## Purpose

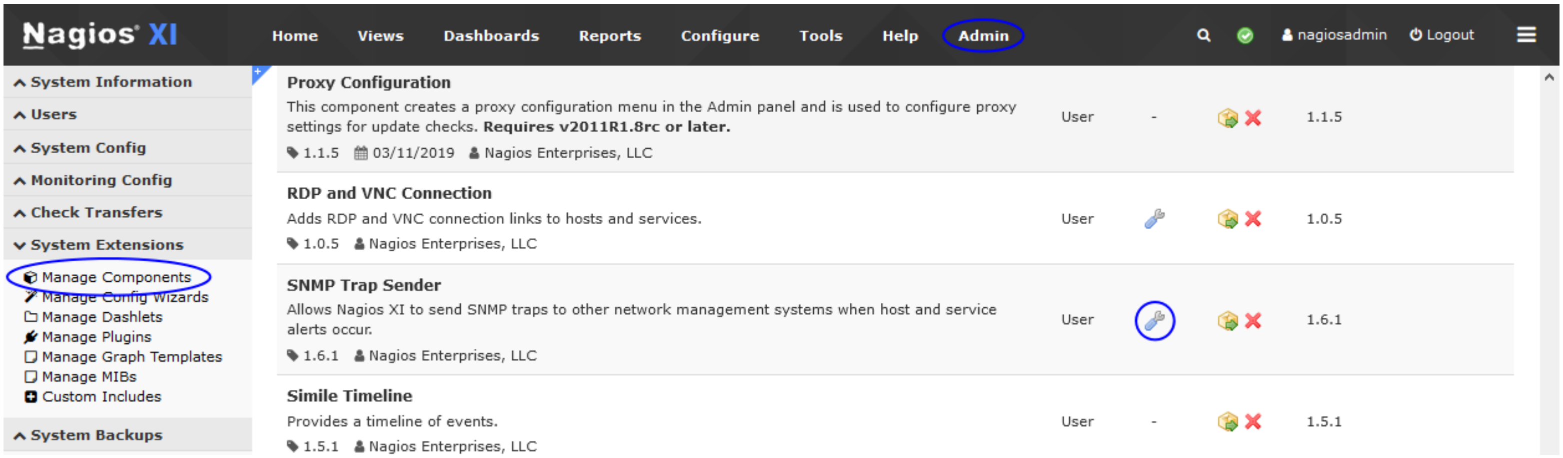
This document describes how to configure Nagios XI to send SNMP Traps to other management hosts or network management systems whenever host or service state changes (alerts) occur.

## Target Audience

This document is intended for use by Nagios XI Administrators.

## Configuring SNMP Traps

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



**Proxy Configuration**
This component creates a proxy configuration menu in the Admin panel and is used to configure proxy settings for update checks. **Requires v2011R1.8rc or later.**
1.1.5 03/11/2019 Nagios Enterprises, LLC
User - 1.1.5

**RDP and VNC Connection**
Adds RDP and VNC connection links to hosts and services.
1.0.5 Nagios Enterprises, LLC
User 1.0.5

**SNMP Trap Sender**
Allows Nagios XI to send SNMP traps to other network management systems when host and service alerts occur.
1.6.1 Nagios Enterprises, LLC
User 1.6.1

**Simile Timeline**
Provides a timeline of events.
1.5.1 Nagios Enterprises, LLC
User - 1.5.1

Click the **Edit Settings** icon for the **SNMP Trap Sender** component.

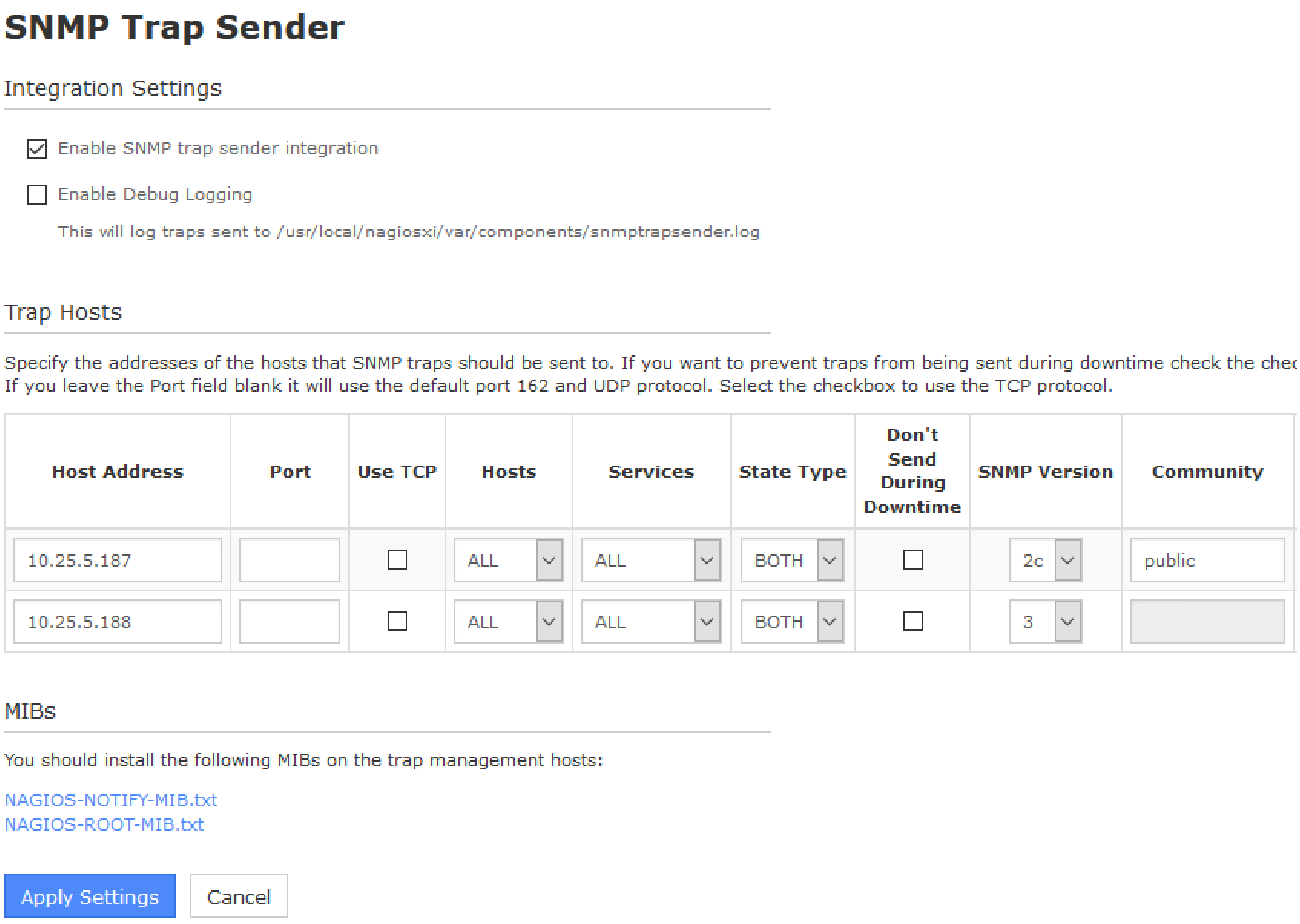
The SNMP trap sender component configuration screen allows you to define trap hosts that Nagios XI should send SNMP traps to when host and service changes (alerts) occur.

### Integration Settings

Check the **Enable SNMP trap sender integration checkbox** to enable this component.

Check the **Enable Debug Loggins** to enable advanced logging for this component.

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.



## 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 chec
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.

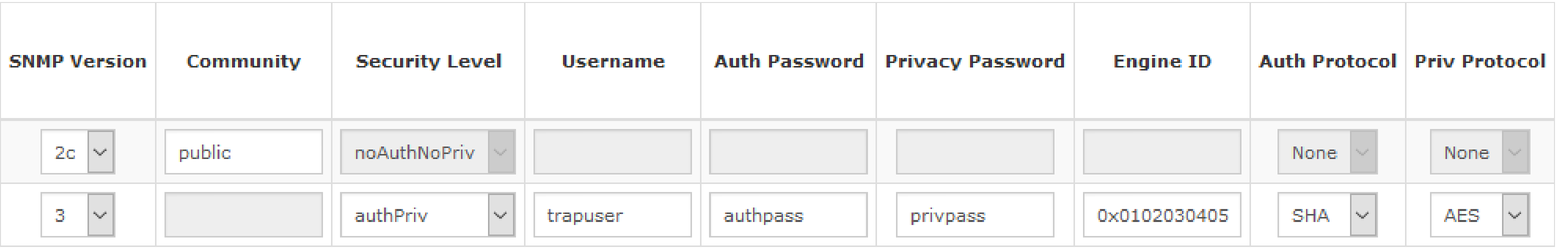
| Host Address | Port | Use TCP | Hosts | Services | State Type | Don't Send During Downtime | SNMP Version | Community |
|---|---|---|---|---|---|---|---|---|
| 10.25.5.187 | | □ | ALL | ALL | BOTH | □ | 2c | public |
| 10.25.5.188 | | □ | ALL | ALL | BOTH | □ | 3 | |

### MIBs

You should install the following MIBs on the trap management hosts:

NAGIOS-NOTIFY-MIB.txt
NAGIOS-ROOT-MIB.txt

The setting span to the right due to the amount of available options for v3.



| SNMP Version | Community | Security Level | Username | Auth Password | Privacy Password | Engine ID | Auth Protocol | Priv Protocol |
|---|---|---|---|---|---|---|---|---|
| 2c | public | noAuthNoPriv | | | | | None | None |
| 3 | | authPriv | trapuser | authpass | privpass | 0x0102030405 | SHA | AES |

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

## Trap Hosts

The first required field is **Host Address** order to send SNMP traps to a host. If the Port field is left blank then it will default to **162 UDP**.

SNMP **v1** & **v2c** require an **SNMP Community** string to be defined for a valid configuration.

SNMP **v3** has a number of options available, they amount required depend 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

In the screenshot on the previous page you can see that if you select SNMP v1 & v2 the v3 options are grayed out and vice versa.

## MIBs

There are two MIB files that can be downloaded. You can upload these files to the system that is receiving the SNMP Traps being sent from Nagios XI.

When finished, click the **Apply Settings** button to save your settings.

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

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

## 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
```

Which will output something like:

```
PROCESSING:
Array
(
     [address] => 10.25.5.2
     [port] =>
     [community] => public
     [hoststateid] => 0
     [servicestateid] => 0
     [statetype] => BOTH
)
RUNNING COMMAND: /usr/bin/snmptrap -v 2c -c public 10.25.5.2 '' NAGIOS-NOTIFY-MIB::nSvcEvent nSvcHostname s "10.25.14.3" nSvcDesc s "Application Log Warnings" nSvcStateID I 3 nSvcOutput s "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."
```

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

### 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 xi-c6x-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.
```

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

## Finishing Up

This completes the documentation on how to send SNMP Traps with Nagios XI.

If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

https://support.nagios.com/forum

The Nagios Support Knowledgebase is also a great support resource:

https://support.nagios.com/kb

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.