Nimsoft® Monitor™

snmpgtw Guide

v1.2 series

Legal Notices

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Nimsoft LLC disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Nimsoft LLC shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Nimsoft LLC and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Nimsoft LLC as governed by United States and international copyright laws.

Restricted Rights Legend

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.227-7014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Nimsoft LLC's standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Trademarks

Nimsoft is a trademark of CA.

Adobe®, Acrobat®, Acrobat Reader®, and Acrobat Exchange® are registered trademarks of Adobe Systems Incorporated.

Intel® and Pentium® are U.S. registered trademarks of Intel Corporation.

Java(TM) is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Netscape(TM) is a U.S. trademark of Netscape Communications Corporation.

Oracle® is a U.S. registered trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of the Open Group.

ITIL® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.

All other trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

Contact Nimsoft

For your convenience, Nimsoft provides a single site where you can access information about Nimsoft products.

At http://support.nimsoft.com/, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- Nimsoft Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about Nimsoft product documentation, you can send a message to support@nimsoft.com.

Contents

Chapter 1: snmpgtw 1.2

This description applies to snmpgtw probe version 1.2.

This section contains the following topics:

snmpgtw Overview

Transform Nimsoft Monitor alarm messages to SNMP trap message readable by any SNMP-based event manager. A predefined set of profiles exist for transforming the Nimsoft Monitor alarm message to some well-known event managers, like HP OpenView, CA Unicenter TNG, and BMC CommandPost.

Documentation Changes

This table describes the version history for this document.

Version	Date	What's New?
1.2	August 2012	Upgraded the probe to use latest version of nimsnmp library; added native support for Windows 64-bit and Linux 32-bit and 64-bit environments.

Related Documentation

Documentation for other versions of the snmpgtw probe (../../snmpgtw.html)

Getting Started with Nimsoft® Probes

Nimsoft® Probes Reference

Chapter 2: snmpgtw Probe Deployment

This section contains the prerequisites, system requirements and deployment information for the snmpgtw probe.

This section contains the following topics:

Supported Platforms

The snmpgtw probe supports the same set of operating systems and databases as supported by the Nimsoft Server solution. Please refer to the Nimsoft Compatibility Support Matrix for the latest information on supported platforms.

System Requirements

The snmpgtw probe should be installed on systems with the following minimum resources:

- Memory: 2-4 GB of RAM. This probe OOTB configuration requires 256 MB of RAM.
- CPU: 3 GHz dual-core processor, 32-bit or 64-bit

Software Requirements

The snmpgtw probe requires the following software environment:

- Nimsoft Monitor Server 5.1.1 or later
- Nimsoft robot version 5.32 or later
- Java Virtual Machine version 1.6 or later (deployed as part of the probe package)
- Infrastructure Manager v4.02 or later
  - .NET v3.5 on the hardware running the Infrastructure Manager application

Probe Deployment Information

There are two ways to distribute archive packages. You can distribute the package within Infrastructure Manager or use the standalone Nimsoft Distribution application.

See Probe Deployment for more information on deploying probes.

Chapter 3: snmpgtw Configuration

The *snmp* gateway converts alarms to SNMP-TRAP messages.

It will transform alarm messages to SNMP-TRAP messages readable by any SNMP based event manager. A predefined set of profiles exists for transforming the alarm message to some well-known event managers, like HP-OpenView's Network Node Manager, CA Unicenter-TNG and BMC CommandPost.

Most SNMP based event managers have capabilities of defining filters based on the incoming object identifier (OID) and the trap information. The Nimsoft SNMP gateway is capable of mapping the various severity levels to enterprise specific trap types. This makes it possible to define a number of trap-definitions on the event manager side to recognize the various severity levels.

Note: snmpgtw version 1.11 and above supports sending traps with trap_type 0. Due to this all the pre configured profiles with traps mapped to '0' start sending traps with trap_type 0. You have to modify the configured profiles manually if traps with trap_type 0 are not required.

This section contains the following topics:

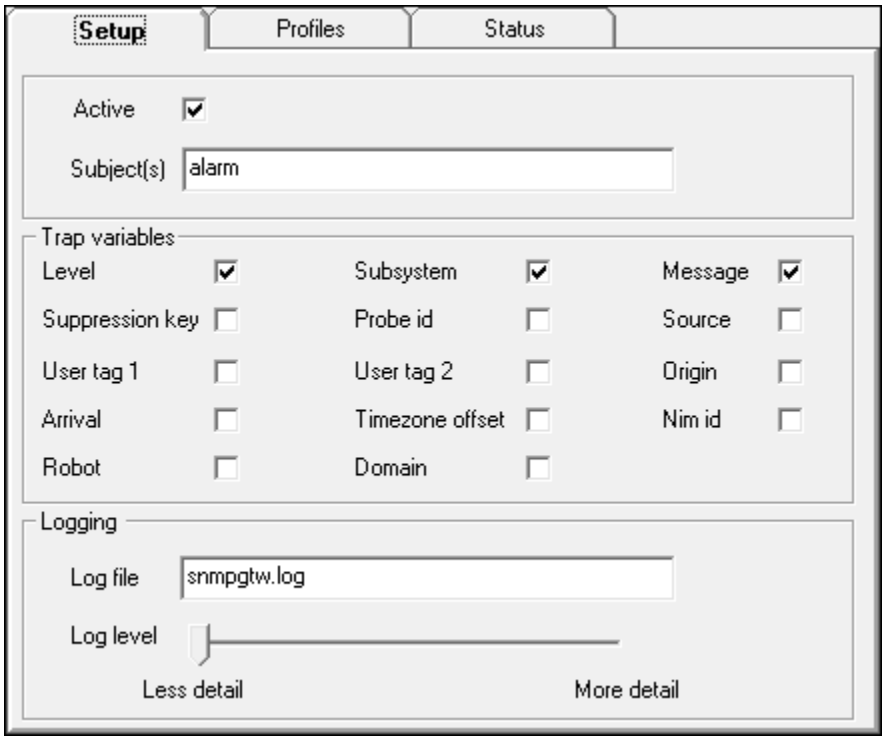
Probe Configuration Interface Installation

The probe configuration interface is automatically downloaded and installed by the Nimsoft Infrastructure Manager when the probe is deployed on a robot.

Probe Configuration

This section contains specific configuration for the probe.

Setup Tab



This tab contains the following fields:

Active

Allows you to activate or deactivate this probe.

Subject(s)

Specifies which Nimsoft subject that is transformed. It is possible to specify a comma-separated list.

Trap variables

Level

Sets the severity of the alarm message (1 to 5).

Subsystems

Uses a sid (*subsystem identification number (e.g. 1.1.1.1)* to categorize alarms is sent along with the alarm message from the probes.

Message

Enables you to create messages.

Suppression key

Enables to avoid storing multiple alarms caused by the same problem. Alarms with the same *source*, *message*, *subsystem* and *severity* information will be suppressed into a single message with only a counter indicating the number of occurrences.

Probe id

Includes the id of the probe in the message.

Source

Specifies the IP address of the source (the device sending packets). Specifying the source IP address can be useful when running the probe on a device with multiple IP addresses.

User tag 1

Defines the user-defined tag to be used as a grouping / locating mechanism. Is displayed in various lists in the NMS Manager.

User tag 2

Defines the user-defined tag to be used as a grouping / locating mechanism. Is displayed in various lists in the NMS Manager.

Origin

Identifies the origin of the data.

Arrival

Includes the arrival time in the message.

Timezone offset

Includes the local time on the sending robot. Also, timezone is returned as string instead of an integer in the trap.

Nim id

Includes the global id in the message.

Robot

Includes the name of the Robot in the message.

Domain

Includes the name of the Domain in the message.

Logging

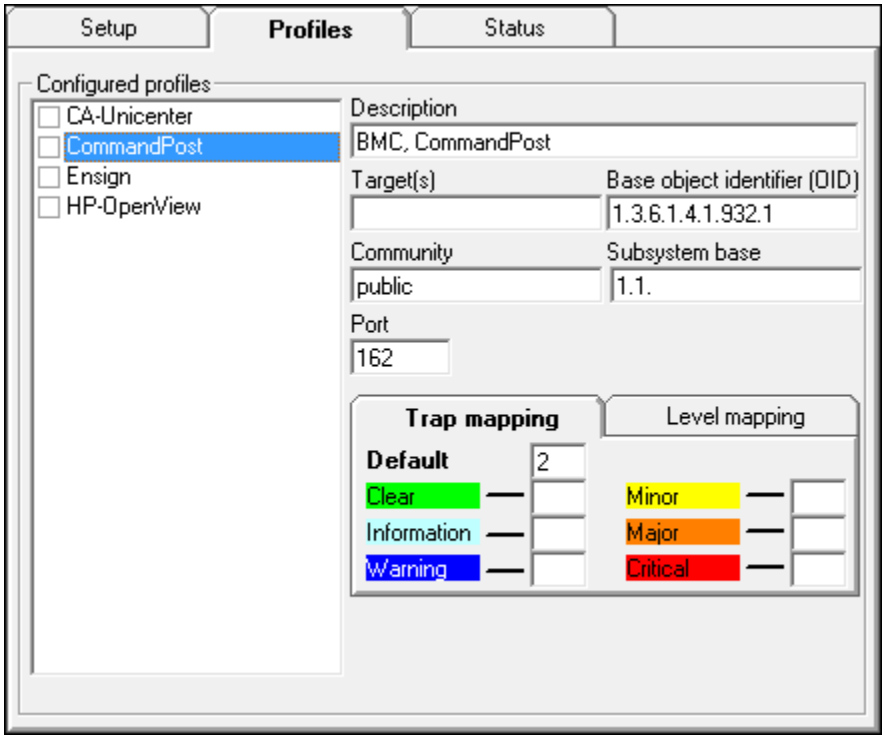
Log file

Specifies the file where the probe logs information about its internal activity.

Log level

Sets the level of details written to the log-file. Log as little as possible during normal operation to minimize disk consumption and increase the amount of detail when debugging.

Profiles Tab



This tab contains the following fields.

Configured profiles

Displays a list of all configured profiles. The checkmark shows whether a profile is actually used. Select a profile to see its setup details.

Description

Provides text describing the profile.

Target(s)

Indicates the network node where the SNMP-TRAPs should be sent (the management console).

Base object identifier

Indicates the SNMP Object identifier to be used in the trap packages generated.

Community

Indicates the SNMP community string used in the SNMP-TRAPs.

Subsystem base

If the receiving management console uses the same subsystem logic as Nimsoft, you may specify a prefix to be added to the subsystem ID in all SNMP-TRAPs generated, in order to make the alarms occur at the right place in the console application.

Trap mapping

If the receiving management console classifies the incoming traps by trap type and takes different actions for different trap types (as HP OpenView does), you may map the severity levels of the alerts to different enterprise specific SNMP-TRAPs.

This allows HP OpenView to take different actions for Information messages than for Critical ones.

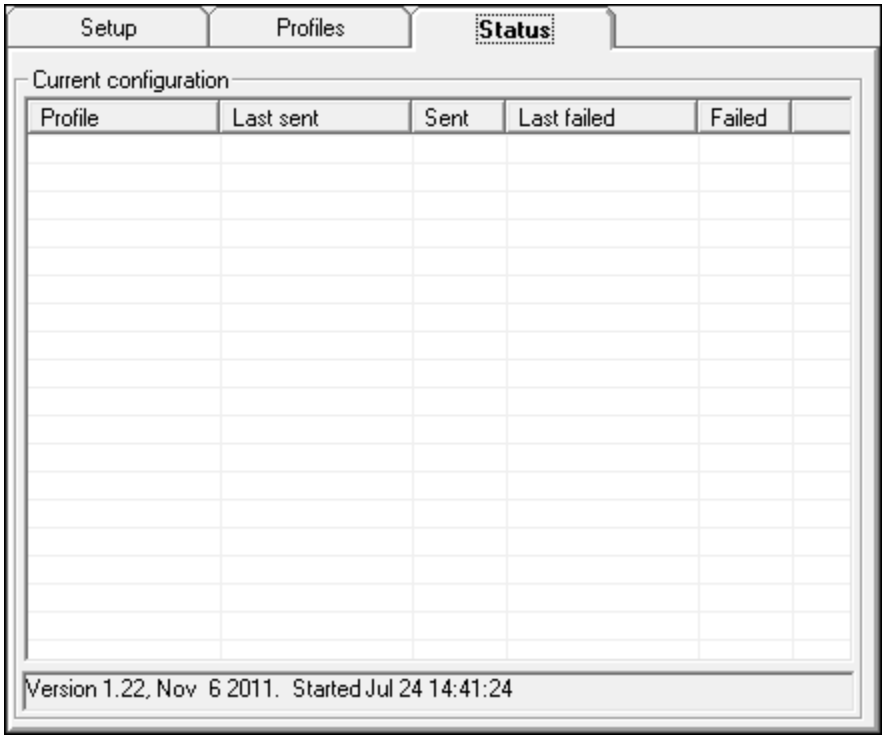
Note: If specifying your own profiles, you must specify a value in at least one of these fields, otherwise the gateway will not send trap-messages. Use the Default field to define a trap type for Nimsoft messages without a severity level.

Level mapping

If the receiving management console uses the same level logic as Nimsoft, only with different codes to identify the levels (as is the case with Ensign and Command post) you may map the Nimsoft levels to the corresponding level in the receiving system by specifying the correct code here.

Status Tab

The **Status** tab displays statistics for the traffic that has been generated via the different profiles since last restart of the SNMP Gateway.



Chapter 4: snmpgtw QoS Metrics

The *snmpgtw* probe does not generate any QoS. Therefore, there are no probe checkpoint metrics to be configured for this probe.