



Extreme ONE OS Switching v22.2.0.0 SNMP MIB Reference Guide

MIB Structure, Supported Objects, and Network
Management

9039338-00 Rev AA
July 2025



Copyright © 2025 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: <https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks>

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses.

End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>



Table of Contents

Abstract.....	iv
Preface.....	v
Text Conventions.....	v
Documentation and Training.....	vi
Open Source Declarations.....	vii
Training.....	vii
Help and Support.....	vii
Subscribe to Product Announcements.....	viii
Send Feedback.....	viii
MIB Overview.....	9
Understanding MIBs.....	9
MIB Structure.....	9
Access to MIB Variables.....	10
Supported MIBs.....	11
Supported MIBs - Extreme ONE OS Base.....	12
Interface Group MIB.....	13
System Group MIB.....	15
System Object ID.....	15
Entity MIB.....	16
ifXTable Extended MIB.....	18
Supported Traps - Extreme ONE OS Base.....	20
Standard MIB Traps.....	20
Enterprise MIB Traps.....	20
Extreme Certificate MIB Traps.....	21
Extreme User MIB Traps.....	21
NTPv4-MIB Traps.....	23
Extreme System Sensor MIB.....	23
CPU and Memory Utilization - MIB Traps.....	25
Extreme Threshold Monitoring MIB.....	26
Traps after Device Reload.....	26
Supported MIB Traps - Extreme ONE OS Switching.....	27
Standard MIB Traps.....	27
LLDP MIB Traps.....	27
Enterprise MIB Traps.....	28
Extreme ONE MLAG MIB.....	28
BFD Enterprise MIB.....	28
BGP Enterprise MIB.....	29
Maintenance Mode MIB.....	30



Abstract

This SNMP MIB reference guide for Extreme ONE OS Switching version 22.2.0.0 delivers a technically rigorous specification of the MIB architecture, object identifiers, and trap mechanisms implemented in Extreme ONE OS and Switching platforms. It defines the hierarchical structure of sysObjectIDs under the enterprise OID tree (.1.3.6.1.4.1.1916.2.504), detailing mappings for platforms such as Extreme 8730 and 9920. The guide enumerates supported MIB groups including Interface Group MIB (RFC 2863), System Group MIB (RFC 1213), Entity MIB (RFC 4133), and ifXTable Extended MIB, with precise OIDs, syntax types, and operational semantics for each object. It documents SNMP trap support across standard and enterprise domains, including link state transitions (linkUp/linkDown), BGP FSM state changes, MLAG peer status, NTP mode transitions, certificate and password expiry events, CPU and memory threshold violations, and hardware resource usage alerts. Trap delivery mechanisms post-device reload are also addressed, including retry logic for coldStart and boot-time traps. The guide supports advanced SNMP management use cases such as real-time fault detection, interface-level traffic monitoring, and secure life-cycle management of credentials and certificates, and is intended for experienced network engineers and IT administrators requiring granular control of Extreme ONE OS-based switching environments.



Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches or routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings






Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says <i>type</i> .
Key names	Key names are written in boldface, for example Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
<i>italic</i> text	Italic text indicates variable content.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and Software Compatibility](#) for Extreme Networks products

[Extreme Optics Compatibility](#)

[Other Resources](#) such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the [Open Source Declaration](#) page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the [Extreme Networks Training](#) page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

[Extreme Portal](#)

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

[The Hub](#)

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

[Call GTAC](#)

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to [The Hub](#).
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at Product-Documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



MIB Overview

[Understanding MIBs](#) on page 9

This document provides conceptual information about MIBs operation and structure on Extreme ONE OS and Extreme ONE OS Switching.

Understanding MIBs

The management information base (MIB) is a database of monitored and managed information on an Extreme device.

The MIB structure can be represented by a tree hierarchy. The root splits into three main branches:

- International Organization for Standardization (ISO)
- Consultative Committee for International Telegraph and Telephone (CCITT)
- Joint ISO and CCITT

These branches have short text strings and integers (object identifiers) to identify them. Text strings describe object names. Integers allow software to create compact, encoded representations of the names.

MIB Structure

Each MIB variable is assigned an object identifier (OID). The OID is the sequence of numeric labels on the nodes along a path from the root to the object. For example, as shown in the following figure, the `sysDescr` is:

1.3.6.1.2.1.1.1

The corresponding name is:

`iso.org.dod.internet.mgmt.mib-2.system.sysDescr`

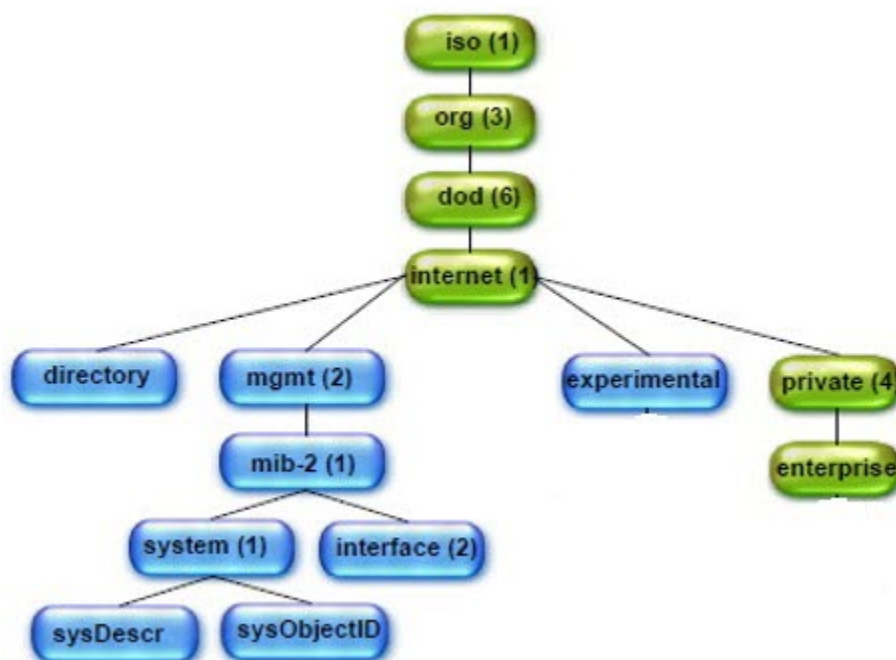
1.3.6.1.2.1.47

The corresponding name is:

`iso.org.dod.internet.mgmt.mib-2.entityMIB`

The other branches are part of the standard MIBs.

Figure 1: MIB tree



Access to MIB Variables

You can use a MIB browser to access the MIB variables. All MIB browsers load MIBs and perform queries.

Once the MIBs are loaded, read-only access provides access levels between the agent and management station. The access levels are described in the following table.

Table 4: MIB access levels

Access level	Description
Not accessible/None	You cannot read or write to this variable.
Read-create	Specifies a tabular object that can be read, modified, or created as a new row in a table.
Read-only	You can only monitor information.
Read-write	You can read or modify this variable.
Accessible-to-notify	You can read this information only through traps.

Supported MIBs

The following MIBs are distributed with Extreme ONE OS in a tar file.

- Entity MIB. For more information, see [Entity MIB](#) on page 16.
- Interface Group MIB. For more information, see [Interface Group MIB](#) on page 13.
- System Group MIB. For more information, see [System Group MIB](#) on page 15.
- ifXTable Extended MIB. For more information, see [ifXTable Extended MIB](#) on page 18.



Supported MIBs - Extreme ONE OS Base

[Interface Group MIB](#) on page 13

[System Group MIB](#) on page 15

[Entity MIB](#) on page 16

[ifXTable Extended MIB](#) on page 18

The following topics list the MIBs and MIB objects supported by Extreme ONE OS.

Interface Group MIB

The Interface Group MIB defines the managed objects for an interface.

The Interfaces Group MIB (ifMIB) is specified in [RFC 2863](#). Extreme ONE OS supports ifTable and ifNumber. The following table describes the supported MIB objects:

Table 5: Supported MIB objects

Name	OID	Syntax	Description
ifNumber	.1.3.6.1.2.1.2.1	Integer32	Number of network interfaces on the system
ifIndex	.1.3.6.1.2.1.2.2.1.1	InterfaceIndex	Value between 1 and the value of the ifNumber
ifDescr	.1.3.6.1.2.1.2.2.1.2	DisplayString (Octet string)	Description of the interface
ifType	.1.3.6.1.2.1.2.2.1.3	IANAifType	
ifMtu	.1.3.6.1.2.1.2.2.1.4	Integer32	Size of the largest packet that can be sent or received on the interface
ifSpeed	.1.3.6.1.2.1.2.2.1.5	Gauge32	Estimation of the interface bandwidth in bits per second
ifPhysAddress	.1.3.6.1.2.1.2.2.1.6	PhysAddress(Octet string)	Interface address at the protocol sub-layer
ifAdminStatus	.1.3.6.1.2.1.2.2.1.7	Integer	Administrative state of the interface: up (1), down (2), testing (3)
ifOperStatus	.1.3.6.1.2.1.2.2.1.8	Integer	Operational state of the interface: up (1), down (2), testing (3), unknown (4), dormant (5), not present (6) lower layer down (7)
ifLastChange	.1.3.6.1.2.1.2.2.1.9	TimeTicks	Value of sysUpTime when the interface entered the current operational state
ifInOctets	.1.3.6.1.2.1.2.2.1.10	Counter32	Number of octets received on the interface
ifInUcastPkts	.1.3.6.1.2.1.2.2.1.11	Counter32	Number of unicast packets delivered by the sublayer to a higher sublayer
ifInNUcastPkts	.1.3.6.1.2.1.2.2.1.12	Counter32	Number of multicast or broadcast packets delivered by the sublayer to a higher sublayer
ifInDiscards	.1.3.6.1.2.1.2.2.1.13	Counter32	Number of discarded inbound packets

Table 5: Supported MIB objects (continued)

ifInErrors	.1.3.6.1.2.1.2.2.1.14	Counter32	Number of inbound packets containing errors that prevented delivery to a higher-layer protocol
ifInUnknownProtos	.1.3.6.1.2.1.2.2.1.15	Counter32	Number of packets received from the interface that were discarded for an unknown or unsupported protocol
ifOutOctets	.1.3.6.1.2.1.2.2.1.16	Counter32	Number of octets sent from the interface
ifOutUcastPkts	.1.3.6.1.2.1.2.2.1.17	Counter32	Number of packets requested by a higher-level protocol that were addressed to a unicast address
ifOutNUcastPkts	.1.3.6.1.2.1.2.2.1.18	Counter32	Number of packets requested by a higher-level protocol that were addressed to a multicast or broadcast address
ifOutDiscards	.1.3.6.1.2.1.2.2.1.19	Counter32	Number of discarded outbound packets
ifOutErrors	.1.3.6.1.2.1.2.2.1.20	Counter32	Number of outbound packets containing errors that prevented transmission
ifOutQLen	.1.3.6.1.2.1.2.2.1.21	Gauge32	Length of the outbound packet queue
ifSpecific	.1.3.6.1.2.1.2.2.1.22	Object Identifier	OID of the MIB

System Group MIB

The System Group MIB defines the essential managed objects, or entities, for a system.

The System Group MIB is specified in [RFC 1213](#). Extreme ONE OS supports the following.

Table 6: Supported MIB objects

Name	OID	Syntax	Description
sysDescr	.1.3.6.1.2.1.1.1	DisplayString (Octet string)	Description of the entity
sysObjectID	.1.3.6.1.2.1.1.2	Object Identifier	OID of the device model
sysUpTime	.1.3.6.1.2.1.1.3	TimeTicks	Amount of time since the network management subsystem was last initialized
sysContact	.1.3.6.1.2.1.1.4	DisplayString (octet string)	Description of the contact person for the entity
sysName	.1.3.6.1.2.1.1.5	DisplayString (octet string)	Name of the entity. Usually the FQDN.
sysLocation	.1.3.6.1.2.1.1.6	DisplayString (octet string)	Physical location of the entity
sysServices	.1.3.6.1.2.1.1.7	Integer	Description of the services that the entity offers

System Object ID

The extremeONEOSProducts object (.1.3.6.1.4.1.1916.2.504) serves as a registry for sysObjectID values corresponding to Extreme ONE OS Base and Extreme ONE OS Switching-supported platforms. Presently, this encompasses definitions for Extreme 8730, Extreme ONE OS, and Extreme ONE OS Switching platforms.

The sysObjectID for Extreme ONE OS and Extreme ONE OS Switching supported products follows a hierarchical structure.

```

enterprises (.1.3.6.1.4.1)
|
extremenetworks (1916)
|
extremeProduct (2)
|
extremeONEOSProducts (504)
|
| - extreme8series (1)
|   |
|   | extreme8730 (1)
|
| - extreme9series (2)
|   |
|   | extreme9920 (1)

```

Entity MIB

The Entity MIB identifies the physical entities that are supported by an SNMP agent.

The Entity MIB is specified in [RFC 4133](#). Extreme ONE OS supports entPhysicalTable. The following table describes the supported MIB objects:

Table 7: Supported MIB objects

Name	OID	Syntax	Description
entPhysicalIndex	.1.3.6.1.2.1.47.1.1.1.1	PhysicalIndex	Value that uniquely identifies the physical entity
entPhysicalDescr	.1.3.6.1.2.1.47.1.1.1.2	SnmpAdminString	Description of the physical entity
entPhysicalVendorType	.1.3.6.1.2.1.47.1.1.1.3	AutonomousType	Vendor-specific indicator of the hardware type for the physical entity
entPhysicalContainedIn	.1.3.6.1.2.1.47.1.1.1.4	PhysicalIndexOrZero	Value of entPhysicalIndex of the physical entity that contains this physical entity
entPhysicalClass	.1.3.6.1.2.1.47.1.1.1.5	PhysicalClass	Indicator of the hardware type of the physical entity
entPhysicalParentRelPos	.1.3.6.1.2.1.47.1.1.1.6	Integer32	Indicator of this child component relative to its sibling components
entPhysicalName	.1.3.6.1.2.1.47.1.1.1.7	SnmpAdminString	Name of the physical entity
entPhysicalHardwareRev	.1.3.6.1.2.1.47.1.1.1.8	SnmpAdminString	Vendor-specific identifier of the hardware revision for the physical entity
entPhysicalFirmwareRev	.1.3.6.1.2.1.47.1.1.1.9	SnmpAdminString	Vendor-specific identifier of the firmware revision for the physical entity
entPhysicalSoftwareRev	.1.3.6.1.2.1.47.1.1.1.10	SnmpAdminString	Vendor-specific identifier of the software revision for the physical entity

Table 7: Supported MIB objects (continued)

entPhysicalSerialNum	.1.3.6.1.2.1.47.1.1.1.1.11	SnmpAdminString	Vendor-specific serial number for the physical entity
entPhysicalMfgName	.1.3.6.1.2.1.47.1.1.1.1.12	SnmpAdminString	Name of the manufacturer of the physical entity
entPhysicalModelName	.1.3.6.1.2.1.47.1.1.1.1.13	SnmpAdminString	Vendor-specific model name for the physical entity
entPhysicalAlias	.1.3.6.1.2.1.47.1.1.1.1.14	SnmpAdminString	Alias for the physical entity, as specified by the network manager
entPhysicalAssetID	.1.3.6.1.2.1.47.1.1.1.1.15	SnmpAdminString	Tracking identifier for the physical entity, as specified by the network manager
entPhysicalIsFRU	.1.3.6.1.2.1.47.1.1.1.1.16	TruthValue	Indicates whether the vendor considers this physical entity to be a field replaceable unit
entPhysicalMfgDate	.1.3.6.1.2.1.47.1.1.1.1.17	DateAndTime	Date that the physical entity was manufactured
entPhysicalUris	.1.3.6.1.2.1.47.1.1.1.1.18	Octet String	Extra information about the physical entity

ifXTable Extended MIB

The ifXTable is a list of interface entries, the number of which is determined by the value of ifNumber.

The ifXTable Extended MIB is specified in [RFC 2863](#), which also specifies the Interface Group MIB. Extreme ONE OS supports the following.

Table 8: Supported MIB objects

Name	OID	Syntax	Comments
ifName	.1.3.6.1.2.1.31.1.1.1.1	DisplayString (Octet string)	Name of the interface
ifInMulticastPkts	.1.3.6.1.2.1.31.1.1.1.2	Counter32	Number of packets addressed to a multicast address at this sublayer
ifInBroadcastPkts	.1.3.6.1.2.1.31.1.1.1.3	Counter32	Number of packets addressed to a broadcast address at this sublayer
ifOutMulticastPkts	.1.3.6.1.2.1.31.1.1.1.4	Counter32	Number of packets requested by a higher-level protocol that were addressed to a multicast address at this sublayer
ifOutBroadcastPkts	.1.3.6.1.2.1.31.1.1.1.5	Counter32	Number of packets requested by a higher-level protocol that were addressed to a broadcast address at this sublayer
ifHCInOctets	.1.3.6.1.2.1.31.1.1.1.6	Counter64	Number of octets received on the interface
ifHCInUcastPktss	.1.3.6.1.2.1.31.1.1.1.7	Counter64	Number of unicast packets delivered by the sublayer to a higher sublayer
ifHCInMulticastPkts	.1.3.6.1.2.1.31.1.1.1.8	Counter64	Number of multicast packets delivered by the sublayer to a higher sublayer
ifHCInBroadcastPkts	.1.3.6.1.2.1.31.1.1.1.9	Counter64	Number of broadcast packets delivered by the sublayer to a higher sublayer
ifHCOctets	.1.3.6.1.2.1.31.1.1.1.10	Counter64	Number of octets sent from the interface

Table 8: Supported MIB objects (continued)

ifHCOOutUcastPkts	.1.3.6.1.2.1.31.1.1.1.11	Counter64	Number of packets requested by a higher-level protocol that were addressed to a unicast address at this sublayer
ifHCOOutMulticastPkts	.1.3.6.1.2.1.31.1.1.1.11	Counter64	Number of packets requested by a higher-level protocol that were addressed to a multicast address at this sublayer
ifHCOOutBroadcastPkts	.1.3.6.1.2.1.31.1.1.1.12	Counter64	Number of packets requested by a higher-level protocol that were addressed to a broadcast address at this sublayer
ifLinkUpDownTrapEnable	.1.3.6.1.2.1.31.1.1.1.13	Integer	Indicates whether linkUp and linkDown traps are generated for the interface
ifHighSpeed	.1.3.6.1.2.1.31.1.1.1.14	Gauge32	Estimation of the interface's current bandwidth
ifPromiscuousMode	.1.3.6.1.2.1.31.1.1.1.16	TruthValue	Value of false (2) if the interface accepts only those packets or frames that are addressed to the interface. Value of true (1) if the interface accepts all packets and frames.
ifConnectorPresent	.1.3.6.1.2.1.31.1.1.1.17	TruthValue	Value of true (1) if the sublayer has a physical connector. Value of false (2) if the sublayer does not have a physical connector.
ifAlias	.1.3.6.1.2.1.31.1.1.1.18	DisplayString	Alias for the interface, as specified by the network manager
ifCounterDiscontinuityTime	.1.3.6.1.2.1.31.1.1.1.19	TimeStamp	Value of sysUpTime at the most recent occurrence of discontinuity for any of the interface's counters



Supported Traps - Extreme ONE OS Base

[Standard MIB Traps](#) on page 20

[Enterprise MIB Traps](#) on page 20

[Traps after Device Reload](#) on page 26

Standard MIB Traps

The following generic traps are supported:

Use this topic to learn about the following standard MIB traps:

Traps	Description
coldstart (1.3.6.1.6.3.1.1.5.1)	The coldStart trap is generated when the sending protocol entity undergoes reinitialization, potentially modifying the agent's configuration or the implementation of the protocol entity.
linkDown (1.3.6.1.6.3.1.1.5.4)	The linkDown trap is triggered by the sending protocol entity upon detecting a failure in one of the communication links represented within the agent's configuration, indicating a loss of connectivity.
linkUp (1.3.6.1.6.3.1.1.5.3)	A linkUp trap is generated when the sending protocol entity identifies that a communication link represented in the agent's configuration has become available.

Enterprise MIB Traps

Use this topic to learn about the following MIB traps:

- [Extreme Certificate MIB Traps](#) on page 21
- [Extreme User MIB Traps](#) on page 21
- [NTPv4-MIB Traps](#) on page 23
- [Extreme System Sensor MIB](#) on page 23

- [CPU and Memory Utilization - MIB Traps](#) on page 25
- [Extreme Threshold Monitoring MIB](#) on page 26

Extreme Certificate MIB Traps

The Extreme Certificate MIB traps enable the configuration of traps for impending app certificate and CA certificate expirations. The feature supports four severity levels of traps. Traps are triggered when any server certificate stored on the device, linked to an application, is nearing expiration within a user-defined timeframe (specified in days).

For information on CLI command for the alert levels, see *Extreme ONE OS Switching Command Reference Guide*.

Only trap notifications are supported, Get or GetNext operations for MIB objects are not supported.

Trap Names and OIDs	Varbinds	Description
extremeCertExpiryWarning .1.3.6.1.4.1.1916.1.59.0.1	extremeCertSubject, extremeCertIssuerName, extremeCertSerialNumber, extremeCertValidNotAfterTime, extremeCertExpiryPendingDays, extremeCertExpiryAlertLevel	This notification is sent before a certificate expires, based on the configured certification expiry alert settings. The specific certificate (extremeCertName) can be identified by referencing the INDEX part of the notification's varbinds in the extremeCertTable.
extremeCertExpired .1.3.6.1.4.1.1916.1.59.0.2	extremeCertSubject, extremeCertIssuerName, extremeCertSerialNumber, extremeCertValidNotAfterTime, extremeCertExpiryExpiredDays	This notification is sent when a certificate has expired. The expired certificate (extremeCertName) can be identified by referencing the INDEX part of the notification's varbinds in the extremeCertTable.

Extreme User MIB Traps

Extreme User MIB traps enable you to configure traps for password expiry notifications. Four severity levels of traps are supported. For information on CLI command for the alert levels, see *Extreme ONE OS Switching Command Reference Guide*.

Only trap notifications are supported, Get or GetNext operations for MIB objects are not supported.

Trap Names and OID	Varbinds	Description
extremePaswdExpiryWarning 1.3.6.1.4.1.1916.1.61.0.1	extremeUserName extremePasswdExpiryDate extremePasswdExpiryPendingDays extremePasswdExpiryAlertLevel	This notification is sent before a user account's password expires, based on the global password expiry alert configuration.
extremePasswdExpiringToday 1.3.6.1.4.1.1916.1.61.0.2	extremeUserName extremePasswdExpiryDate	This notification is sent if the user account's password is expiring on the current day.
extremePasswdExpired 1.3.6.1.4.1.1916.1.61.0.3	extremeUserName extremePasswdExpiryDate extremePasswdExpiryExpiredDays	This notification is sent if the user account's password has already expired. Each notification provides relevant details for timely action.



Note

The following points describe the expire checks and alerts:

- Daily Checks: User and certificate expiry checks run daily at 00:00 UTC, triggering alerts at this time.
- Additional Check : Expiry checks also occur when the security management system starts up.
- Alert Behavior:
 1. Warning alerts are sent only once on the configured alert day..
 2. extremeCertExpired and extremePasswdExpired traps are sent daily until the certificate is replaced or password is reset.
- Expiry Time Display:
 1. extremeCertValidNotAfterTime: Displays exact certificate expiry date and time.
 2. extremePasswdExpiryDate: Displays expiry date with 00:00 time.

NTPv4-MIB Traps

The following table describes the supported NTPv4-MIB traps. Get or GetNext for the MIB objects are not supported.

Trap Names and OIDs	Varbinds	Description
ntpEntNotifModeChange 1.3.6.1.2.1.197.0.1	ntpEntStatusCurrentMode	This notification is generated when the NTP entity changes mode such as not running, not synchronised.
ntpEntStatusCurrentMode 1.3.6.1.2.1.197.1.2.1	NA	The current mode of NTP, and is indicated by the following values: <ul style="list-style-type: none"> • notRunning(1) - NTP is inactive. • notSynchronized(2) - NTP is not synchronized with any time source. • noneConfigured(3) - NTP is unsynchronized and lacks a reference configured. • syncToLocal(4) - NTP is distributing time based on its local clock compromising accuracy and reliability. • syncToRefclock(5) - NTP is synchronized with a local hardware reference clock (for example, GPS). • syncToRemoteServer(6) - NTP is synchronized with a remote upstream NTP server. • unknown(99) - The NTP state is unknown.

Extreme System Sensor MIB

The Extreme System Sensor Notification MIB Objects are supported.

The following table describes Extreme System Sensor Notification MIB Objects:

Trap name and OID	Varbinds	Description
extremeTempSensorStatusChange 1.3.6.1.4.1.1916.1.60.0.1	extremeTempSensorTransitionEvent extremeTempSensorAggrStatus	A notification is triggered whenever a temperature sensor's status changes to normal, alarm, or critical.

The following table describes Extreme Temperature Sensor Objects:

Varbinds	Description
extremeTempSensorAggrStatus 1.3.6.1.4.1.1916.60.1.1	<p>Aggregate Temperature Sensor Status</p> <p>This value encodes the state of multiple temperature sensors, with each sensor occupying 4 bits.</p> <p>Encoding Scheme</p> <p>Byte 1: Sensor 1 (most significant nibble), Sensor 2 (least significant nibble)</p> <p>Byte 2: Sensor 3 (most significant nibble), Sensor 4 (least significant nibble)</p> <p>Handling Odd Number of Sensors</p> <p>If there's an odd number of sensors, the last nibble is padded with zeros (0x0000).</p> <p>The nibbles are set as follows:</p> <ul style="list-style-type: none"> • 0x0000 - for normal state • 0x0001 - for alarm state • 0x0010 - for critical state
extremeTempSensorTransitionEvent 1.3.6.1.4.1.1916.60.1.3	<p>This MIB specifies the temperature sensor state transition that triggers the extremeTempSensorStatusChange notification.</p> <p>The values for each state change are:</p> <ul style="list-style-type: none"> • 1 - Normal to Alarm • 2 - Alarm to Critical • 3 - Normal to Critical • 4 - Critical to Alarm • 5 - Alarm to Normal • 6 - Critical to Normal

CPU and Memory Utilization - MIB Traps

Object Name and OID	Varbind	Description
swCpuRisingThresholdNotification 1.3.6.1.4.1.1588.2.1.1.0.16	swCpuUsage swCpuUsageLimit swCpuNoOfRetries swCpuPollingInterval	This notification is generated when the switch CPU utilization exceeds the predefined 'CPU usage limit' for the configured 'number of retries' and 'polling interval'.
swCpuFallingThresholdNotification 1.3.6.1.4.1.1588.2.1.1.0.17	swCpuUsage swCpuUsageLimit swCpuNoOfRetries swCpuPollingInterval	This notification is generated when the switch CPU utilization comes down to or below the predefined CPU usage limit for the configured number of retries and polling interval.
swMemRisingThresholdNotification 1.3.6.1.4.1.1588.2.1.1.0.18	swMemUsage swMemUsageLimit swMemNoOfRetries swMemPollingInterval	This notification is generated when the switch memory utilization exceeds the predefined memory usage limit for the configured number of retries and polling interval.
swMemFallingThresholdNotification 1.3.6.1.4.1.1588.2.1.1.0.19	swMemUsage swMemUsageLimit swMemNoOfRetries swMemPollingInterval	This notification is generated when the switch memory utilization comes down to/below the predefined memory usage limit for the configured number of retries and polling interval.

Extreme Threshold Monitoring MIB

The following table shows the SNMP threshold monitoring MIB notifications:

Trap Name and OID	Varbinds	Description
ExtremeHWResourceUsageAlert 1.3.6.1.4.1.1916.1.58.0.2	extremeHWResourceOverallUsage	This notification is generated when the monitored resource usages exceeds the configured high threshold level or falls below the low threshold level. The number of notifications that are generated for a particular time period is configured globally. The total number of generated notifications cannot exceed this configuration.

The following table shows the SNMP threshold monitoring MIB objects:

Trap Name and OID	Access	Description
extremeHWResourceOverallUsage 1.3.6.1.4.1.1916.1.58.4.1	read-only	A bitmap of status, where each bit represents an individual resource being monitored. Resource usage status for monitored resources is indicated as 0 (zero) when the usage falls below the configured low threshold for that resource and 1 (one) when the usage exceeds the configured high threshold. If a resource is not supported, its bit value is 0 (zero). The mapping of hex values to bits is per RFC 3417 sec 8.

Traps after Device Reload

When a device reloads, interfaces (management or inband) take time to become operational.

To ensure SNMP traps are delivered successfully, a retry mechanism is implemented for the following traps:

1. Coldstart traps
2. Other traps during device boot-up

The retry mechanism may cause a delay (approximately 60 seconds) between the trap event occurrence and delivery to recipient hosts.



Supported MIB Traps - Extreme ONE OS Switching

[Standard MIB Traps](#) on page 27

[Enterprise MIB Traps](#) on page 28

Use this topic to learn about the MIB traps supported by Extreme ONE OS Switching.

Standard MIB Traps

The following generic traps are supported:

Use this topic to learn about the following standard MIB trap:

LLDP MIB Traps

Trap Name and OID	Description
IldpRemTablesChange 1.0.8802.1.1.2.0.0.1	A IldpRemTablesChange notification is sent when the value of IldpStatsRemTableLastChangeTime changes. It can be used by an NMS to trigger LLDP remote systems table maintenance polls. Note that transmission of IldpRemTablesChange notifications are throttled by the agent, as specified by the 'IldpNotificationInterval' object.

varbind	Description
IldpStatsRemTablesInserts 1.0.8802.1.1.2.1.2.2	Indicates the number of new neighbors.
IldpStatsRemTablesDeletes 1.0.8802.1.1.2.1.2.3	Indicates the number of neighbors that are deleted.
IldpStatsRemTablesDrops 1.0.8802.1.1.2.1.2.4	Indicates the number of neighbors that are discarded.
IldpStatsRemTablesAgeouts 1.0.8802.1.1.2.1.2.5	Indicates the number of neighbors that are aged.

Enterprise MIB Traps

Use this topic to learn about the following enterprise MIB traps:

- [Extreme ONE MLAG MIB](#) on page 28
- [BFD Enterprise MIB](#) on page 28
- [BGP Enterprise MIB](#) on page 29
- [Maintenance Mode MIB](#) on page 30

Extreme ONE MLAG MIB

The following traps are generated when peer is Up or Down:

Trap Names and OIDs	Varbinds
extremeMlagPeerDownTrap 1.3.6.1.4.1.1916.1.63.0.1	<ul style="list-style-type: none"> • extremeMlagPeerAddr: Peer address • extremeMlagPeerAddrType: Peer address type • sysName: The local host name assigned for this switch
extremeMlagPeerUpTrap 1.3.6.1.4.1.1916.1.63.0.2	<ul style="list-style-type: none"> • extremeMlagPeerAddr: Peer address • extremeMlagPeerAddrType: Peer address type • sysName: The local host name assigned for this switch

BFD Enterprise MIB

The following trap notifications are supported. Get/GetNext are not supported for this MIB.

Trap Name and OID	Varbind	Description
extremeBfdSessUp 1.3.6.1.4.1.1916.1.55.0.1	bfdSessDiag bfdSessInterface bfdSessSrcAddrType bfdSessSrcAddr bfdSessDstAddrType bfdSessDstAddr ifName extremeBfdVrfName	A notification is generated when the bfdSessState object for one of the entries in bfdSessTable is about to enter the up (4) state from some other state. The value of bfdSessDiag is set equal to noDiagnostic (0).
extremeBfdSessDown 1.3.6.1.4.1.1916.1.55.0.2	bfdSessDiag bfdSessInterface bfdSessSrcAddrType bfdSessSrcAddr bfdSessDstAddrType bfdSessDstAddr ifName extremeBfdVrfName	A notification is generated when the bfdSessState object for one of the entries in bfdSessTable is about to enter the down (2) or adminDown (1) state from some other state. The values of bfdSessDiag returns the Diagnostic code providing the reason for the new state (for example, pathDown (5)).

BGP Enterprise MIB

The BGP Enterprise MIB notifications are sent for the **peers of IPv6 types**. The BGP Enterprise MIB defines the following trap OIDs and Varbind:

extremeBGP4V2EstablishedNotification: An extremeBGP4V2EstablishedNotification event is generated when the BGP FSM enters the established state.

extremeBGP4V2BackwardTransitionNotification: An extremeBGP4V2BackwardTransitionNotification event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.

Trap Name and OID	Varbinds
extremeBGP4V2EstablishedNotification 1.3.6.1.4.1.1916.1.51.0.1	extremeBgp4V2PeerState extremeBgp4V2PeerLocalPort extremeBgp4V2PeerRemotePort extremeBgp4V2PeerRemoteAddr
extremeBGP4V2BackwardTransitionNotification 1.3.6.1.4.1.1916.1.51.0.2	extremeBgp4V2PeerState extremeBgp4V2PeerLocalPort extremeBgp4V2PeerRemotePort extremeBgp4V2PeerLastErrorCodeReceived extremeBgp4V2PeerLastErrorSubCodeReceived extremeBgp4V2PeerLastErrorReceivedText extremeBgp4V2PeerRemoteAddr

Maintenance Mode MIB

Trap Name and OID	Varbind	Description
extremeMaintenanceModeEntryTrap 1.3.6.1.4.1.1916.1.57.0.1	extremeMaintenanceModeConvergenceStatus extremeMaintModeReasonCode sysName	A trap is generated when the switch enters the maintenance mode
extremeMaintenanceModeExitTrap 1.3.6.1.4.1.1916.1.57.0.2	extremeMaintenanceModeConvergenceStatus extremeMaintModeReasonCode sysName	A trap is generated when the switch exits from the maintenance mode.

Varbinds	Access	Description
extremeMaintenanceModeConvergenceStatus 1.3.6.1.4.1.1916.1.57.1	Accessible-for-notify	This object indicates the convergence status at the time of trap generation, with the following states: <ol style="list-style-type: none"> Completed (1): Convergence finished within the expected time. Default is 90 secs, which is configurable. Timed Out (2): Convergence took longer than the expected convergence time.
extremeMaintModeReasonCode 1.3.6.1.4.1.1916.1.57.2	Accessible-for-notify	This object indicates the reason for entering or exiting maintenance mode, with the following states: <ol style="list-style-type: none"> User Action (1): Maintenance mode is triggered immediately by a user. On Switch Reboot (2): The switch enters maintenance mode during reboot, as specified in the startup configuration (enable-on-reboot).