# Using SNMP with Content Gateway (not V-Series)

Topic 60014 / Updated: 7-July-2010

| Applies To: | Websense Web Security Gateway 7.5.x<br>Websense Web Security Gateway Anywhere 7.5.x<br>Websense Content Gateway 7.5.x |
|---|---|

This article describes how to use Net-SNMP with software installations of Content Gateway (not V-Series appliances) to monitor Content Gateway processes. It assumes that the reader is familiar with SNMP.

> **Note**
> For information about using SNMP with V-Series appliances, please contact Websense Technical Support.

If you are not familiar with SNMP, an introductory article can be found in Wikipedia.

An essential resource and the location of Net-SNMP software is www.net-snmp.org.

For documentation, go to: http://net-snmp.sourceforge.net/docs/man/.

To use SNMP with Content Gateway you must:

- Install the Net-SNMP RPMs
- Configure snmpd.conf to monitor Content Gateway processes and send traps to the SNMP Manager
- Verify the configuration

## SNMP on the Content Gateway host system

Websense Content Gateway version 7.5.x is typically installed on a minimal installation of:

- Red Hat Enterprise Linux 5, update 3 or later, base or Advanced Platform (32-bit only)

RPM compat-libstdc++-33-3.2.3-61.3.i386.rpm is also required.

The minimal installation does not include Net-SNMP.

To see if Net-SNMP is installed on your system, on the command line run:

```
rpm -qa | grep snmp
```

If SNMP is installed, you will see something like:

```
net-snmp-libs-5.3.2.2-5.EL5
net-snmp-5.3.2.2-5.EL5
net-snmp-utils-5.3.2.2-5.EL5
```

**NOTE:** SELinux should be disabled when using Net-SNMP. To confirm that it is disabled, or to disable it, edit **/etc/sysconfig/selinux** and confirm or set **SELINUX=DISABLED**.

## Installing Net-SNMP

If Net-SNMP is not installed, install it now. The necessary RPMs are included with the Red Hat Enterprise Linux distribution media (disks or iso) For Release 5, Update 3 expect version 5.3.2.2-5.EL5.i386. The RPMs can also be downloaded from the Internet.

To install Net-SNMP:

1. Place the following RPMs in a temporary directory:

   ```
   net-snmp-libs-5.3.2.2-5.EL5.i386.rpm
   net-snmp-5.3.2.2-5.EL5.i386.rpm
   net-snmp-utils-5.3.2.2-5.EL5.i386.rpm
   ```

2. Install the RPMs with the following commands:

   ```
   rpm -ivh net-snmp-libs-5.3.2.2-5.EL5.i386.rpm
   rpm -ivh net-snmp-5.3.2.2-5.EL5.i386.rpm
   rpm -ivh net-snmp-utils-5.3.2.2-5.EL5.i386.rpm
   ```

After Net-SNMP is installed, it is important that you use **up2date** to get the latest Net-SNMP updates:

```
up2date -f net-snmp-libs net-snmp net-snmp-utils
```

## Starting and stopping the SNMP service

After configuration is complete (see below) or any time it is necessary to start or stop the SNMP Agent service, use the following commands:

```
[root]# service snmpd start
[root]# service snmpd stop
```

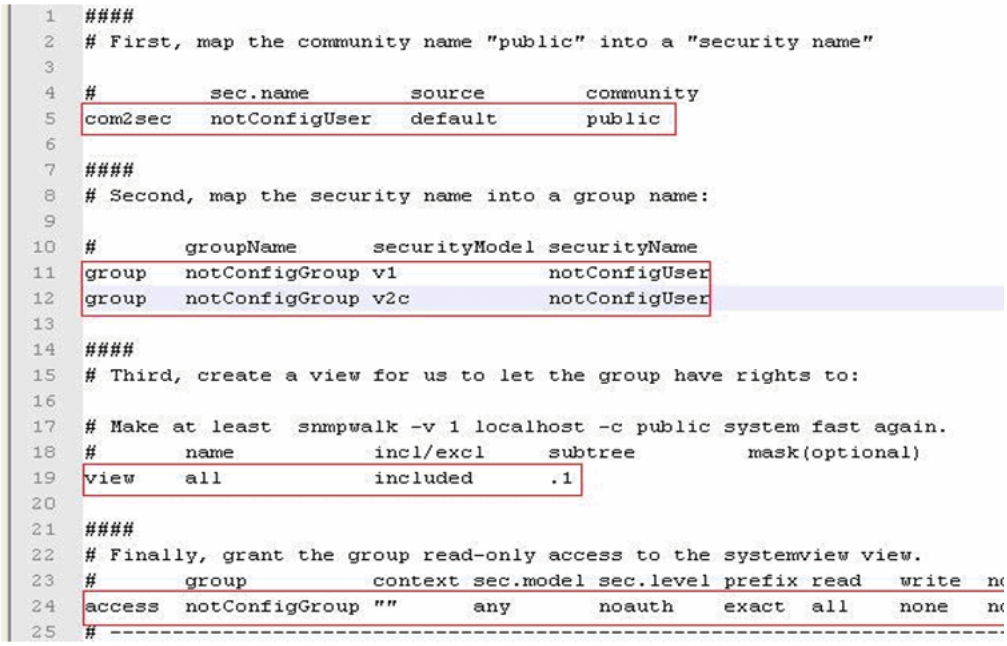
## Basic SNMP configuration:

For detailed configuration information, see the comments in **/etc/snmp/snmpd.conf** and read the man page for **snmpd.conf(5)**.

After initial installation, for security purposes the SNMP service (snmpd) responds only to queries on the system MIB.

The following example shows how to configure **snmpd.conf** to change community names and open write access to the MIB tree.

Edit **/etc/snmp/snmpd.conf**, locate the lines boxed in red in the screen capture below, and modify each line to match the example.



```
1  ####
2  # First, map the community name "public" into a "security name"
3
4  #          sec.name          source          community
5  com2sec    notConfigUser     default         public
6
7  ####
8  # Second, map the security name into a group name:
9
10 #        groupName       securityModel securityName
11 group    notConfigGroup v1            notConfigUser
12 group    notConfigGroup v2c           notConfigUser
13
14 ####
15 # Third, create a view for us to let the group have rights to:
16
17 # Make at least  snmpwalk -v 1 localhost -c public system fast again.
18 #        name            incl/excl     subtree          mask(optional)
19 view     all             included      .1
20
21 ####
22 # Finally, grant the group read-only access to the systemview view.
23 #        group           context sec.model sec.level prefix read   write  no
24 access   notConfigGroup ""      any       noauth    exact  all    none   no
25 # ----------------------------------------------------------------------
```

## Configuring SNMP to monitor and report on Content Gateway processes

To monitor Content Gateway processes, you must add the process names and MAX/MIN process values to the “Process checks” section of **snmpd.conf**. You also need to add the v2 trap specification.

Edit **/etc/snmp/snmpd.conf** and add the following lines in the “Process checks” area:

```
proc content_cop 1 1
proc content_gateway 1 1
proc content_manager 1 1
proc DownloadService 1 1
```

```
proc microdasys 2 1
proc microdasysws 1 1

# send v2 traps
trap2sink IP_address_of_SNMP_Manager:162
informsink IP_address_of_SNMP_Manager:162
rwuser all
agentSecName all
defaultMonitors yes
```

If Websense Web filtering is also running on the Content Gateway machine and you want to monitor it, add:

```
proc EIMServer 1 1
```

## Verify SNMP configuration and trap reporting

Verify that the SNMP Agent (snmpd) is sending process trap messages, and that the SNMP Manager is receiving them.

**snmptrapd** is the process used by the SNMP Manager to listen for SNMP trap messages arriving on port 162 (default). A typical **snmptrapd** startup command might look like:

```
snmptrapd -f -Ls 162
```

where "-f" means do not fork() from the calling shell, and "-Ls" specifies where logging output is sent ("-Ls" sends output to **syslog**). 162 is the standard listening port for SNMP messages. For more detailed information, read the man page for **snmptrapd**.

**NOTE:** The default trap reporting interval for Agents is 10 minutes. If the default period is used, it can take as long as 10 minutes from the time a trap occurs to when the trap message is sent to the SNMP Manager. This parameter is configurable through the snmp "set" operation of "mteTriggerFrequency".

To verify that SNMP Agent is sending trap messages:

1. On the SNMP Agent/Content Gateway machine, start a network packet analyzer and terminate the DownloadService process.
2. In the packet capture data, look for an SNMPv2-Trap message for DownloadService going to the SNMP Manager. The trap message might be similar to:

   ```
   Value: STRING: Too few DownloadService running (# = 0)
   ```

To verify that SNMP Manager is receiving trap messages:

1. On the SNMP Agent/Content Gateway machine, terminate the DownloadService process. Note that it may take several minutes from the time the trap occurs until the trap is sent to the SNMP Manager.
2. On the SNMP Manager machine, check the SNMP trap log for an entry for DownloadService. The name and location of the log file is specified in the **snmptrapd** startup command (example provided above). Here is one way to find the message if it is being logged in /var/log/messages:

   ```
   cat /var/log/messages | grep DownloadService
   ```

An entry might look like:

```
Nov 25 15:09:42 localhost snmptrapd[11980]: 10.10.10.10]: Trap,
DISPAN-EV = STRING , DISMAN-EVENT-MIB::mteHotOID = OID ,
DISMAN-EVENT-IB::prErrMessage.4 = STRING: Too few DownloadService
   running (# = 0)
```

Use **nc** (netcat) to test basic UDP connectivity between the Agent and the Manager. For example, this command could be run on either side of the connection to test the designated UDP ports.

```
[root]# nc -u -v -z -w2 10.228.85.10 161-162
```

where "-u" indicates UPD, "-v" indicates verbose output, "-z" means to scan for listening daemons, and "-w2" indicates to wait 2 seconds before timing out.

Sample results:

```
10.228.85.10: inverse host lookup failed: Unknown host
(UNKNOWN) [10.228.85.10] 161 (snmp) open
```

For more information, see the man page for **nc**.

# Connecting Content Gateway counters to SNMP counters that can be queried remotely

Net-SNMP Agent can be configured to retrieve Content Gateway counter data that can then be queried by SNMP Manager.

For example, SNMP Manager could monitor Content Gateway transaction totals. One way to do this is to:

1. Create a shell script that runs a **content_line** command. For example, in **/opt/WCG/bin** create an executable script called **example_oid.sh**:

   ```
   #!/bin/sh
   #Get the current WCG transaction total
   /opt/WCG/bin/content_line -r wtg.process.txn_total
   ```

   **NOTE:** The example script is for illustrative purposes only. There is no protection or locking to enable more than one SNMP request at a time to Content Gateway.

2. Configure **snmpd.conf** to run the script, capturing the output. Edit **snmpd.conf**. In the “extensible section” or at the end of the file add:

   ```
   exec .1.3.6.1.4.1.23365.53 example /bin/sh
      /opt/WCG/bin/example_oid.sh
   ```

3. From the SNMP Manager system, use an **snmpwalk** command to retrieve the data. For example:

   ```
   snmpwalk -v 2c -c public 10.203.152.7 .1.3.6.1.4.1.23365.53
   ```

   Visually inspect, or script the parsing of the returned data.

# Monitoring Red Hat Enterprise Linux system status with SNMP

**snmpwalk** is a query command that uses SNMP GETNEXT requests to retrieve tree values. The following are several examples of commands that return information about various aspects of system status. For more information, see the comments in **snmpd.conf**, the Linux man page for **snmpd.conf**, and www.net-snmp.org.

For all system status information:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-MIB::hrSWRun
```

or

```
[root]# snmpwalk -v 2c -c public HOST-RESOURCES-MIB::hrSWRun
```

For system information including date and time, initialized devices, kernel parameters, and more:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-MIB::hrSystem
```

For memory size, disk space, usage status, and more:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-
MIB::hrStorage
```

For device ID and descriptions:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-MIB::hrDevice
```

For process ID, process name, parameter, and status:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-MIB::hrSWRun
```

For CPU times and memory consumed by the process:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-
MIB::hrSWRunPerf
```

For installed software package names:

```
[root]# snmpwalk -v 1 -c public HOST-RESOURCES-
MIB::hrSWInstalledName
```