensor alert. Sensor name provided in trap.
Power supply sensor alert	chkpntPowerSupplyTrap .1.3.6.1.4.1.2620.1.3000.5.4.1	String	Power supply sensor alert. Sensor name provided in trap.

Network

Counters

Note: These packet values are applicable to IPv4, non-accelerated packets only.

Counter	OID	Format	Description
Accepted packets	fwAccepted .1.3.6.1.4.1.2620.1.1.4	Integer	Total number of accepted packets since last reboot
Dropped packets	fw.fwDropped .1.3.6.1.4.1.2620.1.1.6	Integer	Total number of dropped packets since last reboot
Rejected packets	fw.fwRejected .1.3.6.1.4.1.2620.1.1.5	Integer	Total number of rejected packets since last reboot
Accepted packets rate	fwPacketsRate .1.3.6.1.4.1.2620.1.1.25.6	String	Accepted packets per second
Accepted bytes throughput	fwAcceptedBytesTotalRate .1.3.6.1.4.1.2620.1.1.25.8	String	Accepted bytes per second
Dropped packets rate	fwDroppedTotalRate .1.3.6.1.4.1.2620.1.1.25.16	String	Dropped packets per second
Dropped bytes throughput	fwDroppedBytesTotalRate .1.3.6.1.4.1.2620.1.1.25.9	String	Dropped bytes per second
Concurrent connections	fwNumConn .1.3.6.1.4.1.2620.1.1.25.3	Integer	Number of concurrent IPv6 and IPv4 connections
Peak concurrent connections	fwPeakNumConn .1.3.6.1.4.1.2620.1.1.25.4	Integer	Peak number of concurrent connections since last reboot
Number of maximum concurrent connections	fwConnTableLimit .1.3.6.1.4.1.2620.1.1.25.10	Integer	Maximum number of connections in the table Note: If running on GAIA and optimization is set to "Automatically", then this value will be `0`. Otherwise it shows the hard limit that is defined on the gateway or cluster object.
Interface statistics	fwIfTable .1.3.6.1.4.1.2620.1.1.25.5	Table	Table containing firewall interface stats
List of interfaces	ifDescr .1.3.6.1.2.1.2.2.1.2	Table	List of interface names (part of interface statistics table)

Counter	OID	Format	Description
Input errors per interface	ifInErrors .1.3.6.1.2.1.2.2.1.14	Table	List of interface input errors according (part of interface statistics table)
Output errors per interface	ifOutErrors .1.3.6.1.2.1.2.2.1.20	Table	List of interface output errors according (part of interface statistics table)

Counters - Packet statistics per interface

Counter	OID	Format	Description
Interface Name	fwIfName .1.3.6.1.4.1.2620.1.1.25.5.1.2	String	Interface name
Incoming packets accepted	fwAcceptPcktsIn .1.3.6.1.4.1.2620.1.1.25.5.1.5	Integer	Number of incoming accepted packets since last reboot
Outgoing accepted packets	fwAcceptPcktsOut .1.3.6.1.4.1.2620.1.1.25.5.1.6	Integer	Number of outgoing accepted packets since last reboot
Incoming accepted bytes	fwAcceptBytesIn .1.3.6.1.4.1.2620.1.1.25.5.1.7	Integer	Total incoming accepted bytes since last reboot
Outgoing accepted bytes	fwAcceptBytesOut .1.3.6.1.4.1.2620.1.1.25.5.1.8	Integer	Total outgoing accepted bytes since last reboot
Incoming dropped packets	fwDropPcktsIn .1.3.6.1.4.1.2620.1.1.25.5.1.9	Integer	Number of incoming dropped packets since last reboot
Outgoing dropped packets	fwDropPcktsOut .1.3.6.1.4.1.2620.1.1.25.5.1.10	Integer	Number of outgoing dropped packets since last reboot
Incoming rejected packets	fwRejectPcktsIn .1.3.6.1.4.1.2620.1.1.25.5.1.11	Integer	Number of incoming rejected packets since last reboot
Outgoing rejected packets	fwRejectPcktsOut .1.3.6.1.4.1.2620.1.1.25.5.1.12	Integer	Number of outgoing rejected packets since last reboot

Traps

Counter	OID	Format	Description
Concurrent connections rate alert	chkpntTrapConcurrentConnRate .1.3.6.1.4.1.2620.1.2000.1.4	String	Connections per second exceeds the threshold
New connection rate alert	chkpntTrapNewConnRate .1.3.6.1.4.1.2620.1.2000.1.3	String	New connections per second exceeds the threshold
Bytes throughput alert	chkpntTrapBytesThroughput .1.3.6.1.4.1.2620.1.2000.1.5	String	Bytes per second exceeds the threshold
Accepted packet rate alert	chkpntTrapAcceptedPacketRate .1.3.6.1.4.1.2620.1.2000.1.6	String	Accepted packets per second exceeds the threshold
Interface unplugged alert	chkpntTrapNetIfUnplugged .1.3.6.1.4.1.2620.1.2000.1.2	String	Interface is removed from the table, trap includes the interface name

Check Point Software Blades

General

Counters

Counter	OID	Format	Description
Major version	fwVerMajor .1.3.6.1.4.1.2620.1.1.22	Integer	Check Point major version
Minor version	fwVerMinor .1.3.6.1.4.1.2620.1.1.23	Integer	Check Point minor version
Policy name	fwPolicyName .1.3.6.1.4.1.2620.1.1.25.1	String	Name of Security Policy currently enforced
Last Install Policy time	fwInstallTime .1.3.6.1.4.1.2620.1.1.25.2	String	Date/Time last Security Policy was installed

Logging

Counter	OID	Format	Description
Log Server connectivity	fwLSConnOverall .1.3.6.1.4.1.2620.1.1.30.1	Integer 0-2	Connectivity with log servers: 0=OK, 1=Warning, 2=Error
Log Server connectivity description	fwLSConnOverallDesc .1.3.6.1.4.1.2620.1.1.30.2	String	Description of connectivity status with log servers
Local logging status	fwLocalLoggingStat .1.3.6.1.4.1.2620.1.1.30.5	Integer 0-3	Status of local logging: • 0=to log servers • 1=local configured • 2=local due to connectivity issues • 3=local due to high rate
Local logging status	fwLocalLoggingDesc .1.3.6.1.4.1.2620.1.1.30.4	String	Description of local logging status

Clusters

Counters

Counter	OID	Format	Description
HA State	haState .1.3.6.1.4.1.2620.1.5.6	String	Member HA state. active – Inspecting traffic standby – Ready to inspect traffic, but there is another active member. This member is now in the standby mode. Active Attention –The member is blocked. Because there are no other available members, it will continue as the active member. down – Member is down or other members see it as down.
HA Status Code	haStatCode 1.3.6.1.4.1.2620.1.5.101	Integer	HA Status Code. 0 – Member is up and working (active or standby) 1 – Attention. There is a problem preventing it to switch to active or standby 2 – HA is down.

Counter	OID	Format	Description
HA started	HaStarted 1.3.6.1.4.1.2620.1.5.5	Table	Cluster is up and running and a cluster policy exists. yes or no.
Cluster interfaces and states	haIfTable .1.3.6.1.4.1.2620.1.5.12	Table	Table of interfaces and states per `cphaprob -a if`

VSX

Counter	OID	Format	Description
Statistics per VS	vsxCountersTable .1.3.6.1.4.1.2620.1.16.23.1	Table	Table showing stats per VSID for: • connections • packets • fw • accepts/rejects/drops
States of all VSs	vsxStatusTable .1.3.6.1.4.1.2620.1.16.22.1	Table	Table showing states of all VSIDs, including HA status for VSLS.

The OIDs for the following integer counters depend on the VD (Virtual Device) index. Run `snmpwalk` for the table vsxStatusVsName (1.3.6.1.4.1.2620.1.16.22.1.1.3) to find the correct VD index.

Counter	OID	Format	Description
Connection table size of VS	vsxCountersConnTableLimit .1.3.6.1.4.1.2620.1.16.23.1.1.4.<VD index>	Integer	Connection table sizes for VS.
Concurrent connections of VS	vsxCountersConnNum .1.3.6.1.4.1.2620.1.16.23.1.1.2.<VD index>	Integer	Concurrent connections for VS.
Peak connections of VS	vsxCountersConnPeakNum .1.3.6.1.4.1.2620.1.16.23.1.1.3.<VD index>	Integer	Peak connections for VS.

Sample Output for vsxStatusVsName (1.3.6.1.4.1.2620.1.16.22.1.1.3)

```
SNMPv2-SMI::enterprises.2620.1.16.22.1.1.3.1.0 = STRING: "VSX-gw"
SNMPv2-SMI::enterprises.2620.1.16.22.1.1.3.2.0 = STRING: "VSX-gw_VR"
SNMPv2-SMI::enterprises.2620.1.16.22.1.1.3.3.0 = STRING: "VSX-gw_VS1"
SNMPv2-SMI::enterprises.2620.1.16.22.1.1.3.4.0 = STRING: "VSX-gw_VSB1"
SNMPv2-SMI::enterprises.2620.1.16.22.1.1.3.5.0 = STRING: "VSX-gw-VSW"
```

The Virtual System `VSX-gw_VS_1` has the index value of 3.0. To find the connection table size of `VSX-gw_VS_1`, use OID `.1.3.6.1.4.1.2620.1.16.23.1.1.4`.3.0

VPN

Counters

Counter	OID	Format	Description
Number of encrypted packets per second	cpvIpsecEspEncPkts .1.3.6.1.4.1.2620.1.2.5.4.5	String	Number of encrypted packets per second
Number of decrypted packets per second	cpvIpsecEspDecPkts .1.3.6.1.4.1.2620.1.2.5.4.6	String	Number of decrypted packets per second

VPN Tunnel Table Counters

Counter	OID	Format	Description
Peer IP address	tunnelPeerIpAddr .1.3.6.1.4.1.2620.500.9002.1.1	IP Address	Peer IP address
Peer name	tunnelPeerObjName .1.3.6.1.4.1.2620.500.9002.1.2	String	Peer name
Tunnel state	tunnelState .1.3.6.1.4.1.2620.500.9002.1.3	Integer	Tunnel state 3 – active 4 – destroy 129 – idle 130 – phase1 131 – down 132 – init
Community	tunnelCommunity .1.3.6.1.4.1.2620.500.9002.1.4	String	Tunnel community
Next Hop	tunnelNextHop .1.3.6.1.4.1.2620.500.9002.1.5	IP Address	Next hop IP address
Tunnel interface	tunnelInterface 1.3.6.1.4.1.2620.500.9002.1.6	String	Tunnel interface
Source IP	tunnelSourceIpAddr .1.3.6.1.4.1.2620.500.9002.1.7	IP Address	Source IP address
Link priority	tunnelLinkPriority .1.3.6.1.4.1.2620.500.9002.1.8	Integer 0-2	Link priority 0 – primary 1 – backup 2 – on-demand

Counter	OID	Format	Description
Probing state	tunnelProbState .1.3.6.1.4.1.2620.500.9002.1.9	Integer 0-2	Probing state 0 – unknown 1 – alive 2 – dead
Peer type	tunnelPeerType 1.3.6.1.4.1.2620.500.9002.1.10	Integer 1-3	Peer type 1 – regular 2 – daip 3 – robo (SmartLSM Gateway)
Tunnel type	tunnelType .1.3.6.1.4.1.2620.500.9002.1.11	Integer 1-2	Tunnel type 1 – regular 2 – permanent

Remote Access

Counters

Counter	OID	Format	Description
Remote Access users table	raUsersTable .1.3.6.1.4.1.2620.500.9000	Table	Table containing Remote Access users tunnel information

SNMP for RAID Environments

The health of a RAID array can be monitored using the Gaia SNMP monitoring daemon. SNMP traps can be set to fire once an OID value is in breach of a configurable threshold.

The raidInfo MIB branch is 1.3.6.1.4.1.2620.1.6.7.7. The data it contains is detailed below.

Data is available in the form of two SNMP tables:

SNMP Table	OID
Volumes	1.3.6.1.4.1.2620.1.6.7.7.1.1
Disks	1.3.6.1.4.1.2620.1.6.7.7.2.1

Each volume in the RAID configuration has an entry in the Volumes table. Each volume entry in the Volumes table contains the following OID values:

Disk Volume Information	OID	Comment
Index	.1	
Volume ID	.2	
Volume Type (RAID level)	.3	For Check Point appliances, will normally be RAID_1
Number Of Disks in the RAID	.4	

Disk Volume Information	OID	Comment
Volume size	.5	Maximum supported LBA (Logical Block Addressing)
Volume state	.6	One of: • OPTIMAL • DEGRADED • FAILED
Volume flags	.7	One or more of: • ENABLED • QUIESCED • RESYNC_IN_PROGRESS • VOLUME_INACTIVE

Each disk participating in the RAID configuration has an entry in the disks table. Each disk entry in the table contains the following OID values:

Physical Disks information	OID	Comment
Index	.1	
Volume ID	.2	
SCSI ID	.3	
Disk number	.4	On Check Point Power-1 9070 appliance: 0 - upper disk, 1 - lower disk
Vendor	.5	
Product ID	.6	
Revision	.7	
Size	.8	Maximum supported LBA (Logical Block Addressing)
State	.9	One of the following: • ONLINE • MISSING • NOT_COMPATIBLE • FAILED • INITIALIZING • OFFLINE_REQUESTED • FAILED_REQUESTED • OTHER_OFFLINE

Physical Disks information	OID	Comment
Flags	.10	One of: • OUT_OF_SYNC • QUIESCED
Sync state	.11	A percentage. Shows how much of the backup disk is synchronized with the primary disk.

Managing Traps

In This Section:

You can create custom traps in Gaia and SecurePlatform. This capability is not supported for IPSO and other operating systems. You can define custom traps based on OIDs in the Check Point MIBs or those standard MIBs that are supported by Check Point.

Recommended Custom Traps

This is a collection of recommended traps to configure for full monitoring. For details on the values of specified appliances, see sk42426 http://supportcontent.checkpoint.com/solutions?id=sk42426.

Memory Trap (RAM)

The memory trap (RAM) is the amount of available free memory. This is no more than 80% of the total memory. To get the total memory, send an SNMP query to 'memTotalReal'.

OID Name	OID Number	MIB File
memAvailReal	.1.3.6.1.4.1.2021.4.6.0	UCD-SNMP-MIB.txt

Clish example: Add snmp custom-trap memFree oid memAvailReal operator Less_Than threshold 30000000 frequency 2 message "Free memory is less than 30 GB". This indicates free memory is less than 30 GB.

Disk Space

Disk space is the root partition ("/") percentage of free space. It is no less than 20%.

OID Name	OID Number	MIB File
diskPercent	.1.3.6.1.4.1.2620.1.6.7.3.3.0	chkpnt.mib

Clish example: Add snmp custom-trap lowDiskSpace oid .1.3.6.1.4.1.2620.1.6.7.3.3.0 operator Less_Than threshold 20 frequency 2 message "Hard disk free space is less than 20 percent." This indicates the hard disk free space is less than 20%.

CPU Trap

The CPU trap is the percentage of CPU time spent processing system-level code. It is calculated over the last minute.

OID Name	OID Number	MIB File
ssCpuSystem	.1.3.6.1.4.1.2021.11.10.0	UCD-SNMP-MIB.txt

Clish example: Add snmp custom-trap cpuSystem oid ssCpuSystem operator Greater_Than threshold 80 frequency 2 message "High system CPU - over 80%". This indicates the CPU is over 80%.

Interface Traps

In interface traps, the possible values are integers: 1 is up and 2 is down. There is no specific recommendation. The value shows the current operational state of the interface.

OID Name	OID Number	MIB File
ifOperStatus	1.3.6.1.2.1.2.2.1.8	IF-MIB.txt

Clish examples:

- Add snmp custom-trap interface3 oid ifOperStatus.3 operator Equal threshold 2 frequency 2 message "Interface 3 is down!" This indicates interface 3 is down.
- Add snmp custom-trap interface2 oid ifOperStatus.2 operator Equal threshold 1 frequency 2 message "Interface 2 is up!" This indicates interface 2 is up.

Power Supply Sensors

The power supply sensors show the power supply status. The possible values (string) are "Up" / "Down". Both values can be trapped.

OID Name	OID Number	MIB File
powerSupplyStatus	.1.3.6.1.4.1.2620.1.6.7.9.1.1.2	chkpnt.mib

Clish examples:

- Add snmp custom-trap powerSupplyDown_Any oid .1.3.6.1.4.1.2620.1.6.7.9.1.1.2 operator Equal threshold Down frequency 2 message "Power supply is down!" This indicates any power supply is down.
- Add snmp custom-trap powerSupplyUp_1 oid .1.3.6.1.4.1.2620.1.6.7.9.1.1.2.1 operator Equal threshold Down frequency 2 message "Power supply 1 is down!" This indicates power supply 1 is up.

Temperature Sensors

The temperature sensor value is in degrees Celsius. To get thresholds and names of the sensors in your machine, enter in expert mode: `# dbget sysEnv:temp`

OID Name	OID Number	MIB File
temperatureSensorValue	.1.3.6.1.4.1.2620.1.6.7.8.1.1.3	chkpnt.mib

Clish examples:

- Add snmp custom-trap temperatureSensorValue_Any oid .1.3.6.1.4.1.2620.1.6.7.8.1.1.3 operator Greater_Than threshold 86 frequency 2 message "Sensor is over temperature!" This **indicates any sensor is over 86ºC.**
- Add snmp custom-trap temperatureSensorValue_CPU0 oid .1.3.6.1.4.1.2620.1.6.7.8.1.1.3.4 operator Greater_Than threshold 86 frequency 2 message "CPU0 is over temperature!" This indicates CPU0 sensor is over temperature.

Fan Sensors

This is the fan speed sensor value in RPM. To get thresholds and names of the sensors in your machine, enter in expert mode: `# dbget sysEnv:fans`

OID Name	OID Number	MIB File
fanSpeedSensorValue	.1.3.6.1.4.1.2620.1.6.7.8.2.1.3	chkpnt.mib

Clish examples:

- Add snmp custom-trap fanSpeedSensorLow_Any oid .1.3.6.1.4.1.2620.1.6.7.8.2.1.3 operator Less_Than threshold 2472 frequency 2 message "Fan speed is low!" This indicates that any of the fans is at low speed.
- Add snmp custom-trap fanSpeedSensorHigh_Any oid .1.3.6.1.4.1.2620.1.6.7.8.2.1.3 operator Greater_Than threshold 19570 frequency 2 message "Fan speed is high!" This indicates that any of the fans is at high speed.
- Add snmp custom-trap fanSpeedSensorLow_3 oid .1.3.6.1.4.1.2620.1.6.7.8.2.1.3.3 operator Less_Than threshold 2472 frequency 2 message "Fan 3 speed is low!" This indicates that Fan 3 is low speed.
- Add snmp custom-trap fanSpeedSensorHigh_2 oid .1.3.6.1.4.1.2620.1.6.7.8.2.1.3.1 operator Greater_Than threshold 19570 frequency 2 message "Fan 2 speed is high!" This indicates that Fan 2 is high speed.

Voltage Sensors

This is the voltage sensor value in volts. To get the thresholds of the sensors in your machine, enter in expert mode: `# dbget sysEnv:volt`

OID Name	OID Number	MIB File
voltageSensorValue	.1.3.6.1.4.1.2620.1.6.7.8.3.1.3	chkpnt.mib

Clish examples:

- Add snmp custom-trap voltageSensorLow_Vbat oid .1.3.6.1.4.1.2620.1.6.7.8.3.1.3.1 operator Less_Than threshold 2.66 frequency 2 message "Vbat voltage is low!" This indicates the Vbat voltage sensor has low voltage.
- Add snmp custom-trap voltageSensorHigh_5VSB oid .1.3.6.1.4.1.2620.1.6.7.8.2.1.3.2 operator Greater_Than threshold 5.35 frequency 2 message "5VSB voltage is high!" This indicates the 5VSB voltage sensor has high voltage.

The snmpmonitor Daemon

`snmpmonitor` is the Check Point daemon that monitors SNMP OIDs for a single MIB value or a single column of MIB values in a table. It sends SNMP traps at regular intervals to a trap sink server for as long as the OID value is in breach of a configurable threshold. A clear trap is sent when the OID value is back within threshold boundaries.

The default `net-snmp` configuration file extracts the community and sink server (trap daemon) information using the `trap2sink` command. Special syntax is required when configuring the monitoring parameters.

The configuration file is located at:

- SecurePlatform: `/etc/snmp/snmpd.conf`
- Gaia: `/etc/snmp/snmpmonitor.conf`

Installing the snmpmonitor Daemon

The `snmpmonitor` daemon is installed automatically on SecurePlatform platforms. You must manually install it on Gaia.

To install the snmpmonitor daemon:

1. Go to sk92999 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk92999&js_peid=P-114a7bc3b09-10006&partition=General&product=Security, and download the daemon.
2. Install the `snmpmonitor` executable:
   a) Copy the GZ archive file to the Gaia appliance or server.
   b) Extract the GZ archive file, run:

```
> gunzip splat_snmp_monitor.gz
```

c) Copy the executable file to `/bin/snmpmonitor`

d) Log in to Expert mode and configure the applicable permissions:
```
# chmod a+x /bin/snmpmonitor
```

3. Run these commands in order:
```
# dbset process:snmpmonitor:path /bin
# dbset process:snmpmonitor:arg:1 /etc/snmp/snmpmonitor.conf
# dbset process:snmpmonitor:env:LD_LIBRARY_PATH
/lib\:/usr/lib\:/opt/<version>/lib
# dbset process:snmpmonitor:runlevel 4
# dbset process:snmpmonitor t
# dbset :save
```
Note: <version> = the Gaia version, for example `R77`.

4. Restart `snmpmonitor`, run:
```
# tellpm process:snmpmonitor
# tellpm process:snmpmonitor t
```
When you complete the installation process, you can start to create custom monitoring rules.

Working with Custom Monitoring Rules

For each OID that you monitor, define custom monitoring rules in the configuration file.

The configuration file is located at:

- `SecurePlatform: /etc/snmp/snmpd.conf`
- `Gaia: /etc/snmp/snmpmonitor.conf`

These parameters are required for each monitoring rule:

- The OID to monitor.
- A comparison operator: one of !=, <, >, ==.
- A threshold value: either an integer (not enclosed within double quotes "") or a string (enclosed within double quotes).
- A polling interval (in seconds).
- A message (For example, "HA sync link 1 down", "Internet VLAN down", "Low REAL memory").

General monitoring rule guidelines:

- You must enclose string values in double quotes.
- Single quotes can be used inside string values.
- Lines that start with the '`#`' character are ignored.
- All lines that do not start with snmp monitor daemon commands are ignored.

To configure SNMP Monitoring:

1. In Expert mode, create or open the configuration file with a text editor.
2. Add monitoring rules to the file as necessary.
   Make sure that you include at least one `trap2sink` command.
3. Save the file.
4. Run `snmp service enable`

cp_monitor

The `cp_monitor` command defines one monitoring rule.

```
# cp_monitor <OID> <Operator> <Threshold> <Frequency> <Message>
```

When the rule expression is true, SNMP sends a message at the specified frequency until the expression evaluates back to false. At that point one or more clear traps are sent to indicate that the OID value is now within acceptable boundaries.

cp_monitor Parameter	Description
`OID`	Use standard OID notation. OID types supported are: Integer, String.
`Operator`	For OIDs of type Integer: Use one of: !=,<,>,== For OIDs of type String: Use one of: !=, ==
`Threshold`	For OIDs of type Integer: an integer value For OIDs of type String: a string enclosed within double quotes ""
`Frequency`	The polling interval in seconds, expressed as a positive integer. The daemon polls each monitored OID at the specified interval.
`Message`	A text string that gives a description of the trap, which must be enclosed within double quotes.

Example:

```
# cp_monitor 1.3.6.1.4.1.2021.4.6.0 < 2000 5 "memAvailReal"
# cp_monitor 1.3.6.1.4.1.2620.1.5.6.0 != "active" 5 "Cluster State"
```

To make sure that the OID used in a `cp_monitor` command is correct, run `snmpget` to see if it returns a value. For example, if attempting to configure the above example `cp_monitor "memAvailReal"` line, then the run `snmpget` and make sure that it returns a value:

```
# "snmpget -v 2c -c public localhost 1.3.6.1.4.1.2021.4.6.0"
```

cp_cleartrap

The optional `cp_cleartrap` command defines the number of clear traps to send and the interval between each one. SNMP sends clear traps when the OID value in a rule returns to its defined threshold.

```
# cp_cleartrap <interval> <retries>
```

Default = three packets at 10 seconds intervals.

Parameter	Description
`Interval`	An integer indicating time between clear trap packets, in seconds.
`Retries`	An integer indicating number of clear trap packets to send.

trap2sink

The `trap2sink` command defines a host that receives traps.

```
# trap2sink <sink-server>[:<port>] <community>
```

You must put a `trap2sink` command in the `snmpd.conf` file. This is because the `snmpmonitor` daemon sends SNMP v2c traps. This command is part of the `net-snmp` syntax.

trap_2_sink Parameter	Description
`sink-server`	A sink server for which traps are sent.
`port`	An optional (UDP) port number on which the server listens. The default is port 162.
`community`	An SNMP community.

Example:

```
# trap2sink 192.0.2.10 public
# trap2sink 192.0.2.10:1610 MyCommunity
```

Sample Configuration File

```
trap2sink 10.10.10.10 public
trap2sink 10.10.10.120:166 communityone
cp_cleartrap 10 2
proc syslogd 11
disk /var 20%
cpmonitor 1.3.6.1.2.1.2.2.1.8.1 == 260 “link I down”
cp_monitor pcErrorFlag.1 != “0” 60 “process monitor”
cp_monitor dskErrorFlag.1 != 0 60 “disk monitor”
cp_monitor 1.3.6.1.4.1.2021.10.1.5.1 > 10060 “CPU load 1 mm”
cp_monitor 1.3.6.1.4.1.2021.10.1.5.2>90 60 “CPU load 5 mm”
cp_monitor 1.3.6.1.4.1.2021.4.4.0 < 2000 60 “memAvailSwap”
cp_monitor 1.3.6.1.4.1.2021.4.6.0 < 2000 60 “memAvailReal”
cp_monitor 1.3.6.1.4.1.2620.1.5.6.0 != “active” 20 “Cluster State”
cp_monitor 1.3.6.1.4.1.2620.1.1.25.3.0 > 50000 20 “Firewall Connections”
cp_monitor 1.3.6.1.2.1.25.2.3.1.6.6>6000060 “/opt hrStorageUsed”
```

Monitoring and Debugging

In This Section:

Interpreting Error Messages

This section lists and explains certain common error status values that can appear in SNMP messages. Within the PDU, the third field can include an error-status integer that refers to a specific problem. The integer zero (0) means that no errors were detected. When the error field is anything other than 0, the next field includes an error-index value that identifies the variable, or object, in the variable-bindings list that caused the error.

The following table lists the error status codes and their meanings.

Error status code	Meaning	Error status code	Meaning
0	`noError`	10	`wrongValue`
1	`tooBig`	11	`noCreation`
2	`NoSuchName`	12	`inconsistentValue`
3	`BadValue`	13	`resourceUnavailable`
4	`ReadOnly`	14	`commitFailed`
5	`genError`	15	`undoFailed`
6	`noAccess`	16	`authorizationError`
7	`wrongType`	17	`notWritable`
8	`wrongLength`	18	`inconsistentName`
9	`wrongEncoding`		

Note - You might not see the codes. The SNMP manager or utility interprets the codes and displays and logs the appropriate message.

The subsequent, or fourth field, contains the error index when the error-status field is nonzero, that is, when the error-status field returns a value other than zero, which indicates that an error occurred. The error-index value identifies the variable, or object, in the variable-bindings list that caused the error. The first variable in the list has index 1, the second has index 2, and so on.

The next, or fifth field, is the variable-bindings field. It consists of a sequence of pairs; the first is the identifier. The second element is one of these options: `value`, `unSpecified`,

noSuchOjbect, noSuchInstance, or EndofMibView. The following table describes each element.

Variable-bindings element	Description
value	Value that is associated with each object instance; specified in a PDU request.
unSpecified	A NULL value is used in retrieval requests.
noSuchObject	Indicates that the agent does not implement the object referred to by this object identifier.
noSuchInstance	Indicates that this object does not exist for this operation.
endOfMIBView	Indicates an attempt to reference an object identifier that is beyond the end of the MIB at the agent.

GetRequest

The following table lists possible value field sets in the response PDU or error-status messages when performing a GetRequest.

Value Field Set	Description
noSuchObject	If a variable does not have an OBJECT IDENTIFIER prefix that exactly matches the prefix of any variable accessible by this request, its value field is set to noSuchObject.
noSuch Instance	If the variable's name does not exactly match the name of a variable, its value field is set to noSuchInstance.
genErr	If the processing of a variable fails for any other reason, the responding entity returns genErr and a value in the error-index field that is the index of the problem object in the variable-bindings field.
tooBig	If the size of the message that encapsulates the generated response PDU exceeds a local limitation or the maximum message size of the request's source party, then the response PDU is discarded and a new response PDU is constructed. The new response PDU has an error-status of tooBig, an error-index of zero, and an empty variable-bindings field.

GetNextRequest

The only values that can be returned as the second element in the variable-bindings field to a GetNextRequest when an error-status code occurs are unSpecified or endOfMibView.

GetBulkRequest

The `GetBulkRequest` minimizes the number of protocol exchanges and lets the SNMPv2 manager request that the response is large as possible.

The `GetBulkRequest` PDU has two fields that do not appear in the other PDUs: non-repeaters and max-repetitions. The non-repeaters field specifies the number of variables in the variable-bindings list for which a single-lexicographic successor is to be returned. The max-repetitions field specifies the number of lexicographic successors to be returned for the remaining variables in the variable-bindings list.

If at any point in the process, a lexicographic successor does not exist, the `endofMibView` value is returned with the name of the last lexicographic successor, or, if there were no successors, the name of the variable in the request.

If the processing of a variable name fails for any reason other than `endofMibView`, no values are returned. Instead, the responding entity returns a response PDU with an error-status of `genErr` and a value in the error-index field that is the index of the problem object in the variable-bindings field.

Working with SNMP Monitoring Thresholds

You can configure a variety of different SNMP thresholds that generate SNMP traps, or alerts. You can use these thresholds to monitor many system components automatically without requesting information from each object or device. The categories of thresholds that you can configure include:

- Hardware
- High Availability
- Networking
- Resources
- Domain Log Server Connectivity

Some categories apply only to some machines or deployments.

Note - SNMP monitoring thresholds are supported from R75.20, R71.30, and higher.

In each category there are many individual thresholds that you can set. For example, the hardware category includes alerts for the state of the RAID disk, the state of the temperature sensor, the state of the fan speed sensor, and others. For each individual threshold, you can configure:

- If it is enabled or disabled
- How frequently alerts are sent
- The severity of the alert
- The threshold point (if necessary)
- Where the alerts are sent to

You can also configure some settings globally, such as how often alerts are send and where they are sent to.

Types of Alerts

- *Active alerts* are sent when a threshold point is passed or the status of a monitored component is problematic.
- *Clear alerts* are sent when the problem is resolved and the component has returned to its normal value. Clear alerts look like active alerts but the severity is set to 0.

Configuring SNMP Monitoring

Configure the SNMP monitoring thresholds in the command line of the Security Management Server. When you install the policy on the gateways the SNMP monitoring thresholds are applied globally to all gateways.

Configuring in Multi-Domain Security Management

In a Multi-Domain Security Management environment, you can configure thresholds on the Multi-Domain Server and on each individual Domain Management Server. Thresholds that you configure on the Multi-Domain Server are for the Multi-Domain Server only. Thresholds that you configure for a Domain Management Server are for that Domain Management Server and its gateways. If a threshold applies to the Multi-Domain Server and the Domain Management Server gateways, set it on the Multi-Domain Server and Domain Management Server. But in this situation you can only get alerts from the Multi-Domain Server if the threshold passed.

For example, because the Multi-Domain Server and Domain Management Server are on the same machine, if the CPU threshold is passed, it applies to both of them. But only the Multi-Domain Server generates alerts.

You can see the Multi-Domain Security Management level for each threshold with the `threshold_config` utility.

- If the Multi-Domain Security Management level for a threshold is Multi-Domain Server: Alerts are generated for the Multi-Domain Server when the threshold point is passed.
- If the Multi-Domain Security Management level for a threshold is Multi-Domain Server and Domain Management Server: Alerts are generated for the Multi-Domain Server and Domain Management Servers separately when the threshold point is passed.

Configuring a Local Gateway Policy

You can configure SNMP thresholds locally on a gateway with the same procedure that you do on a Security Management Server. But each time you install a policy on the gateway, the local settings are erased and it reverts to the global SNMP threshold settings.

You can use the `threshold_config` utility to save the configuration file and load it again later.

On SecurePlatform and Linux, the configuration file that you can back up is: `$FWDIR/conf/thresholds.conf`

On Windows, the configuration file that you can back up is: `%FWDIR%\conf\thresholds.conf`

Configuration Procedures

There is one primary command to configure the thresholds in the command line, `threshold_config`. You must be in the Expert mode to run it. After you run `threshold_config`, follow the on-screen instructions to make selections and configure the global settings and each threshold.

When you run `threshold_config`, you get these options:

- Show policy name - Shows you the name configured for the threshold policy.
- Set policy name - Lets you set a name for the threshold policy.
- Save policy- Lets you save the policy.
- Save policy to file - Lets you export the policy to a file.
- Load policy from file - Lets you import a threshold policy from a file.
- Configure global alert settings - Lets you configure global settings for how frequently alerts are sent and how many alerts are sent.
- Configure alert destinations - Lets you configure a location or locations where the SNMP alerts are sent.
- View thresholds overview - Shows a list of all thresholds that you can set including: the category of the threshold, if it is active or disabled, the threshold point (if relevant), and a short description of what it monitors.
- Configure thresholds - Opens the list of threshold categories to let you select thresholds to configure.

Configure Global Alert Settings

If you select Configure global alert settings, you can configure global settings for how frequently alerts are sent and how many alerts are sent. You can configure these settings for each threshold. If a threshold does not have its own alert settings, it uses the global settings by default.

You can configure these options:

- Enter Alert Repetitions - How many alerts are sent when an active alert is triggered. If you enter 0, alerts are sent until the problem is fixed.
- Enter Alert Repetitions Delay - How long the system waits between it sends active alerts.
- Enter Clear Alert Repetitions - How many clear alerts are sent after a threshold returns to a regular value.
- Enter Clear Alert Repetitions Delay - How long the system waits between it sends clear alerts.

Configure Alert Destinations

If you select Configure Alert Destinations, you can add and remove destinations for where the alerts are sent. You can see a list of the configured destinations. A destination is usually an NMS (Network Management System) or a Check Point Domain Log Server.

After you enter the details for a destination, the CLI asks if the destination applies to all thresholds.

- If you enter yes, alerts for all thresholds are sent to that destination, unless you remove the destination from an individual threshold.
- If you enter no, no alerts are sent to that destination by default. But for each individual threshold, you can configure the destinations and you can add destinations that were not applied to all thresholds.

For each threshold, you can choose to which of the alert destinations its alerts are sent. If you do not define alert destination settings for a threshold, it sends alerts to all of the destinations that you applied to all thresholds.

For each alert destination enter:

- Name - An identifying name.
- IP - The IP address of the destination.
- Port - Through which port it is accessed
- Ver - The version on SNMP that it uses
- Other data- Some versions of SNMP require more data. Enter the data that is supplied for that SNMP version.

Configure Thresholds

If you select Configure thresholds, you see a list of the categories of thresholds, including:

- Hardware
- High Availability
- Networking
- Resources
- Domain Log Server Connectivity

Some categories apply only to some machines or deployments. For example, Hardware applies only to Check Point appliances and High Availability applies only to clusters or High Availability deployments.

Select a category to see the thresholds in it. Each threshold can have these options:

- Enable/Disable Threshold - If the threshold is enabled, the system sends alerts when there is a problem. If it is disabled it does not generate alerts.
- Set Severity - You can give each threshold a severity setting. The options are: Low, Medium, High, and Critical. The severity level shows in the alerts and in SmartView Monitor. It lets you know quickly how important the alert is.
- Set Repetitions - Set how frequently and how many alerts will be sent when the threshold is passed. If you do not configure this, it uses the global alert settings.
- Set Threshold Point - Enter the value that will cause active alerts when it is passed. Enter the number only, without a unit of measurement.
- Configure Alert Destinations - See all of the configured alert destinations. By default, active alerts and clear alerts are sent to the destinations. You can change this for each destination. When you select the destination you see these options:
  - Remove from destinations - If you select this, alerts for this threshold are not sent to the selected destination.
  - Add a destination - If you configured a destination in the global alert destinations but did not apply it to all thresholds, you can add it to the threshold.
  - Disable clear alerts - Cleared alerts for this threshold are not sent to the selected destination. Active alerts are sent.

Completing the Configuration

You can complete threshold configuration and activate the settings.

To complete configuration and activate the settings:

1. On the Security Management Server, install the policy on all Security Gateways.
2. For a local Security Gateway threshold policy or a Multi-Domain Security Management Multi-Domain Server environment, use the `cpwd_admin` utility to restart the CPD process:
   a) Run: `cpwd_admin stop -name CPD -path "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"`
   b) Run: `cpwd_admin start -name CPD -path "$CPDIR/bin/cpd" -command "cpd"`

Monitoring SNMP Thresholds

You can see an overview of the SNMP thresholds that you configure in SmartView Monitor.

To see an overview of the SNMP thresholds:

1. Open SmartView Monitor and select a Security Gateway.
2. In the summary of the Security Gateway data that open in the bottom pane, click System Information.
3. In the new pane that opens, click Thresholds.
   In the pane that opens, you can see these details:
   - General Info - A summary of the total SNMP Threshold policy.
     - Policy name- The name that you set for the policy in the CLI.
     - State - If the policy is enabled or disabled.
     - Thresholds - How many thresholds are enabled.
     - Active events - How many thresholds are currently sending alerts.
     - Generated Events - How many not active thresholds became active since the policy was installed.
   - Active Events- Details for the thresholds that are currently sending alerts.
     - Name - The name of the alert (given in the CLI).
     - Category - The category of the alert (given in the CLI), for example, Hardware or Resources.
     - MIB object - The name of the object as recorded in the MIB file.
     - MIB object value - The value of the object when the threshold became active, as recorded in the MIB file.
     - State - The status of the object: active or clearing (passed the threshold but returns to usual value).
     - Severity - The severity of that threshold, as you configured for it in the CLI.
     - Activation time - When was the alert first sent.

- Alert Destinations - A list of the destinations that alerts are sent to.
  - Name - The name of the location.
  - Type - The type of location. For example, a Domain Log Server or NMS.
  - State - If logs are sent from the gateway or Security Management Server to the destination machine.
  - Alert Count - How many alerts were sent to the destination from when the policy started.
- Errors - Shows thresholds that cannot be monitored. For example, the Security Gateway cannot monitor RAID sensors on a machine that does not have RAID sensors. Therefore it shows an error for the RAID Sensor Threshold.
  - Threshold Name - The name of the threshold with an error.
  - Error - A description of the error.
  - Time of Error - When the error first occurred.

Using SNMP with Other Operating Systems

In This Appendix

Configuring SNMP - SecurePlatform and Linux

Implementing SNMP for SecurePlatform

This is a high-level workflow to enable and configure SNMP for SecurePlatform with CLI commands. Run the SNMP commands from Expert mode.

1. Edit `/etc/snmp/snmpd.conf` to configure the SNMP settings ("Configuring snmpd.conf" on page 43).
2. Configure the SNMP traps.
3. Enable the SNMP service.
   ```
   # snmp service enable
   ```
4. Add a rule to the Rule Base to allow SNMP traffic.
5. Install the policy on the applicable Security Gateways and servers.

Configuring snmpd.conf

Edit `/etc/snmp/snmpd.conf` on the Security Management Server to configure the SNMP settings. These lines must be in the file, do not remove them:

```
master agentx
sysServices 76
smuxpeer 1.3.6.1.4.1.4.3.1.4
```

System Information

These settings contain data about the Security Management Server:

```
sysLocation <string>
sysContact <string>
sysName <string>
sysDescr <string>
sysObjectID <OID>
```

Community Strings (SNMPv1 and SNMPv2)

These strings are passwords that are used to query the SNMP agent.

- For read-only access (`GET` and `GETNEXT`):
  `rocommunity COMMUNITY_NAME [SOURCE [OID]]`
- For read-write access (`GET`, `GETNEXT` and `SET`):
  `rwcommunity COMMUNITY_NAME [SOURCE [OID]]`

Notes:

- The SOURCE token can be used to restrict access to requests from the specified system.
  A restricted source can either be a specific hostname (or specific IP address), or a subnet - represented as either `IP_Address/Subnet_Mask` (for example, 10.10.10.0/255.255.255.0), or represented as `IP_Address/Subnet_Mask_Length` (for example, 10.10.10.0/24).
  If you need to limit the access from specific sources, then along with restricted sources, it is important to include the IP address of the loopback interface 127.0.0.1. Otherwise you cannot query the system locally:
  `[ro/rw]community <COMMUNITY_NAME> 127.0.0.1`
- The OID field restricts access for that community to the subtree rooted at the given OID.

SNMP Trap Settings

Use `cp_monitor` (on page 33) and `trap2sink` (on page 34) to configure SNMP traps for SecurePlatform.

Configuring SNMP Users

`/etc/snmp/snmpd.users.conf` contains the user definitions for SNMPD daemon.

Note - In some SNMP versions, traps are sent only if the `public` community is defined in this file.

To configure SNMP users:

1. Log in to Expert mode.
2. Stop the SNMPD service:
   `# service snmpd stop`
3. Back up the `/etc/snmp/snmp.users.conf` file:
   `# cp /etc/snmp/snmp.users.conf /etc/snmp/snmp.users.conf_ORIGINAL`
4. Add the applicable communities to `/etc/snmp/snmp.users.conf`:

   

   Note - The community should be at least Read-Only (`rocommunity`).

   ```
   # vi /etc/snmp/snmp.users.conf
   rocommunity <my_community_name>
   ```
5. Add the applicable users to `/etc/snmp/snmp.users.conf`
6. Start the SNMPD service:
   `# service snmpd start`
7. Make sure that the SNMPD daemon started:
   `# ps auxw | grep -v grep | grep snmpd`

Configuring SNMP with SecurePlatform Commands

You can configure these basic SNMP features with the SecurePlatform command line:

- Enable and disable the SNMP agent daemon
- Add and delete USM users

All other configurations require you to manually change or add parameters in the configuration file.

- Defining SNMP communities (v1 and v2c)
- Defining SNMP traps

For a detailed, technical reference for the configuration file, see the description on `snmpd.conf` http://linux.die.net/man/5/snmpd.conf

Enabling and Disabling SNMP

To enable SNMP:

1. From the SecurePlatform command line, run
   > `cpconfig`
2. Select SNMP Extension.
3. When prompted, enter `y`.
4. Log in to Expert mode.
5. Run:
   ```
   # snmp service enable
   ```

To disable SNMP:

1. From the SecurePlatform command line, run
   > `cpconfig`
2. Select SNMP Extension.
3. When prompted, enter `n`.
4. Log in to Expert mode.
5. Run:
   ```
   # snmp service disable
   ```

SNMP Agent Commands

snmp service

Description

Enable, disable and show the current status of the SNMP agent daemon.

Syntax

```
snmp service {enable <port>|disable|stat} [snmp user]
```

Parameters

Parameter	Description
`enable <port>`	Starts SNMP agent daemon listening on the specified UDP port.
`disable`	Stops the SNMP agent daemon.
`stat`	Shows the status of the SNMP agent daemon.
`snmp user`	Add an SNMP v3 user to the agent. Authentication and encryption passwords can be specified for the user. Additionally, the user access can be restricted to the specified OID sub-tree.

snmp user

Description

Add, delete and show details of SNMP users. Authentication and encryption passwords can be required for users. Additionally, user access can be restricted to a specified OID sub-tree.

Syntax

```
snmp user add authuser <username> pass <auth_pw> [priv <encrypt_pw>] [oidbase <OID>]
snmp user del <username>
snmp user show [<username>]
```

Parameters

Parameter	Description
`add authuser`	Add an SNMP v3 user to the agent with a required authentication and optionally required encryption password.
`add noauthuser`	Add an SNMP user with no required authentication or encryption password.
`pass <auth_pw>`	Requires the specified authentication password.
`priv <encrypt_pw>`	Requires the specified encryption password.
`oidbase <OID>`	Restricts user access to the specified OID sub-tree.
`del <username>`	Delete the specified user. You can also delete SNMP v1 and v2 users with this command.
`snmp user show [<username>]`	Show details of the specified user, including: access level information and OID sub-tree restrictions. If no user is specified, the command shows all defined users.

Configuring SNMP - IPSO

Configuring SNMP with Voyager

Enabling SNMP

The SNMP daemon is enabled by default. If you choose to use SNMP, configure it according to your security requirements. At minimum, you must change the default community string to something other than public. It is also advised to select SNMPv3, rather than the default v1/v2/v3, if your management station supports it.

Note - If you do not plan to use SNMP to manage the network, disable it. Enabling SNMP opens potential attack vectors for surveillance activity by letting an attacker learn about the configuration of the device and the network.

To enable SNMP:

1. In the tree view, click Configuration > System Management > SNMP.
2. Select Enable SNMP Agent.
3. In SNMP Version, select the version of SNMP to run:
   - v1/v2/v3
   - v3

     Select this option if your management server supports v3. SNMPv3 provides a higher level of security than v1 or v2.
4. Optional: In SNMP Location String, enter a string that contains the location for the system. The maximum length for the string is 128 characters. That includes letters, numbers, spaces, special characters. For example: `Bldg 1, Floor 3, WAN Lab, Fast Networks, Speedy, CA`
5. Optional: In SNMP Contact String, enter a string that contains the contact information for the device. The maximum length for the string is 128 characters. That includes letters, numbers, spaces, special characters. For example: `John Doe, Network Administrator, (111) 222-3333`
6. Click Apply.

Configuring SNMP Agent Addresses

An agent address is a specific IP address at which the SNMP agent listens and responds to requests. The default behavior is for the SNMP agent to listen to and respond to requests on all interfaces. If you specify one or more agent addresses, the system SNMP agent listens and responds only on those interfaces.

You can use the agent address as another way to limit SNMP access. For example, you can limit SNMP access to one secure internal network that uses a particular interface by configuring that interface as the only agent address.

To set an SNMP agent address:

1. In the tree view, click System Management > SNMP.

   The SNMP Addresses table shows the valid interfaces and their IP addresses.
2. Select the header row checkbox to select all or select individual interfaces.

Note - If no agent addresses are specified, SNMP responds to requests from all interfaces.

Version Settings

Defining Community Settings

This section is applicable to SNMP v1 and v2 only.

1. Change the default the default Read-Only community (public). We strongly recommend that you implement this basic security precaution.

Note - If you select the Disable option, all community strings are disabled and SNMP v1 and v2 do not function. This has the same effect as selecting only SNMP v3 in the previous step.

2. Optional: Set a Read-Write Community String.

Warning - Set a read-write community string only if you have reason to enable set operations, only if you enabled SNMPv3 (not v1/v2/v3), and if your network is secure.

V3 - User-Based Security Model (USM)

IPSO supports the user-based security model (USM) component of SNMPv3 to provide message-level security. With USM (described in RFC 3414), access to the SNMP service is controlled on the basis of user identities. Each user has a name, an authentication pass phrase (used for identifying the user), and an optional privacy pass phrase (used to protect against disclosure of SNMP message payloads).

The system uses the MD5 hashing algorithm to provide authentication and integrity protection and DES to provide encryption (privacy). It is recommended that you use both authentication and encryption, but you can employ them independently by specifying one or the other with your SNMP manager requests. The Gaia system responds accordingly.

Note - Check Point systems do not protect traps with authentication or encryption.

SNMP users are maintained separately from system users. You can create SNMP user accounts with the same names as existing user accounts or different. You can create SNMP user accounts that have no corresponding system account. When you delete a system user account, you must separately delete the SNMP user account.

To add a USM user:

1. In the tree view, click Configuration> System Configuration > SNMP.
2. Click Manage SNMPv3 USM Users.
3. In User Name, enter the name.

   The range is 1 to 31 alphanumeric characters with no spaces, backslash, or colon characters. This can be the same as a user name for system access, though the SNMP user account is handled as a separate entity.

4. In Security Level, select one of these options:
   - Authentication & Privacy - The user has authentication and privacy pass phrases and can connect with or without privacy encryption.
   - Authentication, no Privacy - The user has only an authentication pass phrase and can connect only without privacy encryption.
   - Authentication & Privacy Required - The user has authentication and privacy pass phrases and must connect with privacy encryption.
5. In Authentication Pass Phrase, enter a password for the user that is between 8 and 128 characters in length.
6. In Privacy Pass Phrase, enter a pass phrase that is between 8 and 128 characters in length. Used to protect against disclosure of SNMP message payloads.
7. Click Save.

   The new user shows in the table.

To delete a USM user

1. In the tree view, click Configuration> System Configuration > SNMP.
2. In the Manage SNMPv3 USM Users section, find the user and click Delete.
3. Click Save.

To edit a USM user:

1. In the tree view, click Configuration> System Configuration > SNMP.
2. In the Manage SNMPv3 USM Users section, find the user and configure the settings.
3. Click Save.

Configuring Traps

To enable or disable trap types:

1. In the tree view, click Configuration> System Configuration > SNMP.
2. Below Enabled Traps, click Set.

   The Add New Trap Receiver window opens.
3. Select from the Disabled Traps list, and click Add> to set as Enabled Trap.
4. To disable, select from the Enabled Traps list, and click Remove> to Disable Trap.
5. Click Save.
6. In Trap User, select an SNMP user from the drop down list.
7. In Polling Frequency, enter or use the arrows to configure the setting.
8. Click Apply.

To configure trap receivers (management stations):

1. In the tree view, click Configuration> System Configuration > SNMP.
2. From the Add New Trap Receiver section, configure these settings:
   - In Receiver Address, enter the IPv4 address (or the hostname if DNS is set) of a receiver
   - In Community String for New Trap Receiver, enter the community string for the specified receiver
   - In Version, select the SNMP version for the trap receiver
3. Click Save.

To edit trap receivers:

1. In the tree view, click Configuration> System Configuration > SNMP.
2. Change the SNMP Version or the Community string.
3. Click Save.

To delete trap receivers:

1. In the tree view, click Configuration> System Configuration > SNMP.
2. Find the trap and click Delete.

   The Deleting Trap Receiver Entry window opens.

   The window shows this message: Are you sure you want to delete "IPv4 address" entry?
3. Click Yes.

Enabling or Disabling Trap Types

When you enable the specified trap type, the system sends a trap message when that type of event occurs. For example, if you enable authorization traps, the system sends a trap message to the management station when it receives a packet with an incorrect community string.

To enable or disable traps

1. From the navigation tree, click Configuration > System Configuration > SNMP.
2. To enable traps, select Enable next to the name of the trap and click Save.
3. To disable traps, clear Enable next to the name of the trap and click Save.

Setting the Trap PDU Agent Address

The trap PDU address is included in the protocol data unit (PDU) of each trap message sent to the management station that uses it to identify which network device generated the trap.

This address must belong to a configured interface.

If you do not configure an agent address for traps, the system identifies the trap agent address as 0.0.0.0 in SNMP traps (in accordance with RFC 2089).

To set the trap PDU agent address:

1. From the navigation tree, click Configuration> System Configuration.
2. To specify the IP address to be used for sent trap PDU, enter the IP address in the Trap PDU Agent Address field.
3. Click Apply.
4. Click Save to make your changes permanent.