



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Framework Deployment Guide

SNMP Prerequisites

SNMP Prerequisites

Contents

- **1 SNMP Prerequisites**
 - **1.1 Installing Net-SNMP**
 - **1.2 Starting and Stopping Net-SNMP**

Starting in release 8.5.1, you can use Net-SNMP, instead of the Genesys SNMP Master Agent component, to implement SNMP functionality. Net-SNMP supports everything that Genesys SNMP Master Agent does. Genesys strongly recommends that you use the newest version of Net-SNMP Master Agent to make your SNMP configuration as robust as possible.

Net-SNMP and Genesys SNMP Master Agent can run in parallel on the same system, if the following conditions are met:

- Only one SNMP Master Agent can be configured on each Solution Control Server (SCS).
- The ports used by each SNMP Master Agent must be unique, and not used by any other application.

Solution Control Server and Local Control Agent support both implementations.

Installing Net-SNMP

If you choose to use Net-SNMP in addition to, or instead of, Genesys SNMP Master Agent, you must install Net-SNMP on all hosts where you need an SNMP Master Agent to reside. Use the following instructions, according to the operating system running on that host.

Windows 64-bit

To install and configure Net-SNMP on Windows 64-bit Platforms, use the following steps:

1. Download and run Net-SNMP as follows: **[+] Show steps**

- In a web browser, go to <http://sourceforge.net/projects/net-snmp/files/net-snmp%20binaries/5.5-binaries/> and download **net-snmp-5.5.<version>.x64.exe**, where <version> is the latest stable version of the file available.
- Run the downloaded file, making the following selections on the **Choose Components** screen of the Net-SNMP 5.5 Setup Wizard:
 - Expand **Net-SNMP Agent Services** and select **With Windows Explorer**
 - **Net-SNMP Trap Services**
 - **Perl SNMP Modules**

All binaries are created in the installed folder specified in the **Choose Default Location** screen of the setup wizard.

2. Register (or unregister, if required) the Net-SNMP Services by running the appropriate **.bat** file, all of which are located in the Net-SNMP installation folder. **[+] Show files**

:

To Do This ...	To This Service ...	Run this File
Register	Net-SNMP agent	registeragent.bat
	Net-SNMP trap handler	registertrapd.bat

To Do This ...	To This Service ...	Run this File
Unregister	Net-SNMP agent	unregisteragent.bat
	Net-SNMP trap handler	unregistertrapd.bat

After registration, the files are located in the following locations: **[+] Show file locations**

Note: The file locations given in the table are by default, based on the default location specified in Step 1.

Files	Location
snmpd.conf	C:\usr\etc\snmp\snmpd.conf
snmpd.conf (persistent)	C:\usr\snmp\persist\snmpd.conf
snmptrapd.conf	C:\usr\etc\snmp\snmptrapd.conf
Log files	C:\usr\log\snmpd.log

3. Modify the Net-SNMP configuration file, **snmpd.conf** to define system-specific parameters, as follows: **[+] Show steps**

- a. To open the UDP port through which SCS can communicate with the SNMP Master Agent, add the following line to the configuration file:

```
agentaddress udp:<port_num>
```

where <port_num> is any valid port number. This port must not be used by any other process.

You can check if the port has been opened successfully by running the following command:

```
C:\>netstat -aon | findstr <port_num>
```

If it shows the port, then the port is open.

- b. To enable AgentX functionality and open the AgentX port, add the following lines to the configuration file:

```
master agentx
agentxsocket tcp:<host_address>:<port_num>
```

where:

- <host_address> is the IP address of the host on which Net-SNMP is running.
- <port_num> is any valid port number. This port must not be used by any other process.

- c. Configure the SNMP version. Do one of the following:

- For SNMP v1 or SNMP v2, add the following lines to the configuration file:

```
rocommunity public
rwcommunity private
```

These parameters are similar to the **read_community** and **write_community** configuration options in an SNMP Master Agent.

- For SNMP v3, add the following lines to the configuration file:

```
# VACM configuration entries
rwuser <username>
```

```
# create and add a user
createUser <username> MD5 <md5_password> <DES des_password>
```

You can check if SNMP v3 has been configured successfully by running the following command:

```
C:\>snmpget -v3 -u <username> -n "" -l authNoPriv -a MD5 -A <md5_password>
<localhost> sysUpTime.0
```

If any output is displayed, then SNMP v3 has been successfully configured.

You can also create another user based on the initial user by running the following command:

```
C:\>snmpusm -v3 <username> -u initial -n "" -l authNoPriv -a MD5 -A <md5_password>
<localhost> create <newuser> initial
```

4. Configure the MIB Browser for the version of SNMP you are using. Do one of the following: **[+] Show settings**

For SNMP v1 or SNMP v2, set the following:

- SNMP version
- Number of port on which **snmpd** is running

For SNMP v3, set the following:

- SNMP version
- User profile name
- Security user name
- Number of SNMP port on which **snmpd** is running
- Authentication protocol
- Privacy protocol

5. Modify the Net-SNMP configuration file, **snmpd.conf**, to define where SNMP traps are to be sent, as follows: **[+] Show changes**

For SNMP v1 traps, add the line:

```
trapsink <transport>:<host_address>:<port>
```

where:

- <transport> can be udp or tcp.
- <host_address> is the IP address of the host to where SNMP traps are to be sent.
- <port> is the SNMP port on which traps are to be received.

For SNMP v2 traps, add the line:

```
trap2sink <transport>:<host_address>:<port>
```

where:

- <transport> can be udp or tcp.
- <host_address> is the IP address of the host to where SNMP traps are to be sent.

- <port> is the SNMP port on which traps are to be received.

For SNMP v3 traps, add the line:

```
trapsess -v 3 -u <username> -l authNoPriv -Ci -a MD5 -A "<authentication_password>"  
<host_address>:<port>
```

where:

- <host_address> is the IP address of the host to where SNMP traps are to be sent.
- <port> is the SNMP port on which traps are to be received.

6. Prepare start and stop scripts to start and stop Net-SNMP as a service, as shown below. The path and filename of these scripts are stored in the annex of the SNMP Master Agent Application objects.

Start script, for example **startsnmp.bat**

```
net start "<netsnmp_servicename>"  
net start "<netsnmptrap_servicename>"
```

Stop script, for example **stopsnmp.bat**

```
net stop "<netsnmp_servicename>"  
net stop "<netsnmptrap_servicename>"
```

Linux 64-bit

Prerequisites:

- You must be logged in as root.
- The Red Hat Package Manager (RPM) files (RPMs) must have execute permission. If you are unsure, give full permission by running the following command:

```
$chmod -R 777 *
```

To install and configure Net-SNMP on Linux 64-bit Platforms, use the following steps:

1. Download and install the RPM files, as follows: **[+] Show steps**

.

a. Download the following RPM files from <http://rpmfind.net>:

- **net-snmp-libs-<version>.el5**
- **net-snmp-<version>.el5**

where <version> is the latest stable version of the files available.

b. Install the rpm files using the command:

```
$rpm -ivh <rpm file name>
```

The installation places the Net-SNMP files in the following locations, unless otherwise specified during the installation: **[+] Show files**

Files	Location
snmpd.conf	/usr/local/etc/snmp/snmpd.conf
snmpd.conf (persistent)	/var/net-snmp/snmpd.conf
snmptrapd.conf	/var/net-snmp/snmptrapd.conf
Log file	/var/log/snmpd.log
Snmpd.exe (application)	/usr/local/sbin/snmpd
Snmptrapd.exe (application)	/usr/local/sbin/snmptrapd
Init.d script required for running snmpd and snmptrapd	/etc/init.d/snmpd

2. Modify the Net-SNMP configuration file, **snmpd.conf** to define system-specific parameters, as follows: **[+] Show steps**

- a. To open the UDP port through which SCS can communicate with the SNMP Master Agent, add the following line to the configuration file:

```
agentaddress <transport>:<port_num>
```

where:

- <transport> is the type of port to be opened, either udp or tcp. A UDP port is preferred, since it is faster than TCP.
- port_num is any valid port number. This port must not be used by any other process.

You can check if the port has been opened successfully by running the following command:

```
$netstat -aon | findstr <port_num>
```

If it shows the port, then the port is open.

- b. To enable agentx functionality and open the agentX socket, add the following lines to the configuration file:

```
master agentx
Agentxsocket tcp:<host_address>:<port_num>
```

where:

- <host_address> is the IP address of the host on which Net-SNMP is running.
- <port_num> is any valid port number. This port must not be used by any other process.

- c. Configure the SNMP version. Do one of the following:

- For SNMP v1 or SNMP v2, add the following lines to the configuration file:

```
rocommunity public
rwcommunity private
```

These parameters are similar to the **read_community** and **write_community** configuration options in an SNMP Master Agent.

- For SNMP v3, add the following lines to the configuration file:

```
# VACM configuration entries
rwuser username
# create and add a user
createUser username MD5 md5_password DES des_password
```

You can check if SNMP v3 has been configured successfully by running the following command:

```
$snmpget -v3 -u <username> -n "" -l authNoPriv -a MD5 -A <md5_password>
<localhost> sysUpTime.0
```

If any output is displayed, then SNMP v3 has been successfully configured.

You can also create another user based on the initial user by running the following command:

```
$snmpusm -v3 <username> -u initial -n "" -l authNoPriv -a MD5 -A <md5_password>
<localhost> create <newuser> initial
```

3. Configure the MIB Browser for the version of SNMP you are using. Do one of the following: **[+] Show settings**

For SNMP v1 or SNMP v2, set the following:

- SNMP version
- Number of port on which **snmpd** is running

For SNMP v3, set the following:

- SNMP version
- User profile name
- Security user name
- Number of SNMP port on which **snmpd** is running
- Authentication protocol
- Privacy protocol

4. Modify the Net-SNMP configuration file, **snmpd.conf**, to define where SNMP traps are to be sent, as follows: **[+] Show changes**

For SNMP v1 traps, add the line:

```
trapsink <transport>:<host_address>:<port>
```

where:

- <transport> is the type of port through which the traps will be sent, either udp or tcp. A UDP port is preferred, since it is faster than TCP.

- <host_address> is the IP address of the host to where SNMP traps are to be sent.
- <port> is the SNMP port on which traps are to be received.

For SNMP v2 traps, add the line:

```
trap2sink <transport>:<host_address>:<port>
```

where:

- <transport> is the type of port through which the traps will be sent, either udp or tcp. A UDP port is preferred, since it is faster than TCP.
- <host_address> is the IP address of the host to where SNMP traps are to be sent.
- <port> is the SNMP port on which traps are to be received.

For SNMP v3 traps, add the line:

```
trapsess -v3 -u <username> -l authNoPriv -Ci -a MD5 -A "<authentication_password>"  
<host_address>:<port>
```

where:

- <host_address> is the IP address of the host to where SNMP traps are to be sent.
- <port> is the SNMP port on which traps are to be received.

5. Prepare start and stop scripts, based on the commands provided in [Starting and Stopping Net-SNMP](#). The path to these scripts are stored in the annex of the SNMP Master Agent Application objects.

AIX 64-bit

Prerequisites:

- You must be logged in as root.
- The RPM files must have execute permission. If you are unsure, give full permission by running the following command:

```
$chmod -R 777 *
```

To install and configure Net-SNMP on AIX 64-bit Platforms, use the following steps:

1. Download and install the RPM files, as follows: **[+] Show steps**
 - a. Download the following RPM files from <ftp://www.oss4aix.org/RPMS/net-snmp/>:
 - **net-snmp-<version>.ppc.rpm**
 - **net-snmp-utils-<version>.ppc.rpm**where <version> is the latest stable version of the files available.
 - b. Install the rpm files using the command:

```
$rpm -ivh <rpm file name>
```

The installation places the Net-SNMP files in the following locations, unless otherwise specified during the installation: **[+] Show files**

Files	Location
snmpd.conf	/opt/freeware/etc/snmp/snmpd.conf
snmptrapd.conf	/opt/freeware/etc/snmp/snmptrapd.conf
Log file	/var/log/snmpd.log
Snmpd (application)	opt/freeware/sbin/snmpd
Snmptrapd.exe (application)	opt/freeware/sbin/snmptrapd
Init.d script required for running snmpd	/etc/rc.d/init.d/snmpd
Init.d script required for running snmptrapd	/etc/rc.d/init.d/snmptrapd

2. Add the path of the snmpd binary to the PATH environment variable, as follows: **[+] Show steps**

a. To add the path (**opt/freeware/sbin/** if using the default locations) to the path, enter:

```
PATH=$PATH:opt/freeware/sbin
```

b. To confirm the result, enter:

```
echo $PATH
```

The new path, including the path to the Snmpd binary, is displayed.

3. Modify the Net-SNMP configuration file, **snmpd.conf**, to define system-specific parameters, as follows: **[+] Show steps**

a. To open the port through which SCS communicates with the SNMP Master Agent, add the following line to the configuration file:

```
agentaddress <transport>:<port_num>
```

where:

- <transport> is the type of port to be opened, either udp or tcp. A UDP port is preferred, since it is faster than TCP.
- port_num is any valid port number. This port must not be used by any other process.

You can check if the port has been opened successfully by running the following command:

```
$netstat -aon | findstr <port_num>
```

If it shows the port number, then the port is open.

b. To enable agentx functionality and open the agentX port, add the following lines to the configuration file:

```
master agentx
Agentxsocket tcp:<host_address>:<port_num>
```

where:

- <host_address> is the IP address of the host on which Net-SNMP is running.
- <port_num> is any valid port number. This port must not be used by any other process.

c. Configure the SNMP version. Do one of the following:

- For SNMP v1 or SNMP v2, add the following lines to the configuration file:

```
rocommunity public
rwcommunity private
```

These parameters are similar to the **read_community** and **write_community** configuration options in an SNMP Master Agent.

- For SNMP v3, add the following lines to the configuration file:

```
# VACM configuration entries
rwuser username
# create and add a user
createUser username MD5 md5_password DES des_password
```

You can check if SNMP v3 has been configured successfully by running the following command:

```
$snmpget -v 3 -u <username> -n "" -l authNoPriv -a MD5 -A <md5_password>
<localhost> sysUpTime.0
```

If any output is displayed, then SNMP v3 has been successfully configured.

You can also create another user based on the initial user by running the following command:

```
$snmpusm -v3 <username> -u initial -n "" -l authNoPriv -a MD5 -A <md5_password>
<localhost> create <newuser> initial
```

4. Configure the MIB Browser for the version of SNMP you are using. Do one of the following: **[+] Show settings**

For SNMP v1 or SNMP v2, set the following:

- SNMP version
- Port number on which **snmpd** is running

For SNMP v3, set the following:

- SNMP version
- User profile name
- Security user name

- SNMP port number, the port on which **snmpd** is running
- Authentication protocol
- Privacy protocol

5. Modify the Net-SNMP configuration file, **snmpd.conf**, to define where SNMP traps are to be sent, as follows: **[+] Show changes**

For SNMP v1 traps, add the line:

```
trapsink <transport>:<host_address>:<port>
```

where:

- <transport> is the type of port through which the traps will be sent, either udp or tcp. A UDP port is preferred, since it is faster than TCP.
- <host_address> is the IP address of the host to where SNMP traps are to be sent.
- <port> is the SNMP port on which traps are to be received.

For SNMP v2 traps, add the line:

```
trap2sink <transport>:<host_address>:<port>
```

where:

- <transport> is the type of port through which the traps will be sent, either udp or tcp. A UDP port is preferred, since it is faster than TCP.
- <host_address> is the IP address of the host to where SNMP traps are to be sent.
- <port> is the SNMP port on which traps are to be received.

For SNMP v3 traps, add the line:

```
trapsess -v 3 -u <username> -l authNoPriv -Ci -a MD5 -A "<authentication_password>"  
<host_address>:<port>
```

where:

- <host_address> is the IP address of the host to where SNMP traps are to be sent.
- <port> is the SNMP port on which traps are to be received.

6. Prepare start and stop scripts, based on the commands in [Starting and Stopping Net-SNMP](#). The path to these scripts are stored in the annex of the SNMP Master Agent Application objects.

Solaris 10 64-bit

Prerequisites:

- You must be logged in as root, with execute permission. If you are unsure, give full permission by

running the following command:

```
$chmod -R 777 *
```

To install and configure Net-SNMP on Solaris 10 64-bit Platforms, do the following steps:

1. Download and install the Net-SNMP package files, as follows: **[+] Show steps**

- a. Download the **netsnmp-5.7-sol10-sparc-local.gz** file from <ftp://sunfreeware.saix.net/pub/solaris-freeware/sparc/10/>, and extract it with the following command:

```
$gunzip netsnmp-5.7-sol10-sparc-local.gz
```

- b. Install the extracted file as follows:

```
$pkgadd -d netsnmp-5.7-sol10-sparc-local
```

If the error message `Pkgadd command not found` appears, update the PATH environment variable, as follows:

```
$PATH=$PATH:/usr/sfw/bin:/usr/ccs/bin:/usr/sbin
```

To view the list of installed packages, enter the following command:

```
$pkginfo
```

To view the list of files installed by the packages, enter the following command:

```
$pkgchk -v <packagename>
```

To determine what file belongs to which package, enter the following command:

```
$ pkgchk -l -p <path_to_file/filename>
```

The installation places the Net-SNMP files in the following locations, unless otherwise specified during the installation: **[+] Show files**

Files	Location
snmpd.conf	/etc/opt/csw/snmp/snmpd.conf
snmptrapd.conf	/etc/opt/csw/snmp/snmptrapd.conf
Log file	/var/opt/csw/log/snmpd.log
Snmpd (application)	opt/csw/sbin/snmpd
Snmptrapd.exe (application)	opt/csw/sbin/snmptrapd
Init.d script required for running snmpd	/etc/rc.d/init.d/snmpd
Init.d script required for running snmptrapd	/etc/rc.d/init.d/snmptrapd

2. Add the path of the Snmpd binary to the PATH environment variable, as follows: **[+] Show steps**

- a. To add the path (**opt/csw/sbin** if using the default locations) to the path, enter:

```
PATH=$PATH:opt/csw/sbin
```

- b. To confirm the result, enter:

```
echo $PATH
```

The new path, including the path to the Snmpd binary, is displayed.

Note: If you log in with a new session, you must add the path again.

3. Modify the Net-SNMP configuration file, **snmpd.conf**, to define system-specific parameters, as follows:
[+] Show steps

- a. To open the port through which SCS communicates with the SNMP Master Agent, add the following line to the configuration file:

```
agentaddress <transport>:<port_num>
```

where:

- <transport> is the type of port to be opened, either `udp` or `tcp`. A UDP port is preferred, since it is faster than TCP.
- `port_num` is any valid port number. This port must not be used by any other process.

You can check if the port has been opened successfully by running the following command:

```
$netstat -aon | findstr <port_num>
```

If it shows the port, then the port is open.

- b. To enable agentx functionality and open the agentX port, add the following lines to the configuration file:

```
master agentx  
Agentxsocket tcp:<host_address>:<port_num>
```

where:

- <host_address> is the IP address of the host on which Net-SNMP is running.
- <port_num> is any valid port number. This port must not be used by any other process.

- c. Configure the SNMP version. Do one of the following:

- For SNMP v1 or SNMP v2, add the following lines to the configuration file:

```
rocommunity public  
rwcommunity private
```

These parameters are similar to the **read_community** and **write_community** configuration options in an SNMP Master Agent.

- For SNMP v3, add the following lines to the configuration file:

```
# VACM configuration entries  
rwuser username  
# create and add a user  
createUser username MD5 md5_password DES des_password
```

You can check if SNMP v3 has been configured successfully by running the following command:

```
$snmpget -v 3 -u <username> -n "" -l authNoPriv -a MD5 -A <md5_password>
<localhost> sysUpTime.0
```

If any output is displayed, then SNMP v3 has been successfully configured.

You can also create another user based on the initial user by running the following command:

```
$snmpusm -v3 <username> -u initial -n "" -l authNoPriv -a MD5 -A <md5_password>
<localhost> create <newuser> initial
```

4. Configure the MIB Browser for the version of SNMP you are using. Do one of the following: **[+] Show settings**

For SNMP v1 or SNMP v2, set the following:

- SNMP version
- Port number on which **snmpd** is running

For SNMP v3, set the following:

- SNMP version
- User profile name
- Security user name
- SNMP port number, the port on which **snmpd** is running
- Authentication protocol
- Privacy protocol

5. Modify the Net-SNMP configuration file, **snmpd.conf**, to define where SNMP traps are to be sent, as follows: **[+] Show changes**

For SNMP v1 traps, add the line:

```
trapsink <transport>:<host_address>:<port>
```

where:

- <transport> is the type of port through which the traps will be sent, either udp or tcp. A UDP port is preferred, since it is faster than TCP.
- <host_address> is the IP address of the host to where SNMP traps are to be sent.
- <port> is the SNMP port on which traps are to be received.

For SNMP v2 traps, add the line:

```
trap2sink <transport>:<host_address>:<port>
```

where:

- <transport> is the type of port through which the traps will be sent, either udp or tcp. A UDP port is preferred, since it is faster than TCP.
- <host_address> is the IP address of the host to where SNMP traps are to be sent.
- <port> is the SNMP port on which traps are to be received.

For SNMP v3 traps, add the line:

```
trapsess -v 3 -u <username> -l authNoPriv -Ci -a MD5 -A "<authentication_password>"  
<host_address>:<port>
```

where:

- <host_address> is the IP address of the host to where SNMP traps are to be sent.
- <port> is the SNMP port on which traps are to be received.

6. Prepare start and stop scripts, based on the commands provided in [Starting and Stopping Net-SNMP](#). The path to these scripts are stored in the annex of the SNMP Master Agent Application objects.

Starting and Stopping Net-SNMP

If you have installed Net-SNMP on a Windows 64-bit platform, start and stop Net-SNMP as a service, using [Windows Service Manager](#).

Otherwise, use the following commands to start or stop Net-SNMP running on a UNIX host:

Action	Command
Start Net-SNMP	<code>\$service snmpd start</code>
Stop Net-SNMP	<code>\$service snmpd stop</code>
Check Net-SNMP status	<code>\$service snmpd status</code>
Restart Net-SNMP	<code>\$service snmpd restart</code>