



SANscreen® Foundation Installation and Administration Version 3.5



Onaro Inc. • 500 Harrison Street • Boston, MA 02118
Phone (US) 1.800.98.ONARO • Fax 617.338.1444

COPYRIGHT © 2000-2006 by Onaro, Inc.

— 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.

This product 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
Onaro Products.....	viii
Documentation Set	ix
Quick Start Instructions	x
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 Foundation.....	5
2.1 Before You Install SANscreen Foundation... ..	5
2.2 Using the Installation Wizard.....	6
2.3 Verifying New SANscreen Foundation Services	10
2.4 Uninstalling SANscreen Foundation.....	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	22
Chapter 5 Viewing Acquisition Units	25
5.1 The Acquisition Units Screen Described	25
5.1.1 The Main Acquisition Units Table	26
5.1.2 The Event Log.....	27
5.2 Operations	27

5.2.1 Removing an Acquisition Unit.....	28
Chapter 6 Using Data Sources to Discover the SAN	29
6.1 Understanding Data Source Concepts.....	30
6.2 Unsupported Configurations.....	31
6.3 Preparation.....	31
6.4 The Data Sources Screen Described.....	32
6.4.1 The Main Data Sources Table	33
6.4.2 The Event Log.....	35
6.4.3 The Advanced Status Detail Pane.....	36
6.4.4 The Devices Detail Pane	36
6.4.5 The Changes Detail Pane.....	37
6.5 Operations.....	38
6.6 Adding a Data Source	39
6.7 Editing Data Source Properties.....	41
6.8 Starting a Data Source	42
6.9 Stopping a Data Source	42
6.10 Removing a Data Source	43
6.11 Forcing Acquisition	44
6.12 Clearing the Event Log.....	44
6.13 Troubleshooting Data Source Activity	45
6.13.1 Unauthorized Operation.....	45
6.13.2 Faulty Acquisition Unit Status.....	46
6.13.3 Unsuccessful Acquisition or Faulty Data Source	46
Chapter 7 SANscreen Administration Portal	47
Chapter 8 User Management	49
8.1 User Roles.....	50
8.2 SANscreen User Management Screen	51
If You Have User or Guest Privileges	52
8.3 Maintaining User Definitions via LDAP	53
8.3.1 LDAP Configuration Screen.....	53
8.3.2 Validating the LDAP Configuration	56
8.4 Maintaining User Definitions Locally	56
8.4.1 Summary of Operations.....	57
8.4.2 Adding a New User.....	57
8.4.3 Editing a User Definition	58
8.4.4 Deleting a User Account.....	59
8.4.5 Changing User Password	59
Chapter 9 Configuring E-mail	61
Chapter 10 Configuring SNMP Notifications.....	63

Chapter 11 Installing a License	65
Chapter 12 Troubleshooting and Phone Home.....	67
12.1 Download Extended Logs.....	68
12.2 Phone Home.....	69
12.2.1 What Data is Sent to Onaro?	69
12.2.2 How is the Information Sent?.....	70
12.2.3 What Does Onaro Do with the Information It Receives?	70
12.2.4 Configuring the Phone Home Feature	71
Chapter 13 Backing Up and Restoring the Database.....	73
13.1 Backup.....	74
13.2 Restore	75
Appendix A Available Data Sources	77
A.1 3Par InServ	78
A.2 Brocade (API).....	79
A.3 Brocade (HTTP)	81
A.4 Brocade (SNMP Firmware 4.2x / 4.4x)	82
A.5 Cisco	84
A.6 EMC (Clariion CLI).....	85
A.7 EMC (Connectrix 7).....	86
A.8 EMC (Connectrix – 8.1, 8.6, 8.7, 8.8, 8.9, 9.1)	87
A.9 EMC (ECC StorageScope Host Resolver).....	89
A.10 EMC (Solutions Enabler Symmetrix Family API).....	90
A.11 Engenio Arrays.....	91
A.12 HDS (HiCommand)	92
A.13 HP (EVA).....	93
A.14 HP (XP)	94
A.15 IBM (FASTT)	95
A.16 IBM (DS CLI).....	96
A.17 IBM (ESS CLI).....	97
A.18 IBM (SVC)	98
A.19 IBM (TotalStorage DS4000).....	99
A.20 McData (Enterprise Fabric Connectivity Manager).....	100
A.21 McData (Sphereon).....	101
A.22 QLogic SANsurfer	103
A.23 SUN (StorEdge 6130)	104
A.24 SUN (StorEdge 6x20)	105
Appendix B Hardware and Software Requirements.....	107
B.1 SANscreen Server Requirements	107
B.2 Remote Acquisition Unit Server Requirements.....	108

B.3 SANscreen Client GUI Requirements.....	108
Appendix C Copyright Notices	109

Figures

Figure 1: Example of a Common SANscreen Foundation Implementation	2
Figure 2: SANscreen Foundation Client Display	21

Preface

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

It assumes knowledge of the basic screen- and table-handling tools detailed in the *SANscreen Foundation User Manual*, including use of the micro-view toolbar to display detail panes.

Customer Service

For questions, comments, or suggestions, contact Onaro as follows:

e-mail: support@onaro.com
online: http://www.onaro.com/support_login.html
phone: 1.800.98.ONARO (US)
+44 (0) 870.44.ONARO (International)
fax: Fax 617.338.1444

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!

Onaro Products

The following products comprise Onaro's suite of Storage Service Management (SSM) and predictive SAN change solutions.

Product Name	Description
SANscreen Foundation	SANscreen's foundation solution, with features that analyze and validate your storage network environment.
SANscreen Replication Assurance	SANscreen's Replication Assurance solution, used to validate your storage replication environment.
SANscreen Performance Insight	Extended tools and features that analyze the performance of your storage network.
SANscreen Service Insight	Features that offer visibility into your SAN environment, including host-to-storage access paths, storage availability, and change management.
SANscreen Plug-In for Oracle Enterprise Manager 10g Grid Control	SANscreen's plug-in for the Oracle Enterprise Manager 10g, used to provide Database Administrators with a window into their SAN environment.

Documentation Set

The following table lists the full documentation set for Onaro's suite of Storage Service Management (SSM) and predictive SAN change solutions. These manuals are available from the client Help menu.

Manual	Description of Content
SANscreen Foundation Installation and Administration manual	Provides an overview of the SANscreen architecture, instructions to get the system up and running, and other administrative tasks.
SANscreen Foundation User Manual	Details the graphical user interface to SANscreen's foundation solution, including features and procedures available to analyze and validate your storage network environment — and to notify you of problems, discover their root cause, and resolve them. Also describes the SANscreen Foundation reporting capabilities.
SANscreen Replication Assurance User Manual	Details the graphical user interface to SANscreen's Replication Assurance product, including features used analyze and validate your storage replication environment.
SANscreen Performance Insight User Manual	Provides details about the tools and features available to help analyze the performance of your storage network.
SANscreen Service Insight User Manual	Provides details about the tools and features available to help you gain visibility to your SAN environment.
SANscreen Connect API	Details the API interface to SANscreen Foundation's functions. The API allows you to integrate SANscreen Foundation with other applications, such as reporting and monitoring systems.
SANscreen Plug-In for Oracle Enterprise Manager 10g Grid Control Installation and User Guide	Instructions to install, configure, and use the SANscreen plug-in for the Oracle Enterprise Manager 10g.

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 Foundation 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 10 — Configuring SNMP Notifications
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	12 — Troubleshooting and Phone Home

Chapter 1

SANscreen Architecture

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

1.1 Overview of Components

The SANscreen Foundation 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 (page 2) 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:

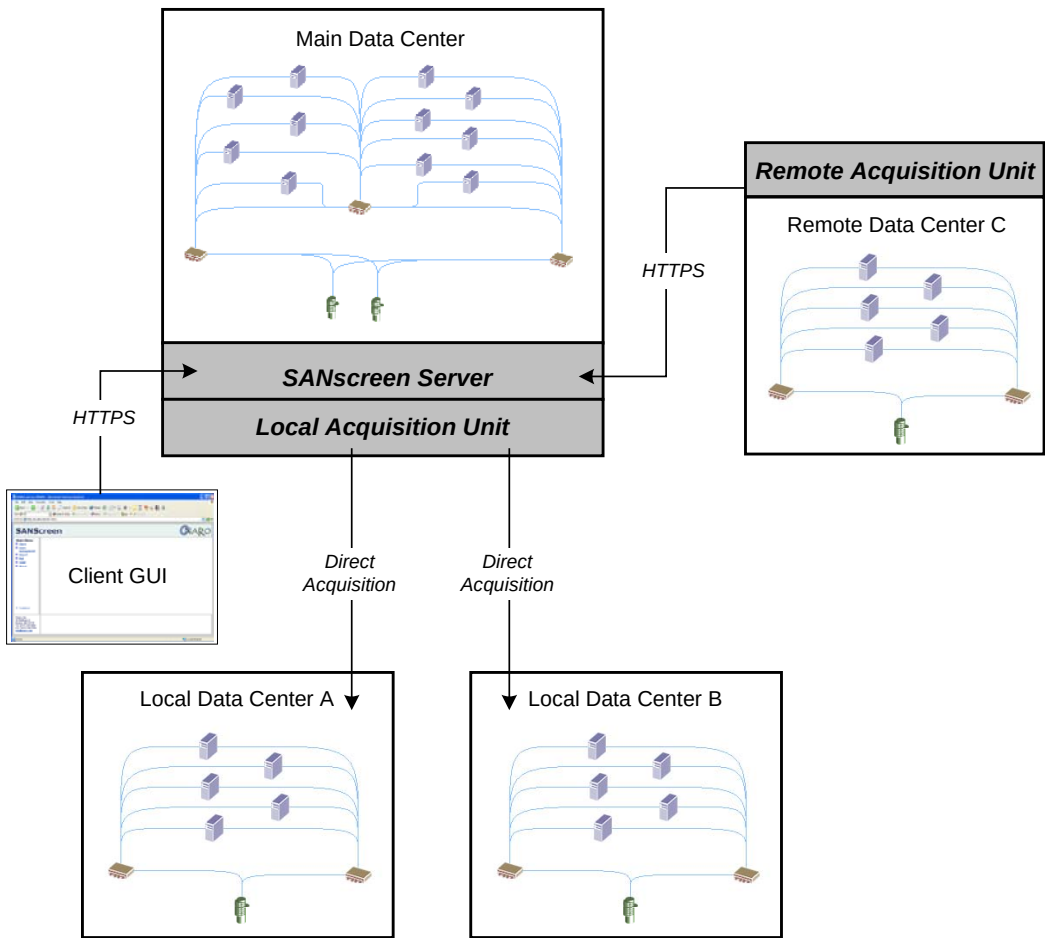


Figure 1: Example of a Common SANSscreen Foundation Implementation

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 Foundation

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

- *Section 2.1 Before You Install SANscreen Foundation...* 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 Foundation Services* (page 10) lists the services that were added to the Windows services environment during the installation process.
- *Section 2.4 Uninstalling SANscreen Foundation* (page 11) tells how to uninstall SANscreen, including related notes.

The installation is self-contained, and includes all the elements required to run and operate SANscreen Foundation — 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 Foundation...

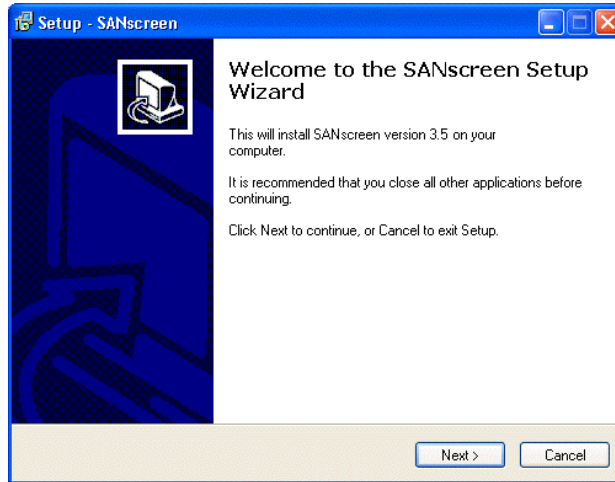
Before installing SANscreen Foundation, make sure you have:

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

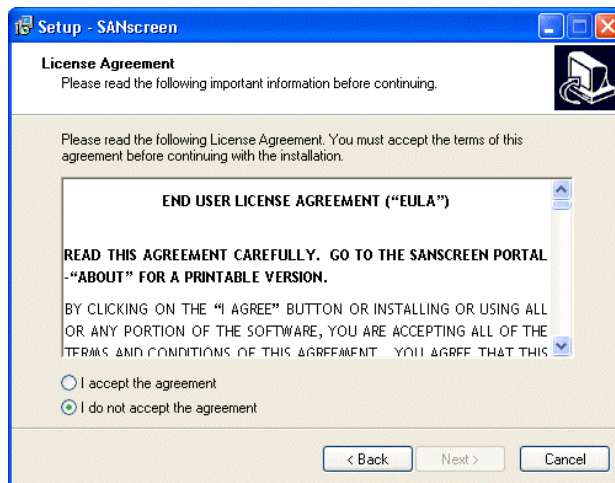
2.2 Using the Installation Wizard

Follow the instructions below to install SANSscreen Foundation:

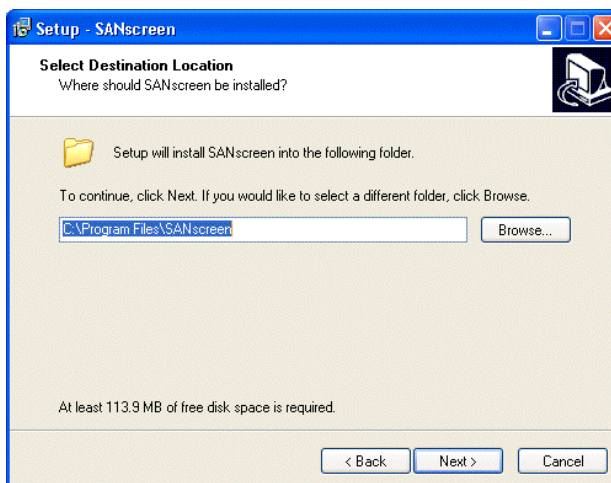
1. Log in to Windows using an account with administrator privileges.
2. Open Windows Explorer, then the directory where the installation files are located. Double click setup.exe. Click Next from the first window to continue:



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

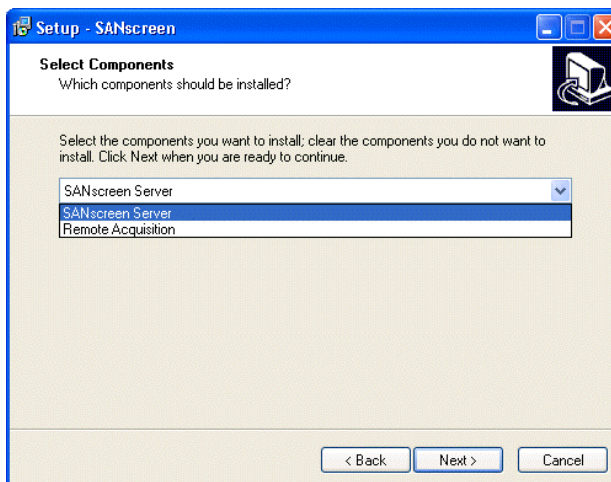


4. The next window prompts for the directory where you want install SANSscreen (defaults to C:\Program Files\Onaro):



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

5. 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.

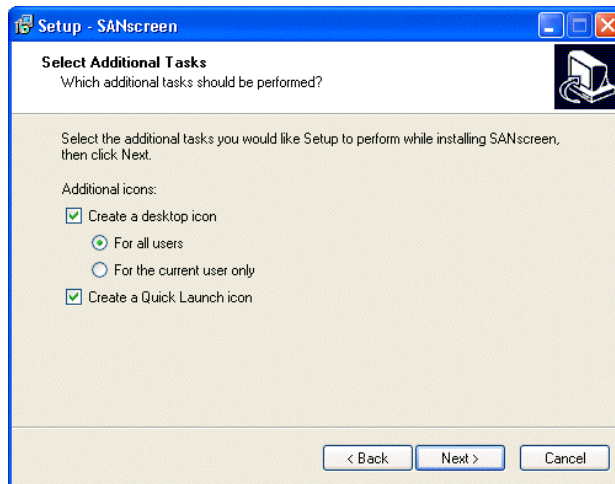


The following steps apply if you selected SANSscreen Server. The Remote Acquisition installation is described in Chapter 3.

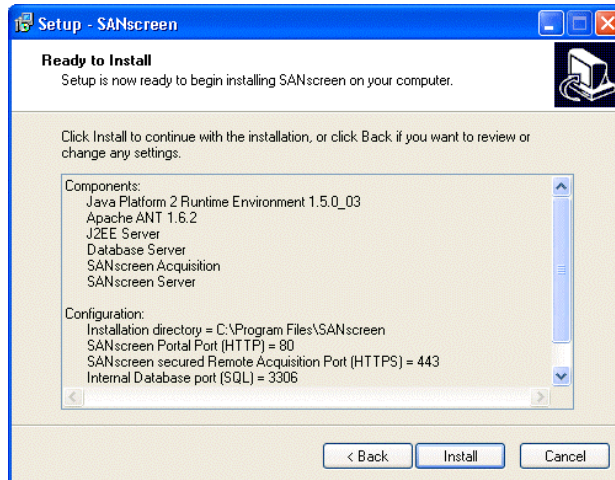
6. Configure system attributes, clicking Next when you're through:

Attribute	Used to Configure the...
SANSscreen Portal Port (HTTP)	Port used by the SANSscreen 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).
SANSscreen Secured Remote Acquisition Port (HTTPS)	Port used by Remote Acquisition Units to send SAN change information to the SANSscreen server through a secured channel. Change this setting if a 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 SANSscreen server is running, to serve as an access point to the database. Change this setting if a port conflict occurs; otherwise leave the default (3306).
Database Size(MB)	Initial size of the SANSscreen SQL database. The default size (200MB) can hold a 200-host SAN for more than ten years. The database allocates additional space dynamically, as needed.

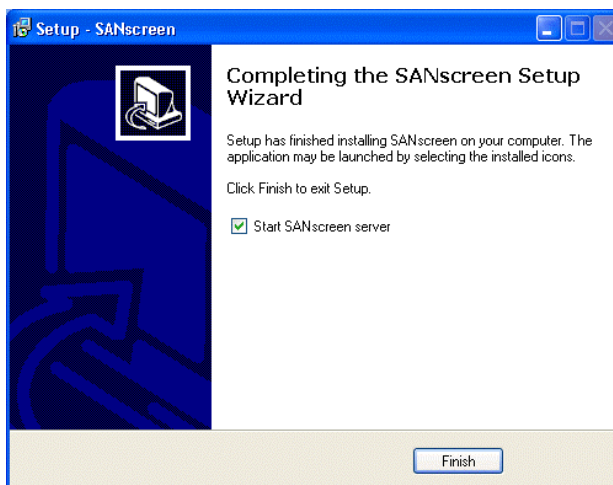
7. Choose the startup shortcuts you want to use for a quick launch, then click Next:



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



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



10. 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. Refer to Chapter 11 for instructions to do this.

2.3 Verifying New SANscreen Foundation Services

After a successful installation, the following 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 these 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 a list of services:

```
net start
```

2.4 Uninstalling SANSscreen Foundation

If you wish to uninstall SANSscreen Foundation:

1. Back up the current version of the SANSscreen database (see page 74).
2. Close all SANSscreen windows.
3. Stop the SANSscreen server (see page 19).
4. Open the Add/Remove Programs feature from the Control Panel.
5. Select the SANSscreen application for removal.

Warning: Uninstalling SANSscreen **permanently deletes** all previously collected 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 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, 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>`

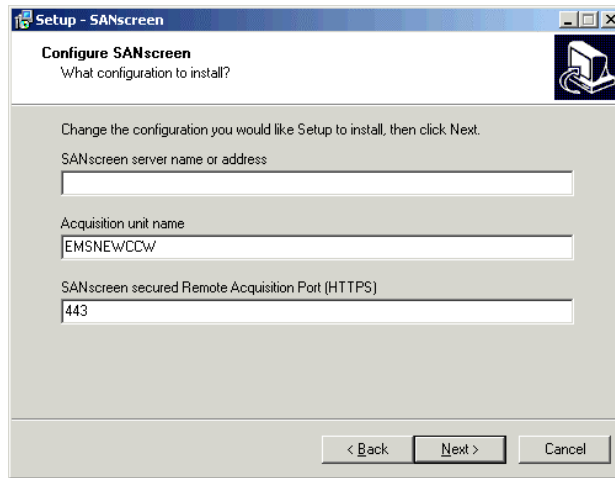
The acquisition port defaults to 443 but may have been changed during the server installation.

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

Follow the instructions below to install the RAU:

1. Follow steps 1 – 4 of the basic installation procedure, described starting on page 6.
2. At step 5, 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 it 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. Review your selections, then 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 the window shown below:



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 this 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 a list of services:

```
net start
```

3.4 Validating the Installation

To validate proper 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. Define the appropriate Data Sources to run 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 Foundation:

- *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.

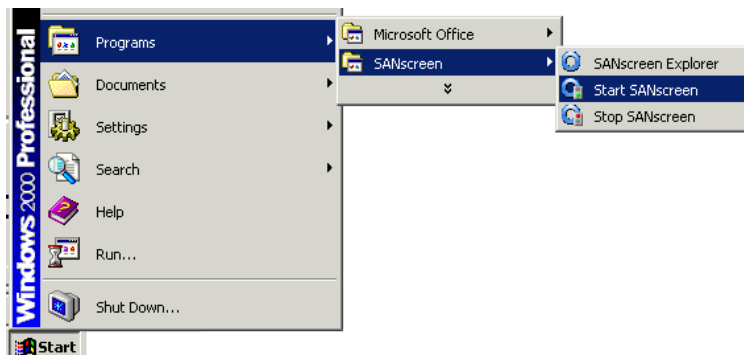
Note: Remote Acquisition Units start and stop with the host server where they are installed.

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 service starts automatically with your PC. This service includes a Local Acquisition Unit, which also starts automatically.

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

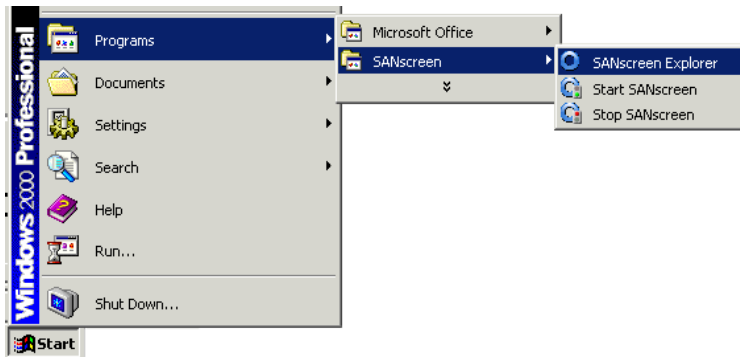


4.2 Starting the SANscreen Client

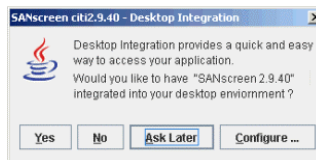
You can run the SANscreen client from the Start menu or from a Web browser, as detailed in the sections that follow.

4.2.1 Using the Start Menu

When launching the client from the SANscreen server, use the Start menu, as follows:



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**. For security purposes, you should change these defaults as soon as possible after installation.

After a successful login, the main client screen opens, illustrated in the figure below.

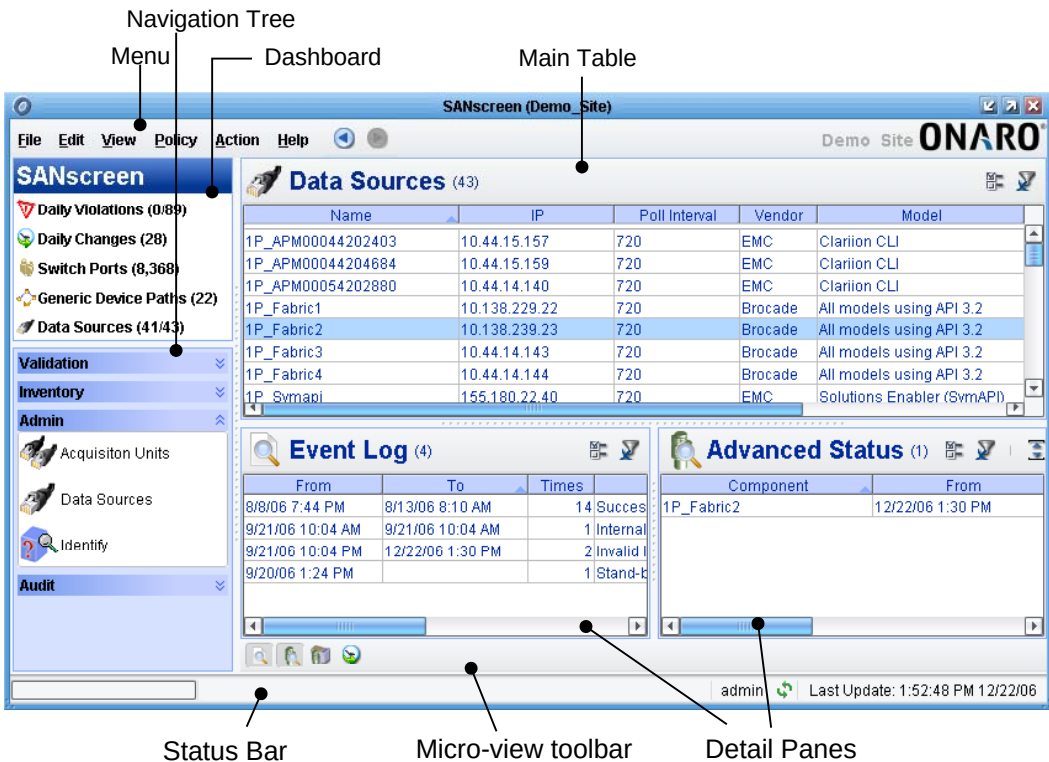


Figure 2: SANscreen Foundation Client Display

Refer to the *SANscreen Foundation 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:

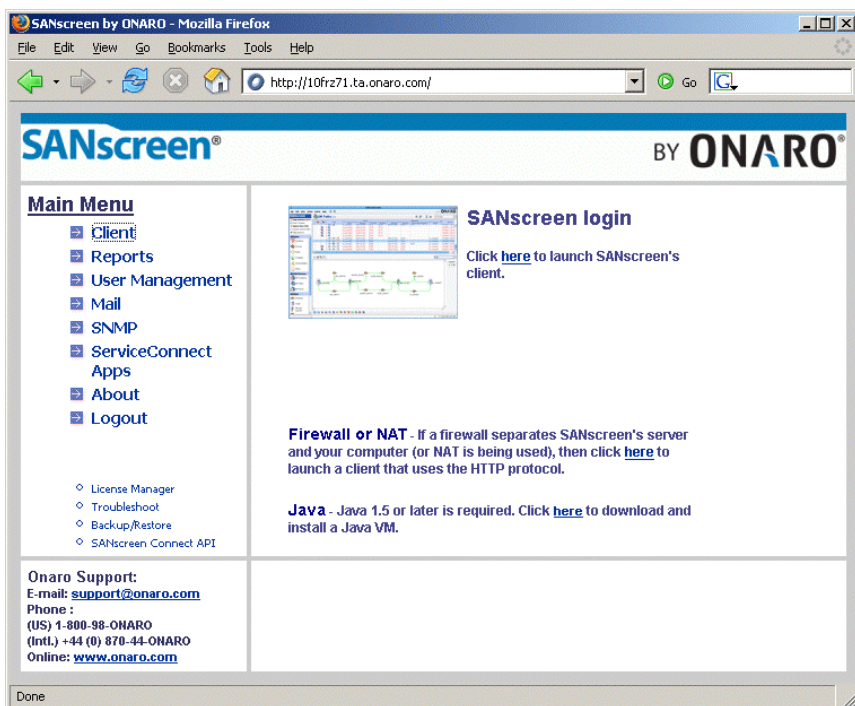
`http://<SANscreen_hostname>:<SANscreen_port>`

The port number will be either 80 or 8080, as configured when the server was installed. It defaults to 80 if not specified in the URL.

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:



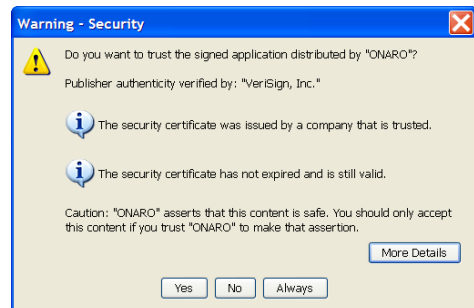
Request the login window by clicking [here](#) to launch SANscreen's client.

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

Note2: If you're running an earlier version of the JRE, Onaro recommends that you upgrade to Java 5.0. SANscreen's client portal offers a link for the Windows JRE.

Note3: 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 browser), then proceed from the login window as described starting on page 20 (enter your user name and password, etc.)



Chapter 5

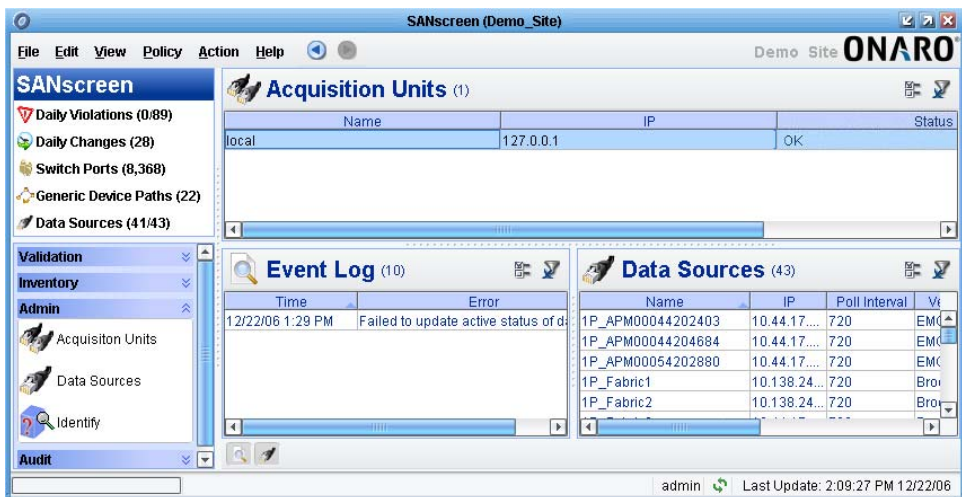
Viewing Acquisition Units

You can monitor the status of all running Acquisition Units, including the Local Acquisition Unit that's installed by default with the SANscreen server. This chapter describes how to do this, as follows:

- *Section 5.1 The Acquisition Units Screen Described* provides an overview of the Acquisition Units screen, and details the information displayed in that screen.
- *Section 5.2 Operations* (page 27) describes the various operations available from the Acquisition Units screen.

5.1 The Acquisition Units Screen Described

Choose Acquisition Units from the navigation tree (shown to the left below) to open the main Acquisition Units display:



This screen comprises up to three tables (one main table and two detail panes, available through the micro-view toolbar):

- 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. Refer to page 26 for more information about this table.
- The **Event Log**  detail pane applies selecting 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. Refer to page 27 for detailed information about this table.
- The **Data Sources**  detail pane also applies after you select an Acquisition Unit in the main table. It lists the Data Sources that are assigned to (i.e., that run within) the selected Acquisition Unit. The fields listed in the detail pane are the same as those in the main Data Sources table, described on page 33. Refer to Chapter 6 for more information about Data Sources.

5.1.1 The Main Acquisition Units Table

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.

The following fields display in the main table for each Acquisition Unit:

Field	Description
Name	Name of the Acquisition Unit, as specified when it was installed for an RAU (see page 15). Always local for the LAU.
IP	IP address of the server where the Acquisition Unit is installed.
Status	Status of the Acquisition Unit: • OK — The Acquisition Unit is up and running. • <i>error message</i> — There is a problem with the Acquisition Unit, as stated by the message.

5.1.2 The Event Log

Click the Event Log button  in the micro-view toolbar to display any events and errors that occurred during the most recent attempt(s) to run the selected Acquisition Unit. Look at the error message to understand the cause, or contact the Onaro support team for assistance.

Field	Description
Time	Date/time of the acquisition attempt, in <i>mm/dd/yy hh:mm</i> format.
Error	Description of the error or event reported.

5.2 Operations

With Acquisition Units displayed, the Action or right-click menu allows the actions described below:



Action	Used to...	See page...
Add Data Source	Define a new Data Source.	39
Clear Data Source Event Log	Clears the event log for all Data Source assigned to the selected Acquisition Unit. The discussion referenced to the right clears the event log for a single Data Source, but the processing is essentially the same.	44
Remove Acquisition Unit	Removes the selected Acquisition Unit and all Data Sources assigned to it.	28

5.2.1 Removing an Acquisition Unit

This operation removes the Acquisition Unit and all Data Sources assigned to it. Use it with caution, and only after the devices corresponding to the Data Sources are no longer used in the SAN.

After completing this operation:

- SANscreen Foundation presents any data that was acquired by the removed Data Sources as non-current. See page 43 for further description of this condition.
- You will no longer see paths that were created based on the information acquired from the removed Data Sources.

To remove an Acquisition Unit:

1. Stop all Data Sources for the Acquisition Unit (see page 42).
2. Right-click the target Acquisition Unit in the main table.
3. Choose Remove Acquisition Unit from the Action or right-click menu.
4. Click Yes in the confirmation box to confirm removal of the Acquisition Unit. The row corresponding to the Acquisition Unit is dropped from the main table.
5. As necessary, use the Delete Inactive Device feature to remove devices permanently. This feature is available from the appropriate Inventory list (host inventory, switch inventory, etc.).

Chapter 6

Using Data Sources to Discover the SAN

This chapter describes how to add and maintain Data Sources within SANscreen Foundation. 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 Unsupported Configurations* (page 31) lists device configurations that cannot be reported by SANscreen.
- *Section 6.3 Preparation* (page 31) tells what information you need to have at hand before proceeding.
- *Section 6.4 The Data Sources Screen Described* (page 32) provides an overview of the Data Sources screen, and details the information displayed in that screen.
- *Section 6.5 Operations* (page 38) describes the various operations available from the Data Sources screen.
- *Section 6.6 Adding a Data Source* (page 39) provides detailed instructions to add a new Data Source.
- *Section 6.7 Editing Data Source Properties* (page 41) tells how to modify a Data Source definition.
- *Section 6.8 Starting a Data Source* (page 42) tells how to start a Data Source.
- *Section 6.9 Stopping a Data Source* (page 42) tells how to stop a Data Source.
- *Section 6.10 Removing a Data Source* (page 43) tells how to remove a Data Source after the devices corresponding to the Data Source are no longer used in the SAN.

- *Section 6.11 Forcing Acquisition* (page 44) tells how to force a Data Source to start the acquisition process.
- *Section 6.12 Clearing the Event Log* (page 44) tells how to clear the log for a Data Source.
- *Section 6.13 Troubleshooting Data Source Activity* (page 45) describes some common problems and how to correct them.

6.1 Understanding Data Source Concepts

A Data Source is a logical SANscreen Foundation component that continuously communicates with one or more SAN devices (or device-management applications), 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 communicates directly with a management agent that's installed on a SAN device or management station. Depending on the management agent, each Data Source is capable of reporting on one or more SAN devices, as follows:

- If the management agent is installed on a SAN device, the Data Source will report on the device itself, and possibly on its sibling devices (for example, all devices of the same type on the same fabric).
- If the management agent is installed on separate hardware, such as a management station, the Data Source will report on all devices managed by that station.

There are many different types of Data Sources, representing the various SAN devices supported by SANscreen Foundation. Refer to *Appendix A, Available Data Sources*, for a complete list of the supported device types, and the parameters specific to each.

SANscreen Foundation 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 devices regularly for their status, at some user-configured interval.

6.2 Unsupported Configurations

SANscreen Foundation does not report changes related to the following device configurations:

- Arrays with no volumes.
- Arrays with no ports.
- Switch devices with no ports.

Although a Data Source might acquire status information from such devices, the information will fail the integrity checking done by the Acquisition Unit, and is not forwarded to the SANscreen server.

6.3 Preparation

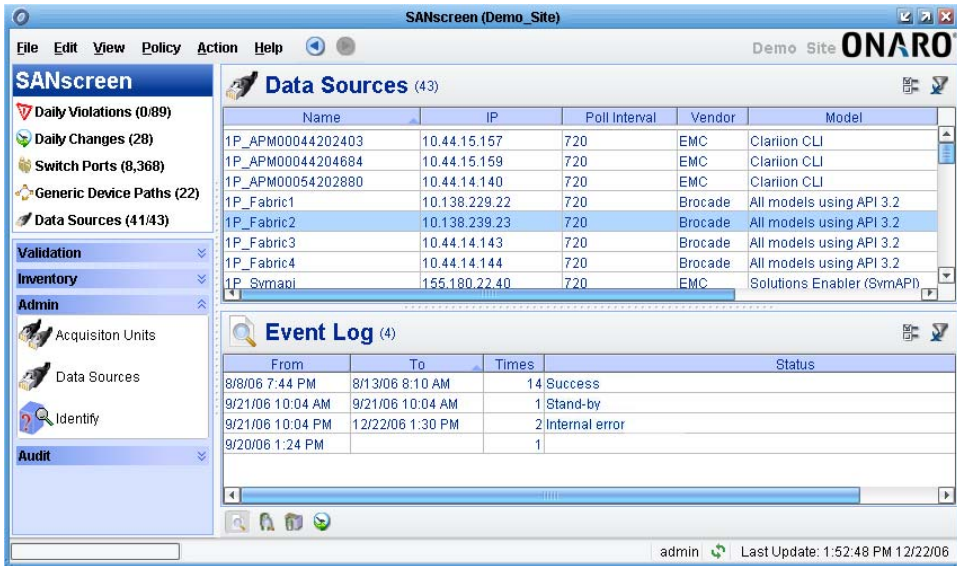
For each Data Source, the specific requirements to define that Data Source depend on the vendor and model of the corresponding SAN device(s). Refer to Appendix A for detailed information.

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.

6.4 The Data Sources Screen Described

Choose Data Sources from the navigation tree (shown to the left below) to open the Data Sources screen:



The screen contains one main table and several detail panes that are available through the micro-view toolbar:

- 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. Refer to page 33 for more information about this table.
- The **Event Log** detail pane applies after you select a Data Source in the main table. It lists the recent acquisition attempts made by the selected Data Source. Refer to page 35 for details about this log.
- The **Advanced Status** detail pane applies after you select a Data Source in the main table, and lists the status of each Data Source (software) component. Refer to page 36 for details about this table.
- The **Devices** detail pane applies after you select a Data Source in the main table. It lists the devices on which the Data Source reports. Refer to page 36 for more information about this table.

- The **Changes**  detail pane applies after you select a Data Source in the main table. It lists the SANscreen changes that resulted from information reported by this Data Source. Refer to page 37 for more information about this table.

6.4.1 The Main Data Sources 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 39).
IP	IP address where the corresponding management agent is installed. This is the IP address of a SAN device or a device-management station.
Poll Interval	Interval (in minutes) at which the Data Source polls its corresponding management agent. <i>Note1:</i> Receipt of an SNMP trap restarts the interval counter. <i>Note2:</i> The information received is only as current as the polling interval for the management agent with which the Data Source communicates.
Vendor	Vendor for the device(s) reported by the Data Source.
Model	Model of the device(s).
State	Current state of the Data Source: • Running — The Data Source is active and running at the configured polling interval. • Acquisition not running — The entire acquisition service is down, including all Data Sources running on the Acquisition Unit. • Stopped — The Data Source has been stopped. • Starting — The Data Source is initializing. This is a temporary state between Stopped and Running. • Stopping — The Data Source is shutting down. This is a temporary state between Running and Stopped.

Field	Description
Recent Status	Status of the latest attempt to acquire information from the devices that are polled by this Data Source: • Success — The attempt is complete and was successful. • Acquiring devices — The acquisition is in process. • Sending data to server — The acquisition results are being forwarded to the server. • 3 out of 5 devices finished successfully — The Data Source successfully reported only a subset of the components it queried. Refer to the Advanced Status detail pane for additional information regarding the failed components. • <i>error message</i> — The acquisition attempt failed for the reason stated.
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 stated by the message. Refer to page 46 for suggestions if you see an error message here.

6.4.2 The Event Log

Click the Event Log button  in the micro-view toolbar to display the acquisition history for the selected Data Source. Each row in this table represents one or more acquisition attempts that are grouped according to their status. If more than one attempt was made with the same resulting status, they are grouped under a single row, and the Times column reflects the number of attempts.

Field	Description
From	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	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. The values are described for the main Data Sources table on page 34.

6.4.3 The Advanced Status Detail Pane

Click the Advanced Status button  in the micro-view toolbar to display detailed information about each software component of the Data Source. Data Sources typically comprise several components that are started and stopped separately by the Data Source. This table displays one line for each component.

Field	Description
Component	Component name.
From	Date and time the component was last started, in <i>mm/dd/yy hh:mm</i> format.
To	Date and time the component last terminated processing, using the same format as described above.
Status	Brief text describing the status of the last (or current) execution of the component. If there is a link to additional information in this field, click the link for extended error details.
Times	Number of times the condition described by the Status field occurred.

6.4.4 The Devices Detail Pane

Click the Devices button  in the micro-view toolbar to display details about the devices on which the Data Source reports. Each row in the Devices table represents a single SAN device.

Field	Description
Device Name	Name of the SAN device.
Type	Type of device (Storage, Host, etc.).
WWN	WWN to identify the device.
Additional Data Sources	Additional Data Sources that report on the same device, if any.

6.4.5 The Changes Detail Pane

Click the Changes button  in the micro-view toolbar to display changes relating to the selected Data Source; in other words, a summary of changes to the SANscreen database that resulted from information reported by this Data Source.

Field	Description
Time	Date/time at which the change took place.
<i>icon</i>	Icon indicating the type of event documented on the line (see the <i>SANscreen Foundation User Manual</i> for a list of icons and their meanings).
Event	Description of the change action that occurred at the time indicated. Changes that resulted from a single action are stamped with the same time, and are summarized on a single row. Click the  button to display more detailed change information for nested events.

6.5 Operations

With Data Sources displayed, the Action or right-click menu allows the actions described below:

Add Data Source	Insert
Edit Data Source	Enter
Remove Data Source	Delete
Start data source	
Stop data source	
Force Acquisition	
Clear Event Log	
Crawl With Data Source	
Manage	

Action	Used to...	See page...
Add Data Source	Open a wizard that lets you add a new Data Source.	39
Edit Data Source	Open a wizard that lets you change the parameters of the selected Data Source.	41
Remove Data Source	Remove the selected Data Source and flag all data acquired from this Data Source as non-current. <i>Note:</i> Only remove a Data Source after it's no longer used. Do not remove a Data Source if it's temporarily out of use.	43
Start Data Source	Start the selected Data Source (applicable only if the Data Source is Stopped).	42
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.	42
Force Acquisition	Force the selected Data Source to initiate a data acquisition, thereby ensuring that the most recent data has been acquired.	44
Clear Event Log	Clear the event log for the selected Data Source.	44
Crawl With Data Source	Solve communication problems between the selected Data Source and a SAN device. Only use this option upon request by the Onaro support team.	—
Manage	Launch the management console/interface for the selected Data Source.	—

The sections that follow describe the actions for which this manual provides more detail, in order as listed above.

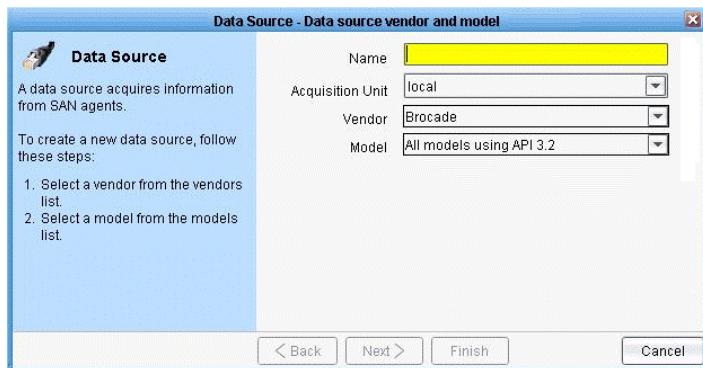
6.6 Adding a Data Source

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. If the new device will be reported by an existing Data Source, there is no need to add a new one.

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).
- As necessary to the specific Data Source, install the management agent through which the Data Source communicates with its device(s). The specifics of this are covered in Appendix A where appropriate.
- Verify that the Local Acquisition Unit and all RAUs are shown in the Acquisition Units table and that they have an OK status (see Chapter 5).

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



1. Enter a name for the Data Source that's unique across all Acquisition Units. Choose a name that will make it easy for you to identify the Data Source. The name 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 model of the device where the management agent is installed. This is the agent from which the Data Source will acquire SAN information. It might be the SAN device itself, or separate hardware, such as a management station.
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:

Data Source - Data source configuration

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

Brocade switch: [Yellow highlighted field]

User name: admin

Password: [Masked]

Poll interval (min): 15

Enable trapping: ☒

Minimum time between traps (sec): 10

Comma separated list of switches to ignore: [Empty field]

Ignore Brocade API error -21 on N-Ports: ☐

Fabric name: [Empty field]

[Back] [Next >] [Finish] [Import] [Cancel]

5. Fill in the information requested by the configuration screen. Invalid field values are **highlighted**, including required fields that are not yet specified, such as the IP address above (Brocade Switch field).

Refer to Appendix A for device-specific details about each parameter. Click Finish when you're through, to activate the Data Source in your environment. (SANscreen activates the Finish button after all required fields are filled in, assuming there are no invalid field values.)

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:

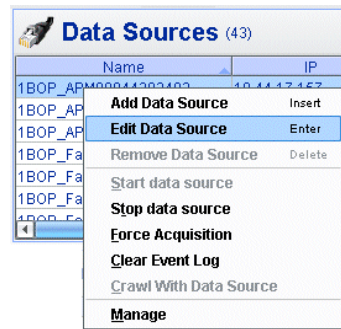
- Allow a reasonable amount of time for the acquisition to complete. Several seconds is generally enough, but some devices may be slow or highly populated and may take several minutes to acquire.
- Select the new Data Source in the main table.
- Examine either the main Data Source table or the acquisition event log for successful acquisitions. If the Status field is Acquiring Devices, the acquisition has not yet finished.

Note: As necessary, press <F5> to refresh the display.

6.7 Editing Data Source Properties

The Edit Data Source option lets you examine and/or modify the parameters for one or more selected Data Sources. You might do this 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. In the main table, right-click the Data Source(s) to edit.
2. Choose Edit Data Source from the Action or right-click 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. If you selected multiple Data Sources, SANscreen displays (and allows you to modify) only the common attributes.
5. Click Finish.

If the Data Source was active (status is Running), it will restart 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 it's not already Running.
- Allow a reasonable period of time for the acquisition to complete, then examine the event log for a successful acquisition.

6.8 Starting a Data Source

Starting a Data Source changes its status from Stopped to Running (with the transitional Starting state in between).

To start a Data Source:

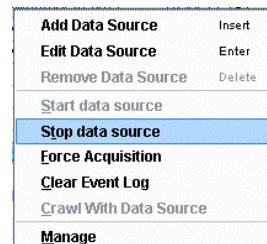
1. Right-click the Data Source in the main table.
2. Choose Start Data Source from the Action or right-click menu.
3. Click Yes to confirm the operation.
4. After several seconds:
 - o Verify that the status changes to Running. As necessary, press <F5> to refresh the display.
 - o Allow a reasonable period of time for an acquisition to complete, then examine the event log for a successful acquisition.

6.9 Stopping a Data Source

Stopping a Data Source changes its status from Running to Stopped (with the transitional Stopping state in between).

To stop a Data Source:

1. Right-click the Data Source in the main table.
2. Choose Stop Data Source from the Action or right-click menu.
3. Click Yes to confirm the operation.
4. After several seconds, verify that the status changes to Stopped. As necessary, press <F5> to refresh the display.



6.10 Removing a Data Source

This operation removes the Data Source and all entities it reported on during the most recent acquisition (volumes, zones, connectivity, etc.). For this reason, you should use this operation with caution, and only *after all devices corresponding to the Data Source are no longer used in the SAN*.

Note: If a second Data Source reports on one or more of the same entities, they are not removed.

One exception exists to this rule, and that is the devices on which the Data Source reported. These are not removed, but are grayed out in the topology view and tables, marking them as inactive. Use the Delete Inactive Device option to remove them, as necessary. This is described in the *SANscreen Foundation User Manual*.

To remove a Data Source:

1. Right-click the target Data Source in the main table.
2. Stop the Data Source (see page 42).
3. Choose Remove Data Source from the Action or right-click 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 to remove a device permanently. This feature is available from the appropriate Inventory list (host inventory, switch inventory, etc.), as detailed in the *SANscreen Foundation User Manual*.

After completing the Remove Data Source operation:

- SANscreen Foundation presents any data that was acquired by the removed Data Source as non-current. This means that all connectivity, ports, volumes, masking, zones, etc. that were discovered solely by the removed Data Source will disappear, and the Data Source Changes detail pane will indicate their removal. The corresponding device itself still appears in SANscreen tables and in the topology pane, but is grayed out.

- You will no longer see paths that were created based on information acquired from the removed Data Source.

6.11 Forcing Acquisition

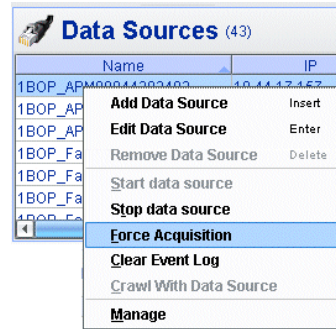
Forcing acquisition causes the selected Data Source to initiate the acquisition process immediately. If the Data Source is already in an acquisition process, SANSscreen ignores this command.

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 Action or right-click menu.
4. Click Yes to confirm the operation.

After forcing acquisition:

- The event log should show a status of Acquiring Devices.
- Allow a reasonable period of time for an acquisition to complete, then examine the event log for a successful acquisition.

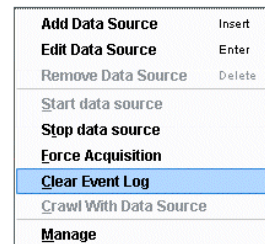


6.12 Clearing the Event Log

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

Follow these steps to clear the event log for a selected Data Source:

1. Right-click the Data Source in the main table.
2. Choose Clear Event Log from the drop-down menu.



3. SANscreen verifies the request. Click Yes to continue.

After completing this process, the event log will contain only the most recent two entries.

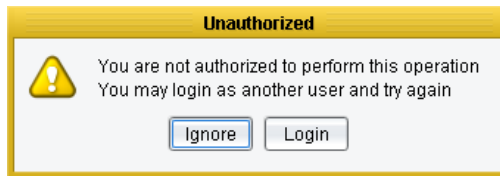
6.13 Troubleshooting Data Source Activity

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

6.13.1 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.

6.13.2 Faulty Acquisition Unit Status

If the 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):

Start – Settings – Control Panel – Administrative Tools – Services

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

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

6.13.3 Unsuccessful Acquisition or Faulty Data Source

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

1. Examine the acquisition failure message in the event log'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

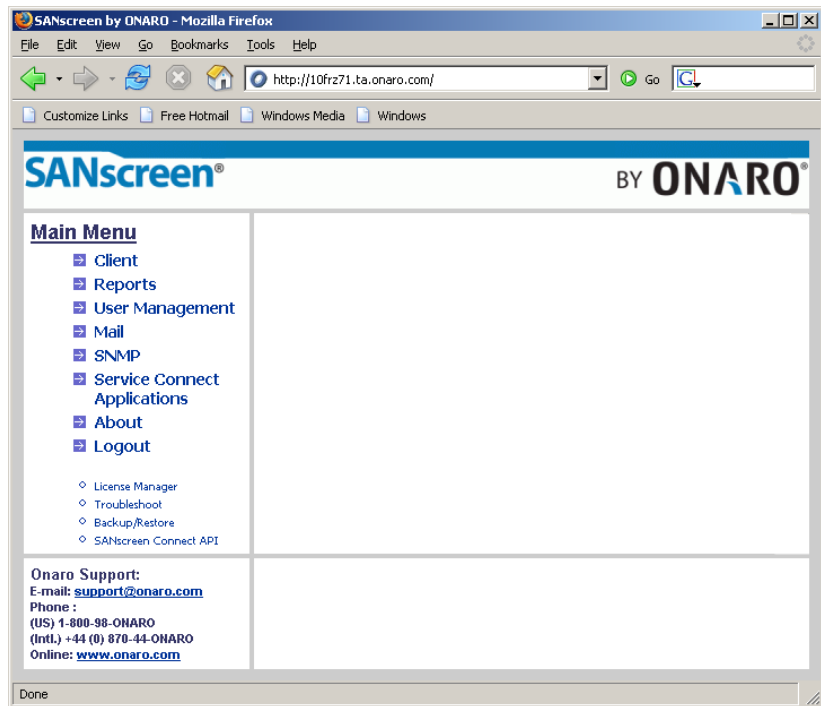
The SANscreen Foundation administration portal is available from any Web browser, by entering the following URL:

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

The port number will be either 80 or 8080, as configured when the server was installed. It defaults to 80 if not specified in the URL.

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

<http://localhost>



The table that follows describes your processing options from the portal.

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. • Provide trend analysis. • Summarize outstanding vulnerabilities. • Detail discovered storage devices. • Summarize SAN access and inventory information. • Summarize violations. • Pre-validate planned tasks. • Display the status of each Data Source. These reports and their use are described in the <i>SANscreen Foundation User Manual</i>.	—
User Management	Define and manage user accounts.	8
Mail	Configure SANscreen to find your e-mail server.	9
SNMP	Tell SANscreen where to send SNMP trap messages.	10
ServiceConnect Applications	Applications developed by Onaro using the ServiceConnect API, including a host portal and a utilization report. Described in the <i>SANscreen Foundation User Manual</i> .	—
About	Display SANscreen current version and copyright information, as well as the JAR version and timestamp for each Data Source.	—
Logout	Log out as the current user.	—
License Manager	Install a new SANscreen license.	11
Troubleshoot	Work with Onaro to resolve system problems.	12
Backup/Restore	Backup and/or restore the SANscreen database.	13
SANscreen Connect API	Open the documentation for the ServiceConnect API interface to SANscreen Foundation, allowing you to integrate SANscreen Foundation with other applications, such as reporting and monitoring systems.	—

Chapter 8

User Management

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 Foundation, 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 describes the User Management screen, and tells how to add, edit and remove SANscreen user accounts:

- *Section 8.1 User Roles* describes the various levels of permissions available to user accounts.
- *Section 8.2 SANscreen User Management Screen* (page 51) 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 53) 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 56) tells how to add and maintain user definitions on the local SANscreen server, including updates to LDAP users that you can only make on the local server.

8.1 User Roles

Each user account is assigned one of the following permission levels:

- **Guest** — Permits you to log in to the SANscreen Foundation client, and to view the various screens; but not perform actions such as defining policy 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 all guest-level privileges, as well as access to SANscreen operations such as defining policy and identifying generic devices. Does not allow you to perform Data Source operations, nor 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.
 - 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.

SANscreen login

Enter your name and password to sign in

User name:

Password:

Note: If you get an HTTP 401 error, most likely you entered the name or password incorrectly. Click the User Management link and try again.

This main body of the User Management window comprises a table that's used to maintain user definitions in the local SANscreen database (shown below for a user having Administrator privileges).

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.

SANscreen®

BY **ONARO®**

Main Menu

- Client
- Reports
- User Management
- Mail
- SNMP
- Service Connect Applications
- About
- Logout

- License Manager
- Troubleshoot
- Backup/Restore
- SANscreen Connect API

User Management

LDAP Configuration

Add new user

Name	Roles			E-mail			
	Guest	User	Administrator				
guest	X				Edit	Delete	Change password
admin	X	X	X		Edit		Change password
onaro	X	X			Edit	Delete	Change password

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.

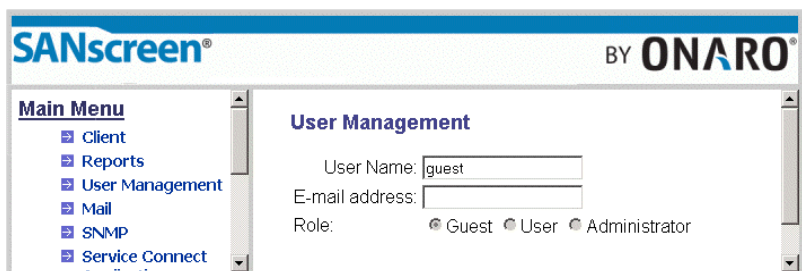
(You can identify LDAP users easily, because they don't have the Change Password option to the far right.)

User entries include the following information, where an X indicates that a column applies for the user. Refer to the field descriptions in *Section 8.4.2 Adding a New User*, starting on page 57, 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 50 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.
E-mail	User's e-mail address.
Edit/Delete/Change Password links	Links used to initiate the corresponding processing. Refer to page 58 to edit an account, page 59 to delete an account, and page 59 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 (assuming your account is managed via the local server), SANscreen opens a screen that allows you to change your own e-mail address and password:



Note: If your account is managed via LDAP and you are logged in from a User or Guest account, you will not be able to make any changes.

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 56) tells how to validate the LDAP server and domain.

Notice that LDAP users display along with users who are defined locally to SANSscreen, on the initial user list (see page 51).

8.3.1 LDAP Configuration Screen

The User Management screen that opens for the Server Administrator contains a button labelled LDAP Configuration (shown on page 51). Click this button to initiate the LDAP configuration process.

SANSscreen® BY **ONARO®**

Main Menu

- Client
- Reports
- User Management
- Mail
- SNMP
- Service Connect Applications
- About
- Logout

LDAP Configuration

☐ LDAP Enable

User principal name attribute:

Role attribute:

Mail attribute:

Distinguished name attribute:

Referral:

Timeout (ms):

LDAP server:

Domain:

SANSscreen server administrators group:

SANSscreen administrators group:

SANSscreen users group:

SANSscreen guests group:

Directory lookup user:

Directory lookup user password:

Confirm directory lookup user password:

◊ License Manager
◊ Troubleshoot
◊ Backup/Restore
◊ SANSscreen Connect API

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 8.4.3 Editing a User Definition</i> starting on page 58).
Distinguished Name Attribute	LDAP attribute that identifies the user's distinguished name (defaults to distinguishedName).
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:///

Field	Description
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
SANscreen Server Administrators Group	Value of the Role Attribute that identifies the user as having Server Administrator privileges (defaults to sansscreen.server.admin).
SANscreen Administrators Group	Value of the Role Attribute that identifies the user as having Administrator privileges (defaults to sansscreen.admin).
SANscreen Users Group	Value of the Role Attribute that identifies the user as having User privileges (defaults to sansscreen.users).
SANscreen Guests Group	Value of the Role Attribute 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 for LDAP users. It's broken down as follows:

- *Section 8.4.1 Summary of Operations* (page 57) presents an overview of the operations available from the main user display.
- *Section 8.4.2 Adding a New User* (page 57) tells how to add a new user account.
- *Section 8.4.3 Editing a User Definition* (page 58) tells how to edit a user-account definition.
- *Section 8.4.4 Deleting a User Account* (page 59) tells how to delete a user account when it's no longer used.
- *Section 8.4.5 Changing User Password* (page 59) 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).	57
Edit a user definition (requires Administrator privileges).	58
Delete a user account (requires Administrator privileges).	59
Change a user password (requires Administrator privileges).	59

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).
- Log in with Administrator privileges.

Click the Add New User button to open this pane:

User Name:

E-mail address:

Password:

Confirm Password:

Role:

☐ Guest ☐ User ☐ Administrator

Add

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).
E-mail Address	Optional. User's e-mail address. Required if the user subscribes to any reports.
Password	Password used to log in to SANscreen under this user account (typically selected by the user him/herself).
Confirm Password	Same as above, for verification.
Role	Role(s) available to the user (i.e., levels of user permissions). Refer to page 50 for a description of the available roles.

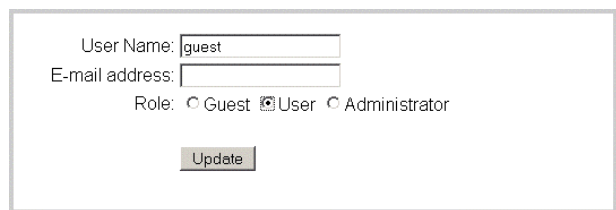
8.4.3 Editing a User Definition

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

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

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

1. Click the **Edit** link to open the change screen:



The screenshot shows a web form for editing a user. It contains three input fields: 'User Name' with the value 'guest', 'E-mail address' which is empty, and a 'Role' section with three radio buttons: 'Guest', 'User' (which is selected), and 'Administrator'. Below these fields is an 'Update' button.

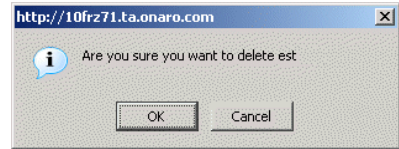
2. Modify the e-mail address and/or role(s), referring to the add-user field descriptions on page 58.
3. Click **Update** to modify the user account settings and redisplay the main user list.

8.4.4 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. SANSscreen confirms the request (right).
- Click OK to confirm the operation and redisplay the main user list.



8.4.5 Changing User Password

A user with Administrator privileges can change the password for any SANSscreen user account defined on the local server. Before doing so, however:

- Notify anyone who logs in under the user account you are modifying.
- Determine what password to use.
- Log in with Administrator privileges.

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:



2. Enter the new password twice.

3. Click Update. SANscreen displays a message telling you that the password was changed successfully.

Chapter 9

Configuring E-mail

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

- To enable proper use of e-mail for reports to which you subscribe. Reports and subscriptions are described in the *SANscreen Foundation User Manual*.
- To use the Phone Home feature described in Chapter 12.

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 – E-mail accounts – View or change existing e-mail account

- Allocate an e-mail account through which SANscreen will send regular reports. 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 properly:

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.

3. 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 E-mail	E-mail account to be identified as the sender on all SANscreen reports. 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.

4. After clicking Submit above, you'll see this message:

E-mail configuration was successfully updated.

To verify that your e-mail server works properly with SANscreen, subscribe to one or more reports. Refer to the *SANscreen Foundation User Manual* for details.

Chapter 10

Configuring SNMP Notifications

SANscreen Foundation 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 Foundation 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 may 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 for the proprietary MIB that supports SANscreen traps, then compile that MIB at your site. The Onaro MIB is compatible with all standard SNMP management software.

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.

SANscreen BY **ONARO**

Main Menu

- Client
- Reports
- User Management
- Mail
- SNMP
- Service Connect Applications
- About
- Logout

License Manager
Troubleshoot
Backup/Restore
SANscreen Connect API

SNMP Configuration

Changes Trap IP: 127.0.0.1 Port: 162

Violations Trap IP: 192.168.0.50 Port: 162

Submit

- 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 should send SNMP change-type trap messages.
Violations Trap IP and Port	IP address and port number to which SANscreen should send SNMP violation-type trap messages.

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

SNMP Configuration was successfully updated.

Verify that an SNMP trap was received for each type of processing requested (changes and/or violations). 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 Foundation 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.

The screenshot shows the SANscreen License Manager web interface. The header features the SANscreen logo and 'BY ONARO'. A left sidebar contains a 'Main Menu' with links to Client, Reports, User Management, Mail, SNMP, Service Connect Applications, About, and Logout. Below the menu are links to License Manager, Troubleshoot, Backup/Restore, and SANscreen Connect API. The main content area is titled 'License Manager' and contains three sections: 'Current license' showing 'License ok' and details (Api: true, Foundation: true, Expiration: Jul 1, 2007, Executive Reports: true); 'Current license:' with a text area showing license details (License.name=Permanent - Edwin, License.version=2.0, Expiration=07/01/2007, Disaster.Recovery=TRUE, Performance=TRUE, Foundation=TRUE) and an 'Update' button; and 'Import license:' with a text input, a 'Browse...' button, and an 'Import' button.

3. Browse to locate the SANscreen license (.lcn) file, then click Import.

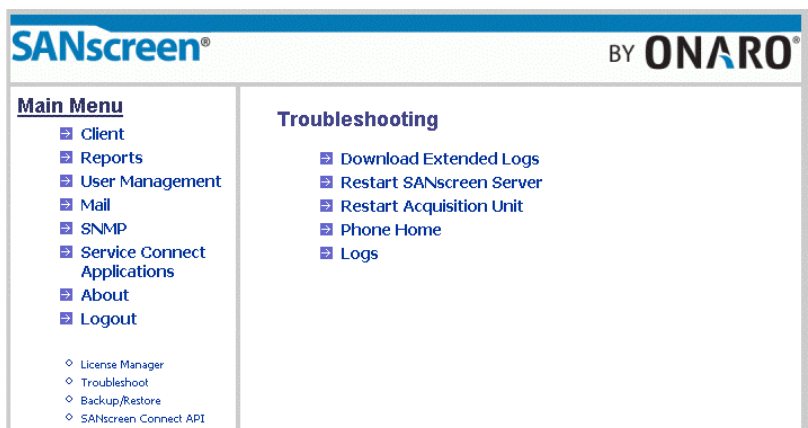
4. Click Update to modify the license using the imported data. SANscreen refreshes the license information, changing the License status to OK and displaying the new Current License.

Chapter 12

Troubleshooting and Phone Home

Follow these steps to access SANscreen's troubleshooting features:

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.



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

Button	Click to ...
Download Extended Logs	Download a file containing your base and extended logs files, as well as the SANscreen database. <i>Section 12.1 Download Extended Logs</i> , next, details this feature

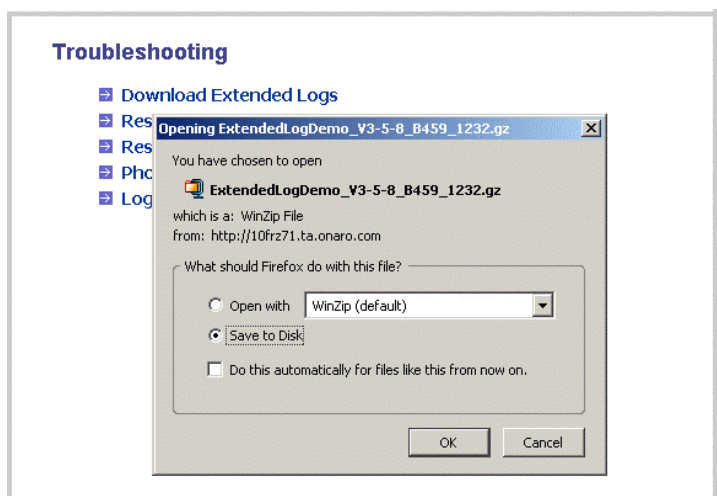
Button	Click to ...
Restart SANscreen Server	Restart the SANscreen server and local Acquisition Unit. Refresh the page after the restart, then log in again to the portal. Be careful — This option is provided for troubleshooting purposes, and should only be used upon request by Onaro support. There is no confirmation.
Restart Acquisition Unit	Restart the local Acquisition Unit. After the restart is finished, SANscreen re-loads all the Data Source views. Be careful — This option is provided for troubleshooting purposes, and should only be used upon request by Onaro support. There is no confirmation.
Phone Home	Configure the feature allowing you to send the SANscreen logs or a database-backup to Onaro for troubleshooting. <i>Section 12.2 Phone Home</i> (page 69) details this feature.
Logs	Not used.

12.1 Download Extended Logs

This feature allows you to download a file containing the SANscreen database, as well as your base and extended logs files — both in text format. These logs are explained in more detail in *Section 12.2 Phone Home*.

After you choose Download Extended Logs, SANscreen prompts you to save the file on your computer. This is illustrated below for a remote connection to the SANscreen server. Click Save to Disk, then OK.

Note: If the SANscreen server is local to your session (<http://localhost>), this screen will have fewer options



Navigate to the folder where you want to save the file, then click Save. By default, the file name is assigned as:

ExtendedLog + *DB name* + *SANscreen version* + ####,
where #### is a unique number.

For example: ExtendedLogMyDB_V3-5-8_1233.gz

12.2 Phone Home

All of Onaro's products are equipped with advanced phone home capabilities, to provide the best possible support for our customers. This mechanism periodically sends predefined, specific, information to the Onaro support team. You are in total control of what information is forwarded to Onaro, and how often it's sent. No data is forwarded unless you first configure SANscreen Foundation to do so.

12.2.1 What Data is Sent to Onaro?

You can configure the system to send base logs, extended logs, and/or backup files — all in text format. The files are formatted as follows before being forwarded to Onaro:

- **Accumulated logs** — Logs are collected from the various system components, including Acquisition Units, the server, and clients. The logs contain system diagnostics and (if they exist) warnings.

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** — The backup contains a full inventory of your topology, a history of your SAN changes, and the SANscreen configuration. It's encrypted (Gzenc) format.

12.2.2 How is the Information Sent?

The information is forwarded to Onaro via FTP, HTTPS, or e-mail, as determined by you. 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.

12.2.3 What Does Onaro Do with the Information It Receives?

The Onaro support team uses this information to ensure the correct operation of SANscreen, to assist in maintaining the validity of your SAN, and to help maintain the integrity of your internal change processes. The Phone Home capability provides 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 you directly.
- **Shorter response time** — When you need assistance from the Onaro support team, most likely all of your SANscreen information will be available to Onaro already. This improves the speed and accuracy of the support provided.

12.2.4 Configuring the Phone Home Feature

In order for Onaro to provide the Phone 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 request the Troubleshoot screen after opening the portal, you'll be asked to log in.
4. Click Phone Home to open the screen shown below:

SANscreen®

BY **ONARO®**

Main Menu

- Client
- Reports
- User Management
- Mail
- SNMP
- Service Connect Applications
- About
- Logout

- License Manager
- Troubleshoot
- Backup/Restore
- SANscreen Connect API

Phone home configuration

Last sent time: Wed 11/08/06 07:43 PM

☐ Base Logs

☐ Extended Logs

☐ Backup file

Sending Duration: Days

Site name:

Send method:

☒ ftp

☐ https

☐ E-mail

Size Limit: MB

Split files if bigger than: MB

Update

Update and send now

5. Fill in the screen fields as described below:

Field	Used to ...
Base Logs	Send your base logs to Onaro. These are the basic logs written by the SANscreen server, SANscreen client, and all installed Acquisition Units. Note: You do <i>not</i> need administrative privileges to access the log files.

SANscreen Installation and Administration

12: Troubleshooting and Phone Home ♦ 71

Field	Used to ...
Extended Logs	Send your extended logs to Onaro. Extended logs include all the basic log files, as well as additional files that detail intermediate acquisition information.
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's recommended that you include the backup 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).
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 ftp, https, or e-mail, 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.
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.

6. When you're through, click:

- o Update to save the configured settings.
- o Update and Send Now to save the configured settings and phone home immediately.

SANscreen confirms with the message:

Phone home configuration is saved.

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.

The screenshot shows the SANscreen administration portal. The top header has the SANscreen logo on the left and "BY ONARO" on the right. A left sidebar contains a "Main Menu" with links: Client, Reports, User Management, Mail, SNMP, Service Connect Applications, About, and Logout. Below Logout are sub-links: License Manager, Troubleshoot, Backup/Restore, and SANscreen Connect API. The main content area is titled "Backup/Restore" and contains two large buttons: "Backup" and "Restore". To the right of the "Backup" button is a button labeled "Backup Database to file". To the right of the "Restore" button is a "Choose file:" label, a text input field, a "Browse..." button, a "Warning: Current database will be discarded!" message, and a "Restore database from file" button.

13.1 Backup

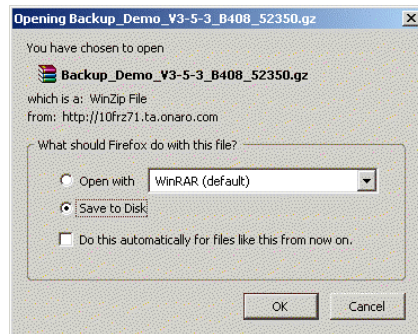
To back up the SANscreen database to a file on your PC:

1. Click Backup Database to File.

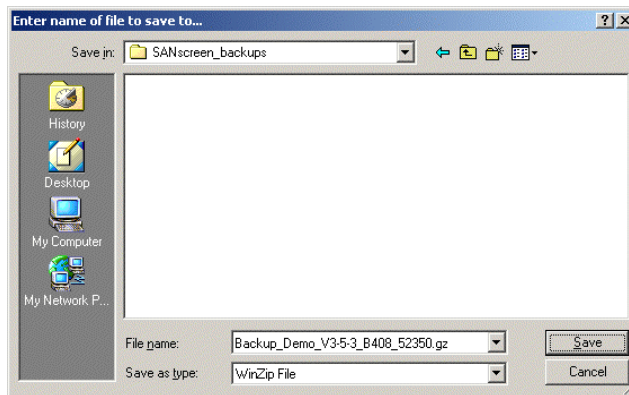
The next steps vary depending on the browser you're using, and are illustrated below for Internet Explorer.

2. SANscreen prompts you to save the file on your computer. This is illustrated to the right for a remote connection to the SANscreen server. Click Save to Disk, then OK.

Note: If the SANscreen server is local to your session (<http://localhost>), this screen will have fewer options



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 file name.



4. Wait while the entire database is backed up. 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.

Warning: You cannot reverse (undo) a restore operation !

To restore the database:

1. Use the Browse button to select the file from which to restore the database.
2. Click Restore Database from File. This completely replaces all your current SANscreen information using data from the selected file, and can take 30 minutes or more.

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

SANscreen's Database was successfully updated.

Appendix A

Available Data Sources

This appendix lists the various SAN devices and management stations from which an installed management agent can communicate with a SANscreen Data Source. For each such device, it tells how to configure the corresponding Data Source to acquire SAN data from the device.

The devices are listed alphabetically according to their Vendor and Model, as summarized in Table 1 on page 77.

Table 1: Summary of Supported Data Sources

Vendor	Description	See page...
3Par	InServ	78
Brocade	Brocade switches using API	79
	Brocade HTTP	81
	Brocade SNMP (Firmware 4.2x / 4.4x)	82
Cisco	All Cisco switches.	84
EMC	Clariion CLI	85
	Connectrix 7	86
	Connectrix – 8.1, 8.6, 8.7, 8.8, 8.9, 9.1	87
	ECC StorageScope Host Resolver	89
	Solutions Enabler Symmetrix Family API	90
Engenio	Engenio Arrays	91
HDS	HiCommand	92
HP	EVA	93
	XP	94

Vendor	Description	See page...
IBM	FAStT	95
	DS CLI	96
	ESS CLI	97
	SVC1	98
	TotalStorage DS4000	99
McData	Enterprise Fabric Connectivity Manager	100
	Sphereon	101
QLogic	QLogic SANsurfer	103
Sun	StorEdge 6130	104
	StorEdge 6x20	105

A.1 3Par InServ

Data Source - Data source configuration

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

SMI-S server: [Empty]

SMI-S port: 5988

Protocol used: HTTP

User name: admin

Password: [Empty]

Poll interval (min): 40

SMI-S namespace: root/PG_InterOp

Import

< Back Next > Finish Cancel

The 3Par InServ is an SMI-S device. When you select this Data Source, you need only identify the server itself. All the other fields are set correctly by SANscreen.

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are highlighted (including required fields that are not yet specified).

Field	Description
SMI-S server	Network address for the SMI-S server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as a hostname that can be resolved through DNS.
SMI-S port	Number of the server port through which the Data Source acquires information.
Protocol used	HTTP (if unsecured access) or HTTPS (if secured).
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 the data (always root/PG_InterOp).

A.2 Brocade (API)

Data Source - Data source configuration

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

Brocade switch: [Highlighted]

User name: admin

Password: [Masked]

Poll interval (min): 15

Enable trapping: ☒

Minimum time between traps (sec): 10

Comma separated list of switches to ignore: [Empty]

Ignore Brocade API error -21 on N-Ports: ☐

Fabric name: [Empty]

Enable Performance Insight: ☐

Performance poll interval (seconds): [Empty]

Buttons: Import, < Back, Next >, Finish, Cancel

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
Brocade switch	Network address for the switch device, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as 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.
Comma separated list of switches to ignore	IP address of one or more switches to ignore, separated by commas. The Data Source will not poll devices that are referenced by this list.
Ignore Brocade API error -21 on N-Ports	Checkbox used to ignore all occurrences of Brocade API error -21, which can indicate a problem in a connected port (N-Port). Sometime this error occurs because of a bug in the Brocade API. Activate this flag <i>only when you are absolutely sure that there are no issues with the connected port, and that the error code indicates a problem in the Brocade API</i> . Contact Onaro prior to marking this checkbox, to receive a better analysis on the issue.
Fabric name	Fabric name to be reported by this Data Source (blank to report the fabric WWN).
Enable Performance Insight	Checkbox used to enable the collection of performance data for this Data Source (requires a Performance Insight license).
Performance poll interval (seconds)	Interval, in seconds, at which the Data Source should poll the device for performance data (applicable only if Enable Performance Insight is marked).

A.3 Brocade (HTTP)

Data Source - Data source configuration

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

Brocade switch: [Yellow highlighted field]

Poll interval (min): 15

Fabric name: [Empty field]

Exclude devices: [Empty field]

Import

< Back Next > Finish Cancel

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are highlighted (including required fields that are not yet specified).

Field	Description
Brocade switch	Network address for the switch device, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as a hostname that can be resolved through DNS.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
Fabric name	Fabric name to be reported by this Data Source (blank to report the fabric WWN).
Exclude devices	Comma-separated list of Brocade devices, identified by IP address, that will not be discovered by this Data Source.

A.4 Brocade (SNMP Firmware 4.2x / 4.4x)

Configure

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

Brocade switch: [highlighted]

SNMP community: public

Poll interval (min): 15

Fabric name:

Has blades: ☐

Starting port index: 0

Enable trapping: ☒

Minimum time between traps (sec): 10

Enable Performance Insight: ☐

Performance poll interval (seconds): 60

Import

< Back Next > Finish Cancel

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
Brocade switch	Network address for the switch device, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as 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.
Fabric name	Fabric name to be reported by this Data Source (blank to report the fabric WWN).
Has blades	Checkbox used to indicate whether the switch has blades. Mark the box if using blades.
Starting port index	Port-starting index of the second switch in the SilkWorm device, used by SANscreen to build a single switch out of the two Data Sources. This field is applicable when specifying the Data Source for the <i>second</i> of two physical switches in the device.

Field	Description
	Brocade directors (SilkWorm 12000, 24000, 48000) are internally built from two individual switch units that work in conjunction with each other. Each unit has its own IP address and requires a separate SNMP Source to discover it; therefore, a fully discovered SilkWorm switch requires two Data Sources. This field identifies the starting port number to the second Data Source. To illustrate: assume we have a directory with 64 ports, comprising two individual switches having 32 ports each. If we create the two Data Sources without a starting port index, the result would be two switches with 32 ports, both identified as ports 0-31. Instead, you must provide the starting port index for the second Data Source, in order to build a single directory. In our example, the index would be 32 to generate the second Data Source for ports 32-63.
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.
Enable Performance Insight	Checkbox used to enable the collection of performance data for this Data Source (requires a Performance Insight license).
Performance poll interval (seconds)	Interval, in seconds, at which the Data Source should poll the device for performance data (applicable only if Enable Performance Insight is marked).

A.5 Cisco

Configure

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

Cisco switch: [highlighted]

SNMP community: public

Poll interval (min): 15

Enable trapping: ☒

Minimum time between traps (sec): 10

Enable Performance Insight: ☐

Performance poll interval (seconds):

Import

< Back Next > Finish Cancel

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
Cisco switch	Network address for the switch, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as 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.
Enable Performance Insight	Checkbox used to enable the collection of performance data for this Data Source (requires a Performance Insight license).
Performance poll interval (seconds)	Interval, in seconds, at which the Data Source should poll the device for performance data (applicable only if Enable Performance Insight is marked).

A.6 EMC (Clariion CLI)

Data Source - Data source configuration

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

Clariion storage: [Yellow highlighted field]

User name: [Yellow highlighted field]

Password: [Empty field]

Poll interval (min): 40

navicli.exe path: C:/Program Files/EMC/Navisphere CLI/

Import

< Back Next > Finish Cancel

Requirement for a Management Agent

Before configuring this Data Source, make sure EMC's NaviCLI is installed on the target device.

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
Clariion storage	Network address for the Clariion storage device, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as 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 navicli.exe executable.

A.7 EMC (Connectrix 7)

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

Connectrix server: [Highlighted]

User name: Administrator

Password: *****

Poll interval (min): 15

Local IP: []

Connectrix port: 1099

Enable trapping: ☒

Minimum time between traps (sec): 10

Import

< Back Next > Finish Cancel

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
Connectrix server	Network address for the Connectrix server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as 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.
Local IP	Local address of the SANscreen server.
Connectrix port	Connectrix port through which the Data Source communicates with the switch management console (required if port numbers were changed on the Connectrix side).
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 (Connectrix – 8.1, 8.6, 8.7, 8.8, 8.9, 9.1)

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
EFC server	Network address for the EFC server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as 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.
Fabric name	Fabric name to be reported by this Data Source (blank to report the fabric WWN).
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).

Field	Description
Minimum time between traps (sec)	Minimum elapsed time between acquisition attempts triggered by traps, in seconds.
Inactive zonesets (comma delimited)	List of inactive zonesets on which to perform acquisition (in addition to performing acquisition on the active zonesets). Separate multiple zonesets using a comma.
Controls which NIC to use	Applicable when the Data Source reports to a Remote Acquisition Unit that has two or more network cards: one used to acquire information about SAN devices, and the other used to connect with the SANscreen server. Indication of which network interface to use on the RAU when reporting on SAN devices.
Enable Performance Insight	Checkbox used to enable the collection of performance data for this Data Source (requires a Performance Insight license).
Performance poll interval (seconds)	Interval, in seconds, at which the Data Source should poll the device for performance data (applicable only if Enable Performance Insight is marked).

A.9 EMC (ECC StorageScope Host Resolver)

Data Source - Data source configuration

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

ECC server: [highlighted]
ECC port: 1521
User name: stsview
Password: [empty]
Poll interval (min): 30

Import

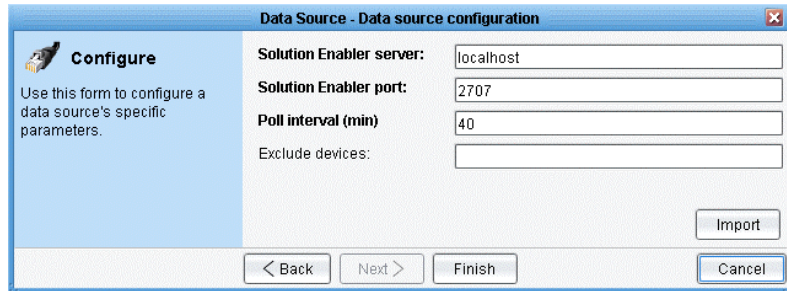
< Back Next > Finish Cancel

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
ECC server	Network address for the Enterprise Control Center (ECC) server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as 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.10 EMC (Solutions Enabler Symmetrix Family API)



For an EMC Symmetrix device, make sure that EMC SYMAPI is installed and has the appropriate licenses to operate. SANscreen communicates with the EMC Symmetrix device using this API.

Requirement for a Management Agent

Before configuring this Data Source, make sure the Solutions Enabler SDK / Server is installed locally on the target device.

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
Solution Enabler server	Network address for the Solution Enabler server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as 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.
Exclude devices	Comma-separated list of devices, identified by Symmetrix ID, that will not be discovered by this Data Source.

A.11 Engenio Arrays

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

Array controller IP:

Poll interval (min):

30

Import

< Back

Next >

Finish

Cancel

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
Array controller IP	IP address to identify one of the array's controllers.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.

A.12 HDS (HiCommand)

Configure

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

HiCommand Device Manager server: localhost

HiCommand Device Manager port: 2001

User name: admin

Password: *****

Poll interval (min): 40

Exclude devices:

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

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
HiCommand Device Manager server	Network address for the HiCommand Device Manager server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as a hostname that can be resolved through DNS.
HiCommand Device Manager 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.
Exclude devices	Comma-separated list of devices, identified by device ID, that will not be discovered by this Data Source.

A.13 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):

CLI home:

Exclude devices:

Requirement for a Management Agent

Before configuring this Data Source, make sure the SSSU command utility is available. The version number of the SSSU must match that of the HiCommand server being accessed by the Data Source.

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
CommandView server	Name of the CommandView manager.
User name	Name used to log in to the CommandView manager.
Password	Password used to log in to the CommandView.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.
CLI home	Full pathname to the CLI home directory where sssu.exe is located
Exclude devices	Comma-separated list of devices, identified by device name, that will not be discovered by this Data Source.

A.14 HP (XP)

Configure

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

CommandView server: [Yellow highlighted field]

User name: admin

Password: *****

Poll interval (min): 40

Path to cvcli.bat: [Yellow highlighted field]

Exclude devices: [Empty field]

Import

< Back Next > Finish Cancel

Requirement for a Management Agent

Before configuring this Data Source, make sure the CV CLI is installed on the target device.

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
CommandView server	Name of the CommandView manager.
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 (\).
Exclude devices	Comma-separated list of devices, identified by serial number, that will not be discovered by this Data Source.

A.15 IBM (FAStT)

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

Array controller IP:

Poll interval (min):

30

Import

< Back

Next >

Finish

Cancel

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
Array controller IP	Network address for the management controller of each array from which this Data Source will acquire information, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as a hostname that can be resolved through DNS. Separate multiple network addresses using a semicolon.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.

A.16 IBM (DS CLI)

Data Source - Data source configuration

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

DS storage: [Yellow highlighted field]

User name: admin

Password: [Masked with asterisks]

Poll interval (min): 40

Storage display name: [Yellow highlighted field]

dscli.exe path: [Empty field]

Import

< Back Next > Finish Cancel

Requirement for a Management Agent

Before configuring this Data Source, make sure IBM's DS CLI is installed on the target device.

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

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

A.17 IBM (ESS CLI)

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

ESS storage: [Yellow highlighted field]

User name: admin

Password: *****

Poll interval (min): 40

Storage display name: [Yellow highlighted field]

esscli.exe path: [Empty field]

Import

< Back Next > Finish Cancel

Requirement for a Management Agent

Before configuring this Data Source, make sure IBM's ESS CLI is installed on the target device.

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
ESS storage	Network address for the ESS device, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as a hostname that can be resolved through DNS.
User name	Name used to log in to the ESS.
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 display name	User-specified alias used as the storage name.
esscli.exe path	Full path to the esscli utility.

A.18 IBM (SVC)

Data Source - Data source configuration

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

SMI-S server: [Highlighted Yellow Field]
SMI-S port: 5999
Protocol used: HTTPS
User name: admin
Password: [Empty Field]
Poll interval (min): 40
SMI-S namespace: root/ibm

[Back] [Next >] [Finish] [Import] [Cancel]

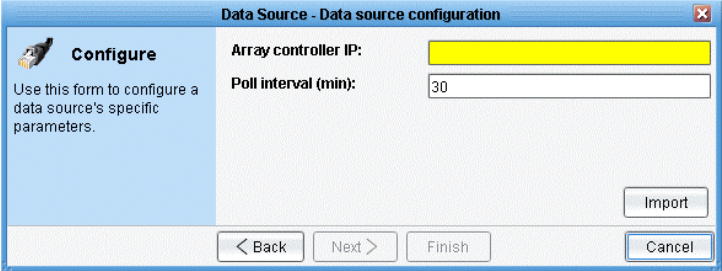
The IBM SVC is an SMI-S device. When you select this Data Source, you need only identify the server itself. All the other fields are set correctly by SANscreen.

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
SMI-S server	Network address for the SMI-S server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as a hostname that can be resolved through DNS.
SMI-S port	Number of the server port through which the Data Source acquires information.
Protocol used	HTTP (if unsecured access) or HTTPS (if secured access).
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 the data (always root/IBM).

A.19 IBM (TotalStorage DS4000)



Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
Array controller IP	Network address for the management controller of each array from which this Data Source will acquire information, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as a hostname that can be resolved through DNS. Separate multiple network addresses using a semicolon.
Poll interval (min)	Interval, in minutes, at which the Data Source should poll the device.

A.20 McData (Enterprise Fabric Connectivity Manager)

Configure

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

EFC server: [Highlighted]

User name: Administrator

Password: *****

Poll interval (min): 15

Enable trapping: ☒

Minimum time between traps (sec): 15

Inactive zonesets (comma delimited):

Enable Performance Insight: ☐

Performance poll interval (seconds):

Import

< Back Next > Finish Cancel

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
EFC server	Network address for the Enterprise Fabric Connectivity (EFC) server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as 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	Minimum elapsed time between acquisition

Field	Description
between traps (sec)	attempts triggered by traps, in seconds.
Inactive zonesets (comma delimited)	List of inactive zonesets on which to perform acquisition (in addition to performing acquisition on the active zonesets). Separate multiple zonesets using a comma.
Enable Performance Insight	Checkbox used to enable the collection of performance data for this Data Source (requires a Performance Insight license).
Performance poll interval (seconds)	Interval, in seconds, at which the Data Source should poll the device for performance data (applicable only if Enable Performance Insight is marked).

A.21 McData (Sphereon)

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
Sphereon switch	Network address for the switch, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as 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.
Fabric name	Fabric name to be reported by this Data Source (blank to report the fabric WWN).
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.
Enable Performance Insight	Checkbox used to enable the collection of performance data for this Data Source (requires a Performance Insight license).
Performance poll interval (seconds)	Interval, in seconds, at which the Data Source should poll the device for performance data (applicable only if Enable Performance Insight is marked).

A.22 QLogic SANsurfer

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

SANSurfer switch: [highlighted]

SNMP community: public

Poll interval (min): 15

Enable trapping ☒

Minimum time between traps (sec): 10

Fabric name: []

Enable Performance Insight: ☐

Performance poll interval (seconds): 60

Import

< Back Next > Finish Cancel

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
SANSurfer switch	Network address for the SANsurfer device, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as 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.
Fabric name	Fabric name to be reported by this Data Source (blank to report the fabric WWN).

Field	Description
Enable Performance Insight	Checkbox used to enable the collection of performance data for this Data Source (requires a Performance Insight license).
Performance poll interval (seconds)	Interval, in seconds, at which the Data Source should poll the device for performance data (applicable only if Enable Performance Insight is marked).

A.23 SUN (StorEdge 6130)

The SUN StorEdge 6x20 is an SMI-S device. When you select this Data Source, you need only identify the server itself. All the other fields are set correctly by SANscreen.

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are **highlighted** (including required fields that are not yet specified).

Field	Description
SMI-S server	Network address for the SMI-S server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as a hostname that can be resolved through DNS.
SMI-S port	Number of the server port through which the Data Source acquires information.

Field	Description
Protocol used	HTTP (if unsecured access) or HTTPS (if secured access).
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 the data (always interop).

A.24 SUN (StorEdge 6x20)

Data Source - Data source configuration

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

SMI-S server: [Empty]
SMI-S port: 5988
Protocol used: HTTP
User name: admin
Password: [Empty]
Poll interval (min): 40
SMI-S namespace: interop

Import
< Back Next > Finish Cancel

The SUN StorEdge 6x20 is an SMI-S device. When you select this Data Source, you need only identify the server itself. All the other fields are set correctly by SANscreen.

Field Descriptions

Refer to the screen shown above for default values. Required fields are shown in **bold**. Invalid field values are highlighted (including required fields that are not specified).

Field	Description
SMI-S server	Network address for the SMI-S server, specified as an IP (<i>nnn.nnn.nnn.nnn</i> format), or as a hostname that can be resolved through DNS.

Field	Description
SMI-S port	Number of the server port through which the Data Source acquires information.
Protocol used	HTTP (if unsecured access) or HTTPS (if secured access).
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 the data (always interop).

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	PC running Microsoft Windows 2000 or 2003 with the latest service pack. A dedicated server is recommended. x64 version highly recommended with 5000+ SAN ports.
CPU	Dual Pentium processors or equivalent. 2.4+ GHz recommended, Quad CPUs highly recommended with 5000+ SAN ports.
Memory	4 GB RAM. 8G + expandable highly recommended with 5000+ SAN ports running Windows Server 2003 x64 Edition.
Available Disk Space	20 GB.
Network	100 Mbps / 1 Gbps Ethernet connection with dedicated IP Address and IP access to all of the SAN devices in the environment.
Permissions	Minimum of local Administrator permissions.
Remote Connectivity	Internet connectivity to allow WebEx access, and/or a remote desktop connection to facilitate installation and post-installation support.

B.2 Remote Acquisition Unit Server Requirements

Component	Requirement
Operating System	PC running Microsoft Windows 2000 or 2003 with the latest service pack. A dedicated server is recommended.
CPU	Dual Pentium processors or equivalent (2.4+ GHz recommended).
Memory	4 GB RAM.
Available Disk Space	5 GB.
Network	100 Mbps /1 Gbps Ethernet connection.

B.3 SANSscreen Client GUI Requirements

Component	Requirement
Operating System	Any Java 5 enabled machine. The Java-based GUI Client supports Windows, Unix, and Macintosh platforms.
CPU	1.5 GHz or better.
Memory	512 MB RAM (1 GB or more recommended).

Note1: When accessing the SANSscreen client, if the Java run-time environment (JRE) is not installed on your PC, SANSscreen displays a message indicating that you need to install it. SANSscreen's client portal provides a Java link directs 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>. If you're running an earlier version of the JRE, Onaro recommends that you upgrade to Java 5.0.

Note2: If a firewall separates the client PC from the SANSscreen server, the RMI method of communicating may not be possible. In this case, you can initiate the SANSscreen client using HTTP.

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.