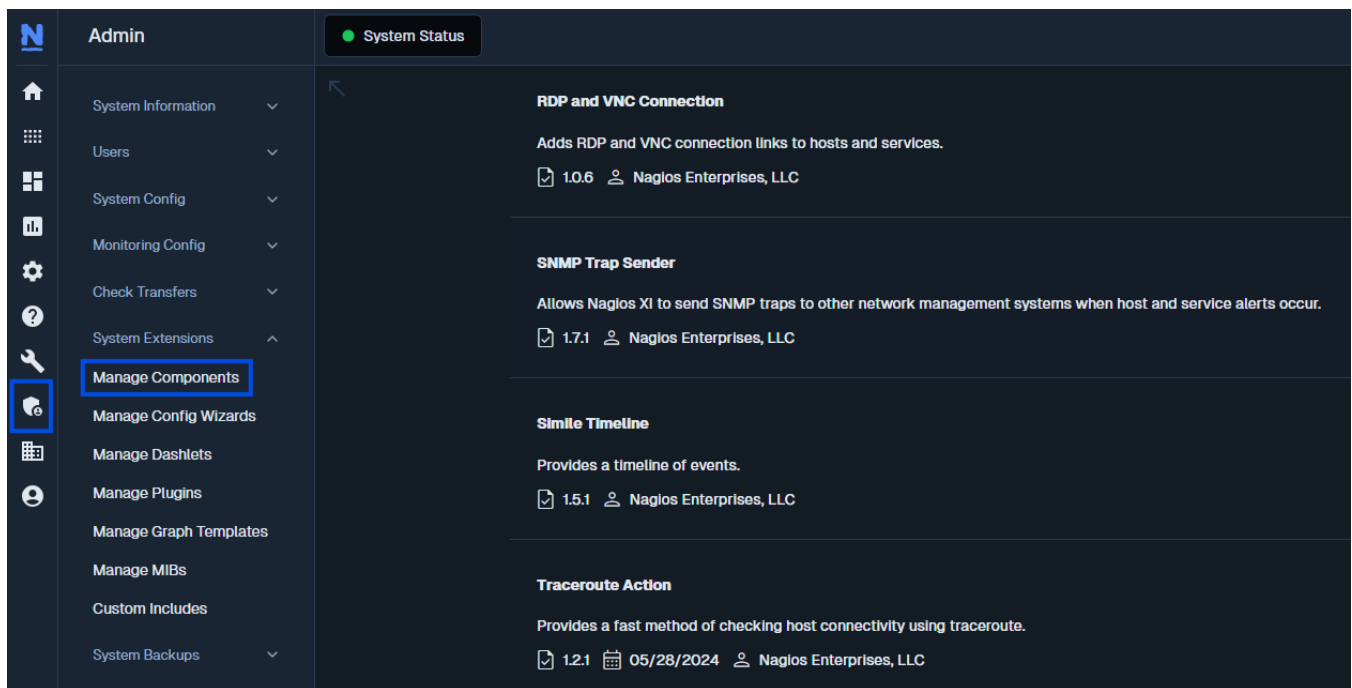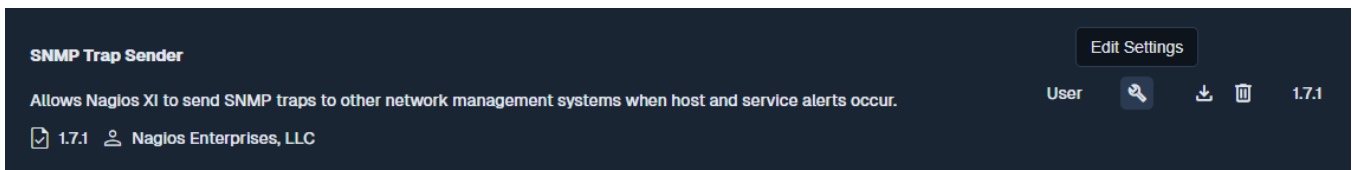# How To Send SNMP Traps In Nagios XI 2024

Purpose

This document is intended for use by Nagios XI Administrators who want to know how to configure Nagios XI to send SNMP Traps to other management hosts or network management systems whenever host or service state changes (alerts) occur.

Configuring SNMP Traps

1. To configure Outbound SNMP traps, navigate to **Admin > System Extensions > Manage Components**.

2. Find the **SNMP Trap Sender** component and click on the **Edit Settings** Icon.

3. The **SNMP Trap Sender** component configuration screen allows you to define trap hosts that Nagios XI should send SNMP traps to when host and service changes (alerts) occur.

- **Integration Settings**
  - Check the **Enable SNMP trap sender integration** box to enable this component.
  - Check the **Enable Debug Logging** box to enable advanced logging for this component.
- **Trap Hosts**
  - The first required field is **Host Address** in order to send SNMP traps to a host.
  - If the **Port** field is left blank, then it will default to **162 UDP**.
  - **SNMP Version**
    - SNMP v2c requires an SNMP **Community** string to be defined for a valid configuration.
    - SNMP v3 has several options available, the amount required depends on the **Security Level** chosen. SNMP v3 configuration is not explained here, instead please refer to the following KB article: Nagios XI – SNMP Trap v3 Configuration

SNMP Trap Sender

Integration Settings

☑ Enable SNMP trap sender integration

☑ Enable Debug Logging
This will log traps sent to /usr/local/nagiosxi/var/components/snmptrapsender.log

Trap Hosts

Specify the addresses of the hosts that SNMP traps should be sent to. If you want to prevent traps from being sent during downtime check the checkbox for each host.
If you leave the Port field blank it will use the default port 162 and UDP protocol. Select the checkbox to use the TCP protocol.

Host Address	General Options		Security Options	
172.28.241.231	Port		SNMP Version	3
	Use TCP	☐	Security Level	noAuthNoPriv
	Hosts	ALL	Username	
	Services	ALL	Auth Password	
	State Type	BOTH	Privacy Password	
	Don't Send During Downtime	☐	Engine ID	
			Auth Protocol	None
			Priv Protocol	None

- **MIBs**
  - There are two MIB .txt files that can be downloaded. You can upload these files to the system that is receiving the SNMP Traps being sent from Nagios XI.
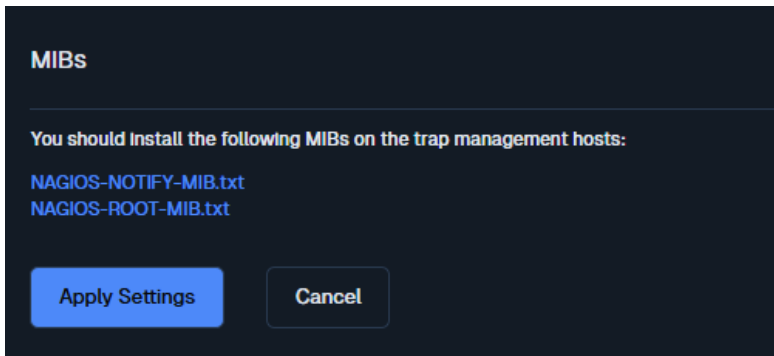
4. Click **Apply Settings** to save your settings.

This is the extent of the configuration options available for the **SNMP Trap Sender** component.

Verifying SNMP Traps

There are a couple of ways to verify that the SNMP traps are being sent and received.

The Sender - Nagios XI Server

You can watch the `/usr/local/nagiosxi/var/eventman.log` file to see the events and `snmptrap` commands. For example:

```
tail -f /usr/local/nagiosxi/var/eventman.log
```

nagiosXI on DESKTOP-N47B94Q - Virtual Machine Connection

File   Action   Media   Clipboard   View   Help

```
            [hostaddress] => 192.168.0.111
            [hostalias] => 192.168.0.111
            [hostdisplayname] => 192.168.0.111
            [service] => Port 18 Status
            [hoststate] => UP
            [hoststateid] => 0
            [servicestate] => CRITICAL
            [servicestateid] => 2
            [lastservicestate] => CRITICAL
            [lastservicestateid] => 2
            [servicestatetype] => HARD
            [currentattempt] => 5
            [maxattempts] => 5
            [serviceeventid] => 18
            [serviceproblemid] => 18
            [serviceoutput] => CRITICAL: Interface Port: 18 Gigabit - Level (index 18) is down.
            [longserviceoutput] =>
            [datetime] => Thu Nov 28 21:09:40 CST 2024
        )

    [referer] => includes/components/xicore/xicore.inc.php > Event Handler Notification Email
    [to] => root@localhost
    [subject] => PROBLEM Service Alert - 192.168.0.111/Port 18 Status is CRITICAL
    [high_priority] => 0
    [message] => ***** Nagios XI Alert *****

Nagios has detected a problem with this service.

Notification Type: PROBLEM

Service: Port 18 Status
Host: 192.168.0.111
Address: 192.168.0.111
State: CRITICAL
Info:
CRITICAL: Interface Port: 18 Gigabit - Level (index 18) is down.
Date/Time: 2024-11-28 21:09:45

Respond: http://172.28.241.231/nagiosxi/rr.php?oid=229&token=f9308deab33db341762165c3e4df37ffcc6618f5
Nagios URL: http://172.28.241.231/nagiosxi/
```

Which will output something like:

```
PROCESSING:
Array (
[address] => 10.25.5.2
[port] =>
[community] => public
[hoststateid] => 0
[servicestateid] => 0
[statetype] => BOTH
)
```

The Receiver

The device that is receiving the SNMP Traps should have some functionality to watch the incoming SNMP traffic.

In this example the receiving device was a CentOS server running SNMPTRAPD and SNMPTT. You can watch the `/var/log/snmptt.log` and `/var/log/snmpttunknown.log` files to see the incoming traps. For example:

```
tail -f /var/log/snmptt/snmptt.log /var/log/snmptt/snmpttunknown.log
```

Which will output something like:

```
Fri Dec 16 11:02:47 2016: Unknown trap (.1.3.6.1.4.1.20006.1.7) received from xic6x-x86 at:
Value 0: xi-c6x-x86
Value 1: 10.25.5.11
Value 2: 15:0:23:05.80
Value 3: .1.3.6.1.4.1.20006.1.7
Value 4: 10.25.5.11
Value 5:
Value 6:
Value 7:
Value 8:
Value 9:
Value 10:
Ent Value 0: .1.3.6.1.4.1.20006.1.3.1.2=win7-02.box293.local
Ent Value 1: .1.3.6.1.4.1.20006.1.3.1.6=Memory Usage
Ent Value 2: .1.3.6.1.4.1.20006.1.3.1.7=3
```

Ent Value 3: .1.3.6.1.4.1.20006.1.3.1.17=UNKNOWN - The WMI query had problems. The target host (10.25.14.3) might not be reachable over the network. Is it down? Looks like a valid name/IP Address. 10.25.14.3 is probably not even pingable. Wmic error text on the next line.

```
Sending 40 bytes to UDP: [192.168.0.225]:161->[0.0.0.0]:41307
0000: 30 26 02 01  01 04 06 70  75 62 6C 69  63 A1 19 02    0&.....public...
0016: 04 2E 32 9D  FA 02 01 00  02 01 00 30  0B 30 09 06    ..2........0.0..
0032: 05 2B 06 01  02 01 05 00                              .+......

Sending 40 bytes to UDP: [192.168.0.225]:161->[0.0.0.0]:41307
0000: 30 26 02 01  01 04 06 70  75 62 6C 69  63 A1 19 02    0&.....public...
0016: 04 2E 32 9D  FA 02 01 00  02 01 00 30  0B 30 09 06    ..2........0.0..
0032: 05 2B 06 01  02 01 05 00                              .+......

Sending 40 bytes to UDP: [192.168.0.225]:161->[0.0.0.0]:41307
0000: 30 26 02 01  01 04 06 70  75 62 6C 69  63 A1 19 02    0&.....public...
0016: 04 2E 32 9D  FA 02 01 00  02 01 00 30  0B 30 09 06    ..2........0.0..
0032: 05 2B 06 01  02 01 05 00                              .+......

Sending 40 bytes to UDP: [192.168.0.225]:161->[0.0.0.0]:41307
0000: 30 26 02 01  01 04 06 70  75 62 6C 69  63 A1 19 02    0&.....public...
0016: 04 2E 32 9D  FA 02 01 00  02 01 00 30  0B 30 09 06    ..2........0.0..
0032: 05 2B 06 01  02 01 05 00                              .+......

Sending 40 bytes to UDP: [192.168.0.225]:161->[0.0.0.0]:41307
0000: 30 26 02 01  01 04 06 70  75 62 6C 69  63 A1 19 02    0&.....public...
0016: 04 2E 32 9D  FA 02 01 00  02 01 00 30  0B 30 09 06    ..2........0.0..
0032: 05 2B 06 01  02 01 05 00                              .+......
```

Finishing Up

This completes the documentation on how to send SNMP Traps in Nagios XI. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum   Visit Nagios Knowledge Base   Visit Nagios Library