

### **Handling AltiGen SNMP Traps Using Net-SNMP**

**Handling AltiGen SNMP Traps Using Net-SNMP** SNMP Trap messages are supported starting with MaxCommunications Server version 6.5. Using an SNMPv3 agent, MAXCS sends SNMP traps to the management console when alarming conditions are detected. This guide will serve as an example to cover configuring a separate PC to receive the trap from the AltiGen server, and pass the information on to a Perl script that sends an email to a predetermined address when a trap is received.

*Disclaimer: Please note that Net-SNMP, Perl, and OpenSSH are not AltiGen certified applications. AltiGen cannot ensure continued support for these products. If changes to any of these programs are made that create a problem, AltiGen may be unable to resolve the problem. Additionally, AltiGen does not carry any liability for any malfunctions or damages that may occur as a result of this document.*

*This document is created to provide a simple illustration of how SNMP messages sent from MaxCommunications server can be received and handled by a PC running an SNMP Trap service. It is NOT meant to be a reference on how to setup a full network monitoring service. The "traphandler" process can be used in conjunction with some other network monitoring solutions, however support for this is outside the scope of AltiGen support. The configuration below was tested on a clean installation of Windows XP SP 2, but should work on all current versions of Windows.*

## **Pre-requisites**

Both Perl and Net-SNMP are required for this project. In order to support encryption for the TRAP message, Net-SNMP also needs OpenSSH installed, which in turn requires Visual C++. All examples here assume that the software is installed using the default options unless specified below.

Install the Visual C++ 2008 redistributable. Be sure to use this link, rather than the "newer" version of the Visual C++ redistributables, as this is the correct one. Install OpenSSL. When prompted, select to install the OpenSSL DLLs to the Windows system directory. OpenSSL asks for a donation at the end of the installation - This is optional. Install Net-SNMP. Be sure to select the option for "Encryption Support" as shown here: Install Strawberry Perl

## **MaxCommunications Server Configuration**

Configure MaxCommunications server to send SNMP traps. In MaxAdmin, go to the "Report" drop down menu and select "SNMP Configuration"

Check "Enable SNMP traps" Use the IP address of the server you've installed Net-SNMP on as the "SNMP Management Station Address" Leave the "SNMP Management Station Port" set at 162 Set the Security Level to "Authentication and Privacy" Select your own "Security User Name". We will use "altigen" here as an example. Set the Authentication Method to "SHA" Select your own "Authentication Password". We will use "22222222" as an example. This password must be a minimum of 8 characters long. Set the Privacy Protocol to "DES" There is currently a bug (6.5.1.514) that prevents 3DES and AES from working. Until this is resolved only use DES. Select your own "Privacy Password". We will use "22222222" as an example. This password

must be a minimum of 8 characters long.

## Set Net-SNMP as a Windows service

Once all of the pre-requisites are installed, configuration of the software can begin. Using the batch file that is included with Net-SNMP, set the Net-SNMP Trap service to run as a Windows service. This batch file can be found in the Windows start menu:

### snmptrapd.conf

The Net-SNMP configuration file for the trap service (snmptrapd.exe) will be located in C:\usr\etc\snmp, and named "snmptrapd.conf". Download this configuration file and extract it to that location. Open it with a text editor (notepad will be fine here) for editing. Do NOT use a word processing program such as WinWord.exe to edit the file. The text of this file can be found here.

This document can be thought of in three parts: The logging section, the authentication section, and the trap handling section. The example document is commentated to show where each of these sections begins and ends. Lines that start with a "#" symbol are comments, and are not read by the snmptrapd.exe program. For the sake of brevity, only uncomment lines will be shown below. After making any changes in this file, the snmptrapd service must be restarted in order for the changes to take effect.

### Logging

The section for logging describes how to format the log file and where it should be located. This section should be left as is.

```
format2 [%y-%m-%l %h:%j:%k] Trap From %b\nSecurity information: %P\nvarbinds: %v\n\n logoption f
C:/usr/log/snmptrapd.log.txt
```

### Authentication

This section corresponds to the authentication and privacy settings previously configured on the AltiGen server. Following the example above, the configuration file will read as below. If you are using a different user name and/or password than the example, edit the file accordingly.

```
createUser -e 0x433a5c416c7469536572765c4578655c616c7469736572762e657865 altigen SHA
22222222 DES 22222222 createUser -e 0x433a5c416c7469536572765c4578655c5350536572762e657865
altigen SHA 22222222 DES 22222222 createUser -e
0x433a5c416c7469536572765c4578655c416c74694b6565702e657865 altigen SHA 22222222 DES
22222222
```

The format for these lines is:

```
createUser -e [engineID] [user name] [Auth Method] [Auth Password] [Privacy Method] [Privacy Password]
```

The reason that there are three separate lines is that there are three separate AltiGen programs that can potentially send SNMP Trap messages (AltiServ.exe, AltiKeep.exe, and SPServ.exe). Each of the hex strings

listed corresponds to the full path name on the MaxCommunications server to that executable. For example, "0x433a5c416c7469536572765c4578655c616c7469736572762e657865" is "C:\Altiserv\Exe\altiserv.exe" written as hex.

The "authUser" line indicates that when the specified user is authenticated, the message should be logged, and allowed to be handed.

```
authUser log,execute altigen
```

## Trap Handling

Net-SNMP's "traphandle" directive allows the information in the received trap to be passed to another program. Although it is possible to direct this information to different programs based on the OID, we will use the "default" option here. "traptoemail" is an example Perl scrip that is included with Net-SNMP that does exactly what the script name says. The emails sent from this script do not perform any authentication, etc. Although this may work with your mail server using the -s option if your mail server and the SNMP trap server are on the same LAN, you may also look at omitting the -s option, and configuring this similar to the manner in which MaxCommunications server currently handles mail. It is not AltiGen's responsibility to provide for email configuration for your environment. The following should all be on a single line in the configuration file.

```
traphandle default C:\strawberry\perl\bin\perl.exe C:/usr/bin/traptoemail -s yourmailserver.yourdomain.com -f yourusername@yourdomain.com targetuser@targetdomain.com
```

## Testing

Once the configuration is done, you can start snmptrapd from the command shell. To do this open, run cmd.exe and type the following at the prompt:

```
C:\usr\bin\snmptrapd.exe -Lo
```

This can be explained as:

C:\usr\bin\snmptrapd.exe - This is the path to the snmptrapd executable. -Lo - This means to log the trap information to "standard output" (in other words, the same command shell you're invoking this command from).

Once you have done this, you should see the following line:

```
NET-SNMP version 5.5
```

Next, generate a trap message from the AltiGen server. The easiest way to do this with the least amount of impact on a running server is to restart the CT-Proxy service (this will cause all instances of MaxClients to drop). If downtime is less critical, you could also unplug a live PRI and then reconnect it.

Because the traps are logging to standard output, you will see them in this screen:

## Starting the service

Once you have finished testing, and are satisfied that the trap handler is working, open the Windows services console (services.msc) and locate the "Net-SNMP Trap Handler" service, and start it. Run one more test to make sure that everything is working. You now have a server that will receive traps from a MaxCommunications server and send them to an email address.

<https://know.altigen.com/questions/1061/>