

# Tidal Enterprise Scheduler: Troubleshooting Sending of SNMP Traps

Document ID: 113172

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions

#### Solution

- Configuration Check
- Verify Trap Has Been Sent
- Destination System Not Receiving Trap

#### Related Information

## Introduction

This document provides basic troubleshooting tips for issues with Tidal Enterprise Scheduler (TES) sending SNMP traps.

## Prerequisites

### Requirements

- List of trap receiving systems, and the port numbers those systems utilize to receive traps
- Permission/ability to edit the TES system's master.props file, or create a file in the Master's config directory
- Permission/ability to restart the TES system after such a configuration is made
- A working TES system and one or more systems with the ability to receive SNMP traps

### Components Used

The information in this document is based on Tidal Master (Windows or Unix).

### Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Solution

### Configuration Check

Complete these steps:

1. Check the SNMP configuration files as specified in Tidal Enterprise Scheduler: Configuring SNMP. Note that only one of the two methods defined in that document should be used. If both are used, unpredictable results can be caused.

2. Verify that the configuration files have been correctly read in to the Master.

- a. In the Master, select **Activities > Configure Scheduler** from the menu.
- b. From the Logging tab, set the Event Manager Log to **High Debug** and click **OK**. Note the previous value so it can be reset later. Typically, it is Severe.
- c. Examine the most recent Master log file, and look for this error:

```
Could not parse snmp configuration file: Content is not allowed in prolog.
```

This indicates there is an error in the snmpconfig.xml file.

- d. Correct this and restart the Master.
- e. Once the error is gone, reset the Event Manager Log level to the previous value.

## Verify Trap Has Been Sent

Complete these steps in order to verify that the Master attempted to send the trap:

1. In the Master, select **Activities > Configure Scheduler** from the menu.
2. From the Logging tab, set the Event Manager Log to **High Debug** and click **OK**. Note the previous value so it can be reset later. Typically, it is Severe.
3. In the Master log file, look for entries similar to these (allowing, of course, for your system uniqueness):

```
enter: snmp handle(ActionSNMP: 9)
enter: snmp execute(ActionSNMP: 9)
try to send SNMP trap message
SNMP job trap is sent to host 'vlillico_4.tidalsoft.local'. Alert ID is '4'
SNMP trap message is sent.
SNMP trap is sent successfully. Snmp ID : 9
exit: snmp execute(ActionSNMP: 9)
Executed action Action: 9
```

These messages indicate that that the Master did send the trap.

Incorrect destination in this line indicates that the configuration file might contain errors in it (see the Configuration Check section):

```
No IP address accessible for SNMP manager, hostname = 'localhost'
```

4. Once this testing is complete, reset the Event Manager Log level to its previous value.

## Destination System Not Receiving Trap

If the destination system is not receiving traps that have been verified as being sent using the above, this should be checked:

- Routing issues Does a ping or tracert ( traceroute on Unix) to the destination host complete successfully.
- Firewall rules SNMP traps are sent with a destination port of 162 (unless changed in the TES SNMP configuration listed above) using UDP. Check both local (software) firewalls on Master and receiving hosts as well as infrastructure-level (hardware) firewalls.

## Related Information

- **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Aug 10, 2011

Document ID: 113172

---