



Installation and Administration

Version 2.9.45



Onaro Inc. • 46 Waltham Street • Boston, MA 02118
Phone 617.338.0068 • Fax 617.338.1444

— All rights reserved. —

This manual and the information contained herein are confidential and proprietary to Onaro Inc. Only Onaro or its Licensees have the right to use the information. Any unauthorized use, disclosure or reproduction is a violation of the licenses and/or Onaro's proprietary rights and will be prosecuted to the full extent of the Law.

Company, brand, product, and service names are trademarks or registered trademarks of their respective holders.

SANscreen has been checked in accordance with Onaro, Inc. quality standards and has been found to comply with Onaro's published specifications.

DISCLAIMER

The information contained in this publication is subject to change without notice. ONARO, Inc. makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Onaro Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

LICENSES and COPYRIGHTS

Onaro® and SANscreen® are registered trademarks of ONARO, Inc. in the United States and other countries.

Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies.

Additional copyright information for third-party code provided with the product is set forth in the documentation.

Table of Contents

Preface	vii
Customer Service	vii
Quick Start Instructions	viii
Chapter 1 SANscreen Architecture	1
1.1 Overview of Components	1
1.2 SANscreen Server and Local Acquisition Unit	3
1.3 Remote Acquisition Unit	3
1.4 SANscreen Client GUI	3
Chapter 2 Installing SANscreen	5
2.1 Before You Install SANscreen... ..	5
2.2 Using the Installation Wizard	6
2.3 Verifying New SANscreen Services	10
2.4 Uninstalling SANscreen	11
Chapter 3 Installing the Remote Acquisition Unit	13
3.1 Before You Install the Remote Acquisition Unit... ..	14
3.2 RAU Installation Procedure	14
3.3 Verifying the New RAU Service	16
3.4 Validating the Installation	16
3.5 Uninstalling the Remote Acquisition Unit	17
Chapter 4 Starting and Stopping SANscreen	19
4.1 Starting and Stopping SANscreen Service	19
4.2 Starting the SANscreen Client	20
4.2.1 Using the Start Menu	20
4.2.2 Using a Web Browser	21
Chapter 5 Viewing Acquisition Units	23
Chapter 6 Using Data Sources to Discover the SAN	25
6.1 Understanding Data Source Concepts	26
6.2 Preparation	26
6.3 The Data Sources Screen Described	27
6.3.1 The Main Data Source Table	28

6.3.2 The History Tab	29
6.4 Operations	30
6.5 Adding a Data Source	31
6.6 Editing Data Source Properties	33
6.7 Starting a Data Source	34
6.8 Stopping a Data Source	34
6.9 Removing a Data Source	35
6.10 Forcing Acquisition	36
6.11 Clearing History	36
6.12 Troubleshooting	37
6.12.1 Unauthorized Operation	37
6.12.2 Faulty Acquisition Unit Status	37
6.12.3 Unsuccessful Acquisition or Faulty Data Source	38
Chapter 7 SANscreen Administration Portal	39
Chapter 8 User Management	41
8.1 User Roles	42
8.2 SANscreen User Management Screen	43
If You Have User or Guest Privileges	45
8.3 Maintaining User Definitions via LDAP	46
8.3.1 LDAP Configuration Screen	46
8.3.2 Validating the LDAP Configuration	49
8.4 Maintaining User Definitions Locally	49
8.4.1 Summary of Operations	50
8.4.2 Adding a New User	50
8.4.3 Changing Your Password	52
8.4.4 Editing a User Definition	53
8.4.5 Deleting a User Account	53
8.4.6 Changing User Password	54
Chapter 9 Configuring E-mail Notification	55
Chapter 10 Configuring SNMP Notification	57
Chapter 11 Installing a License	59
Chapter 12 Troubleshooting: Reviewing the Logs	61
Chapter 13 Backing Up and Restoring the Database	63
13.1 Backup	63
13.2 Restore	64
Chapter 14 Configuring the Mail Home Feature	65

Appendix A Available Data Sources	69
A.1 3Par InServ	69
A.2 Brocade (All Brocade switches)	71
A.3 Brocade (SNMP)	72
A.4 Cisco	73
A.5 EMC (Clariion).....	74
A.6 EMC (Clariion CLI)	75
A.7 EMC (Connectrix).....	76
A.8 EMC (StorageScope Host Resolver)	77
A.9 EMC (Symmetrix Family API)	78
A.10 HDS (HiCommand)	79
A.11 HDS SMI-S.....	80
A.12 HP (EVA).....	80
A.13 HP (XP CLI).....	81
A.14 HP (XP family SMI-S).....	82
A.15 IBM (Enterprise Storage Server).....	82
A.16 IBM (Enterprise Storage Server SMI-S).....	83
A.17 IBM (SVC)	83
A.18 IBM (FASTT)	83
A.19 InRange (FC9000 Director).....	84
A.20 McData (Enterprise Fabric Connectivity Manager)	85
A.21 McData (Sphereon).....	86
A.22 QLogic SANsurfer	87
A.23 SUN (StorEdge 6130)	88
A.24 SUN (StorEdge 6x20)	88
A.25 SMI-S Support Devices.....	88
Appendix B Hardware and Software Requirements	91
B.1 SANscreen Server Requirements	91
B.2 Remote Acquisition Unit Requirements	91
B.3 SANscreen Client GUI Requirements	92
Appendix C Copyright Notices	93

Figures

Figure 1: Example of a common SANscreen Implementation	2
--	---

Tables

Table 1: Summary of Supported Data Sources	70
--	----

Preface

The SANscreen *Installation and Administration* manual is intended for use by SAN administrators, and other members of the storage management team who install and administer SANscreen.

Customer Service

For questions, comments, or suggestions, contact Onaro at:

support@onaro.com

or

617.338.0068

Onaro is proud of being not just a leading-edge technological innovator in the important area of SAN availability assurance, but also a customer-focused and service-oriented company.

We will be happy to hear from you!

Quick Start Instructions

Task	For details see chapter...
1. Understand the SANscreen architecture.	1— SANscreen Architecture
2. Install SANscreen and verify the installation.	2 — Installing SANscreen 3 — Installing the Remote Acquisition Unit
3. Enter the license key.	7 — SANscreen Administration Portal 11 — Installing a License
4. Start the SANscreen server and Acquisition Units.	4 — Starting and Stopping SANscreen
5. Discover the SAN device topology and configurations.	5 — Viewing Acquisition Units 6 — Using Data Sources to Discover the SAN
6. Configure users, e-mail and SNMP notification.	8 — User Management 9 — Configuring E-mail Notification 10 — Configuring SNMP Notification
7. Perform database Backup and Restore operations.	13 — Backing Up and Restoring the Database
8. Configure what information to send automatically to Onaro, on a periodic basis.	14 — Configuring the Mail Home Feature

Chapter 1

SANscreen Architecture

This chapter presents a high level description of the SANscreen architecture.

1.1 Overview of Components

The SANscreen solution comprises three main components:

- **SANscreen Server** — SANscreen's main repository and analysis component. The server stores the SAN information and policies, and provides impact analysis and simulation capabilities.
- **SANscreen Acquisition Unit** — SANscreen's acquisition component, which communicates with SAN devices and provides device information to the SANscreen server. There are two types of Acquisition units:
 - o A **Local Acquisition Unit (LAU)** is installed with the SANscreen server.
 - o A **Remote Acquisition Unit (RAU)** can optionally be installed on a remote server(s), as required.
- **SANscreen Client GUI** — SANscreen's Java-based GUI, which provides access to the various SANscreen features through a Graphical User Interface.

Figure 1 shows an example in which four islands are managed centrally, using:

- The SANscreen server.
- The LAU (to communicate with the main data center and two local data centers).
- An RAU (to communicate with a remote data center).

While communication flows in both directions, the arrows indicate the direction in which communication is initiated:

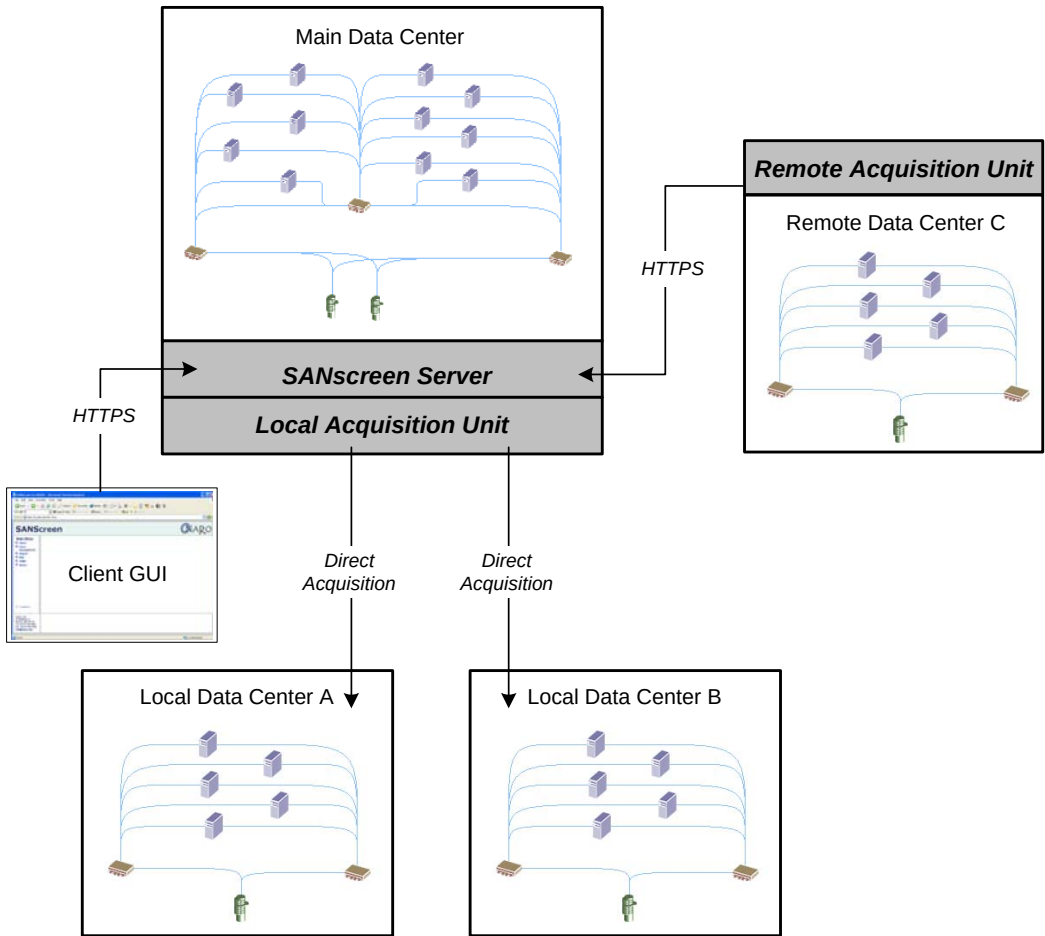


Figure 1: Example of a common SANscreen Implementation

The following sections describe each component in more detail.

1.2 SANscreen Server and Local Acquisition Unit

The SANscreen server comprises:

- An SQL database that stores information about your SAN configuration.
- The impact analysis and simulation engine.
- The Local Acquisition Unit.

The server receives regular updates regarding SAN changes from the Local Acquisition Unit (LAU), and from any Remote Acquisition Unit(s) that are installed (detailed in the next section). These updates are passed through a secured communication channel.

1.3 Remote Acquisition Unit

The Remote Acquisition Unit (RAU) is installed on remote servers to acquire SAN information about remote data centers. The RAU is fully controlled and configured from the SANscreen server, using the secured communication channel. Upon discovery of SAN changes, the RAU sends the information to the SANscreen server through the secured channel.

Installation of an RAU is required to:

- Acquire information from SAN devices that reside behind a firewall.
- Acquire information from SAN devices that are located at a remote site.
- Acquire information from SAN devices that are on a private network.
- Add load balancing to the installation, and provide redundancy to the other (local and remote) Acquisition Units.

1.4 SANscreen Client GUI

The SANscreen client GUI is Java-based, and requires no specific installation. It must run on a PC that's compatible with the client hardware and software requirements, including Java (see Appendix B).

Chapter 2

Installing SANscreen

This chapter steps you through the process of installing SANscreen on the dedicated server, and is broken down as follows:

- **Section 2.1 Before You Install SANscreen...** describes the prerequisites to the installation.
- **Section 2.2 Using the Installation Wizard** (page 6) details the installation steps.
- **Section 2.3 Verifying New SANscreen Services** (page 10) lists the services that were added to the Windows services environment during the installation process.
- **Section 2.4 Uninstalling SANscreen** (page 11) tells how to uninstall SANscreen, including related notes.

The SANscreen installation is self-contained, and includes all the elements required to run and operate SANscreen — including the SANscreen server and a Local Acquisition Unit. After the basic installation, you can install any number of Remote Acquisition Units, to add remote data-centers and private networks to the SAN devices that are managed by SANscreen. Refer to Chapter 3 for instructions to install RAUs.

2.1 Before You Install SANscreen...

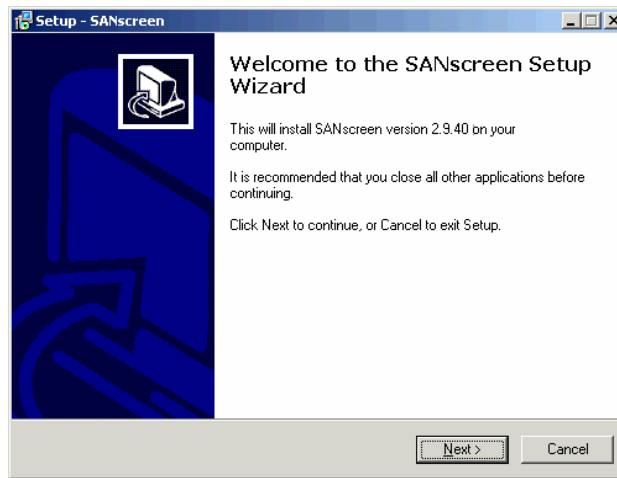
Before installing SANscreen, please make sure you have:

- The SANscreen installation CD.
- A license to operate SANscreen.
- The correct hardware/software environment (detailed in Appendix B).
- A deployment plan that includes hardware and network configurations for the SANscreen server, client, and Remote Acquisition Units, and SANscreen client.

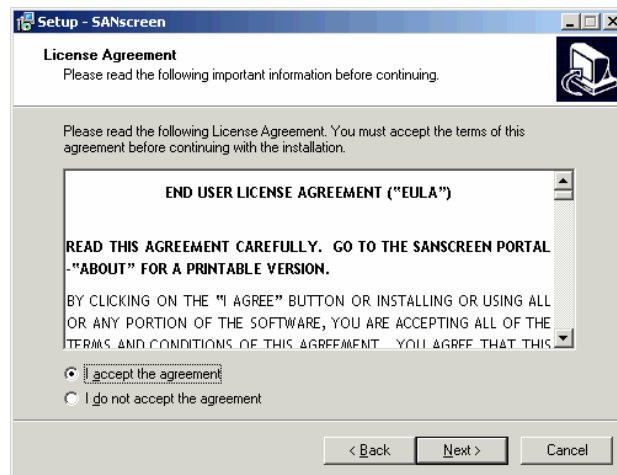
2.2 Using the Installation Wizard

Follow the instructions below to install SANscreen:

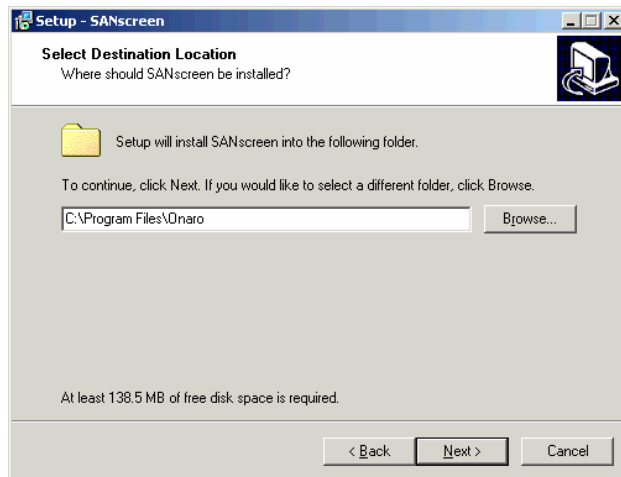
1. Log in to Windows using an account with administrator privileges.
2. Insert the SANscreen Installation CD into the drive.
3. Open Windows Explorer, select the CD directory, then double click setup.exe. Click Next from the first window to continue:



4. The next window is the License Agreement. Mark the Accept button then click Next:

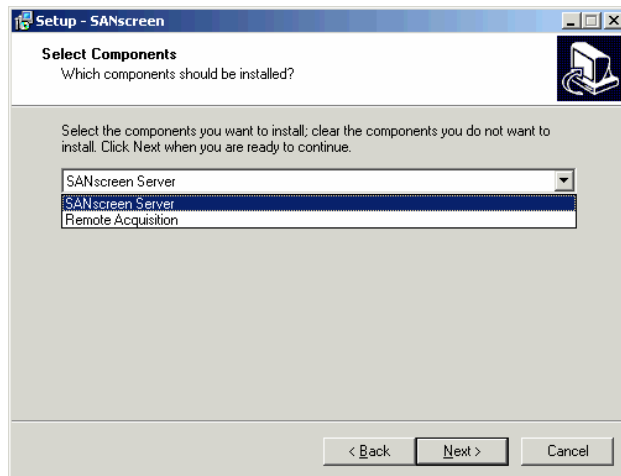


5. The next window prompts for the directory where you want install SANSscreen (defaults to C:\Program Files\Onaro):



Browse to another location, if necessary, then click the Next button to continue.

6. Select the component(s) you want to install, then click Next:
 - o **SANSscreen Server** requests the SANSscreen server and the Local Acquisition Unit.
 - o **Remote Acquisition** requests the Remote Acquisition Unit.



The following steps apply if you selected SANSscreen Server. The Remote Acquisition installation is described in Chapter 3.

7. Use the next window to configure system attributes, clicking Next when you're through:

Setup - SANscreen

Configure SANscreen
What configuration to install?

Change the configuration you would like Setup to install, then click Next.

SANscreen Portal Port (HTTP)
80

SANscreen secured Remote Acquisition Port (HTTPS)
443

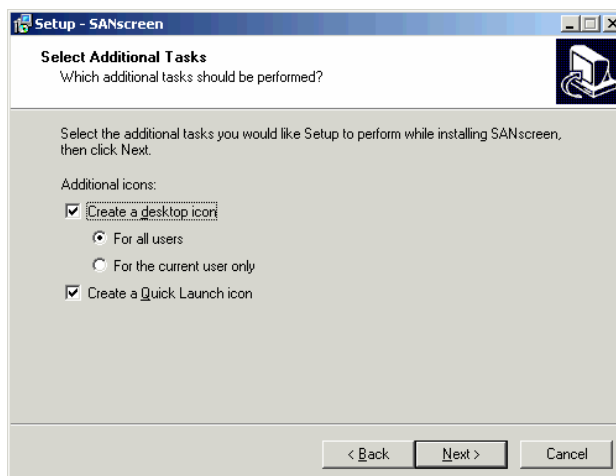
Internal Database port (SQL)
3306

Database size (MB)
200

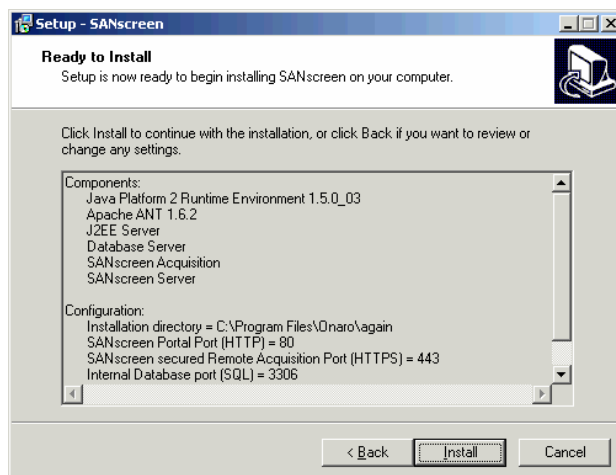
< Back Next > Cancel

Attribute	Used to Configure the...
SANscreen Portal Port (HTTP)	Port used by the SANscreen server to support user Web services, including a portal to launch the client and to perform administration tasks. Change this to 8080 if port 80 is already in use; otherwise leave the default (80).
SANscreen Secured Remote Acquisition Port (HTTPS)	Port used by Remote Acquisition Units to send SAN change information to the SANscreen server through a secured communication channel. Change this setting if port conflict occurs; otherwise leave the default (443). You'll specify this same port number when configuring RAUs (see page 15).
Internal Database Port (SQL)	Port used internally by the PC where the SANscreen server is running, to serve as an access point to the database. Change this setting if port conflict occurs; otherwise leave the default (3306).
Database Size(MB)	Size of the SQL database that provides a repository for the SAN data. The default size (200MB) can hold a 200-host SAN for more than ten years, and is generally a good initial database size.

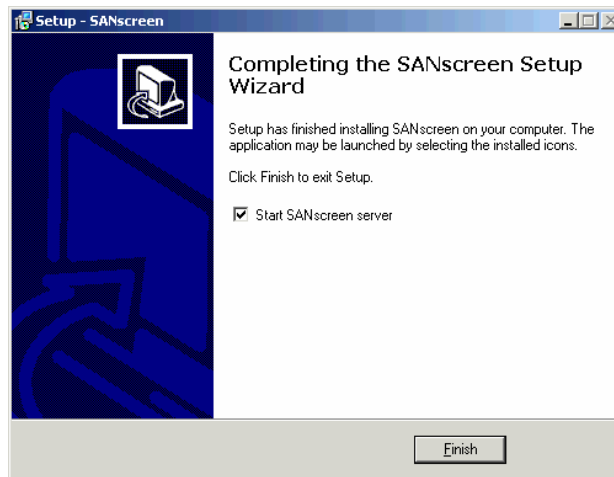
8. Choose the startup shortcuts you want to use for a quick launch, then click Next:



9. Review your installation selections, then either click Back to go back and make changes, or Install to approve the parameters and proceed:



10. After clicking Install above, wait for the installation to complete. This should take approximately 5 minutes, and ends with this window:



11. Mark the Start SANscreen Server box to start SANscreen, then click Finish to end the installation.

You'll have to enter a software license key to enable SANscreen features. Please refer to Chapter 11 for instructions to do this.

2.3 Verifying New SANscreen Services

Following a successful installation, these new SANscreen services should be available in the Windows services environment:

- **SANscreen Server** — The SANscreen server.
- **SANscreen Acq** — SANscreen's Local Acquisition Unit (LAU).
- **MySql** — SANscreen's SQL database.

Look for the new services in the OS Services window:

Start – Settings – Control Panel – Administrative Tools – Services

Alternatively, open the command window (Start – Run) and enter the following command to obtain the list of services:

```
net start
```

2.4 Uninstalling SANscreen

If you wish to uninstall SANscreen:

1. Stop the SANscreen server.
2. Open the Add/Remove Programs feature from the Control Panel.
3. Select the SANscreen application for removal.

Be Careful: Uninstalling SANscreen will **permanently delete** all SANscreen data.

Chapter 3

Installing the Remote Acquisition Unit

This chapter steps you through the process of installing a Remote Acquisition Unit (RAU). Installation of an RAU is required to:

- Acquire information from SAN devices that reside behind a firewall.
- Acquire information from SAN devices that are located at a remote site.
- Acquire information from SAN devices that are on a private network.
- Add load balancing to the installation, and provide redundancy to the other (local and remote) Acquisition Units.

This chapter is broken down as follows:

- **Section 3.1 Before You Install the Remote Acquisition Unit...** describes the prerequisites to the installation.
- **Section 3.2 RAU Installation Procedure** (page 14) details the installation steps.
- **Section 3.3 Verifying the New RAU Service** (page 16) tells how to verify that the new RAU service was added to the Windows services environment.
- **Section 3.4 Validating the Installation** (page 16) tells how to verify that the installation was successful using the SANscreen GUI.
- **Section 3.5 Uninstalling the Remote Acquisition Unit** (page 17) tells how to uninstall the Remote Acquisition Unit.

3.1 Before You Install the Remote Acquisition Unit...

Before installing an RAU, please make sure that:

- The RAU server meets the hardware and software requirements outlined in Appendix B.
- The RAU server has full network access to the SAN devices with which it has to communicate to properly acquire the data it must forward to the SAN server.
- At least one port is open and available between the RAU server and the SANscreen server, to forward change information to the server. If you are unsure about this, validate it by opening a Web Browser on the RAU computer and directing it to the SANscreen server:

`https://<SANscreen_hostname>:<acquisition_port>`

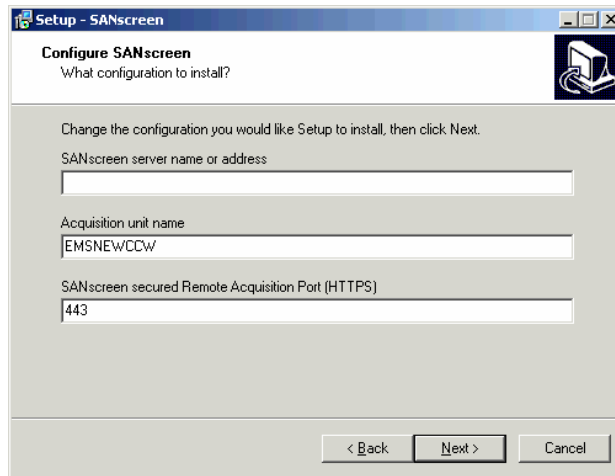
The acquisition port defaults to 443 but may have been changed during the server installation.

If the connection is successful, you'll see a SANscreen response page indicating an open and available port between the RAU and the SANscreen server.

3.2 RAU Installation Procedure

Please follow the instructions below to install the RAU:

1. Follow steps 1 – 5 of the basic installation procedure, described starting on page 6.
2. At step 6, select Remote Acquisition to install the RAU.
3. Using the configuration window shown below, set parameters that are specific to your site. Click Next when you're through.



Attribute	Used to Configure the...
SANscreen Server Name or Address	Hostname or IP address to identify the SANscreen server. The RAU uses this name/IP to open a communications link with the server. If you specify a hostname, make sure the name can be resolved through DNS.
Acquisition Unit Name	Unique name that identifies the RAU.
HTTPS Port	Port used by Remote Acquisition Units to send SAN change information to the SANscreen server. This setting should match the value entered when installing the SANscreen server (see page 8), and must be the same on all RAUs.

4. The wizard displays your installation selections. Either click Back to go back and make changes, or Install to approve the parameters and proceed.
5. After clicking Install above, wait for the installation to complete. This should take approximately 5 minutes, and ends with this window:



6. Mark the Start Remote Acquisition Service box to start the RAU, then click Finish to end the installation.

3.3 Verifying the New RAU Service

After a successful installation, the following SANscreen service should be available in the Windows services environment:

SANscreen Acq — SANscreen’s Remote Acquisition Unit (RAU).

Look for the new service in the OS Services view:

Start – Settings – Control Panel – Administrative Tools – Services

Alternatively, open the command window (Start – Run) and enter the following command to obtain the list of services:

```
net start
```

3.4 Validating the Installation

To validate the installation of the RAU:

1. Go to SANscreen’s Acquisition Units Screen (see Chapter 5) and verify that the new RAU was registered correctly and it has an OK status. If it does not, contact the Onaro support team.
2. Start Data Sources running from the newly installed Remote Acquisition Unit (see Chapter 6).

3.5 Uninstalling the Remote Acquisition Unit

If you wish to uninstall the RAU, use the Add/Remove Programs feature from the Control Panel. Then select the sanscreen application for removal.

Chapter 4

Starting and Stopping SANscreen

This chapter describes the methods available to start and stop SANscreen:

- **Section 4.1 Starting and Stopping SANscreen Service** tells how to start and stop the SANscreen service, including the server and LAU.
- **Section 4.2 Starting the SANscreen Client** (page 20) tell show to start and stop the SANscreen client (also known as the SANscreen Explorer).

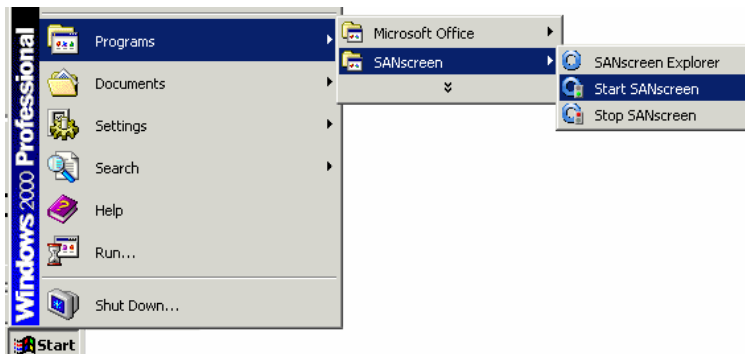
Note: Remote Acquisition Units start and stop with the host server where they are installed. No special instructions are included here.

4.1 Starting and Stopping SANscreen Service

SANscreen operates as a service. It runs in the background, and executes discovery, analysis, and monitoring operations continuously.

As installed, the SANscreen server service starts automatically with your PC. This service includes a Local Acquisition Unit, which also starts automatically.

The SANscreen server and the Local Acquisition Unit can be stopped and restarted using the Start menu, as illustrated below:

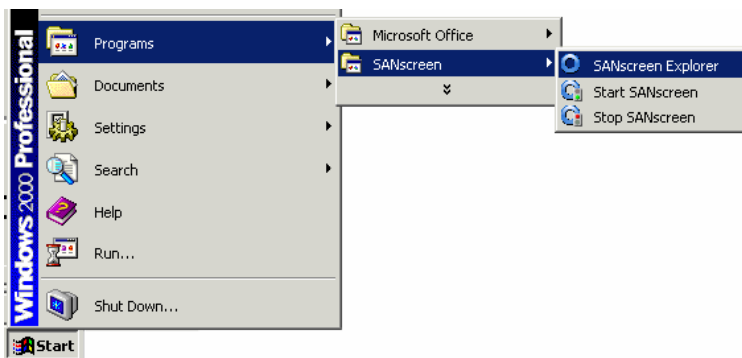


4.2 Starting the SANSscreen Client

You can run the SANSscreen client from the Start menu or from a Web browser, as detailed in the sections that follow.

4.2.1 Using the Start Menu

From the SANSscreen server, use the Start menu as follows to open the SANSscreen client:



The first time you start the client, Java asks if you want to add a shortcut to your Desktop and Start Menu (below). Respond as you wish.



Next a login window opens, illustrated to the right. Enter your user name and password, then click OK. If your user name is authorized and authenticated through an LDAP server, your login name must include an @ sign followed by the domain (e.g., bob@US.onaro.com).



The default (as-installed) user name is **admin**, and the password is **onaro**. It's a good idea to change these defaults as soon as possible after installation.

After a successful login, the main client screen opens:



Refer to the *SANscreen User Manual* for details about how to navigate from this screen, and for general information about working with the SANscreen GUI. The remaining chapters of this manual deal primarily with the Admin category of processing, shown to the left at the bottom of the navigation tree.

4.2.2 Using a Web Browser

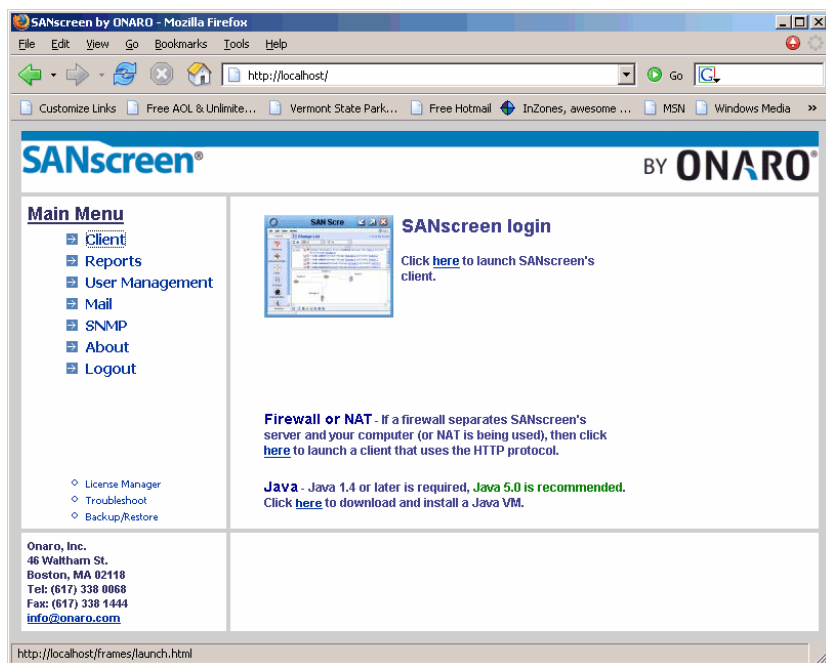
From any Web browser, enter the following URL to access the administration portal on the SANscreen server. The port number will be either 80 or 8080, as configured when the server was installed:

`http://<SANscreen_hostname>:<SANscreen_port>`

If you're accessing the client from the SANscreen server, enter:

`http://localhost`

After connecting with the SANscreen portal, the server opens a window through which you can access various SANscreen Web services. Click the Client link at the top of the Main Menu (left) to access the client login. This is illustrated in the portal window shown below:



Request the login window by clicking [here](#) to launch SANscreen's client.

Note1: If the Java Run Time environment (JRE) is not installed on your PC, SANscreen displays a message indicating that you have to install it. The Java link will direct you to a Windows JRE installation. If you're running a different operating system, please refer to the Java download site at: <http://java.sun.com>.

Note2: If a firewall separates the client PC from the SANscreen server, you cannot use the regular method of communicating. Click [here](#) under the Firewall or NAT notice in this case, to initiate communication via HTTP.

Java opens a security window, illustrated to the right for Internet Explorer. Click Start (or OK, if using another browsers), then proceed from the login window as described starting on page 20 (enter your user name and password, etc.)



Chapter 5

Viewing Acquisition Units

You can monitor the status of all running Acquisition Units, including the Local Acquisition Unit that's installed by default with the SANscreen server. To do this, choose Acquisition Units from the Admin tab (shown to the left below) to open the Acquisition Units screen:

Name	IP	Status
local	127.0.0.1	OK

Name	IP	Poll Interval	Vendor
EFCM	172.31.252.221	60	McData Enterprise Fat
EMC_SSDC	172.30.42.11	60	EMC Connectrix AP
EMC_SSDC2	172.30.42.16	60	EMC Connectrix AP
EMC_stgeb01	10.210.86.31	60	EMC Symmetrix Far
EMC_stgeb02	10.210.86.32	60	EMC Symmetrix Far
EMC_stgeb03	10.210.86.33	60	EMC Symmetrix Far
IBM	172.31.255.15	60	IBM Enterprise Sto
SSDC2	172.30.32.171	60	EMC Symmetrix Far

This screen comprises three tables:

- The main **Acquisition Units** table lists the various Acquisition Units that are installed. The Local Acquisition Unit, illustrated above, is installed by default with the SANscreen server. As you install Remote Acquisition Units, they appear in this main table as well.
- The **Acquisition Units Audit** tab applies after you select (click on) an Acquisition Unit in the main table. It lists any errors that occurred during the latest attempt to run the selected Acquisition Unit. Look at the error message to understand the cause, or contact the Onaro support team for assistance.

- The **Data Sources** tab also applies after you select an Acquisition Unit in the main table. It lists all the Data Sources that are assigned to (i.e., that run within) the selected Acquisition Unit.

Looking at the main table, verify that the Local Acquisition Unit and all RAUs are shown, and that they have an OK status. For any other status, the LAU is not running. If the Local Acquisition Unit is missing, make sure the corresponding service is running correctly (use "net start" and look for "sanscreen acq" or review the Windows services GUI).

Chapter 6

Using Data Sources to Discover the SAN

This chapter describes how to add and maintain Data Sources within SANscreen. Data Sources discover SAN information that's used for analysis and validation. The chapter is broken down as follows:

- **Section 6.1 Understanding Data Source Concepts** introduces the concept of a Data Source.
- **Section 6.2 Preparation** (page 26) tells what information you need to have at hand before proceeding.
- **Section 6.3 The Data Sources Screen Described** (page 27) provides an overview of the Data Sources screen, and details the information displayed in that screen.
- **Section 6.4 Operations** (page 30) describes the various operations available from the Data Sources screen.
- **Section 6.5 Adding a Data Source** (page 31) provides detailed instructions to add a new Data Source.
- **Section 6.6 Editing Data Source Properties** (page 33) tells how to modify a Data Source definition.
- **Section 6.9 Removing a Data Source** (page 35) tells how to remove a Data Source after it's no longer used.
- **Section 6.7 Starting a Data Source** (page 34) tells how to start a Data Source.
- **Section 6.8 Stopping a Data Source** (page 34) tells how to stop a Data Source.
- **Section 6.9 Removing a Data Source** (page 35) tells how to remove a Data Source after the device corresponding to the Data Source is no longer used in the SAN.
- **Section 6.10 Forcing Acquisition** (page 36) tells how to force a Data Source to start the acquisition process.

- **Section 6.11 Clearing History** (page 36) tells how to clear all History for a Data Source.
- **Section 6.12 Troubleshooting** (page 37) describes some common problems and how to correct them.

6.1 Understanding Data Source Concepts

A Data Source is a logical SANscreen component that continuously communicates with a particular SAN device (or device-management application), and provides SAN topology and configuration information to the SANscreen server. Each Data Source runs within a specific Acquisition Unit — either the Local Acquisition Unit, which is a standard part of each SANscreen server, or a Remote Acquisition Unit.

Each Data Source instance is directed to a single information source (SAN device or device-management application). The different types of Data Sources represent the various SAN devices supported by SANscreen. Please refer to *Appendix A, Available Data Sources*, for a complete list of the supported device types, and the parameter settings that are specific to each.

SANscreen Data Sources use a combination of IP-based communication techniques to gather the required data from SAN devices, combining the use of the following communication modes:

- **Event driven mode** — Used to update the system automatically when device information changes, based on SNMP trap messages.
- **Polling mode** — Used to sample the device regularly for its status, at some user-configured polling interval.

6.2 Preparation

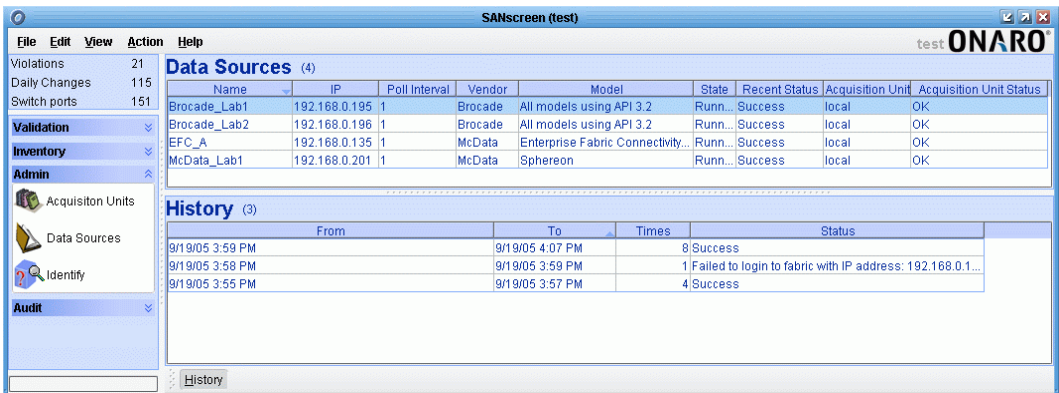
For each Data Source, the specific requirements to define that data source depend on the corresponding SAN device's vendor and model. Please refer to the appendix for detailed information. In general, you will need the following information to complete discovery of your SAN:

1. The IP address, user name, and password to access each SAN switch.
2. The IP address, user name, and password to access each device-management station.

3. The IP address, user name, and password to access each storage system that has IP connectivity.
4. The IP address, user name, and password to access each storage management station.
5. The IP address, user name, and password to access each host server that runs management software for a storage device that does *not* have direct IP connectivity.
6. A list of installed RAUs, and their device connectivity responsibilities.

6.3 The Data Sources Screen Described

Choose Data Sources from the Admin tab (shown to the left below) to open the Data Sources screen:



The screen is divided into two parts:

- The main **Data Sources** table lists all the registered Data Sources. By default, and before any Data Sources are added, this list is empty. After you add the first Data Source, the list shows the parameters and status of each Data Source that's running, across all Acquisition Units.
- The **History** tab applies after you select a Data Source in the main table. It lists the recent acquisition attempts made by the selected Data Source to its corresponding SAN device. If more than one attempt was made with the same resulting status, they are grouped into a single row, and the Times column reflects the number of attempts.

6.3.1 The Main Data Source Table

The following fields display in the main table for each Data Source:

Field	Description
Name	Name assigned to the Data Source when it was created (see page 31).
IP	IP address of the device (or device-management application) corresponding to the Data Source.
Poll Interval	Interval (in seconds) at which the Data Source should poll its corresponding device. <i>Note:</i> Receipt of an SNMP trap restarts the interval counter.
Vendor	Vendor for the device corresponding to the Data Source.
Model	Model of the device corresponding to the Data Source.
State	Current state of the Data Source: • Running — The Data Source is active and can acquire information from the device. • Stopped — The Data Source has been stopped.
Recent Status	Status of the latest attempt to acquire information from the device: • Success — The attempt is complete and succeeded. • Start Acquisition — The acquisition is in process. • <i>error message</i> — The acquisition attempt failed for the reason stated in the message.
Acquisition Unit	Name of the Acquisition Unit where this Data Source is running.
Acquisition Unit Status	Current status of the parent Acquisition Unit: • OK — The Acquisition Unit is up and running. • <i>error message</i> — There is a problem with the Acquisition Unit, as reflected by the message.

6.3.2 The History Tab

Select a specific Data Source in the main table to display its acquisition history. Each line of the History table represents one or more acquisition attempts that are grouped according to their status. All acquisitions that share the same final status are reported on a single line.

Field	Description
From	The starting time of the acquisition(s), in <i>mm/dd/yy hh:mm</i> format. If the line represents more than one acquisition attempt, this is the starting time of the earliest attempt.
To	The ending time of the acquisition(s), formatted as described above. If the line represents more than one acquisition attempt, this is the ending time of the last attempt.
Times	Number of acquisitions reported on this line; in other words, the number of acquisitions that have the same status.
Status	Status of the acquisition(s) reported on this line: • Success — The acquisition(s) completed successfully. • Start Acquisition — The acquisition is in process. • <i>error message</i> — The acquisition attempt(s) failed for the reason stated in the message.

6.4 Operations

With Data Sources displayed, the Action menu (or right-clicking the mouse from the main table) allows the actions described below:

Action
Add Data Source
Edit Data Source
Remove Data Source
Start data source
Stop data source
Force Acquisition
Clear history
Start Data Source Recording
Stop Data Source Recording
Crawl With Data Source
Http
Telnet

Action	Used to...	See page...
Add Data Source	Open a wizard that lets you add a new Data Source.	31
Edit Data Source	Open a wizard that lets you change the parameters of the selected Data Source.	33
Remove Data Source	Remove the selected Data Source and flag all data acquired from this Data Source as non-current. Note: Only remove a Data Source after it's no longer used. Do not remove a Data Source if it is only temporarily out of use.	35
Start Data Source	Start the selected Data Source (applicable only if the Data Source is Stopped).	34
Stop Data Source	Stop the selected Data Source (applicable only if the Data Source is Running). A stopped Data Source does not communicate with its corresponding device and does not retrieve SAN data.	34
Force Acquisition	Force the selected Data Source to initiate the data acquisition process. Use this feature to ensure that the most recent data has been acquired.	36
Clear History	Clear all history for the Data Source	36
Start Data Source Recording	Solve communication problems with the device. You will only use these fields upon request by Onaro support team.	—
Stop Data Source Recording		
Crawl With Data Source		
Http	Initiate a Web Browser and direct it to the SAN device monitored by the selected Data Source. This allows you to manage the device using a Web-based management tool (typically supplied by the vendor).	—

Action	Used to...	See page...
Telnet	Initiate a telnet session to the device, allowing you manage the device via telnet.	—

The sections that follow describe the first seven actions, in order as listed above.

6.5 Adding a Data Source

Add a Data Source when a new switch, storage device, or SAN management tool is added to the SAN environment — and you want to make its information available for analysis in SANscreen.

Before adding a new Data Source:

- Read the device-specific information in *Appendix A, Available Data Sources*.
- Prepare the information required to connect to the device (IP address, login user name, login password, etc).
- Verify that the Local Acquisition Unit and all RAUs are shown in the Acquisition Units table and that they have an OK status in the (see Chapter 5).

Choose Add Data Source from the Action menu to open a wizard that guides you through the process of adding a new Data Source:

1. Enter a unique name for the Data Source. You can choose any name that will make it easy for you to identify the Data Source, as long as it's unique across all Acquisition Units, and comprises alphanumeric characters (a-z, A-Z, 0-9).
2. Choose the Acquisition Unit where the Data Source will run (local specifies the Local Acquisition Unit on the SANscreen server).
3. Choose the vendor and the model of the device assigned to this Data Source; that is, the device from which the Data Source will acquire SAN information.
4. Click Next when you're through, to open the Data Source Configuration screen. This screen is specific to the type of device specified above, and is illustrated here for a Brocade switch:

5. Fill in the information requested by the configuration screen, referring to Appendix A for device-specific details about each parameter. Click Finish when you're through, to activate the Data Source in your environment.

Note: The Import button is used only upon request by the Onaro support team.

After you complete the configuration (above), a new row displays in the main table of the Data Sources screen. Proceed as follows to verify the new Data Source:

- Allow a reasonable amount of time for the acquisition to complete. Several seconds is generally enough, but some devices may be slow or highly populated and may take several minutes to acquire.
- Select the new Data Source in the main table.

- Examine either the main Data Source table or the acquisition History tab for successful acquisitions. If the Status field is Start Acquisition, the acquisition has not finished yet.

Note: As necessary, use the F5 key to refresh the display.

6.6 Editing Data Source Properties

The Edit Data Source option lets you examine and/or modify the Data Source parameters. This may be needed to correct an error in the original definition, or because of a configuration change to the SAN device (e.g. an updated password).

Note: You cannot modify the device name, vendor, or model.

To edit a Data Source:

1. Right-click the Data Source you want to edit in the main table.
2. Choose Edit Data Source from the drop-down menu, then follow the instructions in the edit wizard.
3. Click Next.
4. View and/or update the parameters, referring to Appendix A for details about each field.
5. Click Finish.

If the Data Source was active (status is Running), it will be restarted to run with the new parameters. If it was not active (status is Stopped), it remains inactive.

Verify the change(s) as follows:

- Start the Data Source if needed.
- Allow a reasonable period of time for the acquisition to complete, then examine the History pane for a successful acquisition.

6.7 Starting a Data Source

Starting a Data Source changes its status from Stopped to Running.

To start a Data Source:

1. Right-click the Data Source in the main table.
2. Choose Start Data Source from the drop-down menu.
3. Click Yes to confirm the operation.
4. After several seconds:
 - o Verify that the status changes to Running. As necessary, use the F5 key to refresh the display.
 - o Allow a reasonable period of time for an acquisition to complete, then examine the History pane for a successful acquisition.

6.8 Stopping a Data Source

Stopping a Data Source changes its status from Running to Stopped.

To stop a Data Source:

1. Right-click the Data Source in the main table.
2. Choose Stop Data Source from the drop-down menu.
3. Click Yes to confirm the operation.
4. After several seconds, verify that the status changes to Stopped. As necessary, use the F5 key to refresh the display.

6.9 Removing a Data Source

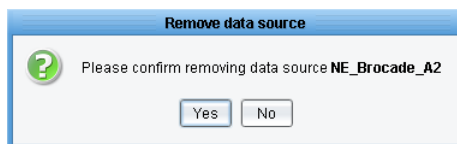
This operation removes the Data Source. Use it with caution, and only after the device corresponding to the Data Source is no longer used in the SAN.

After completing this operation:

- SANscreen presents any data that was acquired by the removed Data Source as non-current. This means that all devices, connectivity, volumes, zones, etc. that were discovered solely by the removed Data Source will disappear, and the Changes tab will indicate their removal. Please notice that the corresponding device itself still appears in SANscreen, but is grayed in the Topology and tables. You can use the "Delete inactive device" to remove them, as necessary.
- You will no longer see the paths that were created based on the information acquired from the removed Data Source.

To remove a Data Source:

1. Right-click the target Data Source in the main table.
2. Stop the Data Source (see page 34).
3. Choose Remove Data Source from the drop-down menu.
4. Click Yes in the confirmation box to confirm removal of the Data Source. After you confirm the removal, the row corresponding to the Data Source is dropped from the main table.
5. As necessary, use the Delete Inactive Device feature from the Topology view to remove a device permanently.



6.10 Forcing Acquisition

Forcing acquisition causes the selected Data Source to initiate the acquisition process immediately. If the Data Source is already in an acquisition process, SANscreen ignores this command.

Follow these steps to force acquisition for a Data Source:

1. Make sure the Data Source is started (status is Running).
2. Right-click the Data Source in the main table.
3. Choose Force Acquisition from the drop-down menu.
4. Click Yes to confirm the operation.

After forcing acquisition:

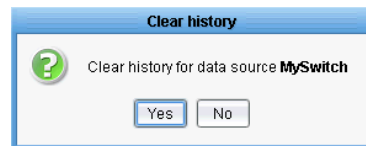
- The History pane should show a status of Start Acquisition.
- Allow a reasonable period of time for an acquisition to complete, then examine the History pane for a successful acquisition.

6.11 Clearing History

The Data Source history shows what acquisitions succeeded and failed. After a few weeks this information typically has no value.

Follow these steps to clear all History for a selected Data Source:

1. Right-click the Data Source in the main table.
2. Choose Clear History from the drop-down menu.
3. SANscreen verifies the request (right). Click Yes to continue.



After clearing the history, the History pane will be empty.

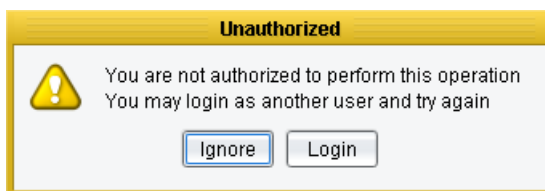
6.12 Troubleshooting

This section describes problems you might encounter while performing the operations described above, in order as follows:

- Unauthorized operation
- Faulty Acquisition Unit status
- Unsuccessful acquisition, or faulty Data Source

6.12.1 Unauthorized Operation

If the following dialog appears when you Click Finish from a wizard:



The operation failed because you are not an authorized user for the requested operation. You must have administrative privileges in order to work with Data Source configurations.

You can:

- Ignore the error and keep working with your current privilege level.
- Log in under a user name that has administrative privileges, and try again.

6.12.2 Faulty Acquisition Unit Status

If an Acquisition Unit Status field contains an error message in the main Data Sources table (i.e., is *not* OK), make sure the Acquisition Unit is running. For example, a Not Connected status indicates that the software is not running.

To verify that the service is running, open the Services window on the server where the Acquisition Unit was installed (on the SANscreen server for a Local Acquisition Unit; otherwise on a remote machine):

Start – Settings – Control Panel – Administrative Tools – Services

Look for the SANscreen Acq service. If the service is not running (status is Stopped), right-click the service and choose Start.

Recheck the status of the Data Source in the main table. The status should change to OK.

6.12.3 Unsuccessful Acquisition or Faulty Data Source

If a Data Source is unsuccessful in acquiring from its SAN device:

1. Examine the acquisition failure message in the History tab's Status field.
2. If the message is related to connectivity, make sure:
 - o The device is operational (not in maintenance).
 - o The device is reachable. (Try to ping the device, or use the Edit Data Source operation to verify that the connectivity parameters are correct (e.g. IP address)).
 - o The device is manageable (e.g. by telnet).
3. If the message is related to device access (e.g., Failed to log in to fabric), use the Edit Data Source operation to verify that the user name and password are correct.

Chapter 7

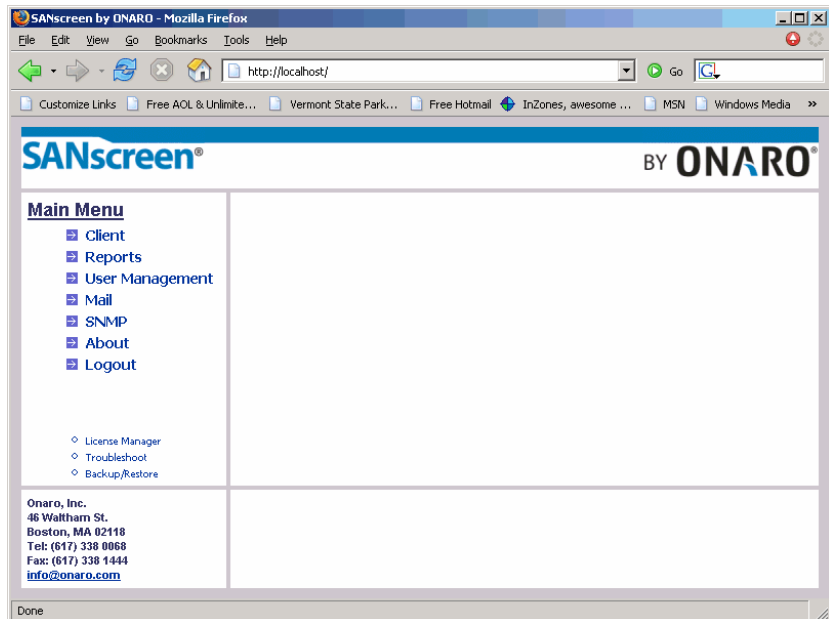
SANscreen Administration Portal

The SANscreen administration portal is available from any Web browser, by entering the following URL. The port number will be either 80 or 8080, as configured at when the server was installed:

`http://<SANscreen_hostname>:<SANscreen_port>`

If you're accessing the client from the SANscreen server, enter:

`http://localhost`



Use the administration portal as follows:

Menu Option	Used to ...	See Chapter
Client	Log in to the client GUI.	4
Reports	Generate various reports that: - Summarize the state of your SAN. - Detail discovered storage devices. - Identify and trends in your SAN configuration. - Report changes. - Detail planned tasks. These reports and their use are described in the <i>SANscreen User Manual</i> .	—
User Management	Maintain user accounts.	8
Mail	Configure SANscreen to find your e-mail server (to enable automatic notifications).	9
SNMP	Tell SANscreen where to send SNMP trap messages.	10
About	Display SANscreen current version and copyright information, as well as the JAR version and timestamp for each defined Data Source.	—
Logout	Log out as the current user.	—
License Manager	Install a new SANscreen license.	11
Troubleshoot	Copy SANscreen log files to your computer.	12
	Restart the SANscreen server, after which you'll be prompted to log in again.* Configure mail-home capabilities.	— 14
Backup/Restore	Backup and/or restore the SANscreen database.	13

* These restart options are available for troubleshooting purposes, and are only used upon request by Onaro support.

Chapter 8

User Management

This chapter describes the User Management screen, and tells how to add, edit and remove SANscreen user accounts.

User accounts, user authentication, and user authorization can be defined and managed in either of two ways.

- Through a Version 2 or 3 LDAP (Lightweight Directory Access Protocol) server, such as the Microsoft Active Directory.
- Through an internal SANscreen user database.

When a user logs in to SANscreen, the server first tries to authenticate through LDAP. If SANscreen cannot find the user on the LDAP server, it looks in its local database.

This chapter is divided as follows:

- **Section 8.1 User Roles** describes the various levels of permissions available to user accounts.
- **Section 8.2 SANscreen User Management Screen** (page 43) describes the main user-management screen, the information displayed, and how to log in to that screen. This section also tells what you'll see if you log in without administrative-level privileges.
- **Section 8.3 Maintaining User Definitions via LDAP** (page 46) describes how to configure SANscreen to obtain its user authentication and authorization from a Version 2 or 3 LDAP server.
- **Section 8.4 Maintaining User Definitions Locally** (page 49) tells add and maintain user definitions on the local SANscreen server, including certain updates to LDAP users that you can only make on the local server.

8.1 User Roles

Each user account is defined as having one of the following levels of permissions:

- **Guest** — Permits you to log in to the SANscreen client, view the various screens, and change your notification levels; but not perform actions such as approving paths and identifying generic devices. If your user account is defined to SANscreen's local user database (and not through LDAP), you can also modify your own password.
- **User** — Permits you guest-level privileges, as well as access to SANscreen operations such as approving paths and identifying generic devices. It does not allow you to perform Data Source operations, nor does it allow you to add or edit SANscreen user accounts other than your own.
- **Administrator** — Varies depending on whether you use LDAP:
 - o If you authenticate and authorize users through LDAP, this level of permission lets you manage Data Sources, and change the notification levels for any user account.
 - o If you use only the local database to manage users, this level of permission lets you perform any operation, including adding new users and managing Data Sources.
- **Server Administrator** — Permits you to control LDAP server configuration, maintain user accounts in LDAP, and perform any other SANscreen operations. This level of permission is only assigned on the LDAP server; you will not see it in the local SANscreen user definitions.

It's a good idea to limit the number of users with Server Administrator or Administrator permissions, while keeping most users at the Guest or User level.

8.2 SANscreen User Management Screen

To manage users, first open the administration portal (see Chapter 7), then click the User Management link from the main menu.

If this is the first time you request the management screen after opening the portal, you'll be asked to log in (right). Make sure to use an account that has Administrator privileges. If your user name is authorized and authenticated through an LDAP server, your login name must include an @ sign followed by the domain (e.g., bob@US.onaro.com).

SANscreen login

Enter your name and password to sign in

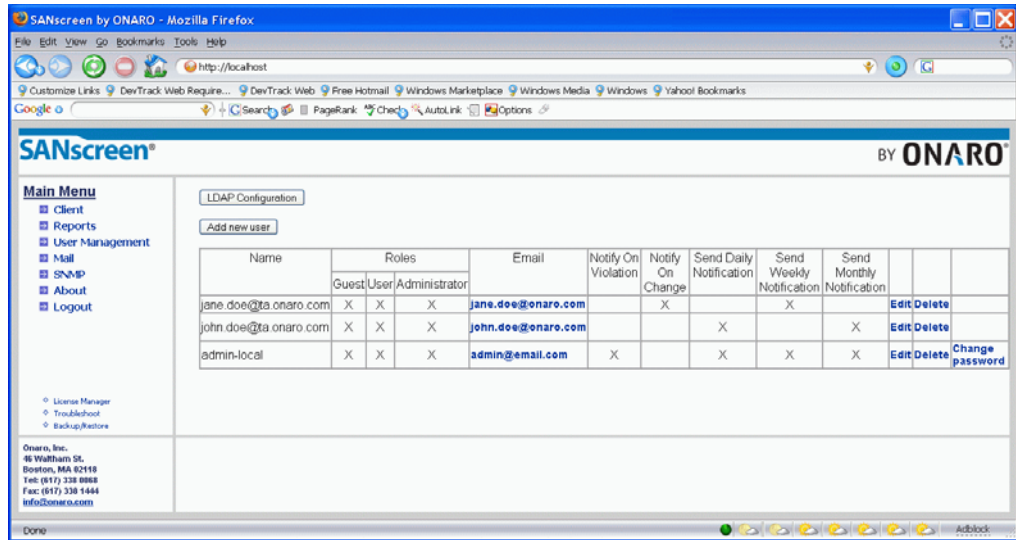
User name:

Password:

Note1: The default user is **admin** and its default password is **onaro**.

Note2: If you get an HTTP 401 error, most likely you have made a mistake entering the name or password. Click the User Management link and try again.

The User Management window looks like this (shown for a user having Server Administrator privileges):



This main body of this screen comprises a table that's used to maintain user definitions in the local SANscreen database, and to update notification levels for all users — including those defined through an LDAP server.

Note: While LDAP user accounts (name, password, role) are not defined using this screen, you can modify the e-mail on record for an LDAP user, and assign notifications using the Edit feature.

Each row represents a single user account defined on SANscreen's local database, or an LDAP user who has logged into the system at least once. (LDAP users do not have the Change Password option to the far right.)

User entries include the following information, where an X indicates that a column applies for the user. Please refer to the field descriptions in *Section 8.4.2 Adding a New User*, starting on page 50, for further details about these fields.

Field	Description
Name	Log-in user name.
Roles	Roles available to the user (i.e., levels of user permissions). Refer to page 42 for a description of the available roles. A higher-level role includes permissions available for the lesser role(s); therefore, for example, if a user is assigned Administrator permissions, the Guest and User boxes are also marked.
Email	User's e-mail address.
Notify on Violation/Change	Indication of which notification(s) the user subscribes to.
Send Daily/Weekly/Monthly Notification	Indication of the frequency with which the user receives notification summaries.
Edit/Delete/Change Password links	Links used to initiate the corresponding processing. Please refer to page 53 to edit an account, page 53 to delete an account, and page 54 to change a password.

If You Have User or Guest Privileges

If you request User Management from a User or Guest account, you will not see the main user list shown above. Instead:

- If your account is managed via the local server, SANSscreen opens a screen that allows you to change your own e-mail address, notifications, and password:

The screenshot shows the SANSscreen web interface. The top header has the SANSscreen logo and "BY ONARO". On the left is a "Main Menu" with links: Client, Reports, User Management, Mail, SNMP, About, Logout, License Manager, Troubleshoot, and Backup/Restore. The main content area contains a form for user management. It includes fields for "User Name" (containing "ems") and "email address". Below these is a "Role" section with radio buttons for "Guest", "User" (selected), and "Administrator". There are checkboxes for "Notify On Violation" (checked), "Notify On Change" (checked), "Daily Mail", "Weekly Mail", and "Monthly Mail". At the bottom of the form are "Update" and "Change Password" buttons.

- If your account is managed via LDAP, SANSscreen opens a screen that allows you to change your notifications:

The screenshot shows the SANSscreen web interface for an LDAP account. The layout is similar to the previous one, but the "Role" section has radio buttons for "Guest", "User", and "Administrator" (selected). Below the role selection, there is a message: "Please modify user role with LDAP administration tool." The notification checkboxes are the same as in the previous screenshot. The "Update" button is present at the bottom of the form.

8.3 Maintaining User Definitions via LDAP

This section describes how to configure SANSscreen to obtain its user authentication and authorization from a Version 2 or 3 LDAP server, such as the Microsoft Active Directory. In order to do this, you must first be defined in the LDAP server as the SANSscreen Server Administrator (initially defaults to `sansscreen.server.admin`).

The LDAP discussion is broken down as follows:

- **Section 8.3.1 LDAP Configuration Screen** describes the settings used to configure use of an LDAP server.
- **Section 8.3.2 Validating the LDAP Configuration** (page 49) tells how to validate the LDAP server and domain.

Please note that LDAP users display along with users who are defined locally to SANSscreen, on the initial user list (see page 43).

8.3.1 LDAP Configuration Screen

The User Management screen that opens for the Server Administrator contain a button labelled LDAP Configuration. Click this button to initiate the LDAP configuration process.

SANSscreen BY **ONARO**

Main Menu

- Client
- Reports
- User Management**
- Mail
- SNMP
- About
- Logout

License Manager
Troubleshoot
Backup/Restore

LDAP Configuration

☐ LDAP Enable

User Principal Name attribute	userPrincipalName
Role Attribute	memberOf
Mail Attribute	mail
Referral	follow
Timeout	2000
LDAP Server	ldap:///
Domain	DC=domain,DC=com
SANSscreen Server Administrators Group	sansscreen.server.admi
SANSscreen Administrators Group	sansscreen.admins
SANSscreen Users Group	sansscreen.users
SANSscreen Guests Group	sansscreen.guests

Directory Lookup User

Directory Lookup User password

Confirm Directory Lookup User password

Update Validate

Fill in this window to configure use of the LDAP server, then click Update to save the changes. The default settings are valid for the Active Directory.

Field	Description
LDAP Enable button	Mark this box to enable LDAP user authentication and authorization.
User Principal Name Attribute	Attribute that identifies each user in the LDAP server (defaults to userPrincipalName).
Role Attribute	LDAP attribute that identifies the user's role (defaults to memberOf).
Mail Attribute	LDAP attribute that identifies the user's e-mail address (defaults to mail). Note: SANscreen picks up the user e-mail address the first time each user logs in, and does not look for it after that. If the e-mail address changes on the LDAP server, make sure to manually change it in the SANscreen (see <i>Section 8.4.4 Editing a User Definition</i> starting on page 53).
Referral	Indication of whether to follow the path to other domains if there are multiple domains in the enterprise. Always use the default (follow).
Timeout	Length of time to wait for a response from the LDAP server before timing out, in milliseconds (defaults to 2 seconds, which is adequate in all cases).
LDAP Server	IP or DNS name to identify the LDAP server, typically provided in this format: ldap:///<ldap-server-address>:port or, to use the default port: ldap:///<ldap-server-address> For the Active Directory, leave this field blank: ldap:///
Domain	LDAP node where SANscreen should start looking for the LDAP user (typically the top-level domain for the organization). For example: DC=<enterprise>,DC=com

Field	Description
SANscreen Server Administrators Group	Value of the Role Attribute (Active Directory - Group name) that identifies the user as having Server Administrator privileges (defaults to sansscreen.server.admin).
SANscreen Administrators Group	Value of the Role Attribute (Active Directory - Group name) that identifies the user as having Administrator privileges (defaults to sansscreen.admin).
SANscreen Users Group	Value of the Role Attribute (Active Directory - Group name) that identifies the user as having User privileges (defaults to sansscreen.users).
SANscreen Guests Group	Value of the Role Attribute (Active Directory - Group name) that identifies the user as having Guest privileges (defaults to sansscreen.guests).
Directory Lookup User	Generic user for which the Validate process should search, to verify that the user lookup works. This is a special LDAP user who has permission to find LDAP users and determine their roles. If the LDAP server restricts the process of finding LDAP users and determining their roles, then you should enter the user information here; otherwise, if any user can perform these functions, you may omit this field. If you omit this field, the Validate process will only verify the LDAP server and domain.
Directory Lookup User Password	Password for the user above (will not redisplay once the screen is updated, for security reasons).
Confirm Directory Lookup User Password	Same password, repeated.

8.3.2 Validating the LDAP Configuration

When you complete the LDAP definition, click the Validate button to check the settings. This:

- Verifies that you specified a correct LDAP server and domain.
- Verifies that SANSscreen can locate, authorize, and authenticate the user specified in the Directory Lookup User field. If you omitted that field in the LDAP definition, the verification process skips this step.

8.4 Maintaining User Definitions Locally

This section describes how to add and maintain user definitions on the local SANSscreen server, including changed e-mail addresses and user notifications for LDAP users. It's broken down as follows:

- **Section 8.4.1 Summary of Operations** (page 50) presents an overview of the operations available from the main user display.
- **Section 8.4.2 Adding a New User** (page 50) tells how to add a new user account.
- **Section 8.4.3 Changing Your Password** (page 52) tells how to change your own password.
- **Section 8.4.4 Editing a User Definition** (page 53) tells how to edit a user-account definition.
- **Section 8.4.5 Deleting a User Account** (page 53) tells how to delete a user account when it's no longer used.
- **Section 8.4.6 Changing User Password** (page 54) tells how to change the password for a user.

8.4.1 Summary of Operations

From the User Management screen, you can:

Action	See page...
Add a new user to the local SANscreen database (requires Administrator privileges).	50
Change your own password. <i>Note:</i> Remember that if you're logged in with guest- or user-level privileges, you can also change your own e-mail address, notifications, and password from the initial login window, above.	52
Edit a user definition (requires Administrator privileges).	52
Delete a user account (requires Administrator privileges).	53
Change a user password (requires Administrator privileges).	54

The sections that follow describe these actions, in order as listed above.

8.4.2 Adding a New User

Add a new user account for each person who requires access to the SANscreen system. Having a different user account for each person provides a way of controlling the access rights, individual preferences, and accountability.

Before adding a new user:

- Allocate a unique user name.
- Determine what password to use.
- Verify the correct user role(s).
- Decide what type of e-mail notifications the user should get. E-mail notifications are explained in Chapter 9.
- Log in with Administrator privileges.

Click the Add New User button to open a wizard that guides you through the process of adding a new user account:

Enter the following information to configure the new user account, then click Add to return to the main user list:

Field	Used to configure the...
User Name	Name assigned to the new user (alphanumeric, including a-z, A-Z, and 0-9).
Password	Password used to log in to SANscreen under this user account (typically selected by the user him/herself).
Retype Password	Same as above, for verification.
Email Address	Optional. User's e-mail address. Required if you request notifications.
Role	Role(s) available to the user (i.e., levels of user permissions). Refer to page 42 for a description of the available roles.
Notify on...	Desired notification settings for the new user. A user can receive an e-mail notification for every violation and/or every SAN change. Any level of notification requires a valid e-mail address (above), and completion of the e-mail configuration detailed in Chapter 9.

Field	Used to configure the...
Daily/Weekly/Monthly Mail	Frequency with which to send notification summaries to the user. These periodic e-mail summarizes list all the SAN change and violation notifications that were sent to the user during the specified period of time.

8.4.3 Changing Your Password

It's a good idea to change your password from time to time. Before doing so, however:

- Notify anyone else who logs in under the same user account.
- Determine what password to use.
- Make sure you're logged in under the user account for which you wish to change the password.

Note: LDAP users cannot change their password through SANscreen.

To change your password:

1. Click the Change Password button from the main User Management display to open this screen:

2. Enter the new password twice.
3. Click Update. SANscreen displays a message telling you that the password was updated successfully, and that you need to log in again using the new password:

If you get the message Wrong password !!! you entered an incorrect old password. Please try again.

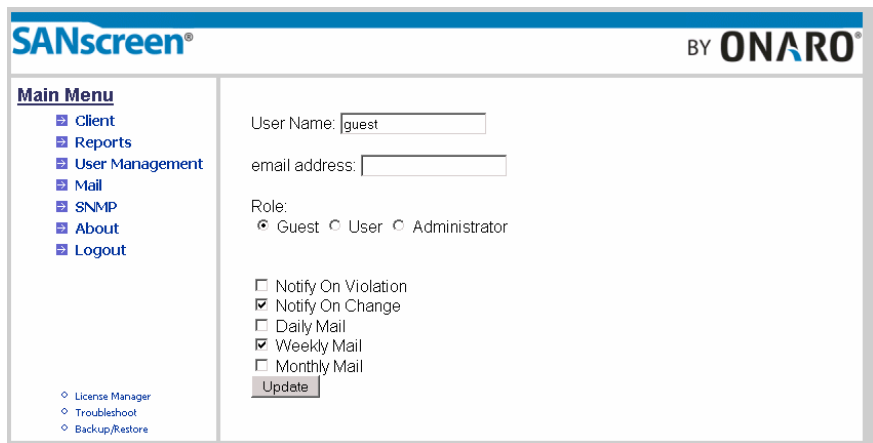
8.4.4 Editing a User Definition

A user with Administrator privileges can edit a user account to change the e-mail address, role(s), and/or notifications information.

Note: For LDAP users, you can only modify the e-mail address and notifications.

In the main user list, locate the row that displays the user account you want to edit. From that row:

- Click the Edit link to open the change screen:



The screenshot shows the SANSscreen web interface. The top header has the SANSscreen logo and 'BY ONARO'. A left sidebar contains a 'Main Menu' with links: Client, Reports, User Management (highlighted), Mail, SNMP, About, and Logout. Below the menu are links for License Manager, Troubleshoot, and Backup/Restore. The main content area is the 'Edit User' form. It includes fields for 'User Name' (containing 'guest') and 'email address'. Below these is a 'Role' section with radio buttons for 'Guest' (selected), 'User', and 'Administrator'. There is a section for notifications with checkboxes: 'Notify On Violation' (unchecked), 'Notify On Change' (checked), 'Daily Mail' (unchecked), 'Weekly Mail' (checked), and 'Monthly Mail' (unchecked). An 'Update' button is at the bottom of the form.

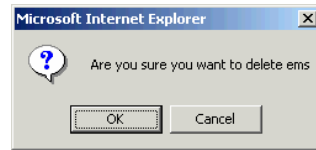
4. Modify the e-mail address, role(s), and/or notifications information, referring to the add-user field descriptions on page 51.
5. Click Update to modify the user account settings and redisplay the main user list.

8.4.5 Deleting a User Account

Any user with Administrator privileges can delete a user account, either when it's no longer used (for a local user definition), or to force SANSscreen to rediscover the user information the next time the user logs in (for an LDAP user).

In the main user list, locate the row that displays the user account you want to delete. From that row:

- Click the Delete link. SANscreen confirms the request (right).
- Click OK to confirm the operation and redisplay the main user list.



8.4.6 Changing User Password

A user with Administrator privileges can change the password for any other SANscreen user that's defined on the local server.

Note: You cannot change the password for a user who is validated through LDAP.

In the main user list, locate the row that displays the appropriate user account. From that row:

1. Click the Change Password link to open this change screen:

 A screenshot of the SANscreen web interface. The header shows 'SANscreen' and 'BY ONARO'. On the left is a 'Main Menu' with links: Client, Reports, User Management, Mail, SNMP, About, and Logout. Below these are links for License Manager, Troubleshoot, and Backup/Restore. The main content area is titled 'Change Password' and contains the following fields: 'User Name:' with a dropdown menu showing 'guest', 'New Password:' with a text input field, and 'Retype New Password:' with a text input field. An 'Update' button is located below the 'Retype New Password' field.

2. Enter the new password twice.
3. Click Update. SANscreen displays a message telling you that the password was updated successfully.

Chapter 9

Configuring E-mail Notification

This chapter tells how to configure SANscreen to find your e-mail server. This is required:

- To enable the proper use of e-mail for user notifications. (SANscreen sends change and violation notifications to each user, via standard e-mail, if configured for the user account as described in Chapter 8.)
- To use the mail home feature described in Chapter 14.

Before you proceed:

- Find the host name or IP address to identify the (SMTP or Exchange) mail server used by your organization. As necessary, you can find this information through the application you use to read your e-mail. In Microsoft Outlook, for example, you can find the name of the server by viewing your account configuration:

Tools – Email account – View or change existing email account

- Allocate an e-mail account through which SANscreen will send notifications. Configure the account to be a valid e-mail address in your organization. (Most mail systems will not send messages unless they are sent from a valid user.)
- If the e-mail server requires a user and password in order to send mail, obtain this information from your system administrator.

To configure e-mail notifications:

1. Make sure you're logged in under an account that has Administrator privileges.
2. From the administration portal (see Chapter 7), click the Mail link from the main menu to open the screen shown below. If this is the first time you request the Mail screen after opening the portal, you'll be asked to log in before you see this screen.

- Enter the following information to configure the e-mail information, then click Submit. Asterisked (*) fields are required.

Field	Used to configure the...
SMTP Server Address	Server that's acting as the SMTP server in your organization, identified using either a hostname or an IP address (<i>nnn.nnn.nnn.nnn</i> format). If you specify a hostname, make sure the name can be resolved through DNS.
Sender Email	E-mail account to be identified as the sender on all SANscreen notifications. This account must be a valid e-mail account within your organization.
User Name	Optional. User name to access the e-mail server, required only if your SMTP server is protected by a user login. This is the same user name you use to log in to the application that lets you read your e-mail.
Password	Optional. Password to access the e-mail server, required only if your SMTP server is protected by a password. This is the same password you use to log in to the application that lets you read your e-mail.
Retype Password	Optional. Same as above, for verification.

- After clicking Submit above, make sure you see this message:

Email Configuration completed successfully

To verify that your e-mail server works properly with SANscreen, edit your own user account to receive change notifications, referring to *Section 8.4.4 Editing a User Definition*, starting on page 53.

Chapter 10

Configuring SNMP Notification

SANscreen supports SNMP notifications for two types of events:

- **Changes** — A notification is sent for each change in the SAN.
- **Violations** — A notification is sent each time a violation occurs. (Violations are described in the *SANscreen User Manual*.)

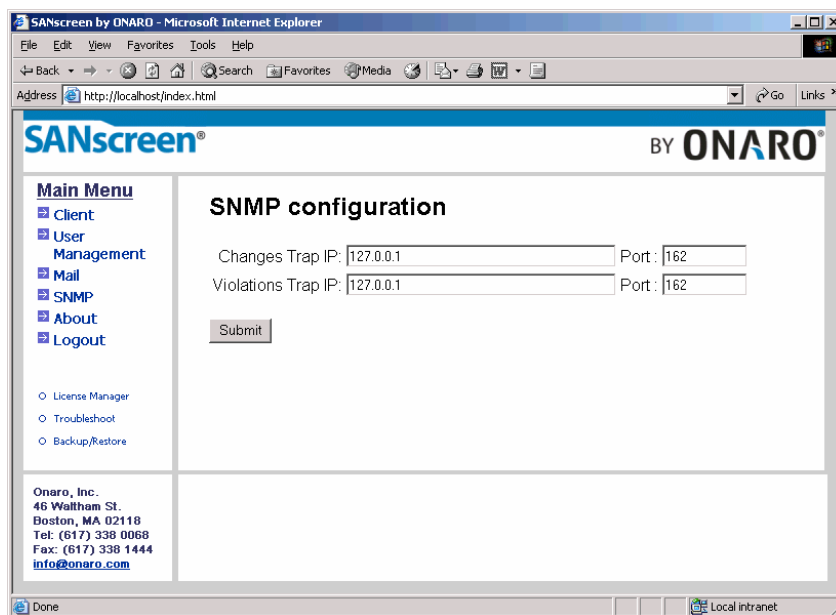
In order to support SNMP notifications, you must tell SANscreen where to send SNMP trap messages.

Before you proceed:

- Determine the IP address of the server that consolidates traps, for each type of event. You will have to consult with your system administrator to obtain this information.
- Determine the port number through which the designated machine obtains SNMP traps, for each type of event. (The default port for SNMP traps is 162.)
- Ask the Onaro support team to send you the SANscreen MIB.

To configure SNMP notifications:

1. Make sure you're logged in under an account that has Administrator privileges.
2. From the administration portal (see Chapter 7), click the **SNMP** link from the main menu to open the screen shown below. If this is the first time you request the **SNMP** screen after opening the portal, you'll be asked to log in before you see this screen.



3. Enter the following information to configure traps, then click Submit:

Field	Used to configure the...
Changes Trap IP and Port	IP address and port number to which SANscreen sends SNMP change-type trap messages.
Violations Trap IP and Port	IP address and port number to which SANscreen sends SNMP violation-type trap messages.

4. After clicking Submit, make sure you see this message:

SNMP Configuration completed successfully

Verify that an SNMP trap was received for each type of processing (change and violation). Consult with your system administrator to do this, because the approach will vary depending on your organization's SNMP trap management and reporting software.

Chapter 11

Installing a License

SANscreen operates with a license that enables specific features on the SANscreen server. After you receive a SANscreen license file from Onaro, follow the instructions below to enable that license:

1. Make sure you're logged in under an account that has Administrator privileges.
2. From the administration portal (see Chapter 7), click the License Manager link to open the screen shown below. If this is the first time you request the License Manager after opening the portal, you'll be asked to log in before you see this screen.

SANscreen BY **ONARO**

Main Menu

- Client
- Reports
- User Management
- Mail
- SNMP
- About
- Logout

License Manager
Troubleshoot
Backup/Restore

Current license

License ok

Expiration Sep 12, 2005
Foundation true

Current license:

```
License.name=Tech writer  
License.version=2.0  
Expiration=09/12/2005  
Foundation=TRUE  
Signature=MCwCFC10Tdo09DhvhzId8IAJkF0c+Qx2AhQcDwAq1vft4XpEbnkhu2Te9cK92A==
```

Update

Import license:

Browse...
Import

3. Browse to locate the SANscreen license (.lic) file, then click Import.
4. Click Update to modify the license using the imported data. SANscreen refreshes the license information, changes the License status to OK, and displays the new license key as the Current License.

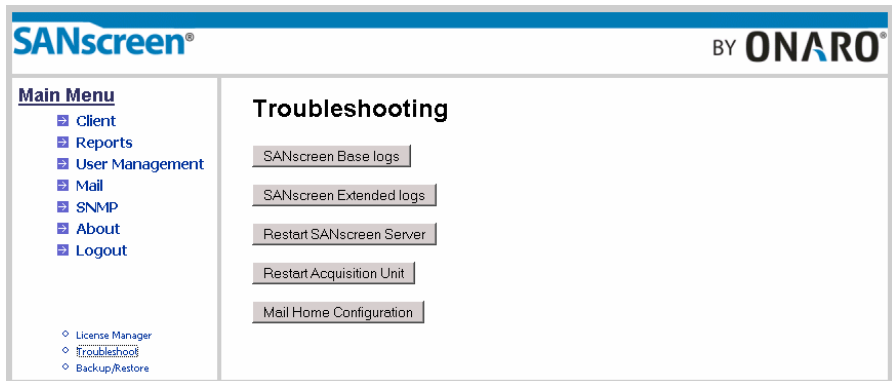
Chapter 12

Troubleshooting: Reviewing the Logs

SANscreen provides various levels of system logs that are available for review, but are most often used by the Onaro support team. Follow the instructions below to copy these logs to your computer:

Note: You do *not* need administrator privileges to access the log files.

1. Open the administration portal (see Chapter 7).
2. Click the Troubleshoot link to open the screen shown below. If this is the first time you request the Troubleshoot link after opening the portal, you'll be asked to log in before you see this screen.

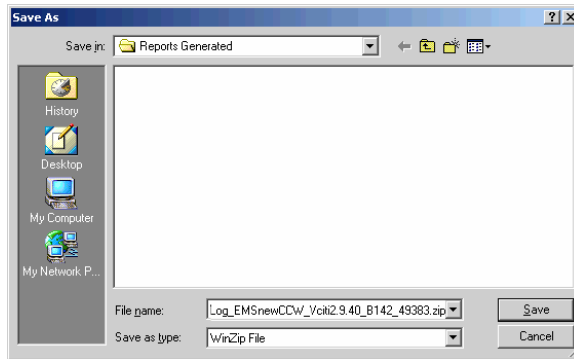
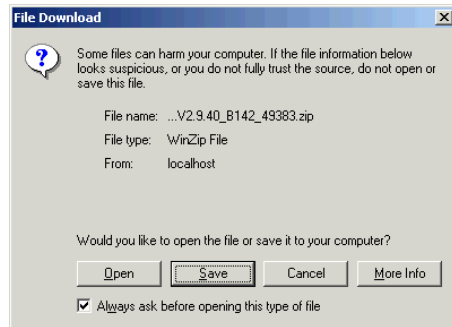


3. Click the button corresponding to the type of log you want to copy:

Button	Click to see...
SANscreen Base Logs	Basic logs written by the SANscreen server, SANscreen client, and all installed Acquisition Units.
SANscreen Extended Logs	Extended logs, which include all the Basic Log files, as well as additional files that detail intermediate acquisition information.

The next steps will vary depending on the browser you're using, and are illustrated below for Internet Explorer.

4. SANscreen notifies you of the type of file it wants to create, then prompts you to save the file on your computer (right). Click Save.
5. Navigate to the folder where you want to save the log files (SANscreen_logs in the following example), then click Save. Do not change the filename.



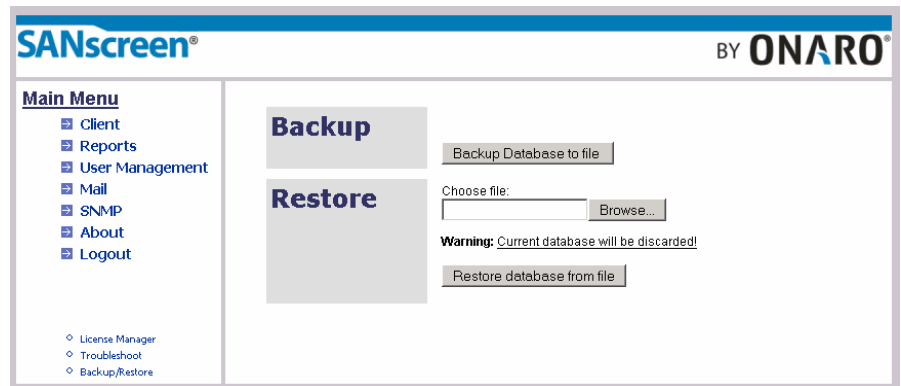
6. Wait while SANscreen copies the log files to the selected folder.

Chapter 13

Backing Up and Restoring the Database

This chapter tells how to backup the SANscreen database to a file, and to restore the database from a file that was backed up previously. In both cases:

- Ensure that you are logged in under an account that has Administrator privileges.
- Open the administration portal (see Chapter 7).
- Click the Backup/Restore link to open the screen shown below. If this is the first time you request the Backup/Restore link after opening the portal, you'll be asked to log in before you see this screen.



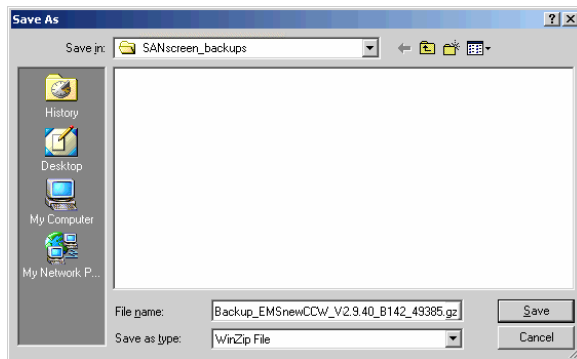
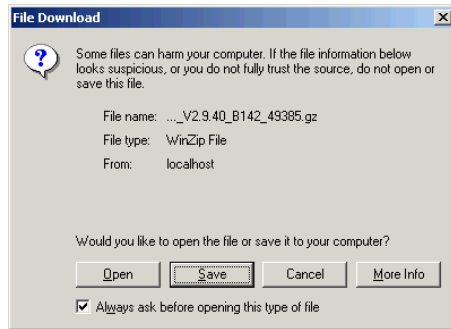
13.1 Backup

To back up the SANscreen database to a file on your PC:

1. Click Backup Database to File.

The next steps vary depending on the browser you're using, and are illustrated below for Internet Explorer.

2. SANscreen notifies you of the type of file backup it will perform then prompts you to save the file on your computer (right). Click Save.
3. Navigate to the folder where you want to save the file (SANscreen_backups in the following example), then click Save. Do not change the filename.



4. Wait while the entire database is backed up. Please be patient — this operation can take several minutes (possibly 30 or more).

13.2 Restore

Before restoring your SANscreen database, it's a good idea to back up the current version. Then:

1. Use the Browse button to select the file from which to restore the database.
2. Click Restore Database from File. This deletes all current SAN information and loads the entire SANscreen database from the selected file. Please be patient — this can take 30 minutes or more.

You'll see this message after the restore operation is completed:

SANscreen's Database was successfully updated.

Chapter 14

Configuring the Mail Home Feature

As a part of Onaro's efforts to provide quality support to its customers, all of Onaro's products are equipped with advanced mail home capabilities. This mechanism periodically sends predefined, specific, information to the Onaro support team. You can configure the system to send base logs, extended logs, and/or backup files — all in text format. The files will be formatted as follows before being forwarded to Onaro:

- **Accumulated logs** — Logs are collected from the various system components — Acquisition Units, server, and client. The logs contain system diagnostics and (if they exist) warnings. There are two forms of logs: base and/or extended, as explained on page 61.

All log files are sent to Onaro in an encrypted (Zipenc) format. In the event of a problem (e.g., a Fiber Switch device is suddenly not reachable), the following information may be included:

- o Information about problems contacting devices, including the device IP.
 - o Information about problems processing the SAN configuration, including the WWNs of specific devices in the SAN.
 - o Information about problems in the SAN presentation. This does *not* include network information.
- **Backup of the environment** — Contains all the topology inventory and history, in an encrypted (Gzenc) format. Also holds the SANscreen configuration.

The information is forwarded to Onaro via SMTP e-mail or FTP, as determined by the user. It contains minimal sensitive information. For example, the sent files do not contain clear text passwords. Instead, the backup includes the hashed result of passwords for user passwords, and encrypted passwords for device passwords.

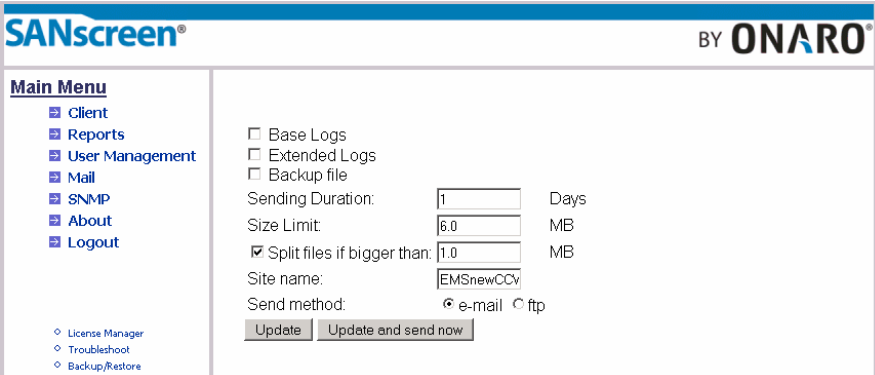
The Onaro support team uses this information to ensure the correct operation of SANscreen, to assist you in maintaining the validity of your SAN, and to help maintain the integrity of the your internal change processes. The mail home capability provides the customer with the following benefits:

- **Proactive support** — On the rare occasion where an imminent problem exists, the Onaro support team will usually identify the problem before the customer, and will contact the customer directly.
- **Shorter response time** — When a customer needs assistance from the Onaro support team, it is likely that all the customer's SANscreen information will already be available to Onaro. This improves the speed and accuracy of the support provided.

Steps to Configure

In order for Onaro to provide the mail home feature, you must configure the settings described in this chapter. To begin:

1. Make sure you're logged in with Administrator privileges.
2. Open the administration portal (see Chapter 7).
3. Click the Troubleshoot link to open the main Troubleshooting screen. (If this is the first time you have entered the Troubleshoot screen, you'll be asked to log in before you see this screen.)
4. Click Mail Home Configuration to open the screen shown below:



The screenshot shows the SANscreen administration interface. The top header features the 'SANscreen' logo on the left and 'BY ONARO' on the right. A 'Main Menu' sidebar on the left contains links for Client, Reports, User Management, Mail, SNMP, About, and Logout. Below these are links for License Manager, Troubleshoot, and Backup/Restore. The main content area is titled 'Mail Home Configuration' and includes several settings: 'Base Logs' (unchecked), 'Extended Logs' (unchecked), and 'Backup file' (unchecked). There are input fields for 'Sending Duration' (set to 1), 'Size Limit' (set to 6.0), and 'Split files if bigger than' (set to 1.0), each followed by a unit of 'Days' or 'MB'. The 'Site name' field contains 'EMSnewCCV'. The 'Send method' is set to 'e-mail' with radio buttons for 'e-mail' and 'ftp'. At the bottom are two buttons: 'Update' and 'Update and send now'.

5. Fill in the screen fields as described below, then click:
 - o Update to save the configured settings.
 - o Update and Send Now to save the configured settings and mail home immediately.

Field	Used to ...
Base Logs	Send your base logs to Onaro. Please refer to the notes about log files on page 65.
Extended Logs	Send your extended logs to Onaro.
Backup File	Send a backup of your SANscreen database to Onaro. The backup holds the SANscreen configuration, and contains all the topology inventory and history. It is recommended that you include the back up files for a POC (Proof Of Concept); otherwise just the logs files are adequate.
Sending Duration	Frequency with which to send the information to Onaro, in days (defaults to daily).
Size Limit	Maximum size of the total data forwarded (defaults to 6 MB).
Split files if bigger than	Maximum size of any single file (defaults to 1 MB). Files will be split if they are larger than this limit.
Site Name	Name to identify your installation, to be included with the data sent to Onaro. We suggest formatting this as <i><company name>_<location></i> .
Send Method	Select e-mail or ftp, to specify which method you prefer to use to forward the information to Onaro. If you specify e-mail, make sure to configure SANscreen to find your e-mail server, as detailed in Chapter 9.

Appendix A

Available Data Sources

This appendix lists the various supported SAN devices, and for each device, the information required to configure the correct acquisition of data from its corresponding Data Source. The appendix is broken down alphabetically according to the Vendor and Model information you can enter when defining a new Data Source, as summarized in Table 1 on page 70.

A.1 3Par InServ

The 3Par InServ is an SMI-S device. Please refer to *Section A.25 SMI-S Support Devices* (page 88) for field descriptions and configuration information. Assign the SMI-S Namespace as shown below:

Field	Description
SMI-S namespace	Always specify “root/tpd”.

Table 1: Summary of Supported Data Sources

Vendor	Description	See page...
3Par	InServ	69
Brocade	All Brocade switches except SNMP.	71
	Brocade SNMP	72
Cisco	All Cisco switches.	73
EMC	Clariion	74
	Clariion CLI	75
	Connectrix	76
	StorageScope Host Resolver	77
	Symmetrix Family API	78
HDS	HiCommand	79
	SMI-S	80
HP	EVA	80
	XP & XP512 CLI disk array	81
	XP family SMI-S	82
IBM	Enterprise Storage Server	82
	Enterprise Storage Server SMI-S	83
	SVC	83
	FAStT	83
InRange	FC9000 Director	84
McData	Enterprise Fabric Connectivity Manager (EFCM)	85
	Sphereon	86
QLogic	QLogic SANsurfer web application	87
Sun	StorEdge 6130	88
	StorEdge 6x20	88
—	SMI-S support devices	88

A.2 Brocade (All Brocade switches)

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
Brocade switch	Network address for the switch device, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
User name	Name used to log in to the switch.
Password	Password used to log in to the switch.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
Enable trapping	Checkbox used to trigger acquisition upon receiving an SNMP trap from the device. If you mark this box, you must also activate SNMP notifications (see Chapter 10).
Minimum time between traps (sec)	Minimum elapsed time between acquisition attempts triggered by traps, in seconds.
Fabric name	Name of the fabric/VSAN where the switch is configured.

A.3 Brocade (SNMP)

Data Source - Data source configuration

Configure

Use this form to configure a data source's specific parameters.

Brocade switch:*

SNMP community:*

Poll interval (min):*

Has blades:* ☐

Enable trapping:* ☒

Minimum time between traps (sec):*

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
Brocade switch	Network address for the switch device, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
SNMP community	SNMP <i>read-only</i> community string used to access the device.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
Has blades	Checkbox used to indicate whether the switch has blades. Mark the box if using blades.
Enable trapping	Checkbox used to trigger acquisition upon receiving an SNMP trap from the device. If you mark this box, you must also activate SNMP notifications (see Chapter 10).
Minimum time between traps (sec)	Minimum elapsed time between acquisition attempts triggered by traps, in seconds.

A.4 Cisco

+5.000

+1.500

+1.125

Configure

Use this form to configure a data source's specific parameters.

Cisco switch:*

SNMP community:*

Poll interval (min):*

Enable trapping:*

Minimum time between traps (sec):*

public

15

☒

10

Import

< Back

Next >

Finish

Cancel

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
Cisco switch	Network address for the switch, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
SNMP community	SNMP <i>read-only</i> community string used to access the device.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
Enable trapping	Checkbox used to trigger acquisition upon receiving an SNMP trap from the device. If you mark this box, you must also activate SNMP notifications (see Chapter 10).
Minimum time between traps (sec)	Minimum elapsed time between acquisition attempts triggered by traps, in seconds.

A.5 EMC (Clariion)

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
Navisphere server	Network address for the Navisphere, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
Navisphere port	Number of the Navisphere port through which the Data Source acquires information.
User name	Name used to log in to the switch.
Password	Password used to log in to the switch.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
Login scope	Login scope, specified according to the Navisphere login policy (Global or Local).
Primary Clariion only	Request only the Clariion that run the Navisphere.

A.6 EMC (Clariion CLI)

Data Source - Data source configuration

Configure

Use this form to configure a data source's specific parameters.

0	+5.000
1	+1.500
0	+1.125

Clariion storage:*

User name:*

Password:*

Poll interval (min):*

navicli.exe path:*

Import

< Back Next > Finish Cancel

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
Clariion storage	Network address for the Clariion storage device, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
User name	Name used to log in to the Clariion storage device.
Password	Password used to log in to the Clariion storage device.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
navicli.exe path	Full pathname to the executable (navicli.exe).

A.7 EMC (Connectrix)

Data Source - Data source configuration

Configure

Use this form to configure a data source's specific parameters.

EFC server:*

User name:*

Password:*

Poll interval (min):*

Enable trapping:* ☒

Minimum time between traps (sec):*

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
EFC server	Network address for the EFC server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
User name	Name used to log in to the Connectrix device.
Password	Password used to log in to the Connectrix device.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the Connectrix device.
Enable trapping	Checkbox used to trigger acquisition upon receiving an SNMP trap from the device. If you mark this box, you must also activate SNMP notifications (see Chapter 10).
Minimum time between traps (sec)	Minimum elapsed time between acquisition attempts triggered by traps, in seconds.

A.8 EMC (StorageScope Host Resolver)

Data Source - Data source configuration

Configure

Use this form to configure a data source's specific parameters.

ECC server:*

ECC port:*

User name:*

Password:*

Poll interval (min)*

Import

< Back Next > Finish Cancel

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
ECC server	Network address for the ECC server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
ECC port	Number of the ECC server port through which the Data Source acquires information.
User name	Name used to log in to the ECC.
Password	Password used to log in to the ECC.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.

A.9 EMC (Symmetrix Family API)

Data Source - Data source configuration

Configure

Use this form to configure a data source's specific parameters.

Solution Enabler server:* localhost

Solution Enabler port:* 2707

Poll interval (min)* 40

Import

< Back Next > Finish Cancel

For an EMC Symmetrix device, make sure that EMC SYMAPI is installed and has the appropriate licenses to operate.

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
Solution Enabler server	Network address for the Solution Enabler server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
Solution Enabler port	Number of the Solution Enabler server port through which the Data Source acquires information.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.

A.10 HDS (HiCommand)

Data Source - Data source configuration

Configure

Use this form to configure a data source's specific parameters.

HiCommand server:* localhost

HiCommand port:* 2001

User name:* admin

Password:* *****

Poll interval (min):* 40

Serial number:*

Import

< Back Next > Finish Cancel

The HDS Data Source supports the HiCommand server. SANscreen communicates with the HiCommand server using the standard HiCommand API.

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
HiCommand server	Network address for the HiCommand server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
HiCommand port	Number of the HiCommand server port through which the Data Source acquires information.
User name	Name used to log in to the HiCommand.
Password	Password used to log in to the HiCommand.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
Serial number	Serial number of the specific storage device on which the Data Source should report. Leave this field blank to retrieve all available storage devices managed by the HiCommand.

A.11 HDS SMI-S

The HDS SMI-S is an SMI-S device. Please refer to *Section A.25 SMI-S Support Devices* (page 88) for field descriptions and configuration information. Assign the SMI-S Namespace as shown below:

Field	Description
SMI-S namespace	Always specify “root/hitachi/dm35”.

A.12 HP (EVA)

Data Source - Data source configuration

Configure

Use this form to configure a data source's specific parameters.

CommandView server:*

User name:*

Password:*

Poll interval (min)*

CV CLI home:*

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
CommandView server	CommandView manager name.
User name	Name used to log in to the CommandView.
Password	Password used to log in to the CommandView.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
CV CLI home	Full pathname to the CLI home directory where sssu.exe is located

A.13 HP (XP CLI)

Configure

Use this form to configure a data source's specific parameters.

CommandView server:*

User name:*

Password:*

Poll interval (min):*

Path to cvcli.bat:*

Storage serial number:

Import

< Back Next > Finish Cancel

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
CommandView server	CommandView manager name.
User name	Name used to log in to the CommandView.
Password	Password used to log in to the CommandView.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
Path to cvcli.bat	Absolute path to the CV CLI batch file (cvcli.bat) – with or without the trailing backslash (\).
Storage serial number	Serial number of the specific HP storage device on which the Data Source should report. Leave this field blank to retrieve all available storage devices managed by the Command View manager.

A.14 HP (XP family SMI-S)

Please refer to *Section A.25 SMI-S Support Devices* (page 88) for field descriptions and configuration information for HP XP family SMI-S devices. Assign the SMI-S Namespace as shown below:

Field	Description
SMI-S namespace	Always specify “root”.

A.15 IBM (Enterprise Storage Server)

Configure

Use this form to configure a data source's specific parameters.

ESS storage:*

ESS storage port:*

User name:*

Password:*

Poll interval (min):*

Storage name:*

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
ESS storage	Network address for the ESS device, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
ESS storage port	Number of the ESS port through which the Data Source acquires information.
User name	Name used to log in to the ESS.

Field	Description
Password	Password used to log in to the ESS.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
Storage name	User-specified alias used as the storage name.

A.16 IBM (Enterprise Storage Server SMI-S)

The IBM Enterprise Storage Server SMI-S is an SMI-S device. Please refer to *Section A.25 SMI-S Support Devices* (page 88) for field descriptions and configuration information. Assign the SMI-S Namespace as shown below:

Field	Description
SMI-S namespace	Always specify “root/IBM”.

A.17 IBM (SVC)

The IBM SVC is an SMI-S device. Please refer to *Section A.25 SMI-S Support Devices* (page 88) for field descriptions and configuration information. Assign the SMI-S Namespace as shown below:

Field	Description
SMI-S namespace	Always specify “root/IBM”.

A.18 IBM (FAStT)

The IBM FAStT is an SMI-S device. Please refer to *Section A.25 SMI-S Support Devices* (page 88) for field descriptions and configuration information. Assign the SMI-S Namespace as shown below:

Field	Description
SMI-S namespace	Always specify “root/Isissi”.

A.19 InRange (FC9000 Director)

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
InRange switch	Network address for the switch, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
User name	Name used to log in to the switch via Telnet.
Password	Password used to log in to the switch via Telnet.
SNMP community	SNMP <i>read-only</i> community string used to access the device.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
Enable trapping	Checkbox used to trigger acquisition upon receiving an SNMP trap from the device. If you mark this box, you must also activate SNMP notifications (see Chapter 10).
Minimum time between traps (sec)	Minimum elapsed time between acquisition attempts triggered by traps, in seconds.

A.20 McData (Enterprise Fabric Connectivity Manager)

Configure

Use this form to configure a data source's specific parameters.

EFC server:*

User name:*

Password:*

Poll interval (min):*

Enable trapping:* ☒

Minimum time between traps (sec):*

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
EFC server	Network address for the EFC server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
User name	Name used to log in to the switch.
Password	Password used to log in to the switch.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the EFC.
Enable trapping	Checkbox used to trigger acquisition upon receiving an SNMP trap from the device. If you mark this box, you must also activate SNMP notifications (see Chapter 10).
Minimum time between traps (sec)	Minimum elapsed time between acquisition attempts triggered by traps, in seconds.

A.21 McData (Sphereon)

Data Source - Data source configuration

Configure

Use this form to configure a data source's specific parameters.

Sphereon switch:*

SNMP community:*

Poll interval (min)*

Enable trapping:* ☒

Minimum time between traps (sec):*

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
Sphereon switch	Network address for the switch, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
SNMP community	SNMP <i>read-only</i> community string used to access the device.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
Enable trapping	Checkbox used to trigger acquisition upon receiving an SNMP trap from the device. If you mark this box, you must also activate SNMP notifications (see Chapter 10).
Minimum time between traps (sec)	Minimum elapsed time between acquisition attempts triggered by traps, in seconds.

A.22 QLogic SANsurfer

Data Source - Data source configuration

Configure

Use this form to configure a data source's specific parameters.

SANSurfer switch:*

SNMP community:*

Poll interval (min)*

Enable trapping* ☒

Minimum time between traps (sec)*

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
SANSurfer switch	Network address for the SANSurfer device, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
SNMP community	SNMP <i>read-only</i> community string used to access the device.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
Enable trapping	Checkbox used to trigger acquisition upon receiving an SNMP trap from the device. If you mark this box, you must also activate SNMP notifications (see Chapter 10).
Minimum time between traps (sec)	Minimum elapsed time between acquisition attempts triggered by traps, in seconds.

A.23 SUN (StorEdge 6130)

The SUN StorEdge 6130 is an SMI-S device. Please refer to *Section A.25 SMI-S Support Devices* (page 88) for field descriptions and configuration information. Assign the SMI-S Namespace as shown below:

Field	Description
SMI-S namespace	Always specify “interop”.

A.24 SUN (StorEdge 6x20)

The SUN StorEdge 6x20 is an SMI-S device. Please refer to *Section A.25 SMI-S Support Devices* (page 88) for field descriptions and configuration information. Assign the SMI-S Namespace as shown below:

Field	Description
SMI-S namespace	Always specify “interop”.

A.25 SMI-S Support Devices

The SMI-S communication method is used by several server devices. The Data Source configuration is the same for all servers that provide an SMI-S interface, as detailed below.

Data Source - Data source configuration

Configure

Use this form to configure a data source's specific parameters.

SMI-S server:*	
SMI-S port:*	5988
User name:*	admin
Password:*	
Poll interval (min):*	40
SMI-S namespace:*	

Import

< Back Next > Finish Cancel

Field Descriptions

Please refer to the screen shot above for default values. Required fields are asterisked (*).

Field	Description
SMI-S server	Network address for the SMI-S server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or a hostname that can be resolved through DNS.
SMI-S port	Number of the server port through which the Data Source acquires information.
User name	Name used to log in to the SMI-S server.
Password	Password used to log in to the SMI-S server.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
SMI-S namespace	SMI-S namespace used to query data (varies by device type).

Appendix B

Hardware and Software Requirements

This appendix details the hardware and software requirements for the SANscreen server, the Remote Acquisition Unit, and the SANscreen client.

B.1 SANscreen Server Requirements

Component	Requirement
Operating System	Dedicated PC running Microsoft Windows 2000 with the Latest Service Pack
CPU	2 x 3.2 GHz or better
Memory	4 GB
Available Disk Space	20 GB
Network	100 Mbps / 1 Gbps Ethernet connection

B.2 Remote Acquisition Unit Requirements

Component	Requirement
Operating System	PC running Microsoft Windows 2000 with the Latest Service Pack
CPU	2 x 3.2 GHz or better
Memory	4 GB
Available Disk Space	5 GB
Network	100 Mbps / 1 Gbps Ethernet connection

B.3 SANscreen Client GUI Requirements

Component	Requirement
Operating System	Any Java 5 enabled machine
CPU	1.5 GHz or better
Memory	1 GB

Appendix C

Copyright Notices

This product includes and/or is shipped with code that is copyrighted by the third parties listed below. Further copyright and license information for open source code is included in the documentation.

This product includes code licensed from RSA Security, Inc.

Some portions licensed from IBM are available at
<http://oss.software.ibm.com/icu4j/>

This product includes software designed by the [MX4J project](#). Copyright © 2001. MX4J. All Rights Reserved.

This product includes software developed by the Apache Software Foundation. Copyright © 1999-2003 the Apache Software Foundation. All Rights Reserved.

This product includes software developed by Intalio Inc. Copyright © 2000-2002 Intalio Inc. All Rights Reserved. ExoLab Project (www.exolab.com).

This product includes JoeSNMP – SNMPv1 & v2 compliant libraries for Java. Copyright © 1999-2001 Oculan Corp. All Rights Reserved.
Copyright © 2001-2003 INCORS GmbH - All Rights Reserved.
Copyright © 1999 the Apache Software Foundation. All Rights Reserved.
Copyright © 2002-2003 ymnk, JCraft, Inc. All Rights Reserved.

This product includes software developed by the JDOM Project (<http://www.jdom.org/>). Copyright © 2001 Brett McLaughlin & Jason Hunter. All Rights Reserved.

This project includes the Ino software package developed by Jordan Russell. Copyright 1997 – 2003 Jordan Russell. All Rights Reserved.

The contents of this file are subject to the Mozilla Public License Version 1.0 (the “License”). You may not use this file except in compliance with the

License. You may obtain a copy of the License at
<http://www.mozilla.org/MPL/>.

Software distributed under the License is distributed on an “AS IS” basis,
WITHOUT WARRANTY OF ANY KIND, either express or implied. See
the License for the specific language governing rights and limitations under
the License.