TECHNICAL PAPER

NETOP™

RemoteControl

Secure Remote Management and Support

How to set up Simple Network Management Protocol (SNMP) for Netop Remote Control

Netop

Netop develops and sells software solutions that enable swift, secure and seamless transfer of video, screens, sounds and data between two or more computers over the Internet. For more information, see www.netop.com.

Table of Contents

1. Overview

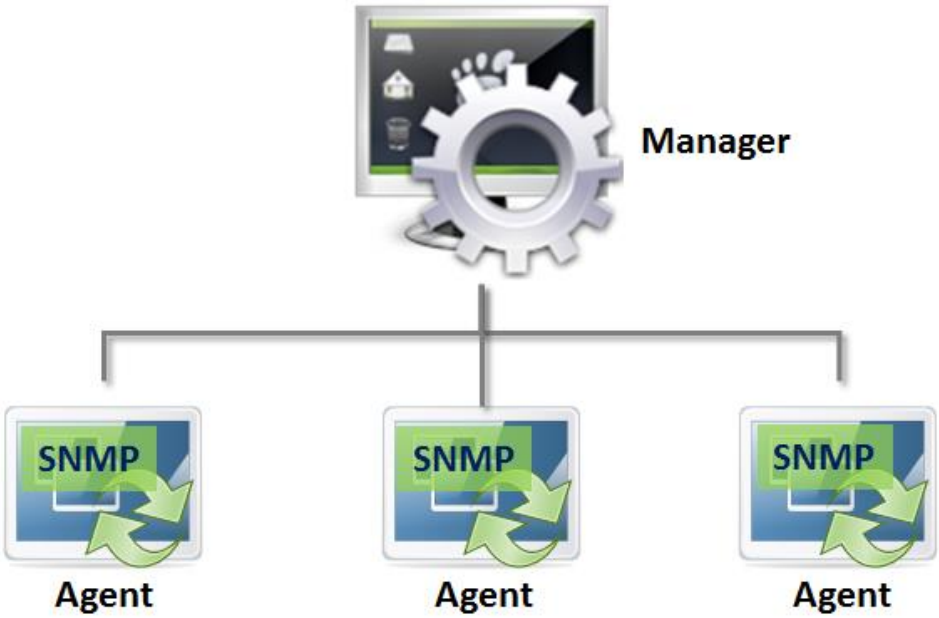
This document contains a very short description of the SNMP, what's required to get it up and running and how and what to do when making SNMP data and events from Netop Remote Control.
For more description see e.g. MSDN (Microsoft) and the Internet.

2. SNMP

Simple Network Management Protocol (SNMP) is use for managing PC's on a network. It is the SNMP Agents that are managed by the SNMP Manager.

The protocol is based on unique enterprise ID's number in the MIB (see below).

SNMP is mainly used by hardware vendors to show hardware status on a network.



2.1. System requirements

Basic requirement to run SNMP Service on a PC: Install the SNMP service from the Windows SDK.

3. Manager

The SNMP manager lets you see the trap messages/events from SNMP agents and to set/get MIB variables.

A simple SNMP manager is e.g. the SNMPc 5.0 which can be downloaded from www.castlerock.com (on a 30 days trial basis).

4. MIB

4.1. MIB Number

All SNMP events (traps), names, data etc. is assigned a unique Object ID number (OID) in the Management Information Base (MIB).

This number is assigned by www.iana.org (Internet Assigned Numbers Authority on behalf of ISO). Danware Data A/S has Private Enterprise Number 8116.

Our Enterprise MIB OID is then:

“iso.org.dod.internet.private.enterprises.Danware Data A/S” or “1.3.6.1.4.1.8116 “.

MIB file

The sub structure of the Danware MIB OID is defined in a *.MIB file. The MIB file is used by applications to translate e.g. Traps from OID’s to clear text

The defined OID’s are used in the agent code (see below) to address data.

This file can be compiled to a MIB.BIN file with the Microsoft MIB compiler (MIBCC.EXE in the SDK), se MSDN for info on how. The MIB file is used by Managers to interpret data on the network.

So if you want meaningful text on the manager display the MIB file. The MIB.BIN file must be placed on the manager PC in the **%systemroot%\system32** directory before the SNMP service is started.

Many SNMP managers can compile MIB files for internal use.

The Danware.mib is placed on our CD.

Creation syntax: `mibcc –n –oout.bin –t Danware.mib`

Copy out.bin %systemroot%\system32\mib.bin

NOTE: Make sure you do not overwrite an existing mib.bin file. To include all other vendor extension Agents, add these to the compilation. For example:

```
MIBCC -n -oOUT.BIN SMI.MIB LMMIB2.MIB MIB_II.MIB WINS.MIB DHCP.MIB
INETSRV.MIB FTP.MIB GOPHERD.MIB HTTP.MIB RoboMon.MIB Danware.MIB
```

4.2. Danware MIB structure

```
Danware (1.3.6.1.4.1.8116)
      Netop (1.3.6.1.4.1.8116.2)
            Manufacturer        (1.3.6.1.4.1.8116.2.1)
            Product             (1.3.6.1.4.1.8116.2.2)
                  Guest         (1.3.6.1.4.1.8116.2.2.1)
                  Teacher       (1.3.6.1.4.1.8116.2.2.10)
                  Host          (1.3.6.1.4.1.8116.2.2.20)
                  Nameserver    (1.3.6.1.4.1.8116.2.2.21)
                  Gateway       (1.3.6.1.4.1.8116.2.2.22)
                  LOgserver     (1.3.6.1.4.1.8116.2.2.23)
                  Accessserver  (1.3.6.1.4.1.8116.2.2.24)
                  Student       (1.3.6.1.4.1.8116.2.2.30)
            VersionNumber       (1.3.6.1.4.1.8116.2.3)
            Status              (1.3.6.1.4.1.8116.2.4)
            Traps               (1.3.6.1.4.1.8116.2.6)
                  Trap1         (1.3.6.1.4.1.8116.2.6.1)
                  Trap2         (1.3.6.1.4.1.8116.2.6.2)
                  Trapx         (1.3.6.1.4.1.8116.2.6.x)
```

For details, see also the **Danware.mib** file.

5. Agent

Netop uses the Standard Windows SNMP service.

The standard SNMP agent (Windows SNMP service) can contain (link to or include) Extension Agents from different manufacturers, e.g. Danware.

5.1. Extension Agents

The Extension Agent is a DLL made by us.

During installation it is registered in the registry for the SNMP Agents to find it: The

“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\

ExtensionAgents” will have at sub string pointing to a registry entry with the path to the extension dll. This could be

"11" = "SOFTWARE\Danware Data A/S\SNMP\ExtensionAgents\NetOpAgent".

The registry-key:

“KEY_LOCAL_MACHINE\ SOFTWARE\Danware Data A/S\SNMP\ExtensionAgents\

NetOpAgent” contains a sub string pointing at the actual dll e.g.:

"Pathname" = "C:\Program Files\Danware Data\NetOp Remote Control\Host\SNetopMP.dll".

In the Windows SNMP service, in properties, the Trap receivers, access rights etc., must be set-up.

6. Application

Static data like manufacturer, version & application info is placed in the Extension dll.

Traps (Log data) are sent from NetOp to the SNetopMP.DLL

Trap data, like explanation text and parameters is exchanged through shared memory.

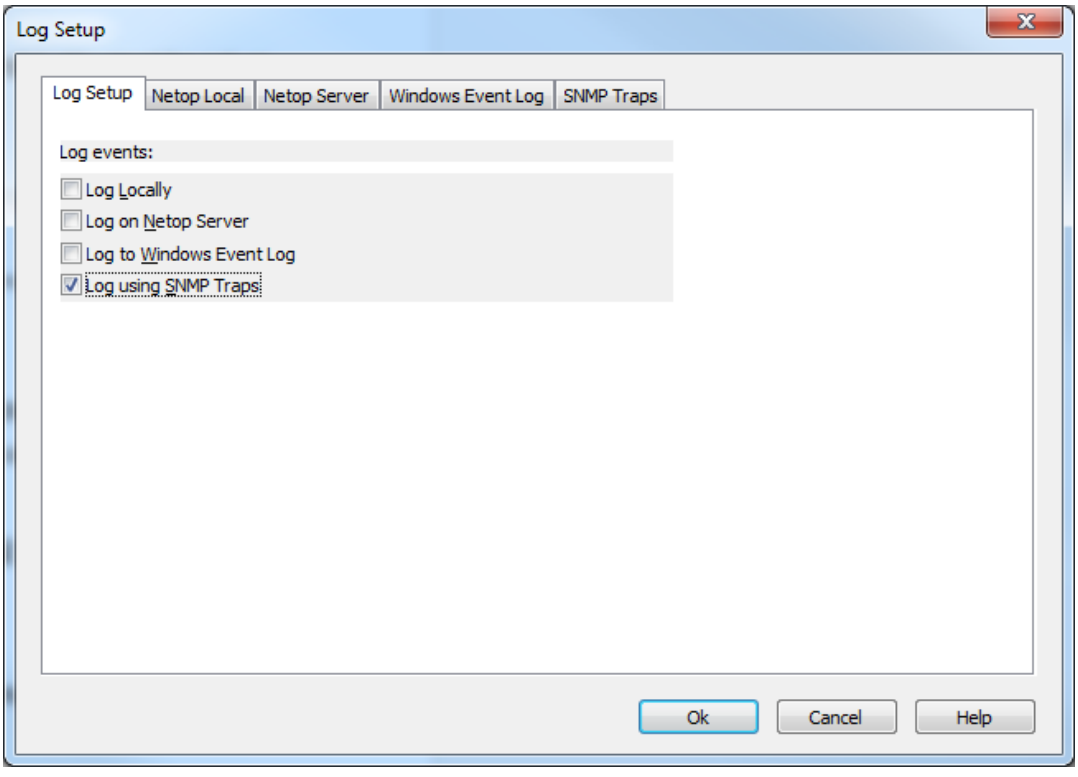
7. Netop Traps

In Netop Remote Control all the log events are implemented as possible SNMP traps.

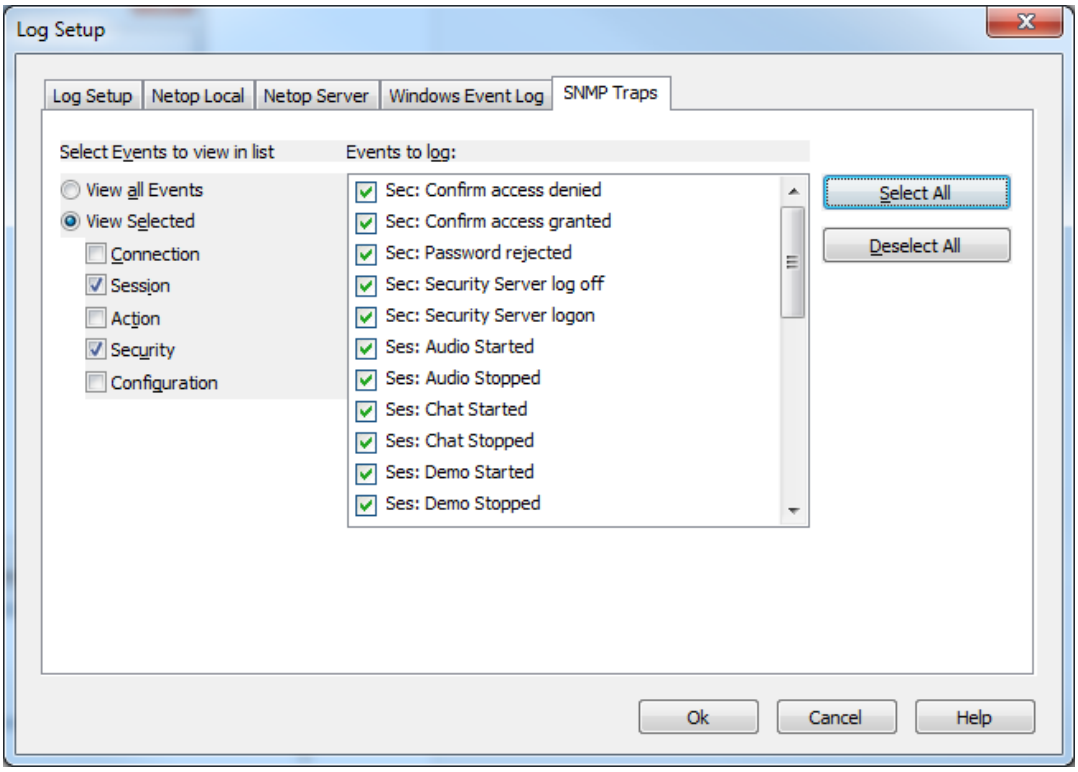
They are selectable from the event dialog as the other event types (log locally on a file, log server file and Windows event log).

8. How to set up and use Netop Remote Control SNMP

1. Install the SNMP service from the Windows SDK.
2. Install NetOp – and thereby the SNetopMP.DLL.
3. In the Netop Host or Guest (version 6.60 or newer) select **Tools** > **Log Setup**. The Log Setup window will be displayed.
4. Select the **Log using SNMP Traps** option.



5. Click the **SNMP Traps** tab and select the events which will be logged in the SNMP traps.



6. Click **Ok** and you've finished the setup.