Cisco Secure Firewall SNMP MIBs Reference Guide

Revised: September 25, 2024

Secure Firewall ASA and Threat Defense MIBs Reference Guide

Cisco Secure Firewall uses SNMP MIBs to support monitoring of the firewall devices running on Cisco Secure ASA, Cisco Firepower 4100/9300, Cisco Firepower 1000, 2100, and Secure Firewall 3100 and 4200 platforms.

About SNMP

SNMP is an application-layer protocol that facilitates the exchange of management information among network devices and is part of the TCP/IP protocol suite. The firewall devices provide support for network monitoring using SNMP Versions 1, 2c, and 3, and support the use of all three versions simultaneously. The SNMP agent running on the firewall interface lets you monitor the network devices through network management systems (NMSes), such as HP OpenView.

You can configure the devices to send traps, which are unsolicited messages from the managed device to the management station for certain events (event notifications) to an NMS, or you can use the NMS to browse the Management Information Bases (MIBs) on the security devices. MIBs are a collection of definitions, and the devices maintain a database of values for each definition. The devices have an SNMP agent that notifies designated management stations if events occur that are predefined to require a notification, for example, when a link in the network goes up or down. The notification it sends includes an SNMP OID, which identifies itself to the management stations. The agent also replies when a management station asks for information.

About MIBs and Traps

MIBs are either standard or enterprise-specific. Standard MIBs are created by the IETF and documented in various RFCs. A trap reports significant events occurring on a network device, most often errors or failures.

SNMP traps are defined in either standard or enterprise-specific MIBs. Standard traps are created by the IETF and documented in various RFCs. SNMP traps are compiled into the appropriate software- Secure Firewall ASA or Secure Firewall Threat Defense.

FXOS MIB files are a set of objects that are private extensions to the IETF standard MIB II. MIB II is documented in RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*. Portions of MIB-II have been updated since RFC 1213. See the IETF website http://www.ietf.org for the latest updates to this MIB.

Important Links

- If needed, you can also download RFCs, standard MIBs, and standard traps from http://www.ietf.org/.
- Browse the complete list of Cisco MIBs, traps, and OIDs from https://github.com/cisco/cisco-mibs/blob/main/supportlists/asa/asa-supportlist.html.
- In addition, download Cisco OIDs by FTP from https://github.com/cisco/cisco-mibs/tree/main/oid.

Secure Firewall MIB Reference Guides

- Supported Secure Firewall ASA MIBS and OIDs for the latest release can be found in the SNMP chapter of the *Cisco Secure Firewall ASA General Operations ASDM or CLI Configuration Guides*: https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html

- Supported FXOS MIBS and OIDs for Cisco Firepower 4100/9300: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/mib/b_FXOS_4100_9300_MIBRef.html
- Supported FXOS MIBS and OIDs for Cisco Firepower 1000, 2100, and Secure Firewall 3100 and 4200 MIBs: https://www.cisco.com/c/en/us/td/docs/security/firepower/2100/mib/b_FXOS_2100_MIBRef.html

MIBs Guidelines and Troubleshooting Tips

- SNMP cannot be configured in the system context. You can get information about interfaces in either the admin or user context using the IF-MIB's.
- If you are running ASA on a Firepower appliance, then you would need to query the FXOS (and not ASA) to get the physical appliance details
- If your NMS cannot get requested information from the managed device, then the MIB that allows that specific data collection might be missing. Typically, if an NMS cannot retrieve a particular MIB variable, either the NMS does not recognize that MIB variable, or the agent does not support the MIB variable.
- If the NMS does not recognize a specific MIB variable, you might need to load the MIB into the NMS, usually with a MIB compiler. For example, you might need to load the Cisco FXOS private MIB or the supported RFC MIB into the NMS to execute the required data collection.
- If the agent does not support a specific MIB variable, you must find out what version of system software you are running. Different software releases support different MIBs.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.