

How to Configure SNMP on Apple OS devices

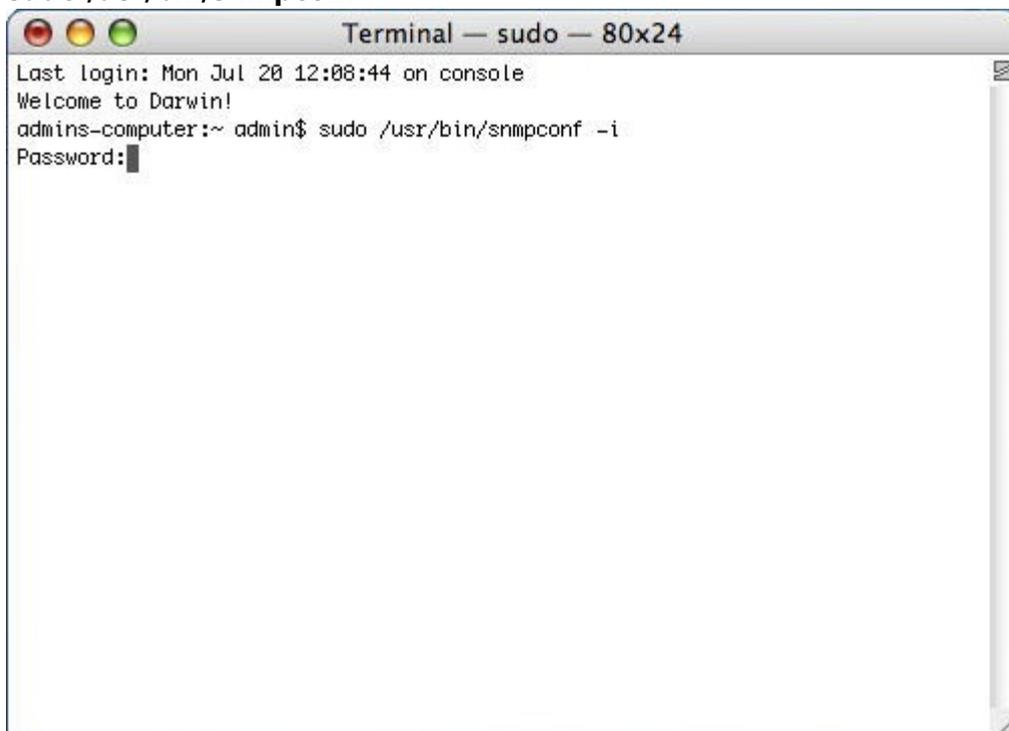
<https://campus.barracuda.com/doc/98217199/>

In order to monitor Macintosh computers running Apple OS X using the default Barracuda RMM policy module, the operating system must be configured to use SNMP. Even if you are not monitoring the operating system itself, if there are any SNMP-enabled applications being monitored on the device, the operating system must also be SNMP-enabled.

To configure SNMP on Apple OS devices, log in with Administrative rights and complete the following steps:

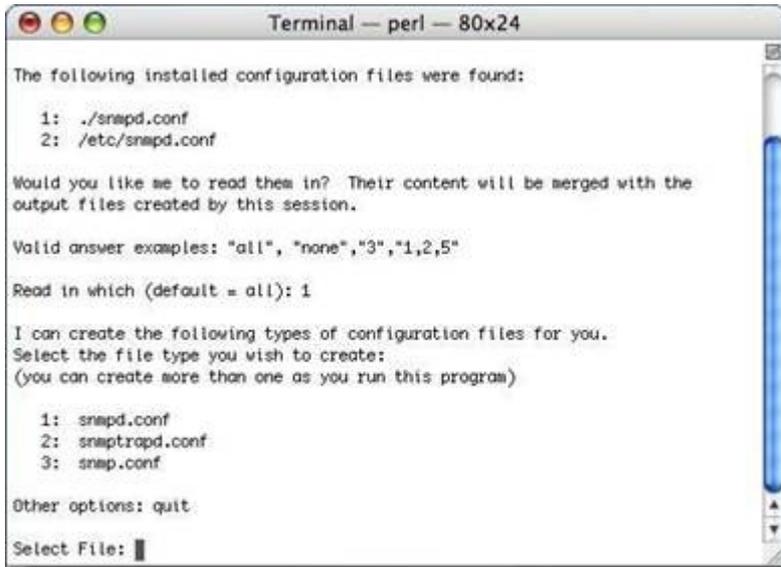
1. Launch a terminal window and issue the following command (you will be prompted to enter your password):

sudo /usr/bin/snmpconf -i



Using the argument `-i` ensures that the file is overwritten with the new settings you are about to choose. Taking a backup of the files before proceeding is prudent.

2. The system presents you with a list of the installed configuration files. Select the first file presented, which should be **./snmp.conf**.



```

Terminal — perl — 80x24

The following installed configuration files were found:

 1: ./snmpd.conf
 2: /etc/snmpd.conf

Would you like me to read them in? Their content will be merged with the
output files created by this session.

Valid answer examples: "all", "none", "3", "1,2,5"

Read in which (default = all): 1

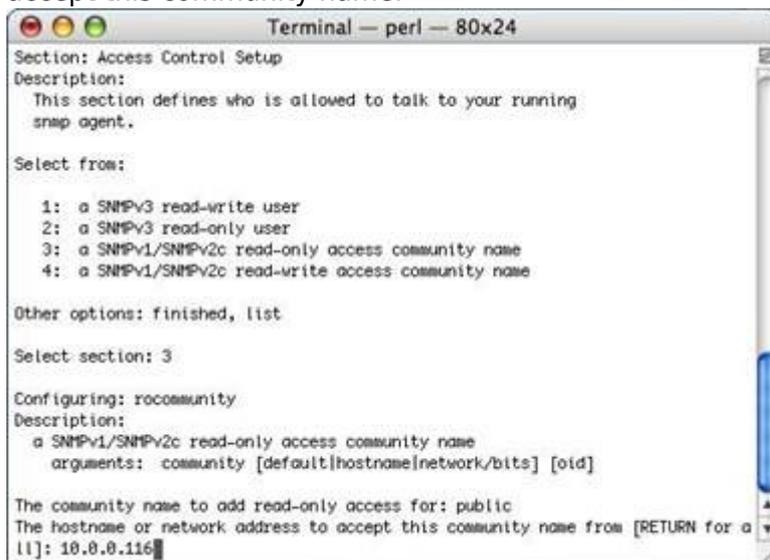
I can create the following types of configuration files for you.
Select the file type you wish to create:
(you can create more than one as you run this program)

 1: snmpd.conf
 2: snmptrapd.conf
 3: snmp.conf

Other options: quit

Select File: █
  
```

3. The configuration utility requires that you make selections by choosing the number representing your choice.
The system offers you a choice of what file to create. The default Barracuda RMM policy module for Apple Macs does not require configuration of SNMP traps, so select `snmpd.conf` to configure the daemon for SNMP.
4. You are now asked which sections of the `snmpd.conf` file you wish to work with. First, select **Access Control Setup**.
5. Select an SNMPv1/SNMPv2c read-only access community name.
 - Enter the community string matching the one that you have configured your Onsite Manager to use. By default, Onsite Manager reads the public community, so this is an acceptable choice under most circumstances.
 - When prompted, enter the IP address of the Onsite Manager as the network address to accept this community name.



```

Terminal — perl — 80x24

Section: Access Control Setup
Description:
  This section defines who is allowed to talk to your running
  snmp agent.

Select from:

 1: a SNMPv3 read-write user
 2: a SNMPv3 read-only user
 3: a SNMPv1/SNMPv2c read-only access community name
 4: a SNMPv1/SNMPv2c read-write access community name

Other options: finished, list

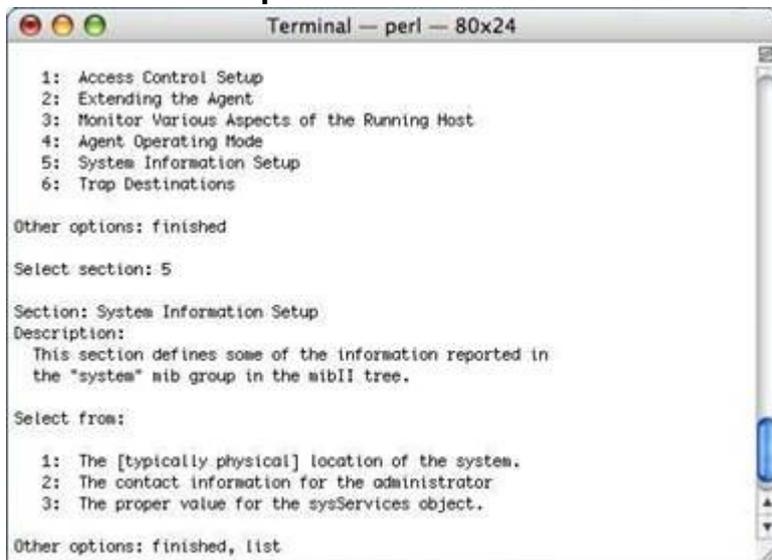
Select section: 3

Configuring: rocommunity
Description:
  a SNMPv1/SNMPv2c read-only access community name
arguments: community [default|hostname|network/bits] [oid]

The community name to add read-only access for: public
The hostname or network address to accept this community name from [RETURN for a
ll]: 10.0.0.116█
  
```

6. Enter **finished** and click **return** to go back to the top-level menu. Next, configure the information that Onsite Manager reads as part of device discovery. Choose **System**

Information Setup.



```
Terminal — perl — 80x24

1: Access Control Setup
2: Extending the Agent
3: Monitor Various Aspects of the Running Host
4: Agent Operating Mode
5: System Information Setup
6: Trap Destinations

Other options: finished

Select section: 5

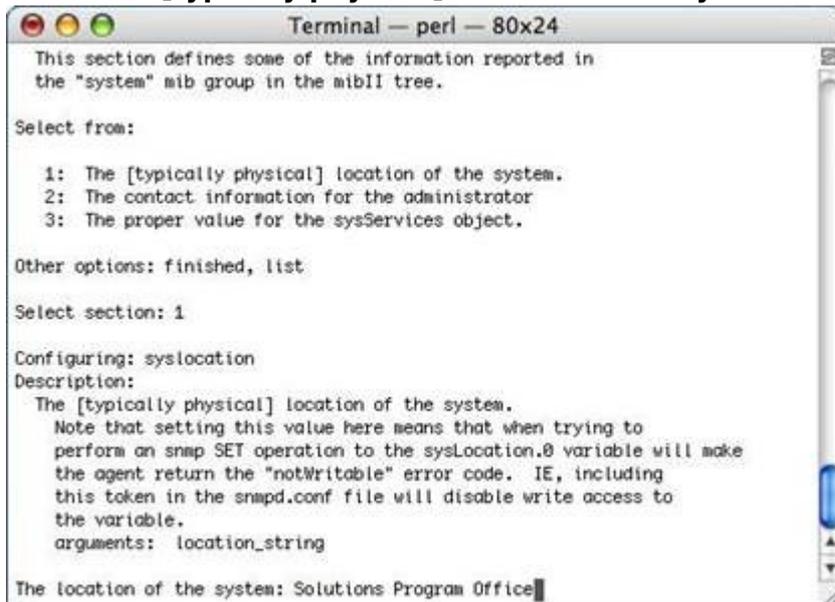
Section: System Information Setup
Description:
  This section defines some of the information reported in
  the "system" mib group in the mibII tree.

Select from:

1: The [typically physical] location of the system.
2: The contact information for the administrator
3: The proper value for the sysServices object.

Other options: finished, list
```

7. Select **The [typically physical] location of the system.**



```
Terminal — perl — 80x24

This section defines some of the information reported in
the "system" mib group in the mibII tree.

Select from:

1: The [typically physical] location of the system.
2: The contact information for the administrator
3: The proper value for the sysServices object.

Other options: finished, list

Select section: 1

Configuring: syslocation
Description:
  The [typically physical] location of the system.
  Note that setting this value here means that when trying to
  perform an snmp SET operation to the sysLocation.0 variable will make
  the agent return the "notWritable" error code. IE, including
  this token in the snmpd.conf file will disable write access to
  the variable.
  arguments: location_string

The location of the system: Solutions Program Office
```

This information is captured as the Text OID `sysLocation.0`.

8. Select the contact information for the administrator and type an appropriate contact value.

```

Terminal — perl — 80x24

1: The [typically physical] location of the system.
2: The contact information for the administrator
3: The proper value for the sysServices object.

Other options: finished, list

Select section: 2

Configuring: syscontact
Description:
  The contact information for the administrator
  Note that setting this value here means that when trying to
  perform an snmp SET operation to the sysContact.0 variable will make
  the agent return the "notWritable" error code. IE, including
  this token in the snmpd.conf file will disable write access to
  the variable.
  arguments: contact_string

The contact information: sporter@levelplatforms.com

Finished Output: syscontact sporter@levelplatforms.com

Section: System Information Setup
  
```

9. Enter finished and hit **return**. Repeat and then type quit and hit **return**. You are prompted with a note that the file exists. Type overwrite and hit **return**.

```

Terminal — perl — 80x24

3: Monitor Various Aspects of the Running Host
4: Agent Operating Mode
5: System Information Setup
6: Trap Destinations

Other options: finished

Select section: finished

I can create the following types of configuration files for you.
Select the file type you wish to create:
(you can create more than one as you run this program)

1: snmpd.conf
2: snmptrapd.conf
3: snmp.conf

Other options: quit

Select File: quit

Error: An snmpd.conf file already exists in this directory.

'overwrite', 'skip', 'rename' or 'append'? : overwrite
  
```

To add a community string to the network scan for a site, follow the steps below:

1. In Service Center, click **Configuration**, then click **Site Management**.
2. Click the site for which you want to edit the scan settings.
3. Click the **Network Discovery** tab.
4. In the **Network Scan (Local Network)** section, click **Modify**.
5. In the **SNMP V1/V2 Community Strings** section, click **Add**.
6. Type the community string in the **Community String Name** text box.
Community strings are case-sensitive. For example, Public and public would be separate communities of SNMP devices.
7. Optionally, type a description in the Description text box.

8. Click **Save**.

Figures

1. snmp1.png
2. snmp2.png
3. snmp3.png
4. snmp4.png
5. snmp5.png
6. snmp6.png
7. snmp7.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.