



## CHAPTER 23

# Cisco NAC Appliance

---

Cisco NAC Appliance is a network-centric integrated solution administered from the Clean Access Manager (CAM) web console and enforced through the Clean Access Server (CAS) and the Clean Access Agent (CAA). Cisco NAC Appliance checks client systems, enforces network requirements, distributes patches and antivirus software, and quarantines vulnerable or infected clients for remediation before clients access the network.

CAM manages one or more CASs. Cisco Security MARS receives event data from CAM. CAM can send both syslog messages and SNMP traps. SNMP traps provide system health status, whereas the syslog message provide details about quarantined or infected hosts, connection attempts, and connection status.

This chapter contains the following topics:

- [Bootstrap the Cisco NAC Appliance, page 23-1](#)
- [Define a Cisco NAC Appliance in MARS Manually, page 23-2](#)

## Bootstrap the Cisco NAC Appliance

Using the Clean Access Manager (CAM) web console, perform the following tasks so that the NAC appliance publishes the required events to Cisco Security MARS.

### Syslog Support

To enable syslog processing support, define the MARS appliance as a syslog server. For detailed steps, see [Configuring Syslog Logging](#) in *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide*.

### SNMP Support

For SNMP support, perform the following tasks:

1. Enable SNMP alerts for the NAC appliance.
2. Define the MARS appliance as a trapsink.

For detailed steps, see [SNMP](#) in *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide*.

## Define a Cisco NAC Appliance in MARS Manually

To define a Cisco NAC appliance manually, you must define the appliance in the MARS web interface. When the appliance is defined and the changes are activated, MARS normalizes the syslog message receive by the appliance against known event types.

To define a NAC appliance in MARS, follow these steps:

**Step 1** Select **Admin > System Setup > Security and Monitor Devices > Add**.

**Step 2** Select **Cisco NAC Appliance 4.1** for the Device Type list.

A the Device Type page appears.

Device Type:

→ \*Device Name:

→ Reporting IP:

**Step 3** Type the name of this appliance in the **Device Name** field.

**Step 4** Type the reporting IP of the appliance in the **Reporting IP** field.

**Step 5** To save your changes, click **Submit**.

The device name appears under the Security and Monitoring Information list. The submit operation records the changes in the database tables. However, it does not load the changes into working memory of the MARS Appliance. The activate operation loads submitted changes into working memory.

**Step 6** To enable MARS to start sessionizing events from this device, click **Activate**.

MARS begins to recognize, map, and sessionize events generated by this appliance and evaluate those events using the defined inspection and drop rules. Any events published by the device to MARS before activation can be queried using the reporting IP address of the device as a match criterion. For more information on the activate action, see [Activate the Reporting and Mitigation Devices, page 1-15](#).