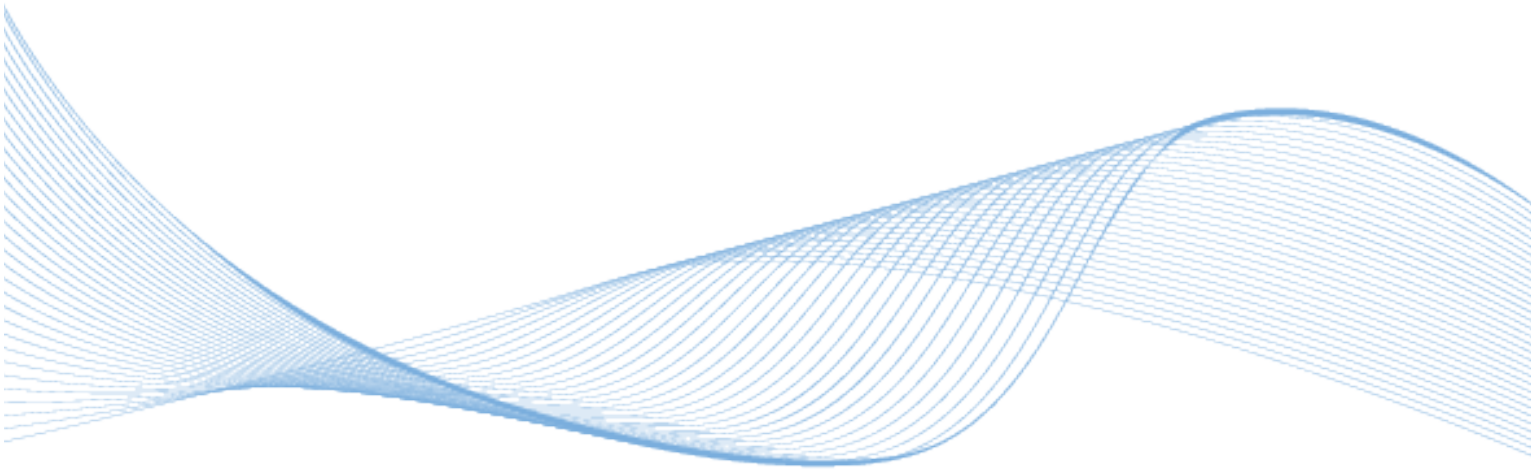
# SVI Maintenance Guide

Document SQ0I001

Version 2.0



## Change History

| Version | Change Made | Author | Authorised | Date |
|---|---|---|---|---|
| 1.0 | Addition of Change History | DR | AC | 13.02.14 |
| 2.0 | Addition of SDR Management section<br>Update of SVI Backup section | AB | SS | 28.09.18 |

# Contents

# 1.0 Introduction

Congratulations on your purchase of the SVI. This guide will talk you through the necessary considerations and setup in order to maintain your SVI. Please read the complete document before performing any maintenance on the SVI

Should you have any problems using this guide, please contact our Support team via email support@squire-technologies.co.uk or by phone on +44 (0) 1305 757314 and they will be happy to advise you.

**Note: All commands in this document are for example purposes and should be used with care.**

# 2.0 Preparation

Before performing any maintenance on your system it is advised to take a backup.

## 2.1 SVI Backup

Squire Technologies have provided a backup script on the system. There are two variants of this script, based on differing methodologies. Please check which one is available on your system.

If the script /usr/bin/svi-backup exists, please use section 2.1.2

If the above does not exist and the script /svi_backup exists, please use section 2.1.1

It is recommended that a backup is taken monthly and stored off the SVI so that in the event of a hardware failure the support team will be able to restore the system with your last known working configuration.

**Note: The "svi_backup" script will backup all configuration but excludes the mysql "cdr_table". This is due to performance issues; to backup the SQL database please use section 2.2.**

### 2.1.1 Original Backup Script

This script exists in the "/" root directory on the SVI known as the "svi_backup" script. This will be symbolically linked to the latest "svi_backup" version at point of installation. If you require a later version please contact support to upgrade.

In order to backup the SVI you will need to run the below command form the "/" directory on the SVI.

"svi_backup backup System-Backup-23-05-2013" then follow the on screen prompts.

Once the backup is complete you will then see a file named below;

"SVI_BACKUP_ System-Backup-23-05-2013.tgz"

### 2.1.2 New Backup Script

This script exists in /usr/bin/, and as such is available to run throughout the system.
The script will display various options as it runs to produce the backup, which will then be created in the "/" root directory with a filename of:

SVI_V2_BACKUP_<filename chosen in script>-DD-MM-YY-HH-MM-SS.tgz

## 2.2 SQL Backup

As the backup script does not backup the mysql “cdr_table”, if you are planning on archiving CDR or MDR data it is recommended to take a full SQL backup of the database. Due to the large amount of data it can cause system performance issues and therefore recommended to be performed in a maintenance window or during a period of low traffic. If this task is completed regularly the performance effect is greatly reduced.

To create a full backup of the SQL database, First log onto the SQL server, then run the command below;

### 2.2.1 For SMSC Products

“mysqldump --routines svi_smsc > SMSC-backup-23-05-2013.sql”

“mysqldump --routines svi_ms > MS-backup-23-05-2013.sql”

### 2.2.2 All other Products

“mysqldump --routines svi_ms > MS-backup-23-05-2013.sql”

# 3.0 Maintenance

Now the system is fully backed up the below maintenance tasks can be performed.

## 3.1 Log Files

All SVI product log files are stored in the "/home/squire" Directory. Depending on the type of product you have purchased and the modules installed, you will notice several different types of log files. You may notice also that depending on the amount of debug turned on during the time period for the log they may also be time stamped. Below is a list of the different log file names;

1. Gateway_dd-mm-yyyy.(hh:mm:ss)
2. MG_dd-mm-yyyy.(hh:mm:ss)
3. MS_dd-mm-yyyy.(hh:mm:ss)
4. SMSC_dd-mm-yyyy.(hh:mm:ss)
5. Security_dd-mm-yyyy.(hh:mm:ss)
6. RTPRouter_dd-mm-yyyy.(hh:mm:ss)
   (This log file is usualy in a separate directory "/home/squire/rtprouter")
7. nohup.out
8. core.*

To assist in maintaining a reasonable amount of logs, Squire Technologies supplies in new systems a script called /usr/bin/cleanlogs.sh, and has set up a cron job that clears logs older than 28 days.

This script can be used to archive old log files as well:

Basic usage: cleanlogs.sh -t -l 7 -d /bkdir/

Command line switches are optional. The following switches are recognized.
-l --Sets the number of days to keep. Default is 7.
-t --This flag will make the script create a tarball of the logs before deletion for backup purposes.
-d --Sets the output directory for the tarballs. Default is /root/.
-h --Displays this help message. No further functions are performed.

NOTE: The logs that are backed up are controlled at the bottom of this script, by calling the 'cLogs' function and passing the logs name as a parameter. The log name MUST exist in /home/squire/

NOTE: The crontab example below will tarball any logs older than a week (7 days then delete them.) This would run at 12:00 noon every Tuesday and save the tarballs to /bkdir/
00 12 * * 2 /home/squire/scripts/cleanlogs.sh -t -l 7 -d /bkdir/ >> /cleanlogs.log

On older systems it is recommended that at the end of the month all logs for the previous month are moved to an old directory and then compressed using "tar" and archived. Once this is complete the files can be removed from the system. An example of moving the logs to an old-logs directory and then using tar to back up the logs for June is described below;

**Note: before using any of the commands below make sure you do not leave a space before the wild card "*" as Linux will see this and select ALL files.**

If for example the directory old-log does not exist then to create a new directory use command;

"mkdir old-logs"

Next move the logs to the "old-logs"

"mv Gateway_*-06-* MG_*-06-* MS_*-06-* Security_*-06-* nohup.out old-logs/"

Once the Logs are moved change into the “old-logs” directory and compress the files using “tar” “tar

–zcvf June-2013-Logs.tgz Gateway_*-06-* MG_*-06-* MS_*-06-* Security_*-06-* nohup.out”

Once the compression is complete you can then remove the logs in “old-logs” from the system using the “rm” command;

“rm –f Gateway_*-06-* MG_*-06-* MS_*-06-* Security_*-06-* nohup.out”

**Note: Before removing a core file the logs from the period for which it occurred should be compressed up separately and uploaded to your space on the squire ftp server and squire support notified so it can be investigated.**

## 3.2 CDR Data

It is recommended to archive CDR information via the SVI Management System keeping only 1-3 months of CDR or MDR information depending on how much data is required for billing purposes.

In order to do this please follow the below steps;

1. Log into the SVI Management System and navigate to the “Calls” tab
2. In the “CDRs” table select “Archive”
3. Then type the file location and name of the archive file “/home/squire/cdrs-june-2013.csv”
4. Next select the time period for the archive
5. Then click done
6. This will create a file in the location set and can be downloaded via an scp client.

The archive button in the GUI calls the “archiveCDRs” script from “/home/squire/scripts”. This script can be call manually run or called via a Linux cron job. The input values of the script are as follows.

1. $1 = database name
2. $2 = file name and location
3. $3 = start date in format yyyy-mm-dd hh:mm:ss
4. $4 = end date in format yyyy-mm-dd hh:mm:ss

Example;

“./archiveCDRs ‘svi_ms’ ‘/home/squire/CDRs.csv’ ‘2013-01-31 23:59:59’ ‘2013-03-01 00:00:00’”

**Note: This script assumes that the database is local to the script. If the database is remote the script can be copied to the remote SQL and run from there.**

## 3.3 PCAP Traces

It is recommended that old custom pcap files are removed from both the “/root” and “/home/squire” directory. You can list the files using command “ll –lrt | grep *.pcap” and the removing then with the “rm” command “rm –f test1.pcap test2.pcap test3.pcap test4.pcap”.

## 3.4 Processor / Memory Usage

Periodically the processor and system memory usage should be checked. To do this you can run the command “top”. None of the SVI processes should be running at 100% this also includes the “tomcat” and “mysql” services. If this is the case please get in contact with support so this can be investigated.

## 3.5 Disk Space

In order to check disk space on the SVI use command “df –ah” this will display a percentage usage for the hard drives configured on the system.

You can then run the following command in the in any directory to display the 20 largest files.

“du -hsx * | sort -rh | head -20”

Depending on the type of file and location this can then be archived off the system or removed.

## 3.6 Debug Configuration

It is very easy to configure a high level of debug when debugging an issue but often this gets left on when the issue is resolved. This in turn prints unnecessary debug information to the log files and increases the amount of disk space used. It is recommended that all debug is constantly turned off during normal operation. The information printed to the log file will then be minimal.

This then allows the system administrator to monitor for any major system errors and increase the level of debug when required for investigation. Debug levels can be turned on and off via the Management System “Right Panel” and clicking on the relevant process tabs.

## 3.7 SDR maintenance

It is recommended that SDRs are regularly archived or deleted to prevent too much data being stored in the SQL database.

The script ‘final_sdr_maintenance.sh’ has been provided in /home/squire/scripts/ to accomplish this via manual use or via daily Linux Cron job.

The script can:
-delete SDRs – in case SDRs are exported via other means (Custom SDRs scripts)
-archive SDRs (save SDRs in test format) and then delete those archived

There is a customizable parameter: post_process, that must be set correctly for the script to be effective.

The format: CSV or tab delimited fields can be chosen by commenting out the unwanted format.

In case of archiving: the script generates CSV format files in /home/squire/cdr/ with the filenames cdr_archive_YYYY-MM-DD__HH-MM-SS__x, then archives and compresses the CSV files with the name cdr_archive_YYYY-MM-DD__HH-MM-SS.tgz

Each individual CSV file contains up to 10000 processed records over 2 days old.

# 4.0 Recommended System Checks

The below points are recommendations that can be reformed at any time to ensure system integrity.

## 4.1 CDR Data

It is recommended that data in the cdr table is checked periodically for ambiguities such as large number of calls with only “Setup” and ”Clear” times with state as “Setup” this can indicate issues with routing and should be investigated.

Any cdr with termination of “Softswitch” and cause codes for 5xx need to be investigated as to the cause of the call failing.

**Note: The information in the CDR table will vary depending on the type of service and traffic that you are providing.**

## 4.2 Failover Test (Redundant System)

It is recommended that periodically, a maintenance window is scheduled so that a redundant system fail over can be performed and restarted to check system redundancy. This test should be carried out, as should the system or network fail at any time during normal operation you can be assured that a production service will continue.

## 4.3 Call / Billing Testing

It is recommended that periodically, the system administrator tests client routes and the system configuration and to ensure the system rate sheets for billing systems are configured correctly to ensure no loss of revenue.