



SANscape[®] Alert User's Guide Version 4.0

Copyright

Copyright © 2001-2005 Dot Hill Systems Corp. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, translated, transcribed, or transmitted, in any form or by any means – manual, electric, electronic, electromechanical, chemical, optical, or otherwise – without prior explicit written permission of Dot Hill Systems Corp., 6305 El Camino Real, P.O. Box 9000, Carlsbad, CA., 92009-1606.

Trademarks

Dot Hill Systems, the Dot Hill logo, SANscape, SANnet, and SANpath are registered trademarks of Dot Hill Systems Corp. All other trademarks and registered trademarks are proprietary to their respective owners.

Changes

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, Dot Hill Systems Corp., assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein. Dot Hill Systems Corp., reserves the right to make changes in the product design without reservation and without notification to its users.

Contents

Preface	v
1. Overview	1
Installing SANscape Alert	1
What is SANscape Alert?	1
How SANscape Alert Operates	2
2. Using SANscape Alert	5
Setting Up the SANscape Alert Configuration	5
To Set Up the Configuration	5
Host Event Log	11
To Set Up the Report Tool	13
UNIX Operating System	13
Microsoft Windows Operating System	14
To Set Up the Mail Receiver Tool	14
Troubleshooting	15
To Stop and Start SANscape Alert on a Solaris Host or Linux Host	16
To Stop and Start SANscape Alert on a Windows 2000 or 2003 Host	16
To Stop and Start SANscape Alert on an HP-UX Host	16
To Stop and Start SANscape Alert on an IBM AIX Host	17

Preface

This guide explains how to use SANscape Alert as a companion utility to SANscape. For information about installing SANscape Alert, refer to the *SANscape Software Installation Guide*.

Unless otherwise specified, the SANnet II Blade SCSI JBOD array, SANnet II 200 SCSI array, SANnet II 220 SCSI array, SANnet II FC array, and SANnet II SATA array are referred to as the array or arrays.

This guide is written for experienced system administrators who are familiar with Dot Hill hardware and software products.

How This Book Is Organized

This book contains the following topics:

Chapter 1 introduces SANscape Alert and provides an overview about how it operates.

Chapter 2 provides steps on how to set up SANscape Alert.

Typographic Conventions

Typeface ¹	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; onscreen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>sccli> about</code>
<i>AaBbCc123</i>	Book titles, new words or terms, words to be emphasized, command-line variables.	Read Chapter 6 in the <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be a superuser to do this. To delete a file, type <code>rm filename</code> .

¹ The settings on your browser might differ from these settings.

Related Documentation

Title	Part Number
<i>SANnet II Blade SCSI JBOD Array Release Notes</i>	83-00003149
<i>SANnet II 200 SCSI Array Release Notes</i>	83-00002366
<i>SANnet II 220 SCSI Array Release Notes</i>	83-00003499
<i>SANnet II 200 FC, SATA, and SATA SE Array Release Notes</i>	83-00003262
<i>SANscape Software Installation Guide</i>	83-00003430
<i>SANscape User's Guide</i>	83-00003431
<i>SANscape CLI User's Guide</i>	83-00003433

Technical Support

For late-breaking *Release Notes* and all manuals for this product, go to the SANnet II SCSI array section, or the SANnet II FC array section, depending on which array you have, at:

<http://www.dothill.com/manuals>

The following information may be required when contacting Technical Support: Dot Hill serial number and part number of hardware; version of Dot Hill supplied software; host computer platform and operating system version; description of the problem and any related error messages.

Please also supply the following information to facilitate our tracking system and improve our response time: customer name, company name; state and country; telephone number with area code; Internet mail address; maintenance contract number, if applicable.

Placing a Support Call

After obtaining the above information, a support call may be placed by Internet mail, fax, or telephone.

Phone: 1-877-DOT7X24 (877-368-7924)

URL: <http://www.dothill.com/support/index.htm>

Corporate Headquarters Contacts

United States (California) Corporate Headquarters

Tel: 1-760-931-5500 or 1-800-872-2783
Fax: 1-760-931-5527
E-mail: support@dothill.com

Netherlands: European Headquarters

Dot Hill Systems Corp., B.V. (Netherlands)
Tel: 31 (0) 53 428 4980; Fax: 31 (0) 53 428 0562
E-mail: bv@dothill.com

Japan: Japanese Headquarters

Nihon Dot Hill Systems Corp., Ltd.
Tel: 81-3-3251-1690; Fax: 81-3-3251-1691
E-mail: nihon@dothill.com

For additional sales offices in the U.K., China, Sweden, Germany, France, Israel, and Singapore, please see our website:

<http://www.dothill.com/company/offices.htm>

Dot Hill Welcomes Your Comments

Dot Hill is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to:

support@dothill.com

Please include the part number (83-00003432) of your document in the subject line of your email.

CHAPTER 1

Overview

This chapter introduces SANscape Alert. Topics covered in this chapter include:

- “Installing SANscape Alert” on page 1
- “What is SANscape Alert?” on page 1
- “How SANscape Alert Operates” on page 2

Installing SANscape Alert

For installation instructions, refer to the *SANscape Software Installation Guide*.

What is SANscape Alert?

Instead of keeping the SANscape Console running in the foreground, you can use SANscape Alert as a companion utility of SANscape that runs as a background service that sends messages when triggered events occur from the hosts and arrays to specified email addresses. Using SANscape Alert, you can:

- Define the types of message traps sent
- Define the timing of messages sent
- Send encrypted messages
- Receive messages and decrypt encrypted messages on the Mail Receiver Tool (which functions as an email viewing program if you do not have a program such as Microsoft Outlook on the receiving computer)

To use SANscape Alert throughout the storage data network, install it as a service on each computer that has a controlling SANscape agent (a controlling agent is the only agent that talks to a specific array).

One major benefit of installing SANscape Alert on all host computers is that it can be configured to ping each computer periodically, and to send a single-point-of-failure message from a SANscape agent to the specified email addresses when a host fails.

SANscape Alert includes the following components:

- SANscape Alert agent (daemon) – Operates in background mode continuously on the computer where it is installed. The daemon can be installed and used on any computer where SANscape is running.
- SANscape Alert Config Tool (UI) – A utility that configures the types of message traps that are sent to the SANscape agent and that are sent to a specific email address as an alert or for informational purposes. Also known as the UI (user interface).
- SANscape Alert Mail Receiver Tool – Displays the messages that are collected. Also known as the POP3 Mail Receiver.

Note – To ensure that SANscape receives email, refer to the “Email and SNMP” appendix in the *SANscape User’s Guide* for information on setting traps.

How SANscape Alert Operates

After connecting to a SANscape agent, SANscape Alert receives all events from the agent. If the event is assigned a trap condition, then SANscape Alert emails the event to the user-specified email address.

Note – For the SANnet II Blade SCSI JBOD array, SANscape Alert sends triggered event notification only for environmental failures and hard drive failures.

If SANscape Alert cannot connect to any agent or the agent is offline, it then tries to discover the agent every five minutes. This prevents SANscape Alert from being disconnected from the agent when network traffic is congested.

In the typical setup shown in Figure 1-1, the array hosts (computers #1, #2, and #3) are used with the array devices (#A, #B, and #C respectively). Each host contains a SANscape agent and a SANscape Alert daemon. Each SANscape Alert daemon can be configured by the Config Tool to send event messages to any email address (shown as computer #5, which uses the Mail Receiver Tool to download the messages).

The SANscape Alert Config Tool and the SANscape Console can be located on any computer on the network and are located on one computer (#4) for convenience only.

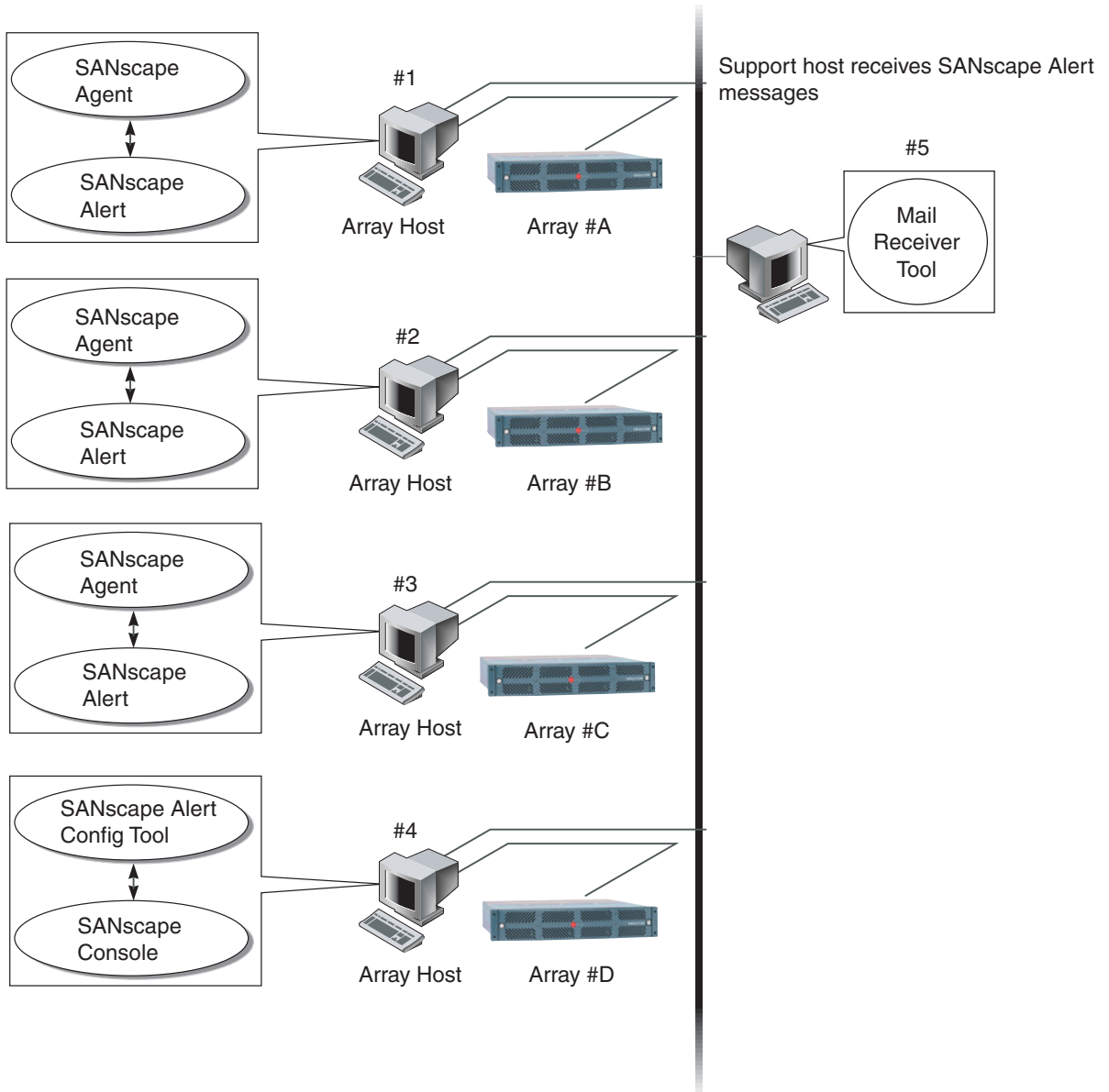


Figure 1-1 Typical SANscape Alert and SANscape Setup

CHAPTER 2

Using SANscape Alert

This chapter provides steps on using SANscape Alert, including the Report Tool and the Mail Receiver Tool. Topics covered in this chapter include:

- “Setting Up the SANscape Alert Configuration” on page 5
 - “To Set Up the Configuration” on page 5
 - “To Set Up the Report Tool” on page 13
 - “To Set Up the Mail Receiver Tool” on page 14
- “Troubleshooting” on page 15

Setting Up the SANscape Alert Configuration

Only one instance of the Config utility can be open at a time. The configuration information is saved in a file named `ssalert_cfg.xml`. (See “Host Event Log” on page 11 for the location of this file.)

Note – To implement any configuration change to a service, you must be connected to a SANscape Alert server and you must click Save Configuration after you have completed the changes.

To Set Up the Configuration

1. Start SANscape Alert.
 - On a Solaris, Linux, HP-UX, or IBM AIX operating system, type:

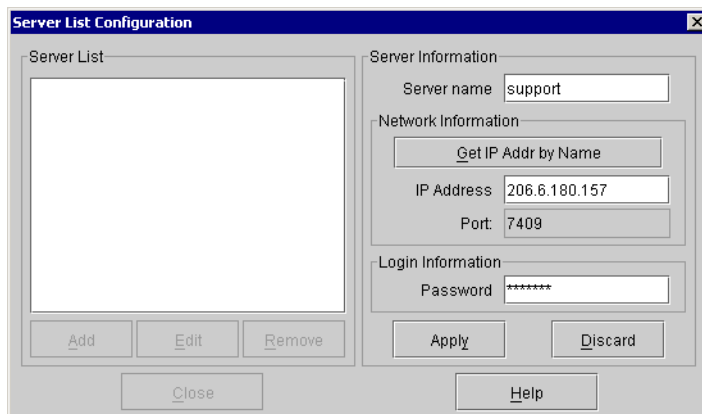
```
# ssalertd
```

- On a Microsoft Windows 2000 operating system, choose **Start → Programs → Dot Hill SANscape → SANscapeAlert → Dot Hill SANscape Alert Config Tool**.
- On a Windows 2003 operating system, choose **Start → All Programs → Dot Hill SANscape → SANscapeAlert → Dot Hill SANscape Alert Config Tool**.

If you have previously configured and connected to one SANscape Alert daemon, the Config Tool automatically connects to the server that you last used.

2. For the first-time installation, you must first set up a connection between the Config Tool and a server where a SANscape Alert daemon is running.
 - a. To create a server connection, choose **Servers** → **Server List Setup**.
 - b. In the **Server List Configuration** dialog box, click **Add** and enter the daemon server name and IP address.
 - c. Keep the default port number, which is displayed automatically and is used by the SANscape Alert Config Tool (UI) to communicate with the SANscape Alert daemon.
 - d. Type the **ssconfig** login password for the server.

This is the same login password that was set when you installed SANscape. If this password has not already been set, you must set it before continuing. Refer to the *SANscape Software Installation Guide* for details.
 - e. Click **Apply**.



The SANscape Alert server name and IP address are displayed in the **Server List**. The SANscape Alert Config Tool can access multiple servers, but can only connect to one server and one service at a time.

If you do not specify a password for each server, you are asked for a password each time you reconnect to a server.

3. Click **Close**.
4. To connect to a SANscape Alert server, choose **Servers** → **Connect to SANscape Alert Agent**, and then select the desired server from the list that is displayed.

Note – In some software versions, this command is displayed as “Connect to DR Agent.”

Note – The SANScape Alert agent must be running in order to connect to the server. Refer to the *SANScape Software Installation Guide* for instructions on starting the agent.

5. Select the **Basic Information** tab to enter information used for the email server and event messages.

The screenshot shows the 'SANScape Alert Configuration Tool' window. The title bar reads 'SANScape Alert Configuration Tool'. Below the title bar, there are 'Servers' and 'Help' menus. The main window title is 'SANScape Alert Server traininglab [127.0.0.1] Information'. There are three tabs: 'Basic Information' (selected), 'Trap Information', and 'SANScape Agent Information'. The 'Basic Information' tab contains several input fields: 'System ID' (206.6.1), 'Location' (Carlsbad), 'Customer Information' (Name: Dot Hill Systems, Phone, Fax, Address), and 'Note' (SANScape Alert). To the right, there is an 'SMTP information' section with fields for 'SMTP Server', 'From', a checkbox for 'My SMTP server need authorization', and 'SMTP server authorization information' (Username, Password). At the bottom, there are four buttons: 'Probe SANScape Agent', 'Save Configuration', 'Close', and 'Help'.

- System ID and Location – Descriptive fields for the server where the service resides.
- Customer and Contact Information – Provides information to be attached to the event emails, which is helpful when the event messages are sent to multiple email locations.
- SMTP Server – The IP address or domain name for the server that SANScape Alert uses to send email. If you enter an incorrect address (or domain name), SANScape Alert cannot find it and mail messages are not sent. If the SMTP server needs authorization, you must enter the necessary information to log in to the SMTP server.

6. Configure the **From** field using the following format:

name@domain

7. To specify the trap messages to be reported, select the **Trap Information** tab and click **Add**.

In the **Add Trap** dialog box, select and enter the desired parameters according to the information in Table 2-1.

Add Trap

Trap information

Content: All XML Format. cc to DotHill Service. use encrypt

Trap Type

Event Periodic

Property of event type trap

Min interval between mails(HH:MM)

Active trap events

Information event

Warning event

Critical event

Property of periodic trap

Minute:

Hour:

Day of month:

Month:

Day of week:

Mail information

use encrypt encrypt key:

pager enabled no content Subject for pager:

mail to:

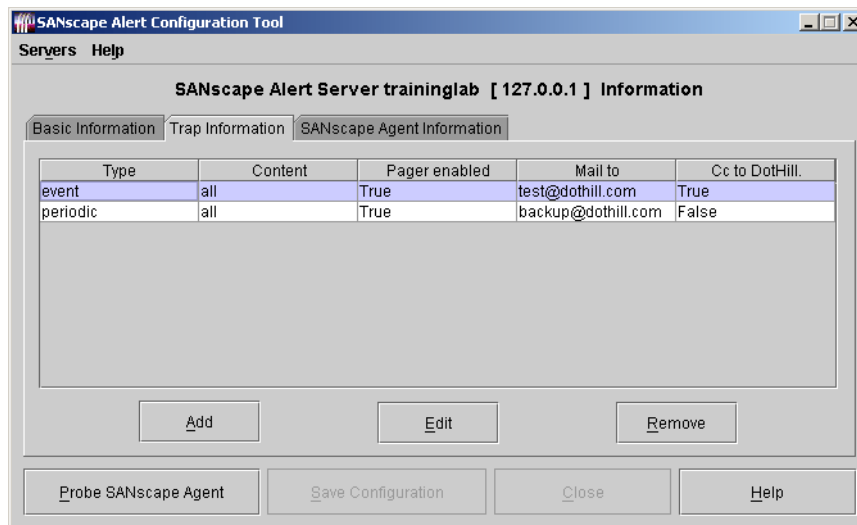
Save Cancel Help

As a minimum, select a trap event, enter the minimum interval between mails, and enter one email address. To enter multiple email addresses, separate each address with a space, comma, or semicolon.

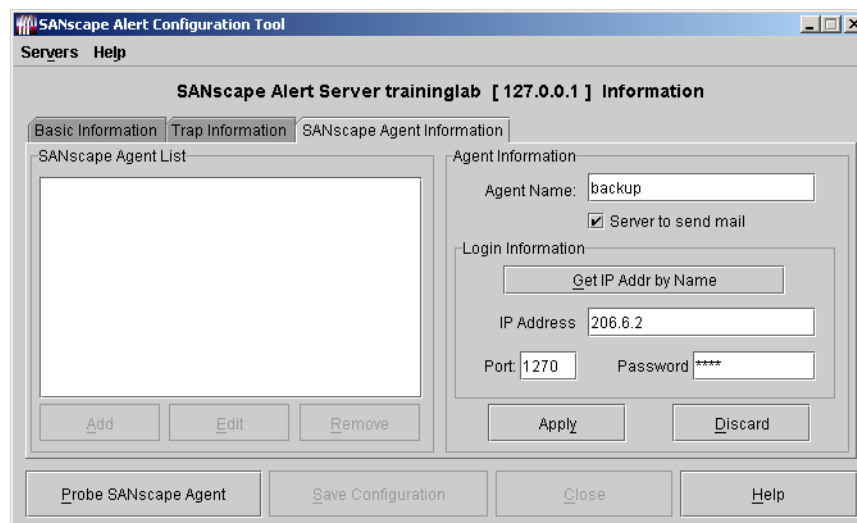
Table 2-1 Trap Information Parameters

Parameter	Values/Description
Content	Specifies the information to include in the email body. Values: all/ event /log /report /hosteventlog If you select an event trap and Minimum interval is 0 or *, the Content must be Event. To select periodic trap, Content cannot be Event.
XML Format	Select to generate the email and report in XML format.
Trap type	Select trap type Property of event type trap or Property of periodic trap.
Minimum interval between mails	For the interval between emails for an event type trap, specify the desired values: * - reports all events as they occur HH:MM - sets a specific time of day in hour:minute format, for reporting the last event message delivered during the time interval, using a 24-hour clock. Example: 16:30 = 4:30PM. Note: Always use the HH:MM format. For example, if you want to set the time interval to every 24 hours, set it to 24:00. Remember to include the colon.
Active trap events	An event trap is activated by an event, with a choice of any three kinds of event.
Periodic trap type	Use crontab format to define when to send emails: minute (0-59) hour (0-23) day of month (1-31) month (1-12) day of week (0-6 with 0=Sunday)
Checkbox – use encrypt	If selected, sends encrypted emails. To encrypt the email sent to Dot Hill, select use encrypt. The encrypt key is an identifier (optional) that is displayed when you download event messages.
Checkbox – pager enabled	To send mail to a pager-enabled mail address, select this box and enter the mail subject in Subject for Pager. If you do not want this mail to include any content, select no content.
Checkbox – no content	
mail to:	Define the email address for mail. You can specify several mail addresses, separated by “ “, “ ”, “;”.

In the following example, all events are selected and sent to **test@dothill.com**.



8. SANscape Alert can connect to multiple SANscape agents at the same time. To connect to one or more SANscape agents, click the **SANscape Agent Information** tab and click **Add**.



For each SANscape agent, specify the Agent Name, Agent IP Address, Port and Password for the **ssconfig** user accessing that agent.

- **Agent Name** – Name that is included in emails. You can use the real machine host name or an alias.
- **Port** – The SANscape agent listener port number. Keep the default value 1270 (other valid values are 1271, 1272, and 1273). If you cannot connect to the agent, change the value and try again.

- **Password** – The password for the `ssconfig` user. Before the SANscape Alert daemon can connect to the SANscape agent, the Service must provide the correct password for the `ssconfig` user.

After you have entered the agent parameters, click **Discard** to cancel changes, or click **Apply** to save the configuration. Each agent listed in the agent sends the specified event messages to the SANscape Alert Service where this configuration has been saved.

9. After you create or edit any configuration, click **Save Configuration** in the main window to save the configuration to SANscape Alert.

SANscape Alert Service restarts to read the configuration file again.

10. To see the current status of each agent at a specific moment, click **Probe SANscape Agent** in the main window.

In the Agent Information window, the colored status buttons indicate if the SANscape Alert Service is active with the SANscape agent on each agent server.

- **Red** – SANscape Alert cannot connect to the SANscape agent.
- **Yellow** – SANscape Alert is seeking the SANscape agent.
- **Green** – SANscape Alert is connected to the SANscape agent.
- **None** – The SANscape agent information has not been saved.

The color and text of this button can change every 20 seconds.

Host Event Log

When there is a triggered event, SANscape Alert attaches the host event log to the email that is sent. The events are logged into the system log of the host where the agent is installed. The following table lists the locations where the events are logged to in each operating system.

Table 2-2 Event Log Location

OS	Event Log Location
Solaris OS	<code>/var/adm/messages</code> (Also shown on the console)
Linux OS	<code>/var/log/messages</code>
Microsoft Windows OS	The application log of the system, which can be viewed using Event Viewer. You can also read the event log directly from the file <code>\Program Files\Dot Hill\SANscape Console\eventlog.txt</code>
HP-UX OS	<code>/var/adm/syslog/syslog.log</code>

Note – For an IBM AIX operating system, the event logs are not logged by default. Refer to the *SANscape User's Guide* for more information about writing events to a logfile for an IBM AIX host.

Because the host can generate a large amount of messages, it is possible to exceed the mail size limit allowed by some SMTP servers. SANscape Alert limits the size of the host event log to 5 Mbyte. This limit can be changed by defining the mail size limit attribute of the smtp element in **ssalert_cfg.xml**. The following table lists the location of this file for each operating system.

Table 2-3 **ssalert_cfg.xml** File Location

OS	ssdgrpt_cfg.xml Location
Solaris, Linux, and HP-UX OS	<code>/opt/dot_hill/SANscapeAlert/</code>
Microsoft Windows OS	<code><install path\service\</code> , where the default install path is <code>C:\Program Files\Dot Hill\Dot Hill\SANscapeAlert\service</code>
IBM AIX	<code>/opt/dot_hill/SANscapeAlert</code>

For example, to define the host event log size limit to 1 Mbyte (1 Mbyte = 1024 x 1024 = 1048576), define the mail size limit attribute as follows:

```
<smtp auth="false" username="" password="XXXX"
mail_size_limit="1048576" from="test@sina.com"
>smtp.sina.com</smtp>
```

Note – If the mail size limit attribute is not defined, SANscape Alert uses the default value of 5 Mbyte.

To Set Up the Report Tool

The report capability enables you to generate a report that contains the configuration of all locally attached arrays.

UNIX Operating System

The following steps describe how to set up the report tool on UNIX systems.

1. On a UNIX operating system, configure the local host to monitor the locally attached arrays.
 - a. From the main window, choose **Array Administration** → **Controller Assignment**. The **Assign Server to Manage a RAID Controller** window is displayed.
 - b. Select a server from the **Server to manage this controller** list and click **Apply**. This enables the selected server to manage an array controller. It also disables all other servers listed from managing the same array.
 - c. Click **Close** to close the view.
2. Add the local server to the `ssaltcli.cfg` file by typing the following command from the server that is attached to and managing the array:

```
# /usr/sbin/ssalertd -c -s password@ip address
```

You are prompted for the `ssconfig` password.

3. Run the following command to generate the report:

```
# /usr/sbin/ssalertd -r
```

The default report file name is `report.xml`. For systems running the Solaris, Linux, or HP-UX operating system, it is saved to `/opt/dothill/SANscapeAlertUI`. For systems running the IBM AIX operating system, it is saved to `/usr/dothill/SANscapeAlertUI`.

Microsoft Windows Operating System

The following steps describe how to set up the report tool on a Microsoft Windows operating system.

1. Change to the directory where `ssalertd.jar` was installed (default `C:\Program Files\Dot Hill\SANscapeAlert\service`).
2. Run the following command:

```
java -cp .\;.\ssalertd.jar sanscape_daemon -x -x
```

where *x*'s are **c** and **s** to generate the report in **xml** format, or **r** and **e** to generate the report in **txt** format.

Note – Whether you generate the report as **xml** or **txt**, the extension remains **xml**.

3. Run the following command:

```
java -cp .\;.\ssalertd.jar sanscape_daemon -r
```

The default report file name is `report.xml` and is saved to the directory where `ssalertd.jar` was installed.

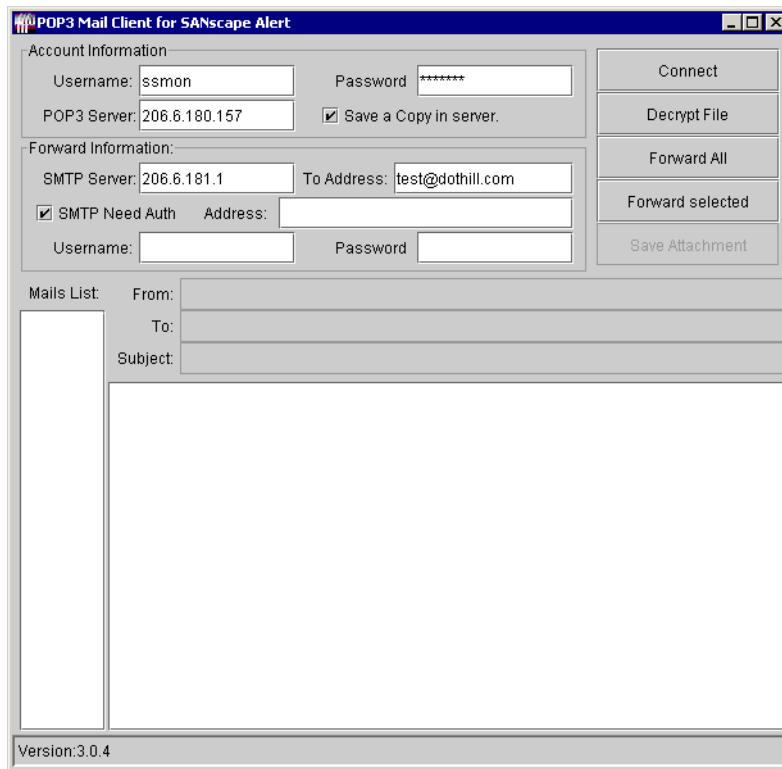
To Set Up the Mail Receiver Tool

The Mail Receiver Tool is optional and can be used in place of your regular email application. It can be used to receive and forward unencrypted and encrypted email.

1. Start the Mail Receiver Tool.
 - On a Solaris, Linux, HP-UX, or IBM AIX operating system, type:

```
# ssalertpop
```

- On a Microsoft Windows 2000 operating system, choose **Start** → **Programs** → **Dot Hill SANscape** → **SANscape Alert** → **SANscape Alert Mail Receiver Tool**.
 - On a Windows 2003 operating system, choose **Start** → **All Programs** → **Dot Hill SANscape** → **SANscape Alert** → **SANscape Alert Mail Receiver Tool**.
2. In the **POP3 Mail Receiver** window, identify the username, password, and email server IP address (POP Server) where the event messages are to be sent.
If needed, specify the appropriate SMTP information.



- a. To receive event messages, click **Connect**.
- b. If decryption is necessary, click **Decrypt File**.
- c. For event information or alerts that need to be sent to additional staff, click **Forward All** or **Forward Selected** and specify the destination address(es).

Troubleshooting

Note – For a list of error messages and prompts, refer to the “Error Codes and Messages” appendix in the *SANscape User’s Guide*.

If you stop receiving email messages from SANscape Alert, it might need to be stopped and restarted.

(UNIX operating system) There are three conditions under which SANscape Alert stops working and does not report its condition.

- If the SANscape agent fails or is stopped and restarted, SANscape Alert stops working.
- If the SANscape Alert Config Tool is running and the daemon is stopped and restarted, a condition might occur whereby the Config Tool can no longer communicate with the daemon.

- If the SANscape agent fails or is stopped, the SANscape Alert daemon does not detect it, stops sending email messages, and continues to show that SANscape Alert is still connected by displaying a green status.

The workaround is to stop and restart SANscape Alert as explained in the following steps.

Note – To start and stop the agents (daemons), you must have superuser (administrator) privileges.

To Stop and Start SANscape Alert on a Solaris Host or Linux Host

Type:

```
# /etc/init.d/ssalertd stop
# /etc/init.d/ssalertd start
```

To Stop and Start SANscape Alert on a Windows 2000 or 2003 Host

1. To start the agent software on a Windows 2000 host, choose **Start** → **Programs** → **Administrative Tools** → **Computer Management**.
To start the agent software on a Windows 2003 host, choose **Start** → **Administrative Tools** → **Computer Management**.
Alternatively, you can right-click **My Computer** and select **Manage**.
2. Click **Services & Applications**.
3. Select the **SANscape Alert server**, and right-click the service you want to stop or start.

To Stop and Start SANscape Alert on an HP-UX Host

Type:

```
# /sbin/init.d/ssalertd stop
# /sbin/init.d/ssalertd start
```


To Stop and Start SANscape Alert on an IBM AIX Host

Type:

```
# /usr/sbin/ssalertd stop  
# /usr/sbin/ssalertd start
```

