HP TippingPoint

440T Threat Protection System MIBs Guide for IPS Mode

Version 4.0

5900-4109
Edition: June 2015

Legal and notice information

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

HP TippingPoint 440T Threat Protection System MIBs Guide for IPS Mode
Publication Part Number: 5900-4109

Contents

About this guide

The 440T Threat Protection System MIBs Guide for IPS Mode describes the management information base (MIB) database that enables you to manage devices in a communications network.

This section covers the following topics:

Target audience

The intended audience includes technicians and maintenance personnel responsible for installing, configuring, and maintaining HP TippingPoint security systems and associated devices.

Users should be familiar with the following concepts:

- Basic networking
- Simple Network Management Protocol (SNMP)
- Network security
- Routing

Related documentation

A complete set of product documentation for the 440T Threat Protection System (TPS) is available online. The product document set generally includes conceptual and deployment information, installation and user guides, CLI command references, safety and compliance information and release notes.

For information about how to access the online product documentation, refer to the *Read Me First* document in your product shipment.

Conventions

This information uses the following conventions.

Typefaces

HP TippingPoint publications use the following typographic conventions for structuring information:

Convention	Element
Bold font	• Key names • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes. Example: Click **OK** to accept.
Italics font	Text emphasis, important terms, variables, and publication titles
`Monospace font`	• File and directory names • System output • Code • Text typed at the command-line
Monospace, italic font	• Code variables • Command-line variables
Monospace, bold font	Emphasis of file and directory names, system output, code, and text typed at the command line

Messages

Messages are special text that is emphasized by font, format, and icons.

⚠ **Warning!** Alerts you to potential danger of bodily harm or other potential harmful consequences.

△ **Caution:** Provides information to help minimize risk, for example, when a failure to follow directions could result in damage to equipment or loss of data.

Note: Provides additional information to explain a concept or complete a task.

Important: Provides significant information or specific instructions.

Tip: Provides helpful hints and shortcuts, such as suggestions about how to perform a task more easily or more efficiently.

Support information

HP TippingPoint is committed to providing quality customer support for our products. If you need customer support for your product, contact the HP TippingPoint Technical Assistance Center (TAC) by using any of the following options.

Note: When you contact support, have the following information about your product available:

- Serial number and/or software version for your product
- System logs or event logs if available for your product

Online support

Go to the HP TippingPoint Threat Management Center (TMC) at:

http://tmc.tippingpoint.com

Phone support

North America: +1 866 681 8324

International: +1 512 681 8324

For a list of international toll-free contact numbers, go to http://tmc.tippingpoint.com, click the **Support** tab, and then click **View All**.

HP website

For the name of the nearest HP authorized reseller, see the Contact HP Worldwide website:

http://www.hp.com/country/us/en/wwcontact.html

MIB files for the Threat Protection System

A management information base (MIB) is a type of database that enables you to manage devices in a communications network. Database entries are addressed through object identifiers (OIDs). MIB files are descriptions of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of the SNMP.

This information includes the following topics:

- Standard SNMP MIBs supported on page 4
- IPS-supported MIBs on page 7

Standard SNMP MIBs supported

This topic contains the following information:

- SNMPv2-MIB on page 4
- IF-MIB on page 5
- EtherLike-MIB on page 5
- IP-MIB on page 5
- SNMP-USER-BASED-SM-MIB on page 6
- SNMP-VIEW-BASED-ACM-MIB on page 6
- Reference sites for standard MIBs on page 7

SNMPv2-MIB

Defines common information typically provided by managed systems. The Threat Protection System (TPS) supports the following items.

Name	Type	Description
System	Group	A collection of objects common to all managed systems. This includes information such as model, contact and location, up time, services, and system ID.
SNMP	Group	A collection of objects providing information on SNMP protocol stats, such as the number of packets received and transmitted.
coldStart	Notification	Signifies that the TPS device is reinitializing itself, typically a reboot.

IF-MIB

Contains objects for managing and monitoring network interfaces. Only physical interfaces have stats in the following tables. Logical interfaces, such as VLAN and Bridge, are listed, but stats are always 0.

Name	Type	Description
ifTable	Table	List of information and stats for each interface of a system. The number of entries is given by the value of ifNumber.
ifXTable	Table	List of interface entries. The number of entries is given by the value of ifNumber. This table contains additional objects for the interface table.
linkUp	Notification	A linkUp notification signifies that a communication link has left the down state and is now in the up state.
linkDown	Notification	A linkDown notification signifies that a communication link has left the up state and is now in the down state.

EtherLike-MIB

Provides information representing attributes of an interface to an Ethernet-like communications medium.

Name	Type	Description
dot3StatsTable	Table	Contains statistics for a collection of ethernet-like interfaces attached to a particular system.
dot3HCStatsTable	Table	Contains 64-bit versions of error counters from the dot3StatsTable.

IP-MIB

Name	Type	Description
IP	Group	A collection of object stats that include such information as IP datagrams received or transmitted.
ipv4InterfaceTable	Table	Contains per-interface IPv4-specific information.

Name	Type	Description
ipv6InterfaceTable	Table	Contains per-interface IPv6-specific information.
IpSystemStatsTable	Table	Contains system-wide, IP version-specific traffic statistics.
IpAddressTable	Table	Contains addressing information relevant to the entity's interfaces.
ipNetToPhysicalTable	Table	Contains the IP Address Translation table used for mapping from IP addresses to physical addresses.

SNMP-USER-BASED-SM-MIB

Defines the SNMPv3 user-based Security Model (USM). The Threat Protection System (TPS) supports the following groups.

Name	Type	Description
usmStats	Group	A collection of scalar objects that provide information such as, then number of unknown user names, engine IDs, or unsupported security levels.

SNMP-VIEW-BASED-ACM-MIB

This MIB defines the SNMPv3 View-based Access Control Model (VACM) for use in the Simple Network Management Protocol (SNMP) architecture. The Threat Protection System (TPS) support the following tables.

Name	Type	Description
vacmContextTable	Table	Locally available security contexts
vacmSecurityToGroupTable	Table	Maps a security contexts with groups
vacmAccessTable	Table	Access rights for groups
vacmViewTreeFamilyTable	Table	Locally held information about families of sub-trees within MIB views

Reference sites for standard MIBs

- IETF: http://www.ietf.org — where all the standard RFCs are kept for MIBs
- http://www.mibdepot.com — a well maintained site with standard and company specific MIBs

IPS-supported MIBs

The Threat Protection System (TPS) supports these MIBs fully except where noted. These are non-standard MIBs with TPT-specific definitions for TippingPoint products only.

TIPPINGPOINT-REG-MIB

Note: This MIB file must be loaded before you load any other TippingPoint MIB files.

Defines the object identifier (OID) sub-tree assigned to TippingPoint by the Internet Assigned Numbers Agency (IANA), as well as sub-trees for registered modules, object and event definitions, agent profiles, management application requirements, and experimental definitions.

The following table describes TIPPINGPOINT-REG-MIB sub-trees:

Object	OID	Description
tpt-reg	1.3.6.1.4.1.10734.1	Sub-tree for the registered modules
tpt-generic	1.3.6.1.4.1.10734.2	Sub-tree for common object and event definitions
tpt-products	1.3.6.1.4.1.10734.3	Sub-tree for specific object and event definitions
tpt-caps	1.3.6.1.4.1.10734.4	Sub-tree for agent profiles
tpt-reqs	1.3.6.1.4.1.10734.5	Sub-tree for management application requirements
tpt-expr	1.3.6.1.4.1.10734.6	Sub-tree for experimental definitions

TPT-COMPACT-FLASH

The Threat Protection System (TPS) provides no notification support for this MIB. Defines the status and operating mode of the external storage card.

The following table describes compact flash data objects:

Object	OID	Description
tpt-compact-flash	1.3.6.1.4.1.10734.3.3.2.14	Sub-tree for all external storage card information.
compactFlashPresent	1.3.6.1.4.1.10734.3.3.2.14.1	Indicates card presence. • 0: present • 1: absent
compactFlashMounted	1.3.6.1.4.1.10734.3.3.2.14.2	Indicates card mount status. • 0: mounted • 1: unmounted
compactFlashFormatted	1.3.6.1.4.1.10734.3.3.2.14.3	Indicates card format status. • 0: formatted • 1: unformatted
compactFlashOperationMode	1.3.6.1.4.1.10734.3.3.2.14.4	Indicates card operation mode. • 0: secure mode—requires authentication • 1: auto-mount enabled— cards are automatically mounted when inserted
vendorInformation	1.3.6.1.4.1.10734.3.3.2.14.5	Sub-tree of external storage card informational details.
serialNumber	1.3.6.1.4.1.10734.3.3.2.14.5.1	Card serial number.
model	1.3.6.1.4.1.10734.3.3.2.14.5.2	Card model name.
capacity	1.3.6.1.4.1.10734.3.3.2.14.5.3	Card capacity.
revision	1.3.6.1.4.1.10734.3.3.2.14.5.4	Card firmware revision.

TPT-HEALTH

Indicates the health status of the IPS. Features monitored temperatures, fan speeds, and voltage levels. The Threat Protection System (TPS) provide no health2CTable support.

Temperature

The Temperature objects monitor the device temperature. Alarms are generated when the temperature at a sensor passes a specified threshold.

The following table describes temperature objects:

Object	OID	Description
healthTempTable	1.3.6.1.4.1.10734.3.3.2.13.1	Lists the readings at the device temperature sensors
healthTempEntry	1.3.6.1.4.1.10734.3.3.2.13.1.1	Entry in the temperature table. Rows are predefined and cannot be created or deleted.
healthTempIndex	1.3.6.1.4.1.10734.3.3.2.13.1.1.1	Index number of the entry
healthTempChannel	1.3.6.1.4.1.10734.3.3.2.13.1.1.2	Location of the temperature sensor.
healthTempValue	1.3.6.1.4.1.10734.3.3.2.13.1.1.3	Temperature in degrees centigrade
healthTempSeverity	1.3.6.1.4.1.10734.3.3.2.13.1.1.4	Can be one of the following values: • 0: normal • 1: informational note • 2: minor • 3: major • 4: critical
healthTempThresholdType	1.3.6.1.4.1.10734.3.3.2.13.1.1.5	Determines the application of thresholds: • 1: minimum; value should not go below threshold • 2: range; value should remain with a designated range

Object	OID	Description
		- 3: maximum; value should not go above threshold
healthTempMajor	1.3.6.1.4.1.10734.3.3.2.13.1.1.6	Major threshold temperature in degrees centigrade
healthTempCritical	1.3.6.1.4.1.10734.3.3.2.13.1.1.7	Critical threshold temperature in degrees centigrade

Fans

The fan objects monitor the fan performance and health.

The following table describes fan objects:

Object	OID	Description
healthFanTable	1.3.6.1.4.1.10734.3.3.2.13.2	Lists all fans inside the device
healthFanEntry	1.3.6.1.4.1.10734.3.3.2.13.2.1	Entry in the fans table. Rows are predefined and cannot be created or deleted.
healthFanIndex	1.3.6.1.4.1.10734.3.3.2.13.2.1.1	Index number of the entry
healthFanChannel	1.3.6.1.4.1.10734.3.3.2.13.2.1.2	String identifying the fan
healthFanValue	1.3.6.1.4.1.10734.3.3.2.13.2.1.3	Speed of the fan in RPM
healthFanSeverity	1.3.6.1.4.1.10734.3.3.2.13.2.1.4	Can be one of the following values: - 0: normal - 1: informational note - 2: minor - 3: major - 4: critical
healthFanThresholdType	1.3.6.1.4.1.10734.3.3.2.13.2.1.5	Determines the application of thresholds:

Object	OID	Description
		- 1: minimum; value should not go below threshold - 2: range; value should remain with a designated range - 3: maximum; value should not go above threshold
healthFanMajor	1.3.6.1.4.1.10734.3.3.2.13.2.1.6	Major threshold speed in RPM
healthFanMinor	1.3.6.1.4.1.10734.3.3.2.13.2.1.7	Critical threshold speed in RPM

Voltage

The voltage objects monitor the voltage levels at various locations within the device.

The following table describes voltage objects:

Object	OID	Description
healthVoltageTable	1.3.6.1.4.1.10734.3.3.2.13.3	List of all voltages at various locations inside the device
healthVoltageEntry	1.3.6.1.4.1.10734.3.3.2.13.3.1	An entry in the voltage table. Rows are predefined and cannot be created or deleted.
healthVoltageIndex	1.3.6.1.4.1.10734.3.3.2.13.3.1.1	Index number of the entry
healthVoltageChannel	1.3.6.1.4.1.10734.3.3.2.13.3.1.2	Location of the voltage sensor
healthVoltageValue	1.3.6.1.4.1.10734.3.3.2.13.3.1.3	Voltage reading in millivolts
healthVoltageSeverity	1.3.6.1.4.1.10734.3.3.2.13.3.1.4	Can be one of the following values: - 0: normal - 1: informational note - 2: minor - 3: major

Object	OID	Description
		- 4: critical
healthVoltageThresholdType	1.3.6.1.4.1.10734.3.3.2.13.3.1.5	Determines the application of thresholds: - 1: minimum; value should not go below threshold - 2: range; value should remain with a designated range - 3: maximum; value should not go above threshold
healthVoltageMajor	1.3.6.1.4.1.10734.3.3.2.13.3.1.6	Major threshold delta above or below the nominal voltage value, in millivolts
healthVoltageMinor	1.3.6.1.4.1.10734.3.3.2.13.3.1.7	Critical threshold delta above or below the nominal voltage value, in millivolts
healthVoltageNominal	1.3.6.1.4.1.10734.3.3.2.13.3.1.8	Optimal voltage value at this sensor location

TPT-MISC-NOTIFY

Notifications for logs and other features.

Note: The MIB file includes references to Network Discovery Scan.

This object applies to all notifications.

Common TPT notification objects

The following table describes general notification objects:

Object	OID	Description
tptMiscNotifyDeviceID	1.3.6.1.4.1.10734.3.3.3.1.31	The unique identifier of the device sending the notification. This is the first payload parameter for all notifications in the TPT-MISC-NOTIFY module.

Management TPT notification objects

The following table describes management notification objects. These notifications communicate with the management station:

Object	OID	Description
tptManagedNotify	1.3.6.1.4.1.10734.3.3.3.0.9	Informs the management station that the device is now being managed by that station
tptUnmanagedNotify	1.3.6.1.4.1.10734.3.3.3.0.10	Informs the management station that the device is no longer being managed by that station

Quarantine TPT notification objects

The following notifications are generated by quarantine actions:

Object	OID	Description
tptQuarantineNotify	1.3.6.1.4.1.10734.3.3.3.0.20	The notification that indicates that a host has been added to or removed from the quarantine list.
tptQuarantineNotifyNetAddr	1.3.6.1.4.1.10734.3.3.3.1.132	The network address of the host being quarantined or removed from the quarantine list.
tptQuarantineNotifyHostNetAddrV6	1.3.6.1.4.1.10734.3.3.3.1.133	The IPv6 network address of the host.
tptQuarantineNotifyReason	1.3.6.1.4.1.10734.3.3.3.1.134	The reason that the host was quarantined. The parameter is undefined if the host was removed.
tptQuarantineNotifySegmentName	1.3.6.1.4.1.10734.3.3.3.1.135	The segment related to the quarantine or removal from the quarantine list.
tptQuarantineNotifyAction	1.3.6.1.4.1.10734.3.3.3.1.136	Whether the host was added to or removed from the quarantine list. • 1: add • 2: remove

System Log TPT notification objects

The following notifications are generated when a critical message, error message, or warning is logged in the system log:

Object	OID	Description
tptSystemLogNotify	1.3.6.1.4.1.10734.3.3.3.0.16	The notification that a critical message, error message, or warning has been logged.
tptSystemLogNotifyText	1.3.6.1.4.1.10734.3.3.3.1.92	The text of the message being logged.
tptSystemLogNotifySequence	1.3.6.1.4.1.10734.3.3.3.1.93	The log file entry sequence number corresponding to this notification. This value will always be 0 (zero).
tptSystemLogNotifySeverity	1.3.6.1.4.1.10734.3.3.3.1.94	The severity of the attack: • 1: critical • 2: error • 4: warning
tptSystemLogNotifyTimeSec	1.3.6.1.4.1.10734.3.3.3.1.95	The time that this message was logged, in seconds since January 1, 1970.
tptSystemLogNotifyTimeNano	1.3.6.1.4.1.10734.3.3.3.1.96	The nanoseconds portion of tptSystemLogNotifyTimeSec.

Audit Log TPT notification objects

The following notifications are generated when a message or warning is logged in the audit log:

Object	OID	Description
tptAuditLogNotify	1.3.6.1.4.1.10734.3.3.3.0.60	Audit log notification uses the following fields: • tptMiscNotifyDeviceID • tptAuditLogNotifyTime • tptAuditLogNotifyAccess • tptAuditLogNotifyType • tptAuditLogNotifyIpAddrType • tptAuditLogNotifyIpAddr

Object	OID	Description
		• tptAuditLogNotifyCategory • tptAuditLogNotifyResult • tptAuditLogNotifyUser • tptAuditLogNotifyMessage
tptAuditLogNotifyTime	1.3.6.1.4.1.10734.3.3.3.1.170	The date and time when the entry was logged.
tptAuditLogNotifyAccess	1.3.6.1.4.1.10734.3.3.3.1.171	The access level of the user initiating the audit check and generating the log. This is a bit field with the following mapping: • 0x0 – normal • 0x1 – operator • 0x4 – administrator • 0x8 – super-user
tptAuditLogNotifyType	1.3.6.1.4.1.10734.3.3.3.1.172	Interface source of the audit log action.
tptAuditLogNotifyIpAddrType	1.3.6.1.4.1.10734.3.3.3.1.173	Type of IP address from which the user connected.
tptAuditLogNotifyIpAddr	1.3.6.1.4.1.10734.3.3.3.1.174	IP address from which the user connected
tptAuditLogNotifyCategory	1.3.6.1.4.1.10734.3.3.3.1.175	Functional area where the audit log was generated: 1: undefined 2: general 3: login 4: logout 5: user 6: time 7: policy 8: update 9: boot 10: report 11: host 12: cfg

Object	OID	Description
		13: device 14: sms 15: server 16: segment 17: license 18: ha 19: monitor 20: ipFilter 21: connTable 22: hostComm 23: tse 24: cf
tptAuditLogNotifyResult	1.3.6.1.4.1.10734.3.3.3.1.176	The result, pass or fail, of an audit check: 1: success 2: failed
tptAuditLogNotifyUser	1.3.6.1.4.1.10734.3.3.3.1.177	The user initiating the audit check and generating the log.
tptAuditLogNotifyMessage	1.3.6.1.4.1.10734.3.3.3.1.178	A description of what configuration change was attempted (and possibly succeeded) by the user.

TPT-POLICY

The following notifications are generated by policy actions:

Object	OID	Description
tptPolicyNotify	1.3.6.1.4.1.10734.3.3.3.0.8	The notification that a policy action has resulted from a signature match.
tptPolicyNotifyClientip	1.3.6.1.4.1.10734.3.3.3.1.139	The client IP address associated with the notification. This value is always set to "".

Object	OID	Description
tptPolicyNotifyDeviceID	1.3.6.1.4.1.10734.3.3.3.1.11	The unique identifier of the device sending the policy notification.
tptPolicyNotifyMetadata	1.3.6.1.4.1.10734.3.3.3.1.140	Additional event information associated with the notification. Because this object is targeted for future support, this value is always set to `N/A`.
tptPolicyNotifyPolicyID	1.3.6.1.4.1.10734.3.3.3.1.12	The unique identifier of the policy that causes the notification.
tptPolicyNotifySignatureID	1.3.6.1.4.1.10734.3.3.3.1.13	The unique identifier of the signature matching the incoming data stream.
tptPolicyNotifySegmentName (obsolete)	1.3.6.1.4.1.10734.3.3.3.1.14	The name of the segment to which the notification applies. Not included in notification.
tptPolicyNotifySrcNetAddr	1.3.6.1.4.1.10734.3.3.3.1.15	The IPv4 address of the source of the packet that triggered the policy action.
tptPolicyNotifySrcNetAddrV6	1.3.6.1.4.1.10734.3.3.3.1.128	The IPv6 address of the source of the packet that triggered the policy action.
tptPolicyNotifySrcNetPort	1.3.6.1.4.1.10734.3.3.3.1.16	The source port of the packet that triggered the policy action.
tptPolicyNotifyDestNetAddr	1.3.6.1.4.1.10734.3.3.3.1.17	The IPv4 address of the destination of the packet that triggered the policy action.
tptPolicyNotifyDestNetAddrV6	1.3.6.1.4.1.10734.3.3.3.1.129	The IPv6 address of the destination of the packet that triggered the policy action.
tptPolicyNotifyDestNetPort	1.3.6.1.4.1.10734.3.3.3.1.18	The destination port of the packet that triggered the policy action.

Object	OID	Description
tptPolicyNotifyStartTimeSec	1.3.6.1.4.1.10734.3.3.3.1.19	The time at which the policy was first triggered, marking the start of the aggregation period for this notification. Measured in seconds since January 1, 1970.
tptPolicyNotifyAlertAction	1.3.6.1.4.1.10734.3.3.3.1.20	The action associated with this notification. • 1: deny • 2: allow
tptPolicyNotifyConfigAction	1.3.6.1.4.1.10734.3.3.3.1.21	The action configured for the policy, which in some cases can differ from the action associated with the notification. • 1: deny • 2: allow
tptPolicyNotifyComponentID	1.3.6.1.4.1.10734.3.3.3.1.22	The component identifier of the policy that causes the notification: • 0: invalid • 1: deny • 2: allow • 7: alert • 8: block • 9: peer
tptPolicyNotifyHitCount	1.3.6.1.4.1.10734.3.3.3.1.23	The number of policy hits occurring during the aggregation period for this notification.
tptPolicyNotifyAggregationPeriod	1.3.6.1.4.1.10734.3.3.3.1.24	The duration of the aggregation period for this notification, in minutes.
tptPolicyNotifySeverity	1.3.6.1.4.1.10734.3.3.3.1.25	The severity of the attack. • 1: warning • 2: minor

Object	OID	Description
		• 3: major • 4: critical
tptPolicyNotifyProtocol	1.3.6.1.4.1.10734.3.3.3.1.26	The network protocol of the packet(s) that triggered the policy action. • 1: ICMP • 2: UDP • 3: TCP • 4: other IP • 5: ARP • 6: other ETH • 7: ICMP v6 • 8: other IPV6
tptPolicyNotifyAlertTimeSec	1.3.6.1.4.1.10734.3.3.3.1.27	The time that the alert was initiated, marking the end of the aggregation period for this notification. Measured in seconds since January 1, 1970.
tptPolicyNotifyAlertTimeNano	1.3.6.1.4.1.10734.3.3.3.1.28	The nanoseconds portion of the AlertTimeSec object.
tptPolicyNotifyPacketTrace	1.3.6.1.4.1.10734.3.3.3.1.29	Indicates if a corresponding packet trace was logged. • 0: not logged • 1: logged.
tptPolicyNotifySequence	1.3.6.1.4.1.10734.3.3.3.1.30	The log file entry sequence number corresponding to this notification. This value is always set to `0` (zero).
tptPolicyNotifyTraceBucket	1.3.6.1.4.1.10734.3.3.3.1.36	The bucket identifier for a packet trace.
tptPolicyNotifyTraceBegin	1.3.6.1.4.1.10734.3.3.3.1.37	The starting sequence number for a packet trace.

Object	OID	Description
tptPolicyNotifyTraceEnd	1.3.6.1.4.1.10734.3.3.3.1.38	The ending sequence number for a packet trace.
tptPolicyNotifyMessageParams	1.3.6.1.4.1.10734.3.3.3.1.39	A string containing parameters separated by vertical bars (|) that match information tagged with Message in the DV.
tptPolicyNotifyStartTimeNano	1.3.6.1.4.1.10734.3.3.3.1.40	The nanoseconds portion of StartTimeSec.
tptPolicyNotifyAlertType	1.3.6.1.4.1.10734.3.3.3.1.41	A bit field defined as follows: • 0x0001 = Alert • 0x0002 = Block • 0x0020 = Peer-to-peer • 0x0040 = Invalid • 0x0080 = Threshold • 0x0100 = Management.
tptPolicyNotifyInputMphy	1.3.6.1.4.1.10734.3.3.3.1.57	The incoming physical port of the triggering packet(s).
tptPolicyNotifyVlanTag	1.3.6.1.4.1.10734.3.3.3.1.58	The VLAN tag of the triggering packet(s).
tptPolicyNotifyZonePair	1.3.6.1.4.1.10734.3.3.3.1.59	A string that identifies the port pair related to this notification. This value is always set to "".
tptPolicyNotifyActionSetID	1.3.6.1.4.1.10734.3.3.3.1.130	The action set UUID associated with this notification.
tptPolicyNotifyRate	1.3.6.1.4.1.10734.3.3.3.1.131	The rate-limit, in kbps, of the action set associated with this notification.
tptPolicyNotifyFlowControl	1.3.6.1.4.1.10734.3.3.3.1.137	The action set flow control associated with this notification.

Object	OID	Description
tptPolicyNotifyActionSetName	1.3.6.1.4.1.10734.3.3.3.1.138	The action set name associated with this notification.

TPT-RESOURCE

Describes memory, power supply, temperature, and voltage information for the device.

File system

The following objects provide information about the device file system objects:

Object	OID	Description
resourceNumberOfFilesystems	1.3.6.1.4.1.10734.3.3.2.5.1	Number of filesystems on the device’s hard disk
resourceFSTable	1.3.6.1.4.1.10734.3.3.2.5.2	Table of filesystem resource information
resourceFSEntry	1.3.6.1.4.1.10734.3.3.2.5.2.1	An entry in the resource filesystem table. Rows cannot be added or deleted.
resourceFSInUseMB	1.3.6.1.4.1.10734.3.3.2.5.2.1.1	Number of MB in use for the filesystem
resourceFSThresholdMaj	1.3.6.1.4.1.10734.3.3.2.5.2.1.2	Major threshold for the percent of MB in use for the filesystem
resourceFSThresholdCrit	1.3.6.1.4.1.10734.3.3.2.5.2.1.3	Critical threshold for the percent of MB in use for the filesystem
resourceFSRangeMin	1.3.6.1.4.1.10734.3.3.2.5.2.1.4	Minimum value of the range of MB in use, usually 0 (zero)
resourceFSRangeMax	1.3.6.1.4.1.10734.3.3.2.5.2.1.5	Total size in MB of the filesystem
resourceFSName	1.3.6.1.4.1.10734.3.3.2.5.2.1.6	Name of this filesystem
resourceFSIndex	1.3.6.1.4.1.10734.3.3.2.5.2.1.7	Number of the table row, starting at one (1)

Memory

The following table provides information about the device memory usage objects:

Object	OID	Description
resourceHPMemoryObjs	1.3.6.1.4.1.10734.3.3.2.5.3	Sub-tree of host processor memory information
resourceHPMemoryInUsePercent	1.3.6.1.4.1.10734.3.3.2.5.3.1	Percentage of host processor memory in use
resourceHPMemoryThresholdMaj	1.3.6.1.4.1.10734.3.3.2.5.3.2	Major threshold value for host processor memory usage
resourceHPMemoryThresholdCrit	1.3.6.1.4.1.10734.3.3.2.5.3.3	Critical threshold value for host processor memory usage
resourceHPMemoryRangeMin	1.3.6.1.4.1.10734.3.3.2.5.3.4	Minimum percentage of host processor memory usage, usually 0 (zero)
resourceHPMemoryRangeMax	1.3.6.1.4.1.10734.3.3.2.5.3.5	Maximum percentage of host processor memory usage, usually 100
resourceHPMemoryTotal	1.3.6.1.4.1.10734.3.3.2.5.3.6	Total size in bytes of host processor memory

CPU

The following table provides information about CPU usage objects:

Object	OID	Description
resourceHPCPUObjs	1.3.6.1.4.1.10734.3.3.2.5.4	Sub-tree of host processor CPU information
resourceHPCPUBusyPercent	1.3.6.1.4.1.10734.3.3.2.5.4.1	Percentage of host processor CPU that is currently busy
resourceHPCPUThresholdMaj	1.3.6.1.4.1.10734.3.3.2.5.4.2	Major threshold value for host processor CPU activity

Object	OID	Description
resourceHPCPUThresholdCrit	1.3.6.1.4.1.10734.3.3.2.5.4.3	Critical threshold value of host processor CPU activity
resourceHPCPURangeMin	1.3.6.1.4.1.10734.3.3.2.5.4.4	Minimum percentage of host processor CPU activity, usually 0 (zero)
resourceHPCPURangeMax	1.3.6.1.4.1.10734.3.3.2.5.4.5	Maximum percentage of host processor CPU activity, usually 100
resourceNPCPUBusyPercentA	1.3.6.1.4.1.10734.3.3.2.5.4.6	Total Utilization of XLR A
resourceNPCPUBusyPercentTier2A	1.3.6.1.4.1.10734.3.3.2.5.4.7	F Thread Utilization of XLR A
resourceNPCPUBusyPercentTier3A	1.3.6.1.4.1.10734.3.3.2.5.4.8	KS Thread Utilization of XLR A
resourceNPCPUBusyPercentTier4A	1.3.6.1.4.1.10734.3.3.2.5.4.9	L Thread Utilization of XLR A
resourceNPCPUBusyPercentB	1.3.6.1.4.1.10734.3.3.2.5.4.10	Total Utilization of XLR B
resourceNPCPUBusyPercentTier2B	1.3.6.1.4.1.10734.3.3.2.5.4.11	F Thread Utilization of XLR B
resourceNPCPUBusyPercentTier3B	1.3.6.1.4.1.10734.3.3.2.5.4.12	KS Thread Utilization of XLR B
resourceNPCPUBusyPercentTier4B	1.3.6.1.4.1.10734.3.3.2.5.4.13	L Thread Utilization of XLR B
resourceNPCPUBusyPercentC	1.3.6.1.4.1.10734.3.3.2.5.4.14	Total Utilization of XLR C
resourceNPCPUBusyPercent2C	1.3.6.1.4.1.10734.3.3.2.5.4.15	F Thread Utilization of XLR C
resourceNPCPUBusyPercent3C	1.3.6.1.4.1.10734.3.3.2.5.4.16	KS Thread Utilization of XLR C
resourceNPCPUBusyPercent4C	1.3.6.1.4.1.10734.3.3.2.5.4.17	L Thread Utilization of XLR C

Chassis temperature

The following table provide information about the chassis temperature objects:

Object	OID	Description
resourceChassisTempObjs	1.3.6.1.4.1.10734.3.3.2.5.5	Sub-tree of chassis temperature information
resourceChassisTempDegreesC	1.3.6.1.4.1.10734.3.3.2.5.5.1	Chassis temperature
resourceChassisTempThresholdMaj	1.3.6.1.4.1.10734.3.3.2.5.5.2	Major threshold value for chassis temperature
resourceChassisTempThresholdCrit	1.3.6.1.4.1.10734.3.3.2.5.5.3	Critical threshold value of chassis temperature
resourceChassisTempRangeMin	1.3.6.1.4.1.10734.3.3.2.5.5.4	Minimum value of the chassis temperature range
resourceChassisTempRangeMax	1.3.6.1.4.1.10734.3.3.2.5.5.5	Maximum value of the chassis temperature range

Important: All values are in degrees Centigrade.

Power supply

The following table provides information about the chassis temperature objects:

Object	OID	Description
resourcePowerSupplyObjs	1.3.6.1.4.1.10734.3.3.2.5.9	Sub-tree of power supply information
resourcePowerSupplyQuantity	1.3.6.1.4.1.10734.3.3.2.5.9.2	Number of power supplies
resourcePowerSupplyMonitoring	1.3.6.1.4.1.10734.3.3.2.5.9.3	Indicates if power supply monitoring is enabled: • 0: disabled • 1: enabled
resourcePowerSupplyTable	1.3.6.1.4.1.10734.3.3.2.5.9.4	Table of power supplies on the device. The number of entries depends on the value of the resourcePowerSupplyQuantity object. The maximum number of entries depends on the implementation.

Object	OID	Description
resourcePowerSupplyEntry	1.3.6.1.4.1.10734.3.3.2.5.9.4.1	An entry in the power supply table. Rows cannot be created or deleted.
powerSupplyUnitIndex	1.3.6.1.4.1.10734.3.3.2.5.9.4.1.1	Index of the power supply units on a device. The first entry is 1.
powerSupplyStatus	1.3.6.1.4.1.10734.3.3.2.5.9.4.1.2	If the device has dual power supplies and power supply monitoring is enabled, this value indicates whether one or both power supplies is functional: • 0: unknown; the device does not have dual power supplies, or power supply monitoring is disabled. • 1: red—critical • 2: yellow—warning • 3: green—normal

System information

The following table provides information about the system objects:

Object	OID	Description
resourceDateTime	1.3.6.1.4.1.10734.3.3.2.5.10	Current date and time of device in seconds since January 1, 1970. There is no time zone offset.
resourceSnmpRunState	1.3.6.1.4.1.10734.3.3.2.5.11	Indicates which SNMP versions are running: • 0: none • 1: SNMP v2 • 2: SNMP v3 • 3: Both v2 and v3
resourceSnmpConfig	1.3.6.1.4.1.10734.3.3.2.5.12	Indicates which SNMP versions are configured: • 0: none • 1: SNMP v2 • 2: SNMP v3

Object	OID	Description
		- 3: Both v2 and v3
resourceRemoteAuthEnabled	1.3.6.1.4.1.10734.3.3.2.5.13	Indicates whether remote authentication is enabled
resourceRemoteAuthTimeout	1.3.6.1.4.1.10734.3.3.2.5.14	The remote authentication timeout in seconds

TPT-TPA-HARDWARE

Describes the device hardware and its components, including ports, chassis, fans, and power supplies.

The following table describes the hardware objects:

Object	OID	Description
hw-numFans	1.3.6.1.4.1.10734.3.3.2.3.7	Number of fan subunits on the device
hw-numPowerSupplies	1.3.6.1.4.1.10734.3.3.2.3.8	Number of power supply subunits on the device
hw-numPEMs	1.3.6.1.4.1.10734.3.3.2.3.9	Number of power entry module subunits on the device
hw-certificateNumber	1.3.6.1.4.1.10734.3.3.2.3.10	Hardware certificate number of the device
hw-serialNumber	1.3.6.1.4.1.10734.3.3.2.3.11	Hardware serial number of the device

Fans

The following table provides information about the fan hardware objects:

Object	OID	Description
hw-fanTable	1.3.6.1.4.1.10734.3.3.2.3.3	Table of fan data for the device. Represented as a table with one row.
hw-fanEntry	1.3.6.1.4.1.10734.3.3.2.3.3.1	An entry in the fan table.

Object	OID	Description
fanSubunit	1.3.6.1.4.1.10734.3.3.2.3.3.1.1	The number for this entry in the fan table. The controller is always 0 (zero).
fanType	1.3.6.1.4.1.10734.3.3.2.3.3.1.3	Type of hardware element: • 0: unequipped • 19: fan controller • 20: fan subunit
fanCfgType	1.3.6.1.4.1.10734.3.3.2.3.3.1.4	Fan configuration: • 0: unconfigured • 1: simplex • 2: duplex • 3: load share • 4: autonomous
fanRunState	1.3.6.1.4.1.10734.3.3.2.3.3.1.5	High-level hardware state of the fan: • 0: out of service • 1: initializing • 2: active • 3: standby • 4: diagnostic • 5: loopback • 6: active-FAF • 7: standby-FAF • 8: active - degraded • 9: standby - degraded
fanQualifier1	1.3.6.1.4.1.10734.3.3.2.3.3.1.6	Further qualification/detail on the high-level hardware state: • 1: degraded • 13: yellow alarm • 14: red alarm

Object	OID	Description
fanQualifier2	1.3.6.1.4.1.10734.3.3.2.3.3.1.7	Further qualification/detail on the high-level hardware state: • 1: degraded • 13: yellow alarm • 14: red alarm
fanQualifier3	1.3.6.1.4.1.10734.3.3.2.3.3.1.8	Further qualification/detail on the high-level hardware state: • 1: degraded • 13: yellow alarm • 14: red alarm
fanQualifier4	1.3.6.1.4.1.10734.3.3.2.3.3.1.9	Further qualification/detail on the high-level hardware state: • 1: degraded • 13: yellow alarm • 14: red alarm
fanStartTime	1.3.6.1.4.1.10734.3.3.2.3.3.1.10	Time at which the fan was powered up
fanVendorID	1.3.6.1.4.1.10734.3.3.2.3.3.1.11	Identifying number of the fan vendor
fanDeviceID	1.3.6.1.4.1.10734.3.3.2.3.3.1.12	An identifying number specific to the fan
fanProductID	1.3.6.1.4.1.10734.3.3.2.3.3.1.13	Versions and other inventory information
fanFPGAVersion	1.3.6.1.4.1.10734.3.3.2.3.3.1.14	Version of the TippingPoint FPGA chip on the fan

For fan health, see Fans on page 10.

Power supply

The following table provides information about the power supply hardware objects:

Object	OID	Description
hw-psTable	1.3.6.1.4.1.10734.3.3.2.3.4	Table of power supply data for the device. Represented as a table with one row.
hw-psEntry	1.3.6.1.4.1.10734.3.3.2.3.4.1	Entry in the power supply table
psSubunit	1.3.6.1.4.1.10734.3.3.2.3.4.1.1	The number for this entry in the power supply table. This number is always 0 (zero).
psType	1.3.6.1.4.1.10734.3.3.2.3.4.1.3	Type of hardware element: • 0: unequipped • 17: power supply • 18: power supply sub-unit
psCfgType	1.3.6.1.4.1.10734.3.3.2.3.4.1.4	Power supply configuration: • 0: unconfigured • 1: simplex • 2: duplex • 3: load share • 4: autonomous
psRunState	1.3.6.1.4.1.10734.3.3.2.3.4.1.5	High-level hardware state of the power supply: • 0: out of service • 1: initializing • 2: active • 3: standby • 4: diagnostic • 5: loopback • 6: active-FAF • 7: standby-FAF • 8: active - degraded • 9: standby - degraded

Object	OID	Description
psQualifier1	1.3.6.1.4.1.10734.3.3.2.3.4.1.6	Further qualification/detail on the high-level hardware state. • 1: degraded • 13: yellow alarm • 14: red alarm
psQualifier2	1.3.6.1.4.1.10734.3.3.2.3.4.1.7	Further qualification/detail on the high-level hardware state. • 1: degraded • 13: yellow alarm • 14: red alarm
psQualifier3	1.3.6.1.4.1.10734.3.3.2.3.4.1.8	Further qualification/detail on the high-level hardware state. • 1: degraded • 13: yellow alarm • 14: red alarm
psQualifier4	1.3.6.1.4.1.10734.3.3.2.3.4.1.9	Further qualification/detail on the high-level hardware state. • 1: degraded • 13: yellow alarm • 14: red alarm
psStartTime	1.3.6.1.4.1.10734.3.3.2.3.4.1.10	Time at which the power supply was powered up
psVendorID	1.3.6.1.4.1.10734.3.3.2.3.4.1.11	Identifying number of the power supply vendor
psDeviceID	1.3.6.1.4.1.10734.3.3.2.3.4.1.12	Identifying number specific to the power supply
psProductID	1.3.6.1.4.1.10734.3.3.2.3.4.1.13	Versions and other inventory information
psFPGAVersion	1.3.6.1.4.1.10734.3.3.2.3.4.1.14	Version of the TippingPoint FPGA chip on the power supply

TPT-TPAMIBS

Describes definitions for TPT device models. This section indicates the addition of the 440T Threat Protection System (TPS) model to the table. For registration identifiers of other TPT models, refer to the *MIBs Guide* for those products on the TMC.

The following table identifies the 440T TPS model:

Object	OID	Description
tpt-model-440T-IPS	1.3.6.1.4.1.10734.1.3.47	Registration for the HP TippingPoint 440T Threat Protection System (IPS).

Using HP Network Node Manager i with MIBs

HP Network Node Manager i (NNMi) is a well-known commercial network management system. Much of this information can be transposed onto other network management systems.

This topic focuses on adding enterprise MIB monitoring and reporting to NNMi. The examples in this topic were created on NNMi running on Windows XP Professional Service Pack 1.

Note: To perform the procedures in this topic, you must have installed NNMi. Refer to the NNMi documentation for more information about that product.

This topic includes the following:

- Loading TippingPoint Enterprise MIBs on page 32
- MIB Application Builder on page 32
- Discovering the device on page 33
- Creating graphs with Application Builder on page 33

Loading TippingPoint Enterprise MIBs

Before you begin, you must configure NNMi to understand the TippingPoint Enterprise MIBs.

1. In the NNMi Root Map, select the **Options** menu.
2. Select **Load/Unload MIBs: SNMP**.
3. Load **TIPPINGPOINT-REG-MIB**.
4. Load the remaining TPT MIBs in any order. NNMi might prompt you when loading the MIBs to add a macro definition. This is normal behavior, and you should accept the MIB.

MIB Application Builder

NNMi includes a tool called MIB Application Builder that allows you to build custom applications that retrieve data using SNMP and to retrieve any information stored in a MIB.

1. Select **Options => MIB Application Builder: SNMP**. The **MIB Application Builder: SNMP** dialog box displays.
2. Select **Edit => New item**. The application prompts you with three fields: Application ID, Application Type and Application Title.
   - Enter 111 for the **Application ID**.
   - Leave the Application Type as Form.
   - Enter an **Application Title**.
3. Select the MIB Objects that have the information that you want to view.
4. Click **Next**. The **MIB Application Builder / Add MIB Objects** screen displays.
5. In the navigation tree, locate **iso.org.dod.internet.private.enterprises**. You are now at the start of the IPS MIBs.

6. In the tree, select the variables that you want to monitor and click **Add**. Click **Close** to return to the previous screen.
7. Depending on how you added the objects, you might need to reorder them. You can reorder the variables by using the Up and Down arrows in the **New MIB Application - Display Fields** form.
8. Click **Next** to continue to the **New MIB Application - NMN Integration** dialog screen.
9. Enter `TippingPoint` after `Configuration->`. The line should appear as **Configuration->TippingPoint** under **Menu Location**. This creates a menu item under the Configuration menu on the main screen.
10. You can select an object on the map. Select **Configuration** from the menu and retrieve the information you created if the device is a TippingPoint device.
11. Close the **MIB Application Builder** dialog box.

Discovering the device

By default, NNMi automatically discovers devices as they arrive on the network. This form of discovery can be a slow process and might not display devices for days (depending on the size of your network). To expedite that process, use the `loadhosts` command.

1. Open your text editor and create a file named `hosts`.
2. In the file, enter the IP address of your device and the hostname. This format is similar to the UNIX /etc/hosts file format. For example, you might enter the following information:

   ```
   192.168.65.20 nds10
   ```

3. Save the file and open a command shell.
4. Run the `loadhosts` command on the file. The command takes the network mask and the file as arguments. For example:

   ```
   loadhosts -m 255.255.255.0 hosts
   ```

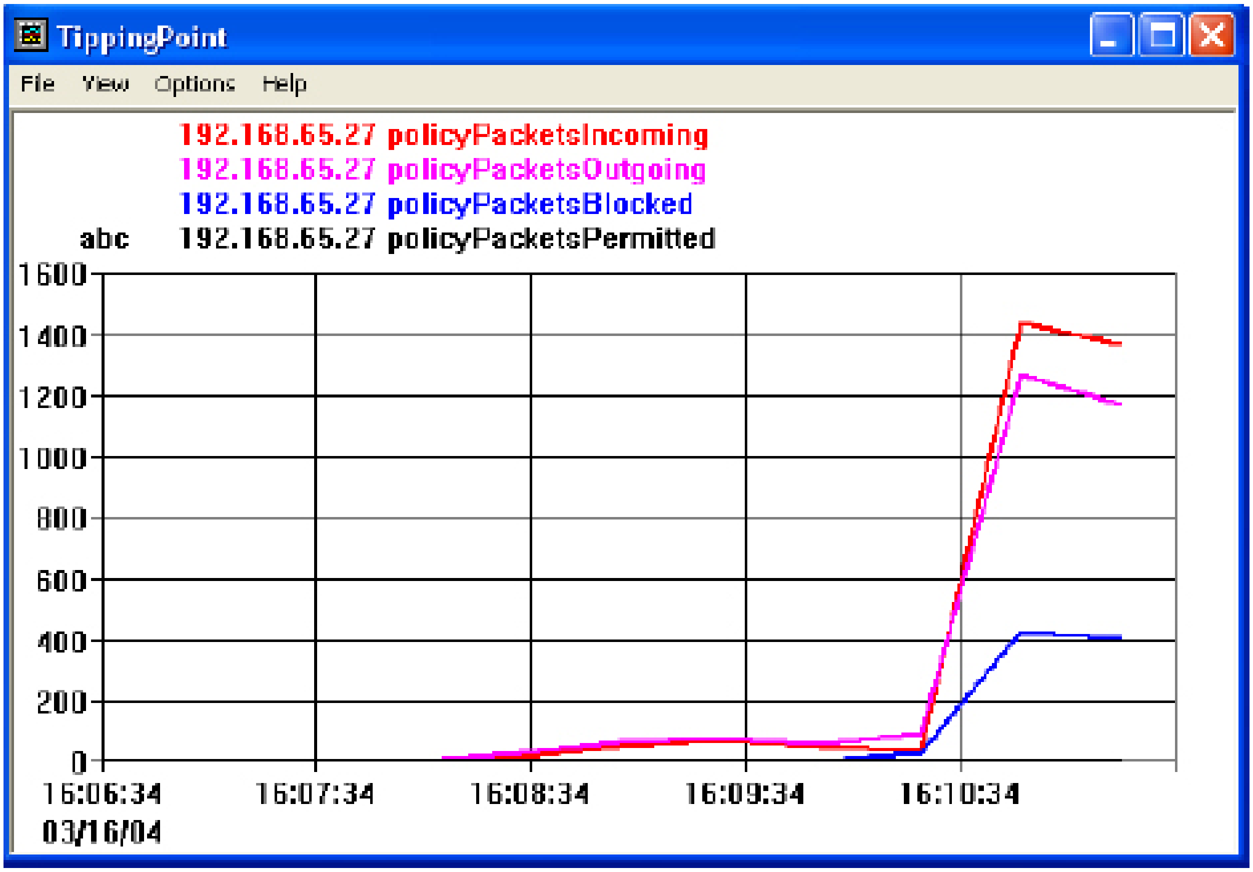
After you run the `loadhosts` command, the device is now discovered by NNMi. When you open the Internet icon on your NNMi map, a green square displays. This icon should be your device or devices. Select this icon and choose **Configuration** from the menu bar to view the device.

NNMi has a number of built-in applications that can retrieve data from standard MIBs. For example, when you open the device configuration, all of the Ethernet interfaces associated with that device are displayed. When you right-click on the interface and choose **Interface Properties**, information for that interface is displayed.

Creating graphs with Application Builder

You can create an application to graph the data with the MIB Application Builder tool.

1. Select the Application Builder from the Options menu.
2. Open your existing applications and double-click to edit.
3. Change the **Application Type** from a **Form** to a **Graph**.
4. Set `10` as the Poll Interval and `abc` as the Y-axis label. You can change these settings to fit your needs.
5. To generate the graph for your device, select the IPS green square. Choose **TippingPoint** from the Configuration menu. A graph displays for the device. Allow the graph to run about 30 seconds to begin trending the data.


TippingPoint
File View Options Help
192.168.65.27 policyPacketsIncoming
192.168.65.27 policyPacketsOutgoing
192.168.65.27 policyPacketsBlocked
abc 192.168.65.27 policyPacketsPermitted
1600
1400
1200
1000
800
600
400
200
0
16:06:34
03/16/04
16:07:34
16:08:34
16:09:34
16:10:34