

Configuration of SNMP on an SSL Appliance

TAC

Document ID: 118665

Contributed by Nazmul Rajib and Jose Escobar, Cisco TAC Engineers.
Nov 17, 2014

Contents

Introduction

Prerequisites

Component Used

Requirement

Configuration

Introduction

You can enable Simple Network Management Protocol (SNMP) on an SSL appliance. The SSL Appliance models 1500, 2000 and 8200 support the standard SNMP MIB2 tables, and use the SNMP v2c version of the protocol. This document provides you the steps to enable SNMP on an SSL Appliance.

Prerequisites

Component Used

The following components have been used on this document:

- SSL appliances 1500, 2000, 8200
- Software Version 3.6 or greater

Requirement

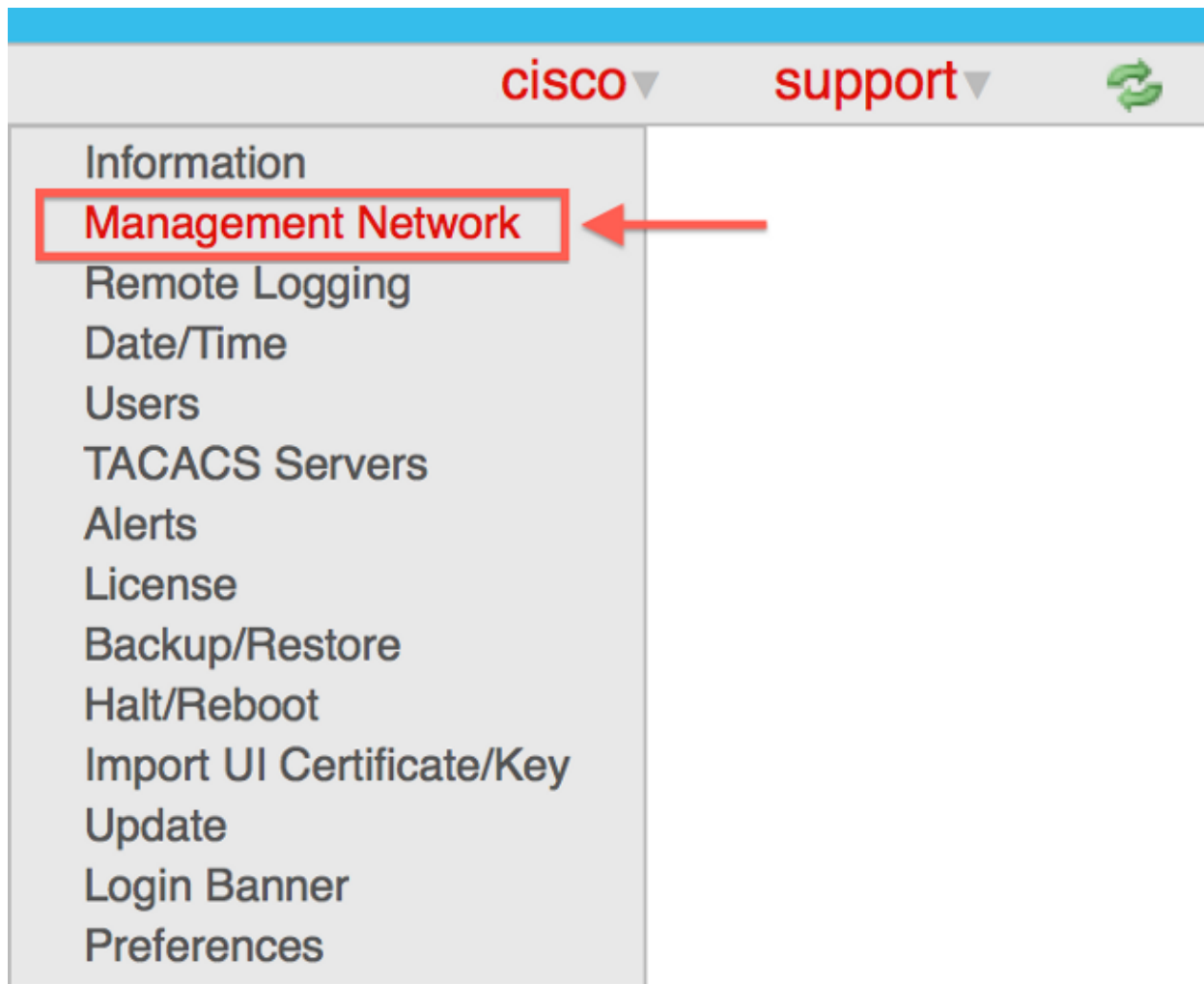
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

You can configure SNMP on an SSL Appliance using the web user interface of the appliance. The steps are:

1. Navigate to the Platform Management menu and select *Management Network*.

Note: The platform management menu shows the hostname of SSL appliance. In this example, it is cisco.



2. Click on the *pencil* icon to edit the settings. The *Edit Management Network* window appears.

Monitor Policies PKI

Management Network ✎ ↻

MAC Address:

MTU: **1500**

Hostname: **cisco**

Primary Nameserver:

Secondary Nameserver:

SNMP: **False**

Host to send traps to:

Allow edit of SNMP values: **False**

SNMP edit access: IP address/mask: **0.0.0.0/0**

SNMP edit access: OID: **1.3.6.1.2.1.1**

System Location:

System Contact:

System Description:

IPv4 Settings ✎ ↻

Mode:

IP Address/Netmask:

Default Gateway:

IPv6 Settings ✎ ↻

Mode: **DHCP**

IP Address/Netmask: **:::0**

Default Gateway:

Link Local Address:

IPv4 Access Control List ⏪ 1/1 ⏩ ⏪ ⏩ ⏪ ⏩ ⏪ ⏩ ↻

Address	Applies To	Action

IPv6 Access Control List ⏪ 1/1 ⏩ ⏪ ⏩ ⏪ ⏩ ⏪ ⏩ ↻

Address	Applies To	Action

3. Fill in the appropriate fields, enable SNMP and configure the SNMP parameters appropriately for your SNMP management system. Click **OK**.

Edit Management Network

MTU	<input type="text" value="1500"/>
Hostname	<input type="text" value="cisco"/>
Primary Nameserver	<input type="text"/>
Secondary Nameserver	<input type="text"/>
SNMP	<input checked="" type="checkbox"/>
Host to send traps to	<input type="text"/>
Allow edit of SNMP values	<input checked="" type="checkbox"/>
SNMP edit access: IP address/mask	<input type="text" value="0.0.0.0/0"/>
SNMP edit access: OID	<input type="text" value="1.3.6.1.2.1.1"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
System Description	<input type="text"/>
SNMP read-only community string	<input type="text"/> (Not Configured)
Confirm read-only community string	<input type="text"/>
SNMP edit community string	<input type="text"/> (Not Configured)
Confirm edit community string	<input type="text"/>

Leave community fields blank if you do not wish to change the community strings.

4. Apply the platform configuration changes.

 Platform Config Changes