HP OpenView Network Node Manager SPI for Secure Polling Agent

for the HP-UX, Linux, Solaris, and Windows® operating system

Software Version: 7.53

User Guide

Document Release Date: July 2008

Software Release Date: July 2008

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Documentation Updates

This manual's title page contains the following identifying information:

- Software Version number, which indicates the software version
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition, visit the following URL:

http://h20230.www2.hp.com/selfsolve/manuals

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

This Web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

Contents

1 Introduction to this Manual

1.1 Purpose of this Manual

This manual is intended for users of HP OpenView SNMP-based management products. It is a guide and reference tool for the specific software package it accompanies. This manual does not attempt to be a tutorial for SNMP.

1.2 Intended Audience

The content of this manual has been created based on the following assumptions:

- The reader has a basic understanding of SNMP.
- The reader may have a basic understanding of networking concepts.
- The reader has at least a basic familiarity with the contents of a Management Information Base (MIB) document.
- The reader understands file and directory structures and associated commands.
- The reader knows how to use typical network software tools, such as ping or telnet.

1.3 Organization of this Manual

The organization of this manual is summarized below. The number of the chapter which begins each major part is given.

1. Getting Started- Chapter 2 describes the steps for installing, testing, and uninstalling the product.

2. Product Introduction- Introduces management through firewalls and describes the options used with Secure Polling Agent.
3. Appendix- The Appendix identifies the owners of the trademarks which are referenced in HP documentation.
4. Glossary– The Glossary contains terms used in HP documentation.
5. Index- The index is provided for readers who wish to use this manual as a reference tool.

1.4 Conventions Used in this Manual

1.4.1 Instructions and Examples

When instructions or examples are given, any text that is outputted to the screen by the computer is printed in slab serif font, and any text that the user types is also in slab serif font. For example, the following text shows a command that is typed by the user and the message that is returned.

```
# grep snmp /etc/services
snmp           161/udp
snmp-trap      162/udp
```

The pound sign (#) indicates the root-user account prompt in UNIX. (Root-user access may be restricted to the system administrator). The percent sign (%) indicates a user account prompt that does not have root-user privileges.

1.4.2 Key Combinations

When key combinations are used, the keys are separated by hyphens. For example, if the Control key and the C key are to be typed together, then the key combination would be represented as follows:
Control-C

1.4.3 Directories and Files

Throughout this document, forward slashes are used to separate directories. On some operating systems, the directory delimiter is a different character. For example, Microsoft Windows systems use a backward slash character (\).

Users of these operating systems must interpret the forward slashes printed in the manual as the correct delimiter as required by the platform.

Absolute file paths (beginning with a forward slash) have an absolute position in the file system; /etc/srconf/mgr/snmpinfo.dat for example. All other file paths are implied to be relative to the top-level directory of the distribution unless otherwise specified. For example, bin/brassd refers to the SNMPv3 SPI Server program brassd in the bin subdirectory of the distribution.

1.4.4 Long Lines of Computer Screen Text

If any lines of text that are meant to be shown on a computer screen exceed 80 characters, the line of text will end in a backslash (\) and be indented on the following line. For example, command-lines typed into a computer or lines in a configuration file can exceed 80 characters and must be wrapped to the next line:

```
snmpCommunityEntry t0000000 public public localSnmpID    \
     nonVolatile
```

1.5 Supplemental Texts

This manual may make references to chapters contained in supplemental documentation. All necessary supplemental documentation should be shipped with this product. However, note that the supplemental texts have their own index, which is separate from this manual. If this manual references any supplemental documentation that was not shipped to you, contact HP.

2 Getting Started

The purpose of this chapter is to provide enough information to “bridge the gap” between receiving a box with a manual and a CD-ROM and using this new software product to work on the project for which it was licensed. Getting started requires a small amount of time and perhaps a bit of help from the local system administrator. By the end of this chapter, the reader should be able to access the programs, files, and examples presented later in this manual.

2.1 Overview

The following definitions describe the processes outlined in this “getting started” chapter:

- Installing
  Deploying the equipment in the actual run-time environment. This includes moving executable programs to the proper directories, setting up default configurations, and setting up online help systems where available.
- Testing
  Running the executable programs with all default settings to make certain that the baseline product is working normally.
- Uninstalling
  Removing all the program’s executable files, configuration files, and directories.

2.2 Introduction

The Secure Polling Agent communicates with the HP Openview SNMPv3 SPI Server to provide SNMP management through firewalls. Before installing the Secure Polling Agent, make sure that HP Openview SNMPv3 SPI Server is installed and tested on NNM Management Station. Second, install the Secure

Polling Agent on a machine that is behind the firewall through which you wish to provide management.

For the following instructions, the host where the HP OpenView SNMPv3 SPI server (brassd) is installed is called the server host. The host where the Secure Polling Agent (rbrassd) is installed is called the remote host.

The instructions in this guide accomplish the following:

- Install the Secure Polling Agent on the remote host.
- Stop the HP Openview SNMPv3 SPI on the server host and restart it with options that enable management through firewalls.
- Start the Secure Polling Agent on the remote host, establishing a connection between the Secure Polling Agent and the HP Openview SNMPv3 SPI Server. Perform a test of the communication.

2.3 Installing NNM Secure Polling Agent

2.3.1 On UNIX Systems

To install NNM Secure Polling Agent, perform the following steps:

1. Log in as root.
2. Insert the CD-ROM provided in the media pack in the drive.
3. Mount the CD-ROM by typing the following command.
   $ mount /dev/dsk/device_name /cdrom
   where device_name is the name of your CD-ROM drive.
4. Change the directory to cdrom directory.
5. Start the installation by executing the following command.
   $ ./install
   The installation message appears on the screen.
6. Check the /tmp/SecProxAgt_install.log file to review the status of the installation.
7. Unmount the CD-ROM by executing the following commands:
   a. $ cd /
   b. $ umount /cdrom

➤ If an error occurs during installation, a message that describes the problem appears on the screen.
If a fatal error occurs during installation, a message that describes the problem appears on the screen and the installation program terminates.
To continue installing NNM Secure Polling Agent, you must fix the error and rerun the installation program.

2.3.2 On Windows Systems

To install NNM Secure Polling Agent, perform the following steps:

1. Log in as a user with Administrator privileges.
2. Insert the CD-ROM provided in the media pack in the drive.
3. Open the Windows Command Prompt and do the following:
   a. Change the current directory to the CD-ROM drive.
   b. Run install.bat
4. Follow the instructions to complete the installation.
5. Check %TEMP%\SecProxAgt.log file to review the status of the installation.

2.4 Stopping and Restarting the SNMPv3 SPI Server

By default, the SNMPv3 SPI Server or Secure Polling Agent is not configured for remote management through firewalls. The first step in management through firewalls is enabling the SNMPv3 SPI Server. The following sections stop the SNMPv3 SPI Server, change the command-line options, and start the SNMPv3 SPI Server.

2.4.1 HP OpenView NNM SPI for SNMPv3

1. Issue the ovstop command to stop Network Node Manager.

   ```
   # ovstop brassagt
   ```

2. Modify the brassagt.lrf file according to the following example. Refer to the user documentation for more information about the file and command-line options.

   Add the -remoteconnect and -remoterange command line options. For example, if the Secure Polling Agent is running at 10.1.1.2, and you want to forward all traffic for 10.1.1.* to the Secure Polling Agent, ensure that the following processes are running:

   On UNIX Systems

   File Location: /etc/opt/OV/share/lrf/brassagt.lrf

   ```
   brassagt:brassd:
   OVs_YES_START::-d -nnm -remoteconnect 10.1.1.2 -remoterange
   10.1.1.0/24 :OVs_NON_WELL_BEHAVED:15:
   ```

   On Microsoft Windows Systems

   File Location: C:\Program Files\HP OpenView\lrf\brassagt.lrf

   ```
   brassagt:brassagt.exe:
   OVs_YES_START::-nnm -remoteconnect 10.1.1.2 -remoterange
   10.1.1.0/24 :OVs_NON_WELL_BEHAVED:15:
   ```

3. Run ovaddobj to register the brassagt.lrf file with the network manager software.

   — On UNIX Systems

   ```
   # /opt/OV/bin/ovaddobj /etc/opt/OV/share/lrf/brassagt.lrf
   ```

   — On Microsoft Windows Systems

   ```
   “C:\Program Files\HP OpenView\bin\ovaddobj”
   “C:\Program Files\HP OpenView\lrf\brassagt.lrf”
   ```

4. Start Network Node Manager with the brassagt option.

   ```
   # ovstart brassagt
   ```

2.5 Starting HP OpenView Secure Polling Agent

The rbrassd program should first be installed on the remote host. On the remote host, change directory to where the Secure Polling Agent is installed[1] and start the rbrassd as follows:

```
# cd <install path>
# ./rbrassd -d
```

➤ If the rbrassd program is started from some other directory, include the path on the command-line. For example: # <install path>/bin/rbrassd –d.

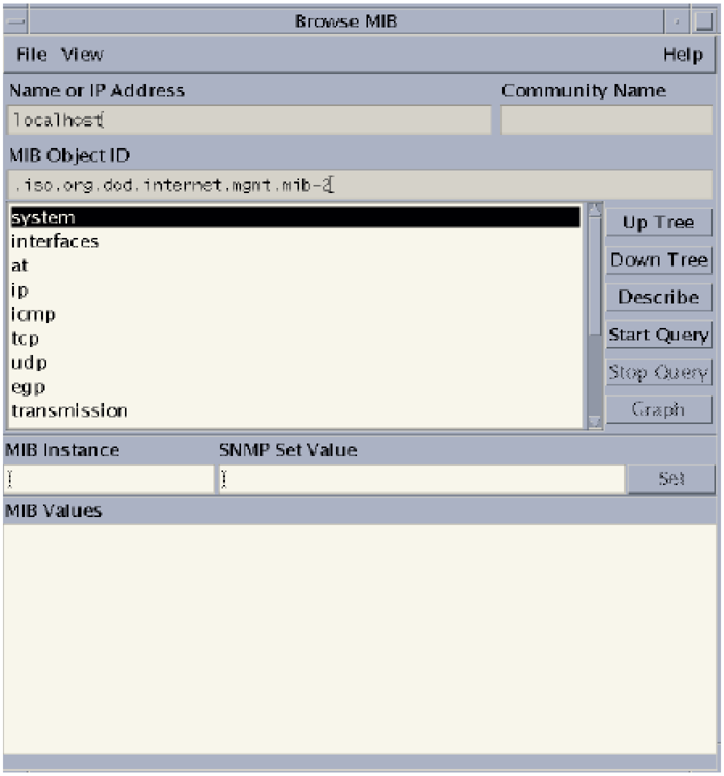
2.6 Testing Communication through Firewalls

This section provides testing information for Secure Polling Agent with HP Network Node Manager and HP NNM SPI for SNMPv3. This section provides the steps a user should follow test the SNMP communication through a firewall. If the SNMP request returns information about the machine, then the test has performed correctly.

2.6.1 Testing with the MIB Browser

1. Run the Network Node Manager SNMP MIB Browser by doing either of the following:
   - Execute the following command.
     xnmbrowser
   - From an OVW map, select Tools->SNMP MIB Browser.

[1] <install path> is the path selected during the installation process. For example, /opt/OV/SPAgt/ for UNIX Systems, or C:\Program Files\HP OpenView\SPAgt on Microsoft Windows Systems.



Name or IP Address: localhost

Community Name:

MIB Object ID: .iso.org.dod.internet.mgmt.mib-2

system
interfaces
at
ip
icmp
tcp
udp
egp
transmission

MIB Instance:

SNMP Set Value:

Figure 1 : The Network Node Manager MIB Browser

2 When the Browse MIB window opens, highlight the system MIB by following the path
iso.org.dod.internet.mgmt.mib-2.system using one of the following options:

— Double-click an item in the MIB document display window to display the branches.

— Single-click an item to select the branch, and then navigate up or down the branches using the Up Tree and Down Tree buttons.

3 Type the IP address of the host running the Secure Polling Agent to perform a SNMP request.

4 Select the Start Query button.
A response will be displayed in the MIB Values Window.

2.6.2 Testing with Command-line Utilities

On the NNM system running the SNMPv3 SPI Server, issue a test using the getmany utility, located in the /opt/OV/snmpv3/utils directory.

Send an SNMP Get request for system information to an agent at a location behind the machine running the Secure Polling Agent, <remotelocation>. Issue the following command line:

```
# ./getmany -v2c <remotelocation> root system
```

For example: Send the request to the agent at 10.1.1.12, an address within the range of the 10.1.1.*.

```
# ./getmany -v3 10.1.1.12 root system
Enter Authentication password : authpass
Enter Privacy password          : privpass
```

2.7 Uninstalling NNM Secure Polling Agent

2.7.1 On UNIX Systems

To uninstall NNM Secure Polling Agent, perform the following steps:

1. Log in as root.
2. Execute the following command.
   $ /opt/OV/SPAgt/remove.spa

2.7.2 On Windows Systems

To uninstall NNM Secure Polling Agent, perform the following steps:

1. Log in as a user with Administrator privileges.
2. On the Windows taskbar, click Start, point to Settings, and then select Control Panel. The Control Panel window opens.
3. Double-click Add/Remove Programs. The Add/Remove Programs dialog box opens.
4. Select HP Secure Proxy Agent from the list of programs, and then click Change/Remove.

2.8Additional Information

2.8.1 Moving Configuration Files and SSL Certificates

By default, the configuration files for HP products are installed in the /etc/srconf/ directory. After the product is installed, a user may move these configuration files to a different directory. If the files are moved, then the user must set the environment variables that identify the locations of the configuration files. If the environment variable is not defined, the application looks only in the default location.

HP agent applications (such as the SNMP Master Agent, snmpdm) look at the value of the SR_AGT_CONF_DIR environment variable to determine which directory contains the configuration files. To set SR_AGT_CONF_DIR, use the following command and specify the new directory location, for example:

On Windows System

```
set SR_AGT_CONF_DIR=D:\MYCONF
```

On UNIX System

```
# setenv SR_AGT_CONF_DIR /usr/config/myconf
```

HP manager applications (such as getmany and setany) look at the value of the SR_MGR_CONF_DIR environment variable to determine which directory contains the configuration files. To set SR_MGR_CONF_DIR, use the following command and specify the new directory location, for example:

On Windows System

```
set SR_MGR_CONF_DIR=D:\MYCONF
```

On UNIX System

```
# setenv SR_MGR_CONF_DIR /usr/config/myconf
```

Environment variables can be changed each time a terminal window is opened, or the variable can be set in the system-wide configuration. Refer to the operating system documentation for more information.

2.8.2 Using the Software as a Non-root User

There are special cases, determined by network managers, when the Master Agent and/or Subagents may be started by a non-root user. These cases should be carefully considered for the following reasons:

- The Master Agent's function is to help control and monitor a system. This functionality is compromised when any user has access to the Master Agent process.
- The Master Agent must bind to the system's privileged port, 161, to perform SNMP Communication. The operating system demands that only root users have access to the privileged port.
- Many Sub agents require privileged access because they manipulate the kernel. It is unsafe to allow any user to have the right to manipulate the kernel.

These issues must be weighed before allowing the Master Agent or Subagents to be run by non-root users.

2.8.2.1 On Windows System

If the user is not logged in to an account with administrative privileges, then the Master Agent must be started on a non-privileged port (that is, a port other than 161 and higher than 1024). Set the system environment variable SR_SNMP_TEST_PORT before attempting to start the Master Agent.

2.8.2.2 On UNIX System

Running Subagents as a Non-root User

Remotely Coupled Subagents, by default, can be started by non-root users on the same machine as the Master Agent. In order to allow Remotely Coupled Subagents to connect to the Master Agent, start the Master Agent (snmpdm) process with the -tcplocal argument.

There are three ways to run Loosely Coupled Subagents as non-root users:

- Change the permissions of the /tmp/.AgentSockets directory and the /tmp/.AgentSockets/A file to full permissions for any user (for example, chmod 777 /tmp/.AgentSockets). The file and directory are created by the Master Agent for master-to-agent communications. This is only a temporary solution because the permissions on the directory and file are reset when the host is rebooted.

- Change the permissions of the Subagent using chmod 755 <Subagent>. This sets the userid to be root. The Subagent then runs with root permissions though it can be started by non-root users. This is effective until the Subagent is rebuilt and the current Subagent binary version is overwritten. In the case that the Subagent is rebuilt, perform this method again.
- Run the Master Agent as a non-root user and run the Subagents using the same non-root user.

Running the Master Agent as a Non-root User

There are two ways to run the Maser Agent as a non-root user:

- Change the permissions of the Master Agent using chmod 755 snmpdm. This sets the userid to be root. The Master Agent then runs with root permissions though it can be started by non-root users.
- Set the Master Agent to bind to a non-privileged port, that is, a port other than 161 and greater than 1024. Then set the Subagents to use the same non-privileged port. Give the Master Agent permission to create files in the /tmp/.AgentSockets directory and to write to the file /tmp/.AgentSockets/A in order to set up the UDP socket for Subagent connections.

If the Master Agent is running as a non-root user, make sure that it has permission to create files and write to the /tmp/.AgentSockets and to the /tmp/.AgentSockets/A file. This allows the Master Agent to set up the UDP socket for Subagent connections. If the Master Agent is bound to a non-privileged port, the socket file name will have the current SNMP port number appended to the name of the file.

2.8.3 Setting the Path for Binary Components

Executable binary components, such as the HP Utilities, are located in a default directory. The name of this directory varies but will be in the form of <ProductName>/bin.

2.8.3.1 On UNIX System

Put the bin directory in the shell’s execution path. For example, to set the binary path to the program utilities, use the following command if the distribution was installed in the /opt/OV/bin directory on a UNIX operating system:

```
# setenv PATH ${PATH}:/opt/OV/bin
```

If the path is not set, then any commands issued must be issued within the bin directory and contain the characters“ ./” before the command.

2.8.3.2 On Windows System

Put the bin directory containing the executable programs explicitly in the execution path. For example, if the software was installed on a 32-bit Intel machine in the default directory, the command would be similar to the following:

```
C:\>set path="C:\Program Files\HP OpenView\bin";%PATH%
```

This command can be issued at the start of each DOS session, or the path may be permanently set in the system-wide configuration. Refer to the operating system documentation for more information.

If the command to add the execution path is typed incorrectly, the path variable may be incorrectly set or overwritten. Use the set command to verify that the path has been correctly appended to the list of entries for the path variable.

If the path is not set, then any commands issued must be issued within the bin directory and contain the characters“.\” before the command.

2.9Troubleshooting

2.9.1 Product Manual cannot be opened

Make sure Adobe Acrobat Reader is installed on your host.

3 The SNMP Secure Polling Agent

3.1 The Secure Polling Agent

The Secure Polling Agent (rbrassd) forwards SNMP requests received from one or more SNMPv3 SPI Server to managed hosts.

The purpose of the Secure Polling Agent is to allow management applications to manage networks separated from the management host by one or more firewalls. To do this, SNMP traffic is redirected over a TCP connection or an SSL/TLS protected TCP connection between the SNMPv3 SPI Server and the Secure Polling Agent. Furthermore, notifications (and Inform messages) are sent back to all interested SNMPv3 SPI Servers over these TCP connections.

3.2 Starting the Secure Polling Agent

To run the Secure Polling Agent with a SNMPv3 SPI Server that is already running, perform the following steps:

1. Verify that the SNMPv3 SPI Server is running on the NNM server host by executing the following command.
   ```
   ovstatus –c brassagt
   ```
2. On the remote host, start the Secure Polling Agent to accept connections from any SNMPv3 SPI Server
   ```
   # rbrassd
   ```

   To specify one host to connect to, specifying the host where the SNMPv3 SPI Server is running, 192.168.5.10, for example:

   ```
   # rbrassd -accept 192.168.5.10
   ```

Start the rbrassd program on the remote host. Do not run the rbrassd program on the same host as brassd.

3.3 Configure HP SNMPv3 SPI Server to Manage Separate Networks

A SNMPv3 SPI Server might be configured to forward SNMP management requests from a HP OpenView SNMPv3SPI-based management application to two separate networks as follows:

```
# brassd -nnm -remoteconnect 10.1.1.2 -remoterange 10.1.1.0/24 \ -
remoteconnect 10.1.2.5 -remoterange 10.1.2.0/24 -secure
```

The -nosecure option specifies to disable SSL protection on the connection between the HP OpenView SNMPv3SPI Server and the Secure Polling Agent.

Assuming that the management application is running at host 192.168.5.10, rbrassd might be run as follows:

```
# rbrassd -accept 192.168.5.10
```

Or, to allow rbrassd to accept connections from any SNMPv3 SPI Server, issue only the rbrassd command:

```
# rbrassd
```

To allow flexibility in configuring firewall rules, SNMPv3 SPI Server may be configured to connect to Secure Polling Agent (rbrassd) or connect from the Secure Polling Agent to the HP OpenView SNMPv3SPI Server. Each connection may be individually configured using command line options.

If you wish to configure a connection from SNMPv3 SPI Server to a Secure Polling Agent, invoke the SNMPv3 SPI Server as follows:

```
# brassd -remoteconnect <ipaddress> -remoterange <iprange1> \
         -remoterange <iprange2> ...
```

For example, if the Secure Polling Agent is running at 10.1.1.2, and you wish to have the SNMPv3 SPI Server forward all traffic to 10.1.1/24, you might use the command string.

```
# brassd -remoteconnect 10.1.1.2 -remoterange 10.1.1.0/24
```

You must fully specify the address in the remote range specification (10.1.1/24 will not work). Simply running the Secure Polling Agent without any options will allow it to accept connections from any SNMPv3 SPI Server.

Configuring a connection from the Secure Polling Agent to the SNMPv3 SPI Server is slightly more complex, as the SNMPv3 SPI Server must be made aware of the range of addresses for SNMP traffic that is to be sent to the Secure Polling Agent. For example:

```
# brassd -remoteaccept <remoteipaddress> -remoterange <iprange1> ...
```

```
# rbrassd -connect <serveripaddress>
```

If the SNMPv3 SPI Server is running on 192.168.1.2, then use the following:

```
# brassd -remoteaccept 10.1.1.2 -remoterange 10.1.1.0/24
```

Execute the following command NNM Secure Polling Agent node:

```
# rbrassd -connect 192.168.1.2
```

> If the connecting entity is started a considerable amount of time before the accepting entity, it may take up to 60 seconds before the connection is completed.

3.4 Configure SNMPv3SPI to use a Secure Connection

The HP SNMPv3SPI server and the Secure Polling Agent use a two-front approach to security policy enforcement. Both the SNMPv3 SPI Server and the Secure Polling Agent can restrict the IP address from which they will accept connections. This provides a moderate amount of security, even if use of Secure Sockets Layer (SSL) is not practical in a particular environment. Additionally, SSL-based protection is available. By default, SSL with mutual certificate-based authentication and encryption is used for the connection between the Secure Polling Agent and the SNMPv3 SPI Server. The certificates are not provided separately by the application, so that users need to create certificates on their own, should they please. For details of security certificate generation, see Chapter 4.

3.5 Secure Polling Agent Command Line Options

Secure Polling Agent uses many, but not all of the command line options as the SNMPv3 SPI Server. The following command line options may be used with the Secure Polling Agent.

- -d
  Do not daemonize. i.e., run in foreground. Ignored on non-Unix-like systems.
- -listen <port>
  Listen at <port> for connection requests from SNMPv3 SPI Servers. If this option is not specified, and no -connect or -accept options is specified, and then rbrassd will listen at port 6844. If either -connect or -accept is specified, rbrassd will not accept connections from any other SNMPv3 SPI Server unless -listen is explicitly specified. The range of addresses for which management requests are sent to this server is specified by the SNMPv3 SPI Server.
- -connect <IP address>:<port>
  Attempt to establish a connection to a SNMPv3 SPI Server located at the specified <IP address>. By default, the remote forwarder listens at port 6844. The <port> only needs to be specified when overriding the default port. The range of addresses for which management requests are sent to this server is specified by the SNMPv3 SPI Server.
- -accept <IP address>:<port>
  Listen for and accept a connection from SNMPv3 SPI Server located at the specified <IP address>. The <port> specifies the port at which rbrassd will listen. If the port is not specified, the default port (6844) is assumed. The range of addresses for which management requests are sent to this server is specified by the SNMPv3 SPI Server.
- -nosecure
  This switch specifies to open a non-SSL connection to the host specified using the previous -remoteconnect or -remoteaccept option. If there have been no -remoteconnect or
  -remoteaccept specifications, then all Secure Polling Agent connections will be opened without using SSL over TCP but will use just TCP. By default, security is requested, the data stream is encrypted, and mutual cryptographic authentication is enforced. Specifying -nosecure will disable this.
- -certdir <directory>
  The directory where the certificates required for mutual authentication are stored. By default, this is /etc/srconf/mgr on UNIX systems, and

certificate (dsspremotecert.pem) in the certificate directory. This option is ignored if neither the SNMPv3 SPI Server nor the Secure Polling Agent requests security.

- -privpassword <pw>
  Only use this option when using a security certificate other than one supplied by HP. The private keys within the application certificates are encrypted to avoid accidental disclosure. rbrassd knows the passwords for the privacy keys within certificates supplied by HP. If you replace dsspmastercert.pem, then use this option to specify the encryption key used when you created the certificate.

3.5.1 Running the Secure Polling Agent with Debugging Messages

The following AP debugging facility options are available to the NNM Secure Polling Agent.

- -apwarn
  Issue warning messages. On by default.
- -aperror
  Issue error messages. On by default.
- -aptrace
  Issue all debug tracing messages.
- -apall
  Issue all debugging messages.
- -appacket
  Issue SNMP packet build and packet parse messages.
- -apverbose
  Issue verbose debug messages.

The following ER diagnostics options are available to the NNM Secure Polling Agent.

- -ertrace
  Issue trace messages.
- -ererror
  Issue error messages.

- -ervarbinds
  Display the contents of all variable binding lists.
- -erpackdump
  Display a hex packet dump of all SNMP messages.
- -erpdus
  Display the protocol data unit header contents.
- -erall
  Display all SNMP traffic.

3.5.2 Microsoft Windows Options

The following options are available only on Microsoft Windows systems.

- -install
  Install as a system service.
- -remove
  Uninstall as a system service.
- -start
  Execute as a system service.
- -stop
  Halt the executing system service.

3.5.3 Running the Secure Polling Agent with Notification Throttling

The Secure Polling Agent automatically filters incoming notifications from an agent if the agent generates more than the predefined number of notifications per second (10 is the default). The number of notifications per second is the stormrate. The Secure Polling Agent throttles the agent by dropping incoming notifications from the agent for 300 seconds, the default, after incoming notification exceed the stormrate. The number of seconds to drop notifications is the stormtime.

The following arguments control the Secure Polling Agent notifications throttling:

- -notrap throttle
  Disable notification throttling. Enabled by default.

- -stormrate num
  Set the stormrate, the rate at which the Secure Polling Agent filters incoming notifications if one agent generates notifications exceeding the predefined number of notifications per second. The default is 10.

- -stormtime num sec
  Set the stormtime, the length of time for the Secure Polling Agent to drop notifications from the agent exceeding the stormrate. The default is 300.

4 Security Certificates

This chapter explains how HP products use secure socket layers (SSL) to implement secure communication between devices on a network and even through a firewall, if SNMPv3 SPI Server or Secure Polling Agent is installed.

By default, this product uses strong SSL security and provides command-line options to relax security requirements, if necessary. For the security features to be available, SSL must be supported both in the product and on the operating system where the product is running.

4.1Overview

This section provides a brief overview of certificates, secure socket layers, ciphers, identify verification, and certificate authorities. This overview is not meant to be a comprehensive tutorial.

4.1.1 Certificates

A network security certificate is a digitally-signed electronic document that associates a cryptographic public key with a software application. Network security certificates also can associate cryptographic public keys with individuals, organizations, and other entities. HP associates public keys with application programs.

In general, certificates contain:

- A subject identifying the software application, person, or organization;
- A public key corresponding to a private key associated with the subject;
- A signature from a recognized, named certificate authority (CA) like VeriSign that ensures that the public key owner and subject are the same (you can also be your own CA); and
- A digest or hash of the certificate's contents that are encrypted using the private key of the certificate authority.

4.1.2 Why use Certificates?

Network security protocols such as SSL, which the HP application programs use for authenticated and encrypted stream communications, use network security certificates as part of the mechanism to verify the identity of their communication peer. For example:

- brassd verifies the identity of rbrassd
- rbrassd verifies the identity of brassd

Identity verification helps the applications ensure they are communicating with recognized and trusted peer programs before exchanging sensitive data.

Certificates can identify an application residing at a specific IP address. Because an IP address and port of a remote network application can be spoofed, a security certificate provides stronger authentication instead of relying on the IP address and port to identify authorized applications. More specifically, security certificates provide greater assurance that an rbrassd is communicating with an authorized brassd, for example.

4.1.3 Certificate Authority

Each of HP's applications that use SSL must have its own network security certificate. Every network security certificate must be digitally signed by a person or organization (called a "certificate authority," or CA) that has verified the identity of the program.

The certificate authority itself must have a network security certificate that identifies the certificate authority, contains the certificate authority's cryptographic public key, and is publicly or readily available. The CA may be an established, well-known organization such as Verisign, or an individual or department in the company.

In either case, the CA must:

1. Verify the identity of the application program for which a network security certificate is to be issued (a one-time occurrence).
2. Have the authority to digitally sign the network security certificate requests.
3. Digitally sign the network security certificate request to produce the network security certificate.

Each brassd and rbrassd requires an identifying certificate. They must have a CA certificate shared with the peer application (rbrassd or brassd) with which it is communicating.

The authentication can fail for one of three reasons:

- The application certificate is wrong
- Both communication applications do not share the same CA certificate
- The CA certificate is wrong.

If the authentication fails, then the connections are terminated.

4.1.4 SSL and TLS

Certificates allow Secure Socket Layers (SSL) and Transport Layer Security (TLS) to negotiate secure communications by authenticating the application's or sender's identity, providing a public key, and establishing the encryption algorithm to be used.

4.1.5 Ciphers

SSL and TLS use asymmetric ciphers, a system that requires a private key to encrypt messages and a public key to decrypt for authenticating the application programs. An email message, for example, is encrypted when a sender applies an algorithm and a private key to plain text to produce encrypted content ("cipher text"). The cipher text can be decoded by applying the decryption algorithm using the corresponding public key contained in the sender's public key. SSL and TLS use these ciphers to hash the certificates and Privacy Encoded Mails (PEMs). Once the identities of the two individuals, computers, or applications have been established, symmetric ciphers are used for data transfer. These ciphers are known by both computers. When an encoded message is received, the computer uses the symmetric cipher to decrypt the message. Using the symmetric cipher algorithm reduces overall computation and makes real-time communications faster and more efficient.

4.1.6 Notes

Some details have been omitted from this explanation for clarity and simplification. For example, this explanation was written with the application's network security certificate being signed by the certificate authority. In reality, several levels of network security certificates can exist between the application's network security certificate and the certificate authority

4.2 Generating and Managing Certificates

HP provides shell scripts or batch files that automate the process of creating network security certificates for HP programs. For organizations unfamiliar with SSL certificates, these shell scripts simplify the creation of the network security certificates by HP programs.

Organizations familiar with SSL certificates can use their established, in-house procedures to create network security certificates for HP programs.

HP provides the SrSSLCert UNIX shell script or SrSSLCert MS-Windows batch file to automate the network security certificates creation process. SrSSLCert is located in the SrSslTools subdirectory in the installation distribution. SrSSLCert should be installed and run only on a single machine that will be used to create network security certificates.

When certificates are created using SrSSLCert, the SSL certificate and corresponding private key are stored in separate files. This separation clarifies that there are two distinct items of SSL information and more closely aligns with the intended use of the different items of SSL security information (i.e., the public key certificate can be publicly accessible, but the private key must be kept private).

4.2.1 Default Directories

Certificates are installed in the appropriate subdirectory according to the operating system:

- /etc/srconf/mgr by default on UNIX systems and C:\etc\srconf\mgr by default on Microsoft Windows systems,
- The subdirectory to which the SR_MGR_CONF_DIR environment variable points, and
- The subdirectory specified by the -certdir command-line option to brassd or rbrassd.

4.2.2 SrSSLCert Script

The SrSSLCert script or batch program is used to generate certificates used by HP applications. The SrSSLCert script will not overwrite existing certificates, so any existing certificates should be renamed before running SrSSLCert.

When using SrSSLCert to create a CA certificate, you will be prompted for a PEM or pass phrase and additional information that identify the organization. Choose this phrase carefully, remember the pass phrase, and ensure it is not compromised. This pass phrase will be used every time a certificate is created.

The SrSSLCert script can also be used to view the contents of a certificate. Viewing certificate contents is described in section 4.6.

OpenSSL must be in the path for this script to function properly. This tool is included in the $OV_BIN directory.

4.2.3 Generating Certificates Using SrSSLCert

Certificate generation using the SrSSLCert script follows three general steps:

1 Create a certificate authority (CA) network security certificate using SrSSLCert. For example:

```
SrSSLCert create snmpricacert
```

2 Create a network security certificate for each application on each host:

- — Use the SrSSLCert script to create the certificate.
- — Repeat the process once for each brassd or rbrassd on each host. For example, one brassd and two rbrassd programs are running:

```
SrSSLCert create dsspmastercert ip [ ip ip ... ]
SrSSLCert create dsspremotecert ip [ ip ip ... ]
SrSSLCert create dsspremotecert ip [ ip ip ... ]
```

```
Usage:  SrSSLCert  <function>  <certificate>  [arg] [arg] [arg]
```

where, <function> can be any of the following : create, display, list, remove, or verify and certificate can be any of the following: dsspmastercert, dsspremotecert, or snmpricacert.

Optional IP addresses can be added to the command line if the host is multi-homed. All of the IP addresses listed on a single command line will reside in one certificate.

4.2.4 Embedding IP Addresses within the SSL Certificates

This release requires the IP address(es) of the hosts on which the HP SNMPv3 SPI server or NNM Secure Polling Agent run be embedded in the SSL certificate(s).

When a HP SNMPv3 SPI server or NNM Secure Polling Agent initiates a connection to a listening daemon, the initiating daemon compares the IP address to which it is connected with the IP address embedded in the SSL certificate served up by the listening daemon. If the IP address in the certificate matches the IP address to which the initiator connected, the SSL connection is completed. If the two IP addresses do not match, the SSL connection is failed.

Embedding a “listeners” IP addresses in the SSL certificate is a standard component of SSL security. For a hacker to hack a connection, the hacker must steal the real daemon’s SSL certificates (with the embedded IP addresses) AND the corresponding private key file in addition to spoofing the IP address of the host on which the real daemon runs.

Each host on which a HP SNMPv3 SPI server or NNM Secure Polling Agent requires a unique SSL certificate for that host. All IP address by which the host will be known (including any NAT addresses) must be embedded in the certificate. If the IP address of the host changes, a new SSL certificate must be created for that host.

The –no_ip_check command-line option, specified on the command line of the connection-initiating HP SNMPv3 SPI server daemon, relaxes this security requirement. This command-line option, bypasses the checking of the IP addresses embedded in the certificate served up by the listening daemon. This command-line option allows an SSL certificate to be copied or moved from host to host, or kept unchanged if the listening daemon’s IP address changes.

4.3 Certificate Authority Creation and Deployment

A new Certificate Authority (CA) certificate must be created the first time new certificates are created. Because the CA certificate is unique for each organization, creating a new CA certificate provides a unique identifier and prevents rogue applications or other OpenSSL applications from connecting to the organization’s applications. This process uses the HP-provided script SrSSLCert to create a CA certificate.

For each certificate, SrSSLCert creates a private key and public key pair. The CA private key is written into disk files and encrypted using a “PEM pass phrase.” The same PEM pass phrase is used to decrypt the private keys when the private key is needed later. The PEM pass phrase for the Certificate Authority certificate is especially important. It should be treated carefully, and not disclosed to unauthorized individuals. Private key files should be kept private by restricting the host operating system’s file permissions.

If the PEM pass phrase for the CA certificate is compromised, the CA’s private key can be decrypted. This compromises the security of all certificates signed by this CA, because additional certificates that appear to be from this CA can be created.

When the application certificates are created, they must be digitally signed using the private key associated with the Certificate Authority certificate. At the time the application certificates are signed, the user will be prompted to enter the PEM pass phrase for the private key associated with the CA certificate.

Once certificates have been created, they must be copied to the appropriate subdirectories.

4.3.1 Procedure

The CA network security certificate is created using the SrSSLCert create snmpricacert command, where snmpricacert specifies that the certificate being created is a CA certificate. This process is performed once to generate a CA network security certificate for the company. This process performs the following three steps:

- Creates a private key/public key pair
- Creates a certificate signing request
- Self-signs the certificate signing request with the associated private key.

The network security certificate containing the certificate authority’s public key is digitally signed using the corresponding private key. The “self-signing” is what differentiates a CA network security certificate from an application network security certificate.

To create the CA certificate:

1. Enter the following command:
   SrSSLCert create snmpricacert
2. Enter a pass phrase and requested information (see section 4.3.1.1).

4.3.1.1 Pass Phrases for CA Certificates

When prompted, the user must enter a pass phrase. The pass phrase encrypts the certificate authority's private key file, which is used by the certificate authority only when signing certificate signing requests. In addition, the private key file should be kept in a secure location on disk.

It is extremely important to specify a difficult-to-guess pass phrase and to ensure that the pass phrase is not compromised.

If the private key pass phrase is compromised, then unauthorized individuals could sign new certificate signing requests.

When prompted, respond with proper values:

- The company name (required)
- The department (optional)
- The contact email address (required)
- The city (required)
- The state or province name (required)
- The two-letter country code (required)
- The contact name (optional)

4.3.1.2 Deploying CA Certificates

The procedure above will create two files: snmpricacert.pem and snmpricacert.privatekey.pem. The snmpricacert.privatekey.pem contains the private key associated with the CA's network security certificate. For added security, it is encrypted by the specified pass phrase.

The snmpricacert.privatekey.pem file should never be installed publicly. It should only reside in a private area on the host used to create the certificate.

The CA's files include snmpricacert.pem and snmpricacert.privatekey.pem. The first file contains the CA's network security certificate; the second file contains the private key associated with the CA's network security certificate.

The snmpricacert.pem disk file must be copied to every machine on which brassd or rbrassd will be used.

The snmpricacert.pem disk file MUST be copied into the /etc/srconf/mgr directory. The snmpricacert.pem file MUST be world-accessible; if is not world-accessible, then some HP application programs may not function correctly.

The private snmpricacert.privatekey.pem file should only exist on the machine that will be used for creating network security certificates. This file must not be copied to any other machine. If this file is ever compromised then:

- A hacker could create network security certificates for HP applications for the network.
- Restoring network security would require that new network security certificates be recreated and redeployed for all HP application programs on all hosts in the network.

4.4 Network or Application Security Certificate Creation and Deployment

A network or application security certificate has to be created for each brassd or rbrassd on the network. These certificates are created using the command below:

SrSSLCert create certtype ip_addr

where:

- create- This option tells the SrSSLCert script to create a new certificate.
- Ip_addr- This option defines the primary IP address of the brassd or rbrassd application in the format xxx.xxx.xxx.xxx. Multiple IP addresses, including NAT addresses, can be specified as additional command parameters.
- certtype -The certtype defines the application with which the certificate will be used. The options dsspmastercert and dsspremotecert create certificates for us with brassd and rbrassd respectively.

Running the command below

SrSSLCert create dsspmastercert 64.55.126.243

Creates a private/public pair (dsspmastercert.64.55.126.243.privatekey.pem and dsspremotercert.64.55.126.243.pem) and a certificate signing request. It also signs the certificate signing request with the CA's private key.

4.4.1 Procedure

A network certificate must be created for each instance of brassd or rbrassd. The SrSSLCert option used to create the certificate depends upon the HP program with which the certificate will be used. Certificates for the HP SNMPv3SPI server (brassd) are created with the option dsspmastercert. Certificates for the NNM Secure Polling Agent (rbrassd) are created using dsspremotecert.

This procedure creates two files: dsspmastercert.<ip_addr>.privatekey.pem and dsspmastercert.<ip_addr>.pem for brassd or dsspremotecert.<ip_addr>.privatekey.pem and dsspremotecert.<ip_addr>.pem for rbrassd. The <ip_addr> portion specifies the primary IP address of the host on which the certificate will be installed.

At a command prompt, enter the following line, including the host IP address on which the application will run:

```
SrSSLCert create dsspmastercert <ip_addr>
SrSSLCert create dsspremotecert <ip_addr>
```

4.4.2 Pass Phrases for Network Security Certificates

The private key files will not be encrypted, and do not need pass phrases. The private key files are kept private by restricting the host operating system's file permissions.

If the private key files are encrypted, each time the private key file is accessed, the daemon will stop and prompt for the pass phrase. This may happen relatively frequently as SSL connections are (re)established with the peer HP OpenView SNMPv3 SPI server or NNM Secure Polling Agent. For this reason, the use of encrypted private key files is discouraged.

It is not recommended to use encrypted private keys because of problems supplying the pass phrase needed for decrypting the private key when needed. To supply the private key decryption pass phrase when needed by SPA, there are several possibilities:

1. Have SPA prompt the user when it needs the pass phrase

   This is most secure. However, if SPA prompts and no one can answer the prompt, it will not reconnect. This is a problem for unattended systems that must recover from network or system outages. SPA would prompt for a decryption pass phrase each time a connection is established, rather than once at daemon start up.

2. Build the pass phrase into the SPA binary

   This will allow the decryption pass phrase to be compromised if someone scanned the binary for text strings.

3. Put the pass phrase in a disk file and read it when decryption is needed

   This option is no more secure than using a non-encrypted private key file. Using one of the following two options:

- An non-encrypted private key file.
- An encrypted private key and keeping the decryption pass phrase in a disk file.

  The security of the private key depends upon the file system security. But using an encrypted private key and keeping the decryption pass phrase in a disk file complicates the software and does not provide additional security.

4 Supply the decryption pass phrase as a SPA command-line argument.

   This may allow the decryption pass phrase to be compromised if a non-secure user on the system were able to display the command used to start SPA. This is pretty common on UNIX, with commands like "ps -ef".

5 SPA to prompt once, and cache the answer in RAM.

   It is recommended to use a not encrypted private key, but ensure it is well-protected by your file system security.

   If you want encrypted private keys, it will require a change to the arguments to the "openssl" command-line command used in the SrSSLCert shell script. You will need to change the arguments to the openssl command that generates the public key/private key pair. However, if you encrypt the private key file, SPA will stop and prompt for the decryption pass phrase. This may happen more frequently than you think, and the SSL connections will not be established until the pass phrase is supplied.

4.4.3 Deploying Network Security Certificate for brassd

When network security certificates are deployed for brassd, the brassd application files include dsspmastercert.< ip_addr>.pem and dsspmastercert.< ip_addr>.privatekey.pem.

To deploy Network Security Certificate for brassd, perform the following steps:

1 Create a new file with the name dsspmastercert.pem

2 Copy the contents of the dsspmastercert.<ip_addr>.pem to dsspmastercert.pem

3 Append the contents of the dsspmastercert.<ip_addr>.privatekey.pem to dsspmastercert.pem and save this file.

4 Copy the dsspmastercert.pem file to /etc/srconf/mgr directory of the host specified by the <ip_addr> portion of the file name. The <ip_addr> portion of the file name helps to identify the machine on which the files must be installed.

4.4.4 Deploying Network Security Certificates for rbrassd

When network security certificates are deployed for rbrassd, the rbrassd application files include dsspremotecert.<ip_addr>.pem and dsspremotecert.<ip_addr>.privatekey.pem.

To deploy Network Security Certificate for rbrassd, perform the following steps:

1. Create a new file with the name dsspremotecert.pem
2. Copy the contents of the dsspremotecert.<ip_addr>.pem to dsspremotecert.pem
3. Append the contents of the dsspremotecert.<ip_addr>.privatekey.pem to dsspremotecert.pem and save this file.
4. Copy the dsspremotecert.pem file to /etc/srconf/mgr directory of the host specified by the <ip_addr> portion of the file name. The <ip_addr> portion of the file name helps to identify the machine on which the files must be installed.

4.5 Verifying Certificates

Public keys and private keys must be used in pairs; that is,

- Something encrypted with the private key can only be decrypted with the associated public key
- Something encrypted with the public key can only be decrypted with the associated private key

The certificate authority digitally “signs” a certificate signing request by:

- Computing a cryptographic hash or checksum over the certificate signing request
- Encrypting the cryptographic hash with the certificate authority’s private key
- Storing the encrypted hash in the newly-created certificate

The certificate’s authenticity is verified by:

- Computing a cryptographic hash or checksum over the certificate signing request

- Decrypting the cryptographic hash stored in the certificate by using the certificate authority's public key
- Comparing the computed hash with the decrypted stored hash

If the two hashes match, then this verifies that the certificate has not been tampered with and that it was signed by the CA's private key associated with its public key.

4.6 Viewing the Contents of a Certificate

Because certificate files are encoded, a special viewer is needed to decrypt and display the public file. The the SrSSLCert script or batch file can display the public certificate by issuing the following command:
SrSSLCert display [cert name]

where [cert name] is replaced with the certificate name to be viewed. The private certificate cannot be viewed in this manner.

4.6.1 Key Lines in the Certificate File When Displayed

To display the certificate file dsspremotecert.192.147.142.192, the following command would be entered:
SrSSLCert display dsspremotecert.192.147.142.192

The resulting output displays important information, including the expiration date, the program for which the certificate was issued, and the IP address of the host on which the application resides. Key lines in this example include:

- Issuer shows the name of the issuing certificate authority.
- Validity shows the date the certificate was issued (Note Before) and the date the certificate expires (Not After field).
- Subject: CN=HP Openview Network Node Manager Secure Polling Agent displays the "common name" (CN) of the program with which the certificate is used.
- CA:FALSE indicates that this certificate is not a certificate authority certificate. If this file was a CA certificate, the value in this field would be true.

- The field DNS:192.147.142.192 provides the IP address of the machine where the certificate resides. This field will be different in all certificates. If the IP address does not match the IP address in the CA certificate, then the connection will fail.

- Certificate:

```
Data:
   Version: 3 (0x2)
   Serial Number:
      c3:8c:fd:cc:52:8d:c5:19
   Signature Algorithm: sha1WithRSAEncryption
   Issuer: O=HP/emailAddress=support@hp.com,
      L=Knoxville, ST=Tennessee, C=US, CN=Personne
   Validity
       Not Before: Oct 19 15:24:23 2006 GMT
       Not After : Oct 14 15:24:23 2026 GMT
   Subject: CN= HP OpenView Network Node Manager Secure Polling
Agent
   Subject Public Key Info:
       Public Key Algorithm: rsaEncryption
       RSA Public Key: (1024 bit)
          Modulus (1024 bit):
             00:cb:82:c0:60:8c:1b:68:13:fc:d0:73:2c:d2:53:
             8b:32:78:0d:65:64:51:0d:03:27:d1:b1:b7:8d:78:
             3e:62:58:f8:e5:4a:4c:2a:28:65:21:d5:4d:0f:e0:
             55:a7:3f:64:84:3f:24:a2:d4:78:eb:59:c5:1f:aa:
             c2:f0:85:0d:88:ea:6b:87:6e:13:a0:d5:73:f6:2e:
             0b:20:8c:30:36:f1:f0:d8:27:f5:fd:63:de:38:e8:
             80:b5:c9:2f:e7:52:57:fa:6d:fb:b2:c1:90:d8:56:
             af:c9:b3:44:99:82:99:5e:af:0a:68:4b:e7:e1:2c:
             ae:7d:3f:09:cd:39:fc:1e:99
         Exponent: 65537 (0x10001)
 X509v3 extensions:
    X509v3 Basic Constraints: critical
       CA:FALSE
    X509v3 Key Usage: critical
          Digital Signature, Non Repudiation, Key Encipherment
    X509v3 Subject Key Identifier:
          75:F1:33:66:F0:8D:DB:9C:48:F4:4C:17:1F:FD:6B:B0:09:B2:06:26
    X509v3 Authority Key Identifier:

keyid:0E:78:E5:0A:D5:D2:6A:97:7F:F8:CB:FB:07:63:EA:A1:88:E3:E9:D6
          DirName:/O=HP/emailAddress=support@hp.com/
```

```
               L=Knoxville/ST=Tennessee/C=US/CN=Personne
            serial:EE:84:D7:BF:EE:17:E5:4E

        X509v3 Subject Alternative Name:
            DNS:192.147.142.192
    Signature Algorithm: sha1WithRSAEncryption
       6a:bd:49:72:54:4f:6c:be:29:29:39:9a:94:50:ae:65:be:fb:
       7b:ac:b6:b9:d7:1e:07:23:87:39:fa:76:25:62:0a:0f:73:53:
       03:f1:d5:84:17:a1:6d:eb:25:c4:03:0b:75:3e:17:a4:21:a9:
       d8:f6:86:de:1c:f8:ac:d0:d4:ff:4a:57:9d:5b:26:71:3d:a1:
       26:67:06:c5:be:f6:f8:ae:8c:e1:b4:14:f0:98:83:90:e6:7b:
       e2:bb:90:8e:c7:46:91:b1:b3:f8:5c:0e:81:5d:f5:3e:3d:e7:
      d8:5c:64:84:29:45:d8:f5:29:70:d4:3d:8b:c6:da:9f:d7:3e:
      9b:d6
```

4.7 Additional Information

For additional information about generating certificates, refer to Network Security with OpenSSL by John Viega, Matt Messier, and Pravir Chandra, available from O'Reilly Press (ISBN 059600270X, **http://www.opensslbook.com/**). Additional information is also available on the OpenSSL Web site, **http://www.openssl.org.**

A Trademarks

Accelerated Technology, Microtec, Nucleus, XRAY, and VRTX are registered trademarks of Mentor Graphics Corporation.

Adobe, Adobe Acrobat, Adobe Acrobat Reader, PostScript are trademarks or registered trademarks of Adobe Systems, Incorporated.

AlphaStation, Compaq, DEC, DIGITAL, HP OpenView Network Node Manager, HP/UX, Itanium, OpenVMS, PA-RISC, VMS, and VT-100 are trademarks or registered trademarks of Hewlett-Packard Corporation.

A/UX, Apple, and AppleTalk are registered trademarks of Apple Computer, Incorporated.

CodeView, Microsoft, FrontPage, MS-DOS, Windows, Windows NT, and Windows Server are trademarks or registered trademarks of Micros ft Corporation.

CORBA is a registered trademark of Object Management Group, Inc. Cygwin and Red Hat are trademarks of Red Hat, Incorporated. DG/UX is a trademark of Data General Corporation.

eHealth is a trademark and SPECTRUM is a registered trademark of Concord Communications, Inc.

EmWeb is a trademark of Agranat Systems, Incorporated.

FreeBSD is a registered trademark of The FreeBSD Foundation.

Green Hills and INTEGRITY are registered trademarks and velOSity is a trademark of Green Hills Software, Inc.

Intel is a registered trademark of the Intel Corporation.

IPNET and IPLITE are trademarks or registered trademarks of Interpeak AB. Java, Solaris, and SunOS are trademarks of Sun Microsystems, Incorporated. LINUX is a registered trademark of Linus Torvalds.

Lucent and Lucent Technologies are registered trademarks of Lucent Technologies. Motif, Nucleus, OSF/1, OSF/Motif, and UNIX are registered trademarks and The Open Group is a trademark and X Window System are trademarks of The Open Group.

MOTOROLA is a registered trademark of Motorola, Inc.

NetWare is a registered trademark of Novell, Incorporated.

Neutrino and QNX are trademarks or registered trademarks of QNX Software Systems.

OpenSSL and the SSL implementation used in this product are copyright 1998-2005 The OpenSSL Project. All rights reserved. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

OS-9 is a registered trademark of RadiSysMicroware Communications Software Division,
Inc.

OSE is a registered trademark of OSE Systems. Paradigm LOCATE is a trademark of Paradigm Systems.

pSOS is a trademark and VxWorks is a registered trademark of Wind River Systems, Incorporated.

ROM-link is a trademark of Soft Advances.

RomPager is a trademark of Allegro Software Development Corporation. SCO is a trademark of The SCO Group, Incorporated.

Soft-ICE is a trademark of Compuware Corporation.
SPARC is a registered trademark of SPARC, International. SUSE is a registered trademark of SUSE LINUX AG, a Novell business.

All other trademarks or registered trademarks are the property of their respective holders.

Glossary

An understanding of the following general terms will help in comprehending this manual:

Access Restriction

Access to the SNMP agents configured with a community string can be restricted based
upon the source address of requests. If address restriction is selected, only managers
included in the list of IP addresses will be able to query the agent using the new community
string.

Access View

The access level determines the MIB objects that members (users/communities) of a security group can retrieve with SNMP Get requests or set with SNMP Set requests. There are two types of access views, read and write:

— The read access view determines objects that can be retrieved using SNMP Get requests.

— The write access view determines objects that can be set using SNMP Set requests.

Administrative User

In order for EnterPol® to configure SNMP agents through EnterPol® modules like Simple Policy Pro or CIAgent Policy Pro, the EnterPol database must contain an administrative user that is already configured on the SNMP agent. This is because configuration is applied using SNMP set requests. This administrative user must have permission to set all MIB objects that may be set during the distribution of a policy. The Administration panels allow you to discover the administrative users in the EnterPol database.

AES

Advanced Encryption Standard. A symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption. The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce selected the algorithm called Rijndael. AES is not available outside the United States due to export restrictions.

API

Application Programming Interface.

ASN.1

Abstract Syntax Notation One. A description language used to describe SNMP data types in a machine architecture-independent format.

authentication

Authentication within the context of SNMP means that the SNMP entity can assert with certainty that the purported sender of a message is in fact the sender of that message.

Authentication Passphrase

The authentication passphrase is used to calculate a unique authentication key for each
SNMP agent on which the new SNMPv3 user is configured. The authentication key verifies the authenticity of the SNMPv3 messages sent by a manager using the new SNMPv3 username. A passphrase is similar to a password except that spaces are acceptable.
Example: auth password for DayShiftSupervisor

The best authentication passphrase is one that can not be guessed easily. Passphrases should be at lease eight characters long.

BER

Basic Encoding Rules. The Basic Encoding Rules describe how SNMP data should be encoded “on the wire” in such a way that machines with potentially very different architectures can understand it.

CMIP

The ISO-OSI network management protocol. The Common Management Information Protocol.

COEX

This is an informal reference to RFC3584, “Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework.”

Community

The term community refers to the SNMPv1 or SNMPv2c configured requires name. A community is used when making SNMPv1 or SNMPv2c requests to an SNMP agent.

Configuration Policy

A configuration policy consists of one or more security groups and the users or communities assigned to those groups. When a security group is included in a policy, all the users or communities assigned to that group will be configured on the SNMP agent.
Note: SNMP agents that will be configured using the new policy should support the security models and security levels defined for the security groups selected. For example, a policy containing an SNMPv3 user configuration should not be configured on an agent that supports only SNMPv1 and/or SNMPv2c.

connectionless protocols

Connectionless protocols allow packets between network correspondents to be routed
individually rather than through a pre-established “connection.” IP is such a connectionless protocol.

connection-oriented protocols

Connection-oriented protocols transmit packets between network correspondents along predetermined routes which are established at connection setup.

Context

Contexts are generally used when an SNMP agent has multiple subagents that support the same MIB. By making a request with a context the agent can correctly forward the request to the subagent that has registered for the context. Typically most MIB objects will be supported under the default SNMP context. A non-default context should only be specified if you know the SNMP agent being configured has MIB objects supported under a different context.

CVS

Concurrent Versions System. A front end to the revision control system (see RCS). CVS keeps a single copy of shared files in a source “repository”; it contains all the information to permit extracting previous software releases at any time based on either a symbolic revision tag, or a date in the past.

DES

Data Encryption Standard. An encryption algorithm often used as a privacy mechanism.

DNS

The Domain Name System. A networked database primarily used to identify mail handlers and to resolve IP addresses from symbolic names.

HMAC

Hash-based Message Authentication Codes. A mechanism (defined in RFC2085) for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, e.g., MD5, SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying has function.

IESG

The Internet Engineering Steering Group. A standards body responsible for approving technology as Internet Standards.

IETF

The Internet Engineering Task Force. A standards body that forms Working Groups to develop technology for the Internet community. When a protocol is deemed ready to move forward in the standards process, the IETF sends its recommendations to the IESG.

instrumentation

Instrumentation refers to the system-dependent program code written by an agent developer to gather the information that can be accessed using SNMP. For example, the number of packets in and out of an interface must be counted in order that this information can be retrieved. The instrumentation does the counting.

IP

Internet Protocol. IP is a connectionless network-layer protocol.

ISO

International Standards Organization. A standards body responsible for many different kinds of standards. The ‘networking branch’ of standards is usually referred to as the OSI.

ISODE

ISODE is a freely available development environment created as a research tool and represents an effort to promote the use of the International Organization for
Standardization (ISO) interpretation of open systems interconnection (OSI), particularly in the Internet and RARE research communities. For more information, see How to Manage Your Network Using SNMP: The Network Management Practicum by Marshall Rose and Keith McCloghrie. The full reference information is provided on page C-6.

Master Agent

The EMANATE® Master Agent. The EMANATE architecture includes the Maser Agent and zero to many Subagents. The Master Agent includes such things as authentication, privacy, packet receipt and sending, BER processing, Subagent management, and so forth.

As much as is possible, the difficult processing has been centralized in the Master Agent to leave the Subagents as simple as possible.

MD5

Message Digest Algorithm 5. A “fingerprinting” algorithm (defined in RFC1321) that is often used as an authentication mechanism. Using a shared secret, the recipient of a [SNMP] message can verify that the message was not altered “in flight.”

MIB

Management Information Base. Each SNMP agent implements a set of “managed objects.” These objects are described in MIB documents written in the ASN.1 data description language.

MIB family

For the purpose of writing method routines, SNMP variables are separated into families. A family consists of all of the leaf MIB variables with the same immediate parent node, or root (the Object Identifier without the instance information). For example, in MIB-II the following variables form a single family since they are all children of ifEntry
(1.3.6.1.2.1.2.2.1):

ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
...skipping entries between...	
ifOutQLen	1.3.6.1.2.1.2.2.1.21
ifSpecific	1.3.6.1.2.1.2.2.1.22

Note that ifNumber (1.3.6.1.2.1.2.1) is also a member of the interfaces group, but it is not a member of the same family since it is not a child of ifEntry.

MIB view

A MIB view is a subset of MIB objects at an SNMP entity which can be managed.

monolithic agent

A compile-time extensible SNMP agent. In contrast to a run-time extensible agent, a monolithic agent requires that new MIB objects be incorporated into the agent through recompilation and relinking. EMANATE® /Lite is an example of a monolithic agent.

Notification Targets

Notification targets are managers or agents that are selected to receive information from SNMP events. Notifications can be sent as either Traps or Informs. A Trap is a one way communication from an agent to a manager. An Inform contains the same information as a Trap; however, with an Inform the manager sends a verification response back to the agent. The user sending the notification must be assigned to a security group that has access to the notification OID and OID of other objects within the notification.

NVT ASCII

Network Virtual Terminal ASCII. A subset of the ASCII code defined by RFC854 for use with the telnet protocol. NVT ASCII consists of printable ASCII characters and selected control characters such as carriage-return.

OID

Object Identifier. Each object in an SNMP MIB has an associated Object Identifier which uniquely identifies the object in a global tree of objects.

OSI

Open Systems Interconnect. A set of networking standards endorsed by the ISO.

privacy

Privacy within the context of SNMP means that the contents of an SNMP packet can be interpreted correctly only by the sender and intended recipient of the SNMP packet.

Privacy Passphrase

The privacy passphrase is used to calculate a privacy key which is used to encrypt SNMP messages sent by this user. Encryption of the SNMP message ensures privacy as the message is transmitted across the network. A passphrase is similar to a password except that spaces are acceptable. Example:

priv password for HelpDesk

The best privacy passphrase is one that can not be guessed easily. Passphrases should be at lease eight characters long.

RCS

Revision Control System. A system of managing multiple revisions of files. RCS is useful for text that is revised frequently, for example C programs, documentation, graphics, papers, and form letters.

RFC

Request for Comment. Documents maintained by the IETF standards body containing standards in various stages of completion. RFC documents are available via the Internet for no fee and in printed form for a nominal printing charge.

Security Group

The security group defines:

- The security model that will be supported (SNMPv1, SNMPv2c, or SNMPv3).
- The security level that will be supported (if SNMPv3 is the security model).
- The access level (or views) (read, write and notify permissions).

Users assigned to a security group take on the access limitations defined for the group. It is often useful to name a security group to indicate the access level. It is also helpful to create a security group for a specific level of access.

Examples:

Administrator
ShiftSupervisor
public

Multiple users can be assigned to the same security group, however, each user can only be assigned to one security group.

Security Level

SNMPv3 users can be configured to use one or more of the following security levels:

- Authentication with privacy
- Authentication without privacy
- No authentication and no privacy

For security levels that use authentication, an authentication protocol must be specified in the configuration entry. For security levels that use privacy, a privacy protocol must also be specified in the configuration entry. Support privacy if this user might be used to communicate sensitive information that should not be transmitted across the network as plain text.

SHA-1

Secure Hash Algorithm. A “fingerprinting” algorithm (similar to MD5) that is often used as an authentication mechanism. Using a shared secret, the recipient of a [SNMP] message can verify that the message was not altered “in flight.”

SNMP

Simple Network Management Protocol. The specification for this Historic protocol is published in RFC1157.

SNMPv2c

Community-based SNMPv2. A Historic protocol published in RFC1901 which combines SNMPv2 operations (such as GetBulk) with SNMPv1 trivial authentication.

SNMPv2*

Simple Network Management Protocol version 2 “star”. A Historic proposed protocol (published as Internet Drafts) which predates SNMPv3 and should no longer be used.

SNMPv3

Simple Network Management Protocol version 3. The specification for this Full Standard protocol is published in RFC3410-3418. SNMPv3 provides a Full Standard administrative framework (authorization, access control, etc.) and remote configuration/remote administration MIB.

Subagent

An EMANATE® Subagent. See “Master Agent” for a description of the EMANATE architecture. A Subagent traditionally implements a single MIB document, such as the FDDI-MIB or the Host Resources MIB.

TCP

The Transmission Control Protocol is a connection-oriented transport-layer protocol. It attempts to achieve reliability through retransmission.

Triple-DES or 3DES

The 3DES-EDE privacy protocol (3DES) is an extension to the User-based Security Model (USM). The designated portion of an SNMP message is encrypted and included as part of the message sent to the recipient.

UDP

The User Datagram Protocol is a connectionless end-to-end transport-layer protocol.

User

The term user refers to the SNMPv3 USM users configured on an SNMP agent. The user   is used when making an SNMPv3 request to an agent that supports SNMPv3. A user is set up to support one or more of the following security levels:

- Authentication with privacy
- Authentication without privacy
- No authentication and no privacy

The username can be the name of a person, group or management application. For example:

Administrator
public
EnterPol

VarBind

An SNMP variable binding. A VarBind includes an OBJECT IDENTIFIER and a value (which may be NULL).

Index